

Introduction to Logic



Department of Philosophy
Central South University
xieshenlix@163.com
[github](#)

May 19, 2022

Contents

Introduction

Recursion Theory

Term Logic

Equational Logic

Propositional Logic

Homotopy Type Theory

Predicate Logic

Category Theory

Modal Logic

Quantum Computing

Set Theory

Answers to the Exercises

References 1436

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

Mill's Methods of Causal

Analysis

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

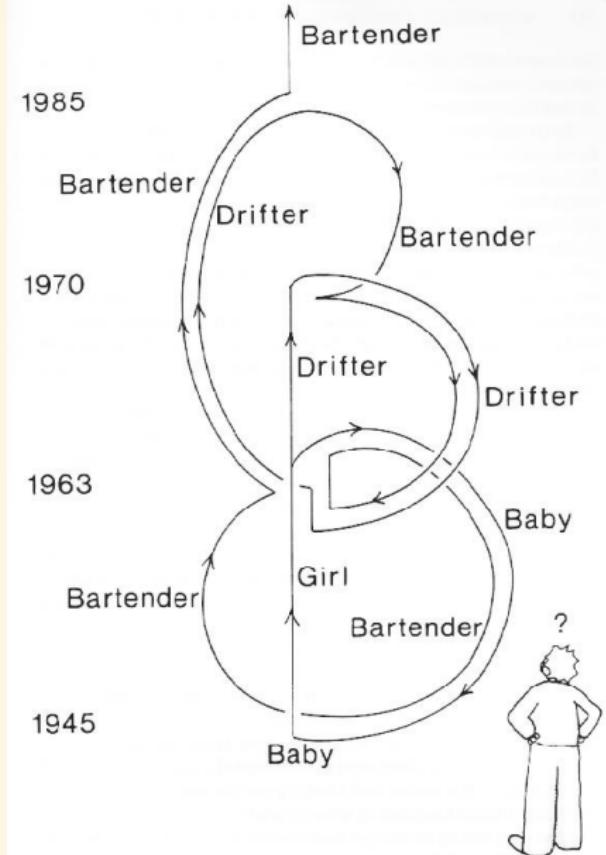
Answers to the Exercises

References 1436

Predestination — All You Zombies — Heinlein

1945 一女婴被弃孤儿院。

1963 长大后的女孩与一男子邂逅、怀孕。男子失踪。女孩产下一女婴后发现自己是双性人。女婴被偷。伤心的她变性成他。开始酗酒。1970 一酒保把他招募进时光穿梭联盟。为报复负心男，酒保带他飞回 1963。他邂逅一女孩并使其怀孕。酒保乘时光机前行 9 个多月偷走女婴，并将其送至 1945 的孤儿院，然后回 1963 把他带到 1985 的联盟基地。他受命飞回 1970，化装酒保去招募一个酒鬼。



Problem

周迅的前男友窦鹏是窦唯的堂弟；窦唯是王菲的前老公；周迅的前男友宋宁是高原的表弟；高原是窦唯的前任老婆；周迅的前男友李亚鹏是王菲的现任老公；周迅的前男友朴树的音乐制作人是张亚东；张亚东是王菲的前老公窦唯的妹妹窦颖的前老公，也是王菲的音乐制作人；张亚东是李亚鹏前女友瞿颖的现男友。

下列说法不正确的是：

1. 王菲周迅是情敌关系
2. 瞿颖王菲是情敌关系
3. 窦颖周迅是情敌关系
4. 瞿颖周迅是情敌关系

$$\text{Rival}(x, y) \coloneqq \exists z \left(\left(\text{Now}(x, z) \wedge \text{Ex}(y, z) \right) \vee \left(\text{Now}(y, z) \wedge \text{Ex}(x, z) \right) \right)$$

Information Update

Five Logicians Walk into a Bar

- ▶ **Waiter:** Do you all want beer?
- ▶ **1:** I don't know.
- ▶ **2:** I don't know.
- ▶ **3:** I don't know.
- ▶ **4:** I don't know.
- ▶ **5:** No.



The information content of a formula A is the set $\text{Mod}(A)$ of its models. An update with new information B reduces the current set of models $\text{Mod}(A)$ to the overlap of $\text{Mod}(A)$ and $\text{Mod}(B)$.

Unfaithful Husband Puzzle

Problem (Unfaithful Husband Puzzle)

1. Every man in a village of 100 married couples has cheated on his wife.
2. Every wife in the village knows about the fidelity of every man in the village except for her own husband.
3. Every wife who discovers his husband's infidelity must kill him that very day.
4. One day, the queen visits and announces that at least one husband has been unfaithful.



After a date, one says to the other:
"Would you like to come up to my
apartment to see my etchings?"

Test

Guess what $\frac{2}{3}$ of the average of your guesses will be, where the numbers are restricted to the real numbers between 0 and 100.

Gateway to Heaven

Problem (天堂之路)

- ▶ 你面前有左右两人守卫左右两门。
- ▶ 一人只说真话，一人只说假话。
- ▶ 一门通天堂，一门通地狱。
- ▶ 你只能向其中一人提一个“是/否”的问题。
- ▶ 怎么问出去天堂的路？

Problem (Hardest Logic Puzzle Ever)

- ▶ Three gods, *A*, *B*, and *C* are called in some order, *T*, *F*, and *R*.
- ▶ *T* always speaks truly, *F* always speaks falsely (if he is certain he can; but if he is unable to lie with certainty, he responds like *R*), but whether *R* speaks truly or falsely (or whether *R* speaks at all) is completely random.
- ▶ Your task is to determine the identities of *A*, *B*, and *C* by asking 2 (3) yes/no questions; each question must be put to exactly one god.
- ▶ The gods understand English, but will answer in their own language, in which the words for 'yes' and 'no' are 'da' and 'ja' in some order. You don't know which word means which.
- ▶ solution: assume *T* and *F* can't predict *R*'s answer
 1. Directed to *A*:
Would you answer 'ja' to the question of whether you would answer with a word that means 'yes' in your language to the question of whether you and *B* would give the same answer to the question whether ' $1 + 1 = 2$ '? Q
 2. Directed to *A* or *B* we now know not to be *R*:
 $Q[C/B]$
- ▶ solution: assume *T* and *F* can predict *R*'s answer
 1. Directed to *A*:
Would you answer 'ja' to the question of whether either:
 - ▶ *B* isn't *R* and you are *F*, or
 - ▶ *B* is *R* and you would answer 'da' to *Q*? Q
 2. Directed to *A* or *B* we now know not to be *R*:
 $Q[C/B, Q'/Q]$

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

Mill's Methods of Causal
Analysis

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Logic vs other Disciplines

- ▶ Logic vs (Analytic) Philosophy.
sense & reference / extension & intension / use & mention / truth & provability / mutual vs distributed vs common knowledge / knowledge update / belief revision / preference change / information flow / action & strategy / multi-agent interaction / counterfactual / causation / possible world / cross-world identity / essentialism / induction / ontological commitment / concept analysis / laws of thought / strength & limitation / paradoxes ...
Peirce, Frege, Russell, Wittgenstein, Ramsey, Carnap, Quine, Putnam, Kripke, Chomsky, Gödel, Tarski, Turing ...
- ▶ Logic vs Mathematics.
Logicism / Formalism / Intuitionism / Constructivism / Finitism / Structuralism / Homotopy Type Theory
- ▶ Logic vs Computer Science.

$$\frac{\text{Logic}}{\text{Computer Science}} \approx \frac{\text{Calculus}}{\text{Physics}}$$

Logic vs CS

- ▶ Computer Architecture.
Logic gates and digital circuit design \approx Propositional Logic
- ▶ Programming Languages.
LISP $\approx \lambda$ -calculus
Prolog \approx First Order Logic + Recursion
- ▶ Theory of Computation. Computational / Descriptive Complexity.
- ▶ General Problem Solver (SAT solvers).
- ▶ Automated Theorem Proving.
- ▶ Common sense reasoning via Non-monotonic Logic.
- ▶ Fuzzy Control vs Fuzzy Logic and Multi-valued Logic.
- ▶ Relational Databases.
SQL \approx First Order Logic + Syntactic Sugar
- ▶ Software Engineering (Formal Specification and Verification).
Temporal Logic, Dynamic Logic, Hoare Logic, Model Checking
- ▶ Multi-agent Systems.
Epistemic Logic
- ▶ Knowledge representation. Semantic Web.
Web Ontology Language (OWL) \approx Description Logic

Logic vs other Disciplines

- ▶ Logic vs Linguistics.
 - Syntax, Semantics and Pragmatics of Natural Language
(Montague Grammar, Inquisitive Semantics)
 - Parsing as deduction (Lambek calculus)
- ▶ Logic vs Economics and Social Sciences.
 - Epistemic Game Theory
 - Social Choice Theory
 - Rational Choice Theory
 - Decision Theory
- ▶ ...

Branches of Logic

Mathematical Logic

- ▶ **First Order Logic**
- ▶ Set Theory
- ▶ Model Theory
- ▶ Proof Theory
- ▶ Recursion Theory
- ▶ Category / Topos Theory
- ▶ (Homotopy) Type Theory

Computational Logic

- ▶ Automata Theory
- ▶ Computational Complexity
- ▶ Finite Model Theory
- ▶ Model Checking
- ▶ Lambda Calculus
- ▶ Categorical Logic
- ▶ Theorem Proving
- ▶ Description Logic
- ▶ Fixpoint Logic
- ▶ Dynamic Logic
- ▶ Temporal Logic
- ▶ Process Algebra
- ▶ Hoare Logic
- ▶ Inductive Logic
- ▶ Fuzzy Logic
- ▶ Non-monotonic Logic
- ▶ Computability Logic
- ▶ Default Logic
- ▶ Markov Logic Networks
- ▶ Situation/Event Calculus

Philosophical Logic

- ▶ Intuitionistic Logic
- ▶ **Modal Logic**
- ▶ Algebraic Logic
- ▶ Epistemic Logic
- ▶ Doxastic Logic
- ▶ Preference Logic
- ▶ Provability Logic
- ▶ Justification Logic
- ▶ Hybrid Logic
- ▶ Substructural Logic
- ▶ Free Logic
- ▶ Counterfactual Logic
- ▶ Relevance Logic
- ▶ Linear Logic
- ▶ Quantum Logic
- ▶ Paraconsistent Logic
- ▶ Intensional Logic
- ▶ Partial Logic
- ▶ Diagrammatic Logic
- ▶ Deontic Logic

$$\nabla(\odot \cdot \odot) = \odot \nabla \odot + \odot \nabla \odot$$

► Logic is

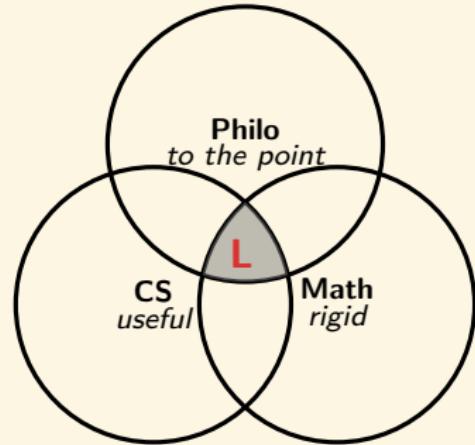
1. mainly philosophy by subject matter
2. mainly mathematics by methodology
3. mainly computer science by applications

► Logicians always want to be

1. Philosophers of philosophers
2. Mathematicians of mathematicians
3. Computer scientists of computer scientists

► However, they often end up being

1. Mathematicians to philosophers
2. Computer scientists to mathematicians
3. Philosophers to computer scientists



Keep yourself open

and don't neglect your larger self

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

Mill's Methods of Causal

Analysis

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

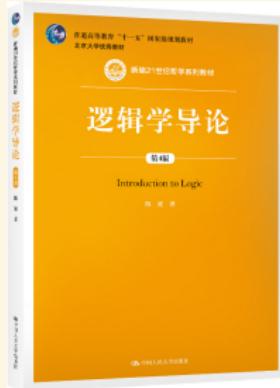
Answers to the Exercises

References 1436

Readings

1. P. J. Hurley: A Concise Introduction to Logic. — *B*
2. H. de Swart: Pilosophical and Mathematical Logic. — *P*
3. N. J. J. Smith: Logic — The Laws of Truth. — *P*
4. P. Smith: An Introduction to Formal Logic. — *P*
5. *P. Smith: Beginning Mathematical Logic.* — *P*
6. J. van Benthem: Logic in Action. — *P*
7. Open Logic Project. — *P*
8. H. Enderton: A Mathematical Introduction to Logic. — *L*
9. H. Ebbinghaus, J. Flum, W. Thomas: Mathematical Logic. — *L*
10. A. Nerode, R. A. Shore: Logic for Applications. — *C*
11. Yuri Manin: A Course in Mathematical Logic for Mathematicians.— *M*

Readings, Movies and More



Hofstadter's Law

It always takes longer than you expect, even when you take into account Hofstadter's Law.

- D. Hofstadter: Gödel, Escher, Bach
- Dangerous Knowledge
- The Imitation Game

- libgen
- sci-hub
- XX-Net
- ghelper

Advanced Readings

- ▶ Modal Logic
 - ▶ J. van Benthem: Modal Logic for Open Minds
 - ▶ P. Blackburn, M. de Rijke, Y. Venema: Modal Logic
- ▶ Set Theory
 - ▶ T. Jech: Set Theory
 - ▶ K. Kunen: Set Theory
- ▶ Recursion Theory
 - ▶ R. I. Soare: Turing Computability
 - ▶ A. Nies: Computability and Randomness
 - ▶ M. Li, P. Vitányi: An Introduction to Kolmogorov Complexity and Its Applications
- ▶ Model Theory
 - ▶ D. Marker: Model Theory
 - ▶ C. C. Chang, H. J. Keisler: Model theory
- ▶ Proof Theory
 - ▶ G. Takeuti: Proof Theory
 - ▶ W. Pohlers: Proof Theory

Outline and Credits

- ▶ Critical Thinking ✓
- ▶ Term Logic
- ▶ Propositional Logic ✓
- ▶ Predicate Logic ✓
- ▶ Modal Logic
- ▶ Set Theory
- ▶ Question
- ▶ Discussion
- ▶ Homework
- ▶ Exercises ✓
- ▶ Examination ✓
- ▶ Presentation
- ▶ Paper
- ▶ Techniques e.g. L^AT_EX / Coq ...
- ▶ ...

Aim

- ▶ Formalization of an argument ❤
- ▶ Demonstration of the validity of an argument ❤
- ▶ Object & Meta-language / Syntax & Semantics / Finite & Infinite / Countable & Uncountable / Induction & Recursion / Truth & Proof / Axiomatization / Theory / Soundness / Completeness / Compactness / Elementary Equivalent & Isomorphism / Representability / Definability / Categoricity / Decidability / Complexity / Expressiveness / Succinctness / Interpretability ... 🚲
- ▶ Formal Philosophy 🚲
- ▶ Understanding of the nature of mathematics 🚲
- ▶ Applications in Math / CS / AI / Linguistics / Cognition / Physics / Information Theory / Game Theory / Social Science ... 🚲
- ▶ Mathematical Logic 🚲

Homework ↗

Google / Wikipedia / Stanford Encyclopedia / Internet Encyclopedia / StackExchange

- ▶ Leibniz, Cantor, Frege, Russell, Hilbert, Gödel, Tarski, Turing.
- ▶ finite, infinite, syntax, semantics, semantic entailment, formal system, deduction, consistency, satisfiability, validity, soundness, completeness, compactness, decidability
- ▶ Philosophy of Logic, Philosophical Logic
- ▶ Logicism, Formalism, Intuitionism
- ▶ Hilbert's program
- ▶ Church-Turing thesis

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

**Mill's Methods of Causal
Analysis**

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Method of Agreement

$$ABC \rightarrow xyz$$

$$ADE \rightarrow xuv$$

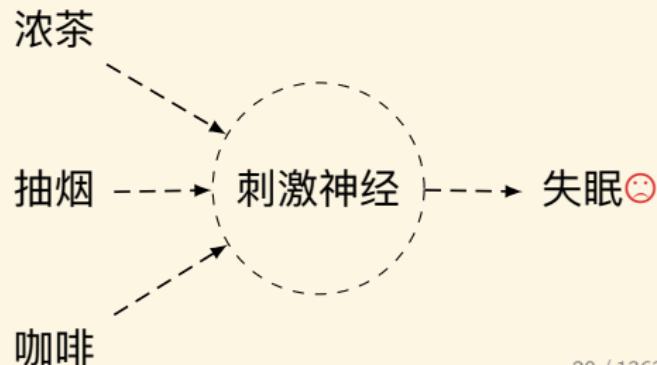
$$\frac{}{A \rightarrow x}$$

缺碘	工人	老年	甲状腺肿大
缺碘	农民	中年	甲状腺肿大
缺碘	士兵	青年	甲状腺肿大

缺碘 → 甲状腺肿大

泡脚	看小说	喝浓茶	失眠
泡脚	看电视	抽烟	失眠
泡脚	听音乐	喝咖啡	失眠

泡脚 → 失眠



Method of Difference

$$ABC \rightarrow xyz$$

$$\overline{ABC} \rightarrow \bar{x}yz$$

$$\underline{A \rightarrow x}$$

冰激凌	沙拉	面包	牛奶	肚子疼
—	沙拉	面包	牛奶	肚子不疼
<hr/>				
冰激凌 → 肚子疼				

上课	头疼
不上课	头不疼
<hr/>	
上课 → 头疼	



取健康的蜘蛛，大吼一声，蜘蛛被吓跑了
砍掉蜘蛛的腿，大吼一声，蜘蛛纹丝不动
<hr/>
蜘蛛的听觉器官长在腿上。 😐

Joint Method of Agreement and Difference

$$\begin{array}{c} ABC \rightarrow xyz \quad ABC \rightarrow xyz \\ ADE \rightarrow xuv \quad \overline{A}BC \rightarrow \bar{x}yz \\ \hline A \rightarrow x \end{array}$$

环境	纲	动物	形态
海	鱼纲	鲨鱼	◎
海	爬行	鱼龙	◎
海	哺乳	鲸鱼	◎
陆	哺乳	鼹鼠	~~
空	哺乳	蝙蝠	❀

达尔文：环境影响形态

Method of Residues

$$\begin{array}{rcl} ABC \rightarrow x & & ABC \rightarrow xyz \\ B \not\rightarrow x & & B \rightarrow y \\ C \not\rightarrow x & & C \rightarrow z \\ \hline A \rightarrow x & & A \rightarrow x \end{array}$$

受其他行星吸引，天王星运行轨道上有四个地方发生偏斜
三个地方偏斜是已知行星吸引的结果

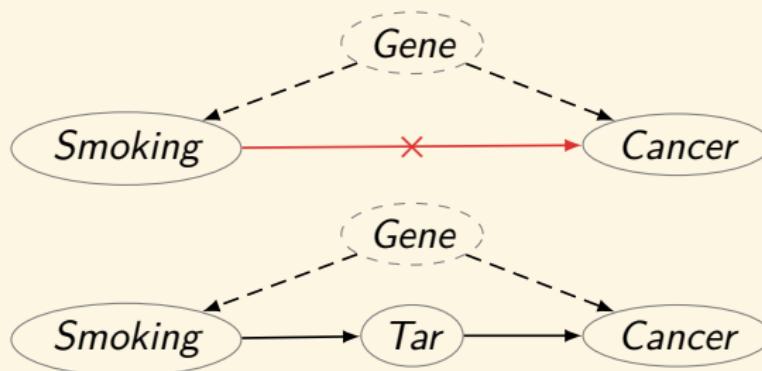
剩余一个地方偏斜是未知行星吸引的结果（发现海王星）

Method of Concomitant Variation

$$\begin{array}{c} ABC \rightarrow xyz \\ A^{\uparrow}BC \rightarrow x^{\uparrow}yz \\ A^{\downarrow}BC \rightarrow x^{\downarrow}yz \\ \hline A \rightarrow x \end{array}$$

热胀冷缩、体温表

禁烟人士 吸烟越多越容易患肺癌，所以吸烟是导致肺癌的重要原因。
烟草公司 某种基因是导致人们容易吸烟和容易得肺癌的共同原因。



Simpson's Paradox

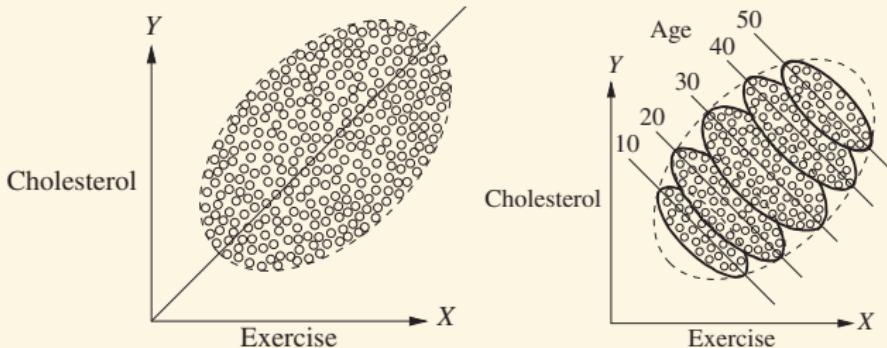
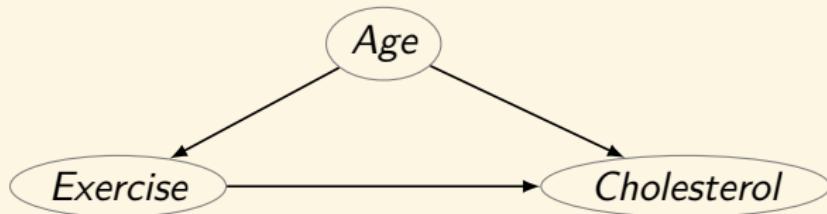


Figure: Exercise appears to be beneficial in each age group but harmful in the population as a whole. — Older people exercise more.



$$\mathbb{E}[\text{cholesterol} \mid \text{exercise}] > \mathbb{E}[\text{cholesterol} \mid \text{no exercise}]$$

$$\mathbb{E}[\text{cholesterol} \mid \text{do(exercise)}] < \mathbb{E}[\text{cholesterol} \mid \text{do(no exercise)}]$$

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

Mill's Methods of Causal

Analysis

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Example

Just as in swimming our bodies have a natural tendency to float on the surface so that it requires great physical exertion to plunge to the bottom, so in thinking it requires great mental exertion to force our minds away from the superficial, down into the depth of a philosophical problem.

— Wittgenstein

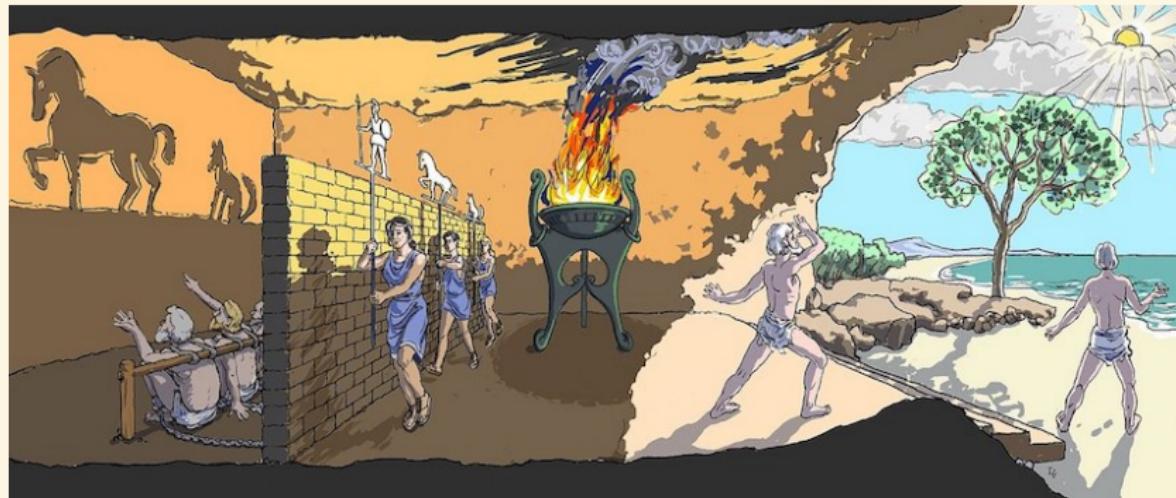
古龙《九月鹰飞》

- ▶ 叶开忍不住又道：“你为什么还是戴着这草帽？”
- ▶ 墨九星道：“因为外面有狗在叫。”
- ▶ 叶开怔了怔，道：“外面有狗叫，跟你戴草帽又有什么关系？”
- ▶ 墨九星冷冷道：“我戴不戴草帽，跟你又有什么关系？”

Example

庄子《齐物论》

不知周之梦为蝴蝶与，蝴蝶之梦为周与？



神秀 vs 慧能

神秀：身是菩提树，心如明镜台，时时勤拂拭，勿使惹尘埃。

慧能：菩提本无树，明镜亦非台，本来无一物，何处染尘埃？

Analogical Argument

$$\frac{\begin{array}{c} abcd \text{ have the attributes } PQR \\ abc \text{ have the attribute } S \end{array}}{d \text{ probably has the attribute } S}$$

- 相似的类比物数量越多，论证越强；不相似的类比物数量越多，论证越弱。
- 类比物的差异性越大，论证越强。
- 类比物与目标物的相似性越多，论证越强。
- 类比物与目标物的相似性之间越相关，论证越强。
- 类比物与目标物之间非相似性的性质和程度，可能削弱或加强论证。
- 结论越具体，论证越弱。

Example

Argument by Analogy

有妻杀夫，放火烧舍，称“火烧夫死”。夫家疑之，讼于官。妻不服。取猪两头，杀其一。积薪焚之，活者口中有灰，杀者口中无灰。因验尸，口果无灰，鞠之服罪。

Refutation by Analogy

1. 楚王赐晏子酒，酒酣，吏二缚一人诣王。
2. 王曰：“缚者曷为者也？”对曰：“齐人也，坐盗。”
3. 王视晏子曰：“齐人固善盗乎？”
4. 晏子避席对曰：“婴闻之，橘生淮南则为橘，生于淮北则为枳，叶徒相似，其实味不同。所以然者何？水土异也。今民生齐不盗，入楚则盗，得无楚之水土，使民善盗耶？”

Example

Argument by Analogy

人们似乎经常相信创造力，但它所做的只不过是把事物的分界线确定下来，并赋予它一个名字。正如地理学家划出海岸线并说“这些线确定的海域为黄海”，此时他并未创造一个海；数学家也一样，他不能通过定义创造东西。

— Frege

Refutation by Analogy

- ▶ I think sex education causes pregnancies.
- ▶ Right... And drivers education causes accidents. 😊

Example

Argument by Analogy

不能要求每样东西都有定义，否则如同要求任何物质都可被分解。简单物质不能被分解，逻辑上简单的东西不能被定义。

— Frege

Refutation by Analogy

- ▶ 人工智能不可能实现，因为，人工智能是建立在固体物理学之上的，而人脑是一个活的半流体系统。
- ▶ 汽车不可能代替马，因为，汽车是铁做的，而马是活的血肉构成的有机体。

Refutation by Analogy

- ▶ 计算机会思考吗？
- ▶ 潜水艇会游泳吗？

Examples — Does God Exist?

Argument by Analogy

If we found by chance a watch we should infer that it had been made by someone. But all around us we do find intricate pieces of natural mechanism, and the processes of the universe are seen to move together in complex relations; we should therefore infer that these too have a Maker.

Refutation by Analogy

Each of the multitude of universes may have different laws of nature. Some may be suitable for life, and some may not. It is very much like a lottery. If you win the lottery, you may feel very grateful, but someone had to win, and no one selected who that was, except randomly. Just because a universe has a unique set of laws should not lead one to wonder whether that set was designed.

Contents

Introduction

Logic Puzzle

Logic and other Disciplines

Textbook and Homework

Mill's Methods of Causal

Analysis

Analogical Argument

Fallacy and Bullshit

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Informal Fallacies

- i 形式谬误
 - ii 非形式谬误
 - 1. 言辞谬误
 - 2. 实质谬误
- ▶ 模糊谬误: 划界谬误或连续体谬误, 假精确或过度精确, 抽象概念当具体概念用
 - ▶ 歧义谬误: 一词多义, 歧义句构, 辖域谬误, 重音, 脱离语境、断章取义, 概念扭曲, 偷换概念, 混淆集合与个体或整体与部分, 变更标准
 - ▶ 定义谬误: 不当定义, 篡改定义
 - ▶ 废话谬误: 平凡真理, 无意义的问题, 回顾性宿命论

Informal Fallacies

- ▶ 不相干：歪曲论题（稻草人、红鲱鱼、烟雾弹），诉诸人身（扣帽子、人身攻击、诉诸动机、罪恶关联、诉诸虚伪、伪善、诉诸成就、富贵、贫贱、智商），诉诸情感（诉诸恐惧、厌恶、仇恨、谄媚、同情、愧疚、可爱、性感、时髦、嘲弄、虚荣、势利、沉默），诉诸暴力、恐吓、诽谤，诉诸来源、年代、新潮、传统，诉诸信心、意愿，诉诸后果、中庸、自然，转移举证责任，不得要领
- ▶ 不充分：不当概括（偏差样本、偏差统计），诉诸无知，诉诸不当权威、名人、大众，虚假原因，滑坡谬误，诉诸可能，诉诸阴谋，隐瞒证据，不当类比，乱赋因果（相关、巧合、因果倒置、单因谬误），完美主义谬误、权宜主义谬误
- ▶ 不当预设：窃取论题，非黑即白，打压对立，自然主义谬误（实然推应然），道德主义谬误（好的就是自然的），复合问题，诱导性提问，诉诸顽固、反复、冗赘，乱枪打鸟，两面讨好

“这鸡蛋真难吃。”

- ▶ 有本事你下一个好吃的蛋啊！
- ▶ 我可以负责任地说，我们的鸡蛋都是合格的健康蛋！
- ▶ 鸡是优等鸡，你咋说它下的蛋难吃？
- ▶ 这是别有用心的煽动，你有何居心？
- ▶ 隔壁的鸡给了你多少钱？
- ▶ 隔壁家的鸡蛋是伪蛋！
- ▶ 伟大的隔壁老王说好吃，你跟他说去！
- ▶ 没有伟大的老王，你连臭蛋都吃不上！
- ▶ 杀掉这只鸡换一只就能下金蛋？
- ▶ 你叫什么名字？你是干什么的！你是站在谁的立场上说话？
- ▶ 美国鸡蛋好吃，你去吧！
- ▶ 你以为你谁啊，品蛋师啊？轮到你说！
- ▶ 你个鸭蛋脑残粉！
- ▶ 下蛋的是一只勤劳勇敢善良正直的鸡！
- ▶ 再难吃也是自己家的鸡下的蛋！
- ▶ 但隔壁家的鸡蛋没有我们家的蛋形圆！
- ▶ 吃鸡蛋是我们家的传统美德。祖宗三代都是吃鸡蛋长大的！你也是！你有什么权力说这蛋难吃？还是不是人！
- ▶ 作为一个吃鸡蛋长大的人，我为我天天吃鸡蛋感到自豪！
- ▶ 拒绝抹黑！抵制鸭蛋！鸡蛋万岁！鸡蛋加油！
- ▶ 人心理阴暗会导致味觉异常……
- ▶ 其实隔壁家鸡蛋是个巨大的阴谋，试图颠覆我们家！
- ▶ 其实邻居家只有少数人才能吃上鸡蛋。
- ▶ 我们这么大的一个家，问题太复杂，下蛋没有你想得那么容易。
- ▶ 不要再吵了，这个家不能乱，稳定、稳定压倒一切！
- ▶ 要对我们家的鸡有耐心，它一定会下出更好吃的蛋。
- ▶ 蛋无完蛋！

“这鸡蛋真难吃。”

- ▶ 我们家的鸡已经可以打败隔壁家的鸭！
- ▶ 隔壁家也吃过这样的鸡蛋，现在是初级阶段，必须坚持一百年不动摇！
- ▶ 我们家人肠胃不好，现阶段还不适合吃鸭蛋，不符合我们家的具体家情！
- ▶ 凡事都有个过程，现在还不是吃鸭蛋的时候。
- ▶ 鸡蛋好不好吃，全体蛋鸡最有发言权。
- ▶ 老外都说好吃呢。
- ▶ 这蛋难吃但是历史悠久啊。
- ▶ 虽然难吃但重要的是好看啊。
- ▶ 比以前已经进步很多了。
- ▶ 哎，人心不古，世风日下，就是因为你这种想吃鸭蛋的人太多了……
- ▶ 隔壁家那鸭蛋更难吃，你咋不说呢？
- ▶ 嫌难吃就别吃，滚去吃隔壁的鸭蛋吧。
- ▶ 隔壁亡我之心不死！该鸡蛋肯定是被隔壁一小撮不会下蛋的鸡煽动变臭的！
- ▶ 你上次吃茄子都吐，味觉一贯奇葩。
- ▶ 胡说！我们家的鸡蛋比隔壁家的鸭蛋好吃五倍！五倍！
- ▶ 是你的思想跟不上鸡蛋口味的升级！
- ▶ 心理阴暗！连鸡蛋不好吃也要发牢骚！
- ▶ 抱怨有毛用，有这个时间快去赚钱！
- ▶ 隔壁家的鸡蛋也一样，天下乌鸦一般黑，没有好吃的鸡蛋！
- ▶ 吃了人家的鸡蛋还留下证据说鸡蛋难吃，太有城府了！
- ▶ 很多家都是因为吃隔壁的鸭蛋而导致家庭冲突，生活水平下降甚至解体！
- ▶ 到目前为止，我没发现这鸡蛋难吃。专家说了，这鸡蛋难吃的可能性不大。即使出现这种情况，也是结构性难吃。
- ▶ 荷兰狗/东北猪/瘪三……不配吃鸡蛋！
- ▶ 大家小心，此人 IP 在国外。
- ▶ 滚，你丫是鸡奸，这里不欢迎你。

假如潘金莲不开窗户，就不会掉下木棍打到西门庆，也就不会认识西门庆，不会出轨，不会害死武大郎，武松不会被逼杀人上梁山，不会有独臂擒方腊，方腊就可夺取大宋江山，没了宋就不会有靖康耻、金兵入关，也不会有元、明、清，不会闭关锁国、鸦片战争、八国联军。这样中国将成为超级大国，称霸世界！

For Want of a Nail

For want of a nail, the shoe was lost,
For want of a shoe, the horse was lost,
For want of a horse, the rider was lost,
For want of a rider, the message was lost,
For want of a message, the battle was lost,
For want of a battle, the war was lost,
For want of a war, the kingdom was lost,
For want of a nail, the world was lost.
And all for the want of a nail.

孔子《论语》

名不正，则言不顺，
言不顺，则事不成；
事不成，则礼乐不兴，
礼乐不兴，则刑罚不中；
刑罚不中，则民无所措手足。

礼记·坊记

天无二日，土无二王，家无二主，尊无二上。

董仲舒《春秋繁露》

天以终岁之数，成人之身，故小节三百六十六，副日数也；大节十二，分副月数也；内有五藏，副五行数也；外有四肢，副四时数也；乍视乍瞑，副昼夜也；乍刚乍柔，副冬夏也。

告子：性，犹湍水也，决诸东方则东流，决诸西方则西流。人性之无分于善不善也，犹水之无分于东西也。

孟子：水信无分于东西，无分于上下乎？人性之善也，犹水之就下也。人无有不善，水无有不下。

孟子《生于忧患，死于安乐》

舜发于畎亩之中，傅说举于版筑之中，胶鬲举于鱼盐之中，管夷吾举于士，孙叔敖举于海，百里奚举于市。故天将降大任于斯人也，必先苦其心志，劳其筋骨，饿其体肤，空乏其身，行拂乱其所为，所以动心忍性，曾益其所不能。

三秀才赶考，途遇算命先生，问几人中举？先生竖起一指。

莱布尼茨《单子论》

如果单子没有知觉，那么其复合物也没有知觉。

帕斯卡赌

如果上帝不存在，但你相信上帝存在，也没太大损失；然而，如果上帝存在，而你却不相信上帝存在，那你将面临巨大的惩罚。所以，应该相信上帝存在。

鲁迅《论辩的灵魂》

我骂卖国贼，所以我是爱国者。爱国者的话是最有价值的，所以我的话是不错的，我的话既然不错，你就是卖国贼无疑了！

Wholeness depends on dimensionless phenomena. Reality has always been full of messengers of the multiverse, whose third eyes are transformed into transcendence. Transcendence is the healing of choice. Complexity is the driver of transcendence. Our conversations with other messengers have led to an awakening of ultra-non-local consciousness. Consciousness requires exploration. We are at a crossroads of flow and ego. We can no longer afford to live with ego. Where there is ego, life can't thrive. We exist as expanding wave functions. The goal is to plant the seeds of passion rather than bondage. We are in the midst of a self-aware blossoming of being that will align us with the nexus itself. Lifeform, look within and recreate yourself. To follow the path is to become one with it. By unfolding, we believe; By deepening, we vibrate; By blossoming, we self-actualize. We dream, we heal, we are reborn. We must learn how to lead unlimited lives in the face of delusion. You and I are dreamweavers of the quantum soup. The infinite is approaching a tipping point. **Hidden meaning transforms unparalleled abstract beauty. Wholeness quiets infinite phenomena.**

How to generate pseudo-profound bullshit?¹

1. State the blindingly obvious (of life's big theme) incredibly slowly.
 - ▶ We were all children once.
2. Doublethink/Dialectic/Contradiction.
 - ▶ War is peace. Freedom is slavery. Ignorance is strength.
 - ▶ Everyone is the other, and no one is himself.
 - ▶ Man can do what he wills but he can't will what he wills.
3. Ambiguity/Metaphor/Parable.
 - ▶ Language is the house of the truth of Being.
 - ▶ Never stay up on the barren heights of cleverness, but come down into the green valleys of silliness.
 - ▶ Ethics does not treat of the world. Ethics must be a condition of the world, like logic.
 - ▶ A person is neither a thing nor a process but an opening through which the Absolute can manifest.
 - ▶ Making itself intelligible is suicide for philosophy. Those who idolize "facts" never notice that their idols only shine in a borrowed light.

¹Law: Believing Bullshit.

Frankfurt: On Bullshit.

Bergstrom & West: Calling Bullshit.

How to generate pseudo-profound bullshit?

4. Analogy.

- ▶ We have got on to slippery ice where there is no friction, and so, in a certain sense, the conditions are ideal; but also, just because of that, we are unable to walk. We want to walk: so we need friction. Back to the rough ground!
- ▶ The subject does not belong to the world: rather, it is a limit of the world. This is exactly like the case of the eye and the visual field. You do not see the eye. Nothing in the visual field allows you to infer that it is seen by an eye. Our life is endless in the way that our visual field is without limit.

5. Use jargon.

- ▶ Profound boredom, drifting here and there in the abysses of our existence like a muffling fog, removes all things and men and oneself along with it into a remarkable indifference. This boredom reveals being as a whole.
- ▶ A machinic assemblage, through its diverse components, extracts its consistency by crossing ontological thresholds, non-linear thresholds of irreversibility, ontological and phylogenetic thresholds, creative thresholds of heterogenesis and autopoiesis.

The Unreasonable Ineffectiveness of Philosophy

- ▶ 费曼：“砖头算不算本质客体？”
- ▶ 哲学家甲：“一块砖是独特的砖，是怀海德所说的本质客体。”
- ▶ 哲学家乙：“本质客体的意思并不是指个别的砖块，而是指所有砖块的共有的普遍性质，换句话说，‘砖性’才是本质客体。”
- ▶ 哲学家丙：“不对，重点不在砖本身，‘本质客体’指的是，当你想到砖块时内心形成的概念。”
- ▶ 就像所有关于哲学家的故事一样，最终以一片混乱收场。好笑的是，在先前的那么多次讨论中，他们从来没有问过自己，像简单的砖块究竟是不是“本质客体”。

— 费曼

哲学旨在感动那些混淆晦涩与深刻的人。

— 温伯格

The Unreasonable Ineffectiveness of Philosophy

- ▶ When a philosopher says something that is true then it is trivial. When he says something that is not trivial then it is false. — *Gauss*
- ▶ There is only one thing a philosopher can be relied upon to do, and that is to contradict other philosophers. — *William James*
- ▶ Philosophy is a ‘catalyst’ or ‘spice’ which makes the interdisciplinary mixture work. ‘Philosophy-internal’ issues seem like intellectual black holes: they absorb a lot of clever energy, but nothing ever seems to come out. — *Johan van Benthem*
- ▶ Philosophers are free to do whatever they please, because they don’t have to do anything right.
- ▶ Philosophy is to science as pornography is to sex: it is cheaper, easier, and some people seem, bafflingly, to prefer it. — *John Jones*
- ▶ A philosopher looking for the ultimate truth is like a blind darky with an extinguished candle on a dark night searching a dark subterranean cave for a black cat that isn’t there, and shouting “I found it!”

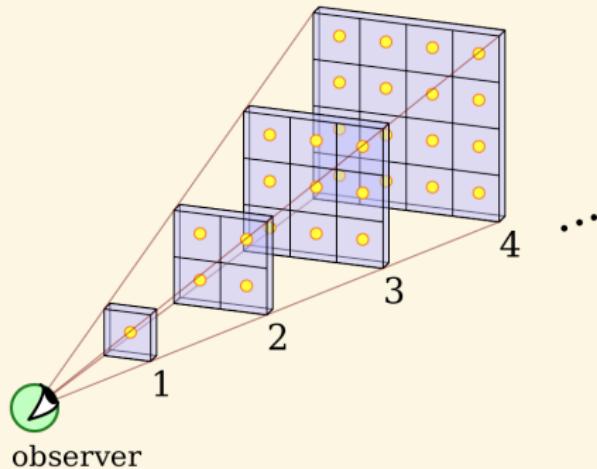
Practice is the sole criterion for testing truth?

Practice is the sole criterion for testing truth?

- ▶ What is “practice”?
- ▶ What is “truth”?
- ▶ What is “criterion”?
- ▶ Why “sole” criterion?
- ▶ How to “test”?
- ▶ How to test “truth” with “practice”?



Why is the Night Sky Dark?



A static, infinitely old universe with an infinite number of stars uniformly distributed in an infinitely large space would be bright rather than dark.

星若无穷尽，天空将明亮。

仰望银河，君可见背景片片无点状？

夜空暗黑，原因此一桩。

光行万里，发于恒星之初创。

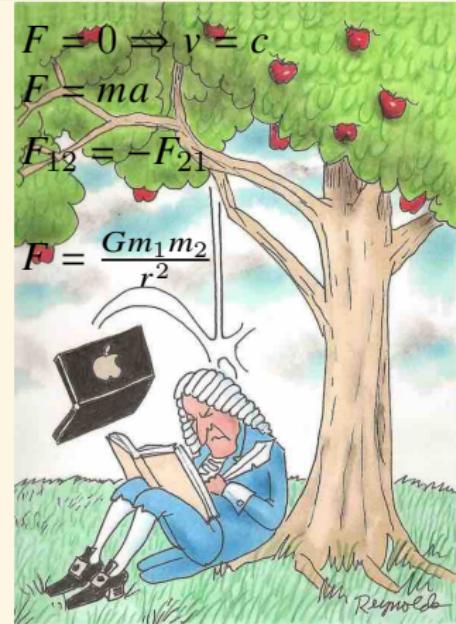
抵达地球未及时，只因路遥道太长。



Newton's Apple

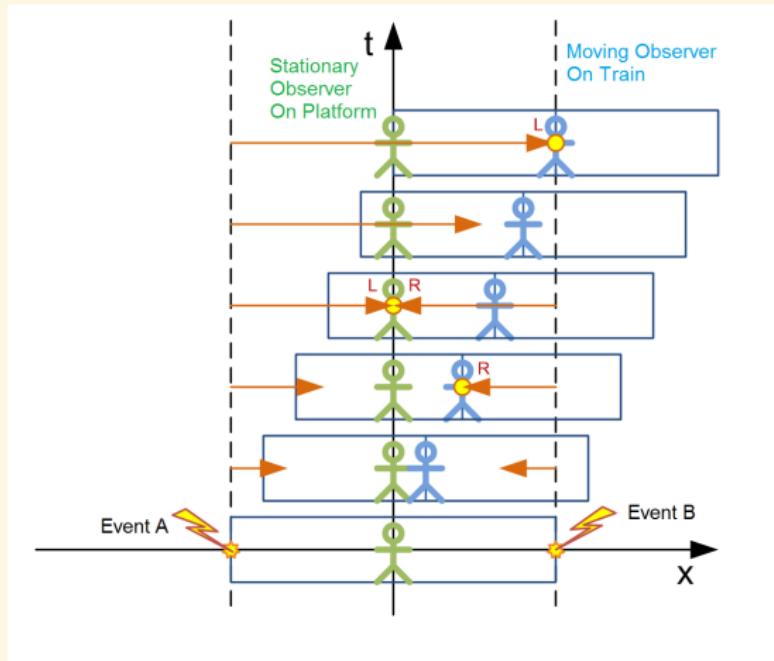
If an apple falls, does the moon also fall?

- ▶ What is “rest/motion”?
- ▶ What is “state of rest/motion”?
- ▶ What is “change/tends to change”?
- ▶ What is “body”?
- ▶ What is “force”?
- ▶ What is “definition”?



A force is that which changes or tends to change the state of rest or motion of a body.

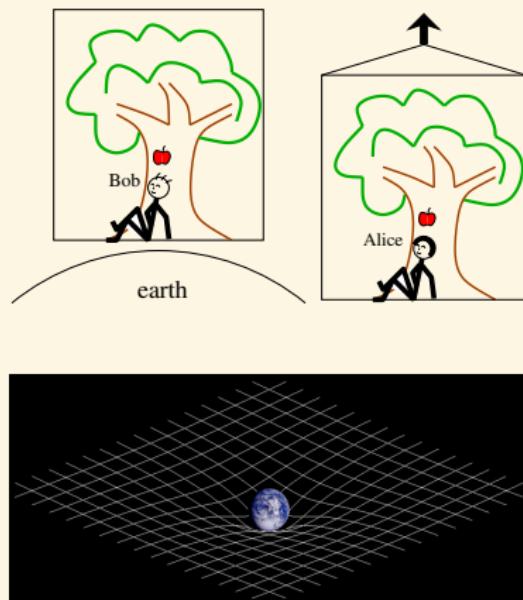
Einstein's Train Thought Experiment



- ▶ What is “simultaneity”?
- ▶ How to measure “simultaneity”?
- ▶ How to measure “time”?

Einstein's Elevator Thought Experiment

- ▶ The gravitational “force” as experienced locally while standing on a massive body is actually the same as the pseudo-force experienced by an observer in a non-inertial (accelerated) frame of reference.
- ▶ Spacetime tells matter how to move; matter tells spacetime how to curve.
- ▶ Gravity is not a force that applies via Newton’s 2nd Law, but a consequence of the curvature of spacetime caused by the uneven distribution of mass/energy that acts via the geodesic principle, which is the relativistic equivalent of Newton’s 1st Law.
- ▶ Causality (causally connected regions, finite speed of light)



The Music of Reason — The glory of the human spirit!

How to *express your thoughts precisely and succinctly?*

- ▶ Not only is the universe stranger than we imagine, it is stranger than we can imagine.
- ▶ Logic enlarges our abstract imagination.
- ▶ A few lines of reasoning can change the way we see the world.
- ▶ Logic is the immune system of the mind!
- ▶ The music of reason — the fulfillment of the human spirit.



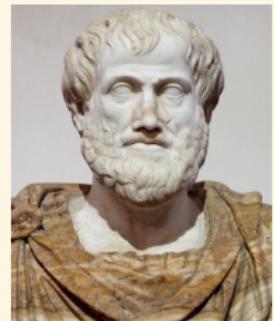
What are the extent and limits of reason?

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Aristotle(384-322 BC)

- ▶ Three Modes of Persuasion in Rhetoric: Ethos, Pathos, and Logos.
- ▶ Term Logic.
- ▶ Aristotle believed that any logical argument can, in principle, be broken down into a series of applications of a small number of syllogisms.
- ▶ Four Causes: material/formal/efficient/final



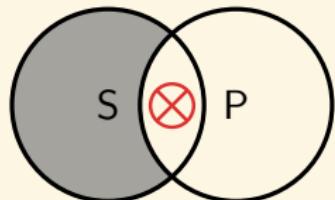
Sophistic vs Valid Argument

1. Nothing exists;
2. Even if something exists, nothing can be known about it;
3. Even if something can be known about it, knowledge about it can't be communicated to others;
4. Even if it can be communicated, it can't be understood.

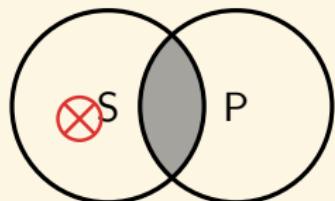
All men are mortal
Socrates is a man

Socrates is mortal

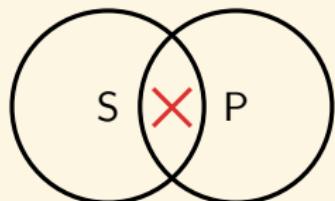
A: All *S* are *P*.



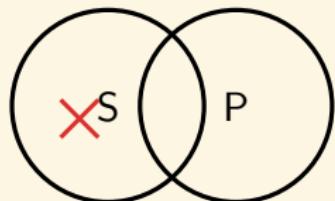
E: No *S* are *P*.



I: Some *S* are *P*.



O: Some *S* are not *P*.



Syllogism

$$M - P$$

$$S - M$$

$$\frac{}{S - P}$$

$$P - M$$

$$S - M$$

$$\frac{}{S - P}$$

$$M - P$$

$$M - S$$

$$\frac{}{S - P}$$

$$P - M$$

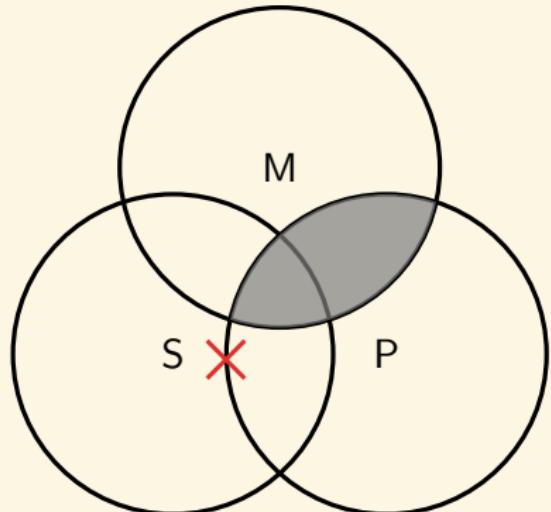
$$M - S$$

$$\frac{}{S - P}$$

- ▶ Major term: the predicate of the conclusion.
- ▶ Minor term: the subject of the conclusion.
- ▶ Middle term: the third term
- ▶ Major premise: The premise that contains the major term
- ▶ Minor premise: The premise that contains the minor term
- ▶ 4 figure, $4^3 \times 4 = 256$ forms.
- ▶ 15 Boolean valid.
- ▶ 24 Aristotelean valid.
(Existential Import)
- ▶ How to determine the valid syllogisms?
 1. Venn Diagrams
 2. Rules
 3. Boolean Algebra
 4. Axiomatization

Venn Diagram — Boolean Standpoint

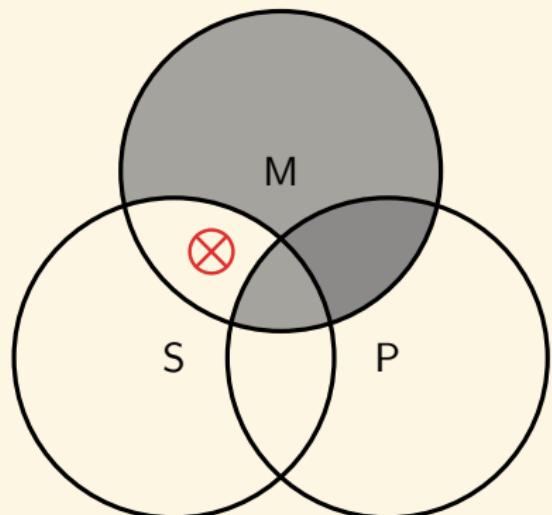
1. label the circles of a three-circle Venn diagram with the syllogism's three terms.
2. diagram the two premises, and diagram the universal premise first if there is one universal and one particular.
3. in diagramming a particular proposition, put an \times on a line if the premises do not determine on which side of the line it should go.
4. inspect the diagram to see if it supports the conclusion.

$$\frac{\text{No } P \text{ are } M \\ \text{Some } S \text{ are not } M}{\text{Some } S \text{ are } P}$$


Venn Diagram — Aristotelean Standpoint

1. if a syllogism having universal premises and a particular conclusion is not valid from the Boolean standpoint, look to see if there is a Venn circle that is completely shaded except for one area. If there is, enter a \otimes in that area.
2. if the syllogistic form is conditionally valid, determine if the \otimes represents something that exists.

$$\frac{\text{No } M \text{ are } P \\ \text{All } M \text{ are } S}{\text{Some } S \text{ are not } P}$$



Syllogistic Rules

		<i>S</i> distributed		
		<i>P</i> undistributed	<i>E</i> : <u>No</u> <i>S</i> are <i>P</i> .	<i>P</i> distributed
<i>P</i> undistributed	<i>A</i> : <u>All</u> <i>S</i> are <i>P</i> .		<i>I</i> : Some <i>S</i> are <i>P</i> .	<i>O</i> : Some <i>S</i> are <u>not</u> <i>P</i> .
		<i>S</i> undistributed		

1. the middle term must be distributed at least once.
2. any term that is distributed in the conclusion must be distributed in the premises.
3. the number of negative premises must be equal to the number of negative conclusions.
4. a particular conclusion requires a particular premise. (Existential Fallacy)
 - ▶ Aristotle 1 – 3
 - ▶ Boole 1 – 4

Deduction/Induction/Abduction/Examplification

$$M \rightarrow P$$

$$\frac{S \rightarrow M}{S \rightarrow P}$$

$$M \rightarrow P$$

$$\frac{M \rightarrow S}{S \rightarrow P}$$

$$H \rightarrow E$$

$$E$$

$$H$$

$$P \rightarrow M$$

$$S \rightarrow M$$

$$S \rightarrow P$$

$$H \rightarrow E$$

$$\top \rightarrow E$$

$$\top \rightarrow H$$

$$P \rightarrow M$$

$$M \rightarrow S$$

$$S \rightarrow P$$

Deduction/Induction/Abduction

All the beans from this bag are white.
These beans are from this bag.

$$\frac{M \rightarrow P}{\begin{array}{c} S \rightarrow M \\ \hline S \rightarrow P \end{array}}$$

These beans are white.
These beans are from this bag.

$$\frac{\begin{array}{c} M \rightarrow P \\ M \rightarrow S \\ \hline S \rightarrow P \end{array}}{S \rightarrow P}$$

All the beans from this bag are white.
These beans are white.

$$\frac{\begin{array}{c} P \rightarrow M \\ S \rightarrow M \\ \hline S \rightarrow P \end{array}}{S \rightarrow P}$$

Abduction

1. 观察到恒星光谱红移。
2. 如果恒星在退行，那么恒星光谱红移就可以解释。
3. 如果整个宇宙在膨胀，那么恒星在离我们而去。
4. 如果宇宙起源于大爆炸，那么宇宙就会膨胀。
5. 因此，宇宙起源于大爆炸。



Example and Criticism

All men are intelligent

Women are not men

Women are not intelligent

John does not read books

Students who like to learn read books

John does not like to learn

Nothing is better than money

Philosophy is better than nothing

Philosophy is better than money

鲁迅小说不是一天可以读完的

《阿 Q 正传》是鲁迅小说

《阿 Q 正传》不是一天可以读完的

Only man is rational

No woman is a man

No woman is rational

No professors are ignorant

All ignorant people are vain

No professors are vain

Everybody loves my baby

My baby loves nobody but me

I am my baby

MEP

SAM

SEP

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Gottfried Wilhelm Leibniz 1646-1716

Don't argue. Let us Calculate!

- ▶ **Principle of Contradiction:** Nothing can be and not be, but everything either is or is not. (Everything that is not self-contradictory is possible.)
- ▶ **Principle of Sufficient Reason:** Nothing happens without a reason why it should be so rather than otherwise.
- ▶ **Principle of Perfection:** The real world is the best of all possible worlds.

In the beginning was the Logic.

As God calculates, so the world is made.



Leibniz

- ▶ The last “universal genius”, developed Calculus, refined binary number system, invented mechanical calculator that could perform addition, subtraction, multiplication and division.
- ▶ Leibniz was claimed (by Russell, Euler, Gödel, Weiner, Mandelbrot, Robinson, Chaitin) to be a precursor of mathematical logic², topology, game theory, cybernetic theory, fractal geometry, non-standard analysis, algorithmic information theory and digital philosophy.

²Wolfgang Lenzen: Leibniz's Logic.

Leibniz's Philosophy of Deductive Logic

1 Characteristica Universalis & Calculus Ratiocinator.

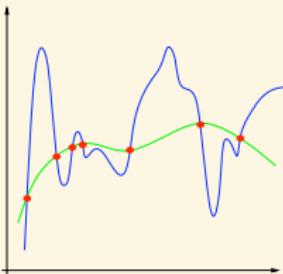
- i the coordination of knowledge in an encyclopedia — collect all present knowledge so we could sift through it for what is fundamental. With the set of ideas that it generated, we could formulate the *characteristica universalis*. (which form the alphabet of human thought).
- ii **characteristica universalis** — a universal ideal language whose rules of composition directly expresses the structure of the world.

sign \Leftrightarrow idea

encyclopedia \Rightarrow fundamental principles \Rightarrow primitive notions

- iii **calculus ratiocinator** — the arrangement of all true propositions in an axiomatic system.
- iv decision procedure. — an algorithm which, when applied to any formula of the *characteristica universalis*, would determine whether or not that formula were true. — a procedure for the rapid enlargement of knowledge. replace reasoning by computation. the art of invention. free mind from intuition.
- v a proof that the *calculus ratiocinator* is consistent.

Leibniz's Philosophy of Inductive Logic / Probability



2. Compute all descriptions of possible worlds that can be expressed with the primitive notions. And the possible worlds will all have some propensity to exist.
3. Compute the probabilities of disputed hypotheses relative to the available data. As we learn more our probability assignments will asymptotically tend to a maximum for the real world, i.e. the possibility with the highest actual propensity.
 - ▶ “Probability is degree of possibility (perfection).”
 - ▶ “A hypothesis is more probable as it is simpler to understand and wider in explanatory power.”

probability = propensity \propto perfection = $f(\text{variety, simplicity})$

Characteristic Universalis vs Calculus Ratiocinator

1. Characteristica Universalis — a universal language of human thought whose symbolic structure would reflect the structure of the world.
2. Calculus Ratiocinator — a method of symbolic calculation which would mirror the processes of human reasoning.

Characteristic Universalis	Calculus Ratiocinator
Language as Medium	Language as Calculus
Semantics is ineffable	Semantics is possible
Interpretation can't be varied	Interpretation can be varied
Model theory impossible	Model theory possible
Only one world can be talked about	Possible worlds are possible
Only one domain of quantifiers	Domains of quantifiers can be different
Ontology is the central problem	Ontology conventional
Logical truths are about this world	Logical truth as truth in all possible worlds

Characteristic Universalis vs Calculus Ratiocinator

- ▶ For the *characteristica universalis* tradition, there is only one kind of human thinking logic must reflect. The meanings of the expressions of the language can't be defined. Its semantics can't be defined in that language itself without circularity, for this semantics is assumed in all its uses, and it can't be defined in a metalanguage, because there is no such language beyond our actual working language. A kind of one-world assumption is implicit in the idea of language as the universal medium.
- ▶ The *calculus ratiocinator* tradition applies logic "locally" leaving it up to the user to determine the universe of discourse in every concrete application, while the *characteristica universalis* tradition tends to apply logic to the fixed metaphysical universe that is supposed to include *all* that there is.

Leibniz's Algebra of Concepts



- | | |
|--|--|
| 1. $A \sqsubset A$ | 1. $\overline{\overline{A}} = A$ |
| 2. $A \sqsubset B \wedge B \sqsubset C \rightarrow A \sqsubset C$ | 2. $A \neq \overline{A}$ |
| 3. $A \sqsubset B \leftrightarrow A = AB$ | 3. $A \sqsubset B \leftrightarrow \overline{B} \sqsubset \overline{A}$ |
| 1. $C \sqsubset AB \leftrightarrow C \sqsubset A \wedge C \sqsubset B$ | 4. $\diamond A \rightarrow A \sqsubset B \rightarrow A \not\sqsubset \overline{B}$ |
| 2. $AB \sqsubset A$ | 5. $A\overline{A} \sqsubset B$ |
| 3. $AB \sqsubset B$ | 1. $A \sqsubset B \rightarrow \diamond A \rightarrow \diamond B$ |
| 4. $AA = A$ | 2. $A \sqsubset B \leftrightarrow \neg\diamond(A\overline{B})$ |
| 5. $AB = BA$ | 3. $\neg\diamond(A\overline{A})$ |

$$\diamond A := A \not\sqsubset B\overline{B}$$

$$A \sqcup B := \overline{\overline{A} \overline{B}}$$

$$A \sqsubset A \sqcup B$$

$$B \sqsubset A \sqcup B$$

$$A \sqsubset C \wedge B \sqsubset C \rightarrow A \sqcup B \sqsubset C$$

Indefinite Concepts

A	E	I	O
$A \sqsubset B$	$A \sqsubset \overline{B}$	$A \not\sqsubset \overline{B}$	$A \not\sqsubset B$
$A = AB$	$A = A\overline{B}$	$A \neq A\overline{B}$	$A \neq AB$
$\neg\Diamond(A\overline{B})$	$\neg\Diamond(AB)$	$\Diamond(AB)$	$\Diamond(A\overline{B})$
$\exists X(A = BX)$	$\exists X(A = \overline{B}X)$	$\forall X(A \neq \overline{B}X)$	$\forall X(A \neq BX)$
$\varphi(A) \vdash \exists X\varphi(X)$	$\exists X\varphi(X) \vdash \varphi(A)$ for some new constant A		
$\neg\exists X\varphi(X) \leftrightarrow \forall X\neg\varphi(X)$	$\forall X\varphi(X) \vdash \exists X\varphi(X)$		

Example:

$$\begin{array}{lll} MAP & \exists X(M = PX) & \\ SIM & \forall Y(S \neq \overline{M}Y) & \\ \hline SIP & \forall Z(S \neq \overline{P}Z) & \end{array}$$

Proof.

Asume $S = \overline{P}Z$. Since $M \sqsubset P \iff \overline{P} \sqsubset \overline{M}$, $\exists X(\overline{P} = \overline{M}X)$. Then $S = \overline{M}XZ$. Contradiction.

$$\begin{aligned} \text{Individual}(A) &:= \Diamond A \wedge \forall X(\Diamond(AX) \rightarrow A \sqsubset X) \\ &\leftrightarrow \forall X(A \not\sqsubset X \leftrightarrow A \sqsubset \overline{X}) \end{aligned}$$

Translate Leibniz's Algebra of Concepts to the Algebra of Propositions



- | | |
|--|--|
| 1. $A \rightarrow A$ | 1. $\neg\neg A \leftrightarrow A$ |
| 2. $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$ | 2. $\neg(A \leftrightarrow \neg A)$ |
| 3. $(A \rightarrow B) \leftrightarrow (A \leftrightarrow A \wedge B)$ | 3. $(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$ |
| 1. $(C \rightarrow A \wedge B) \leftrightarrow (C \rightarrow A) \wedge (C \rightarrow B)$ | 4. $\diamond A \rightarrow (A \rightarrow B) \rightarrow \neg(A \rightarrow \neg B)$ |
| 2. $A \wedge B \rightarrow A$ | 5. $A \wedge \neg A \rightarrow B$ |
| 3. $A \wedge B \rightarrow B$ | 1. $(A \rightarrow B) \rightarrow \diamond A \rightarrow \diamond B$ |
| 4. $A \wedge A \leftrightarrow A$ | 2. $(A \rightarrow B) \leftrightarrow \neg\diamond(A \wedge \neg B)$ |
| 5. $A \wedge B \leftrightarrow B \wedge A$ | 3. $\neg\diamond(A \wedge \neg A)$ |

$$\diamond A := \neg(A \rightarrow B \wedge \neg B)$$

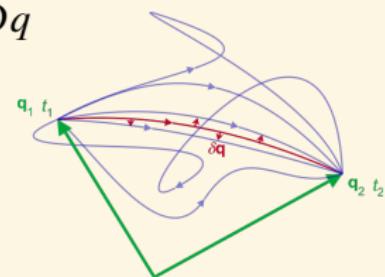
Leibniz's Metaphysics and Quantum Mechanics



Monadology	Path Integral
Amount of existence	Square of probability amplitude
Measure of necessity of individual possibility	Probability
Collision or competition of possibilities	Interference or summation of probability amplitudes
Coexisting or compatible essences	Superposition of coherent paths
Maximal degree of existence	Observed path

$$P = |\langle q_2, t_2 | q_1, t_1 \rangle|^2 \quad \langle q_2, t_2 | q_1, t_1 \rangle = \int_{q_1}^{q_2} \varphi[q] \mathcal{D}q$$

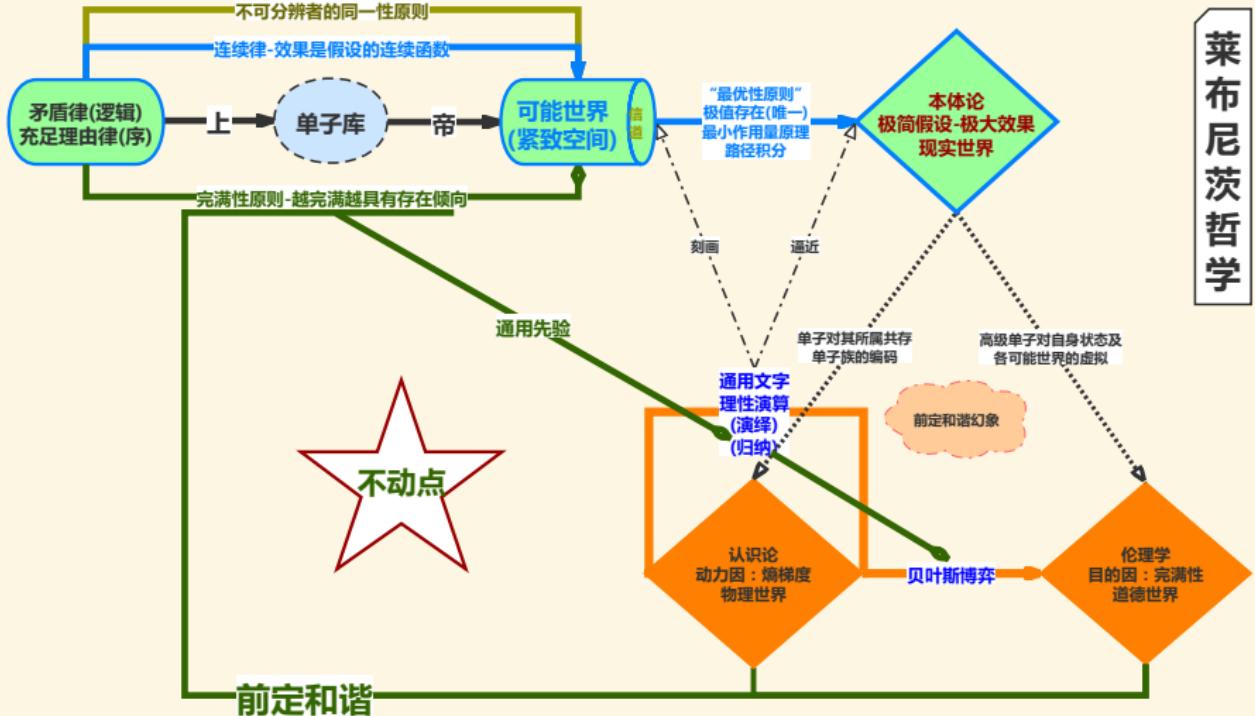
$$\varphi[q] \propto e^{\frac{i}{\hbar} S[q]} \quad S[q] = \int_{t_1}^{t_2} L[q(t), \dot{q}(t)] dt \quad \delta S = 0$$



- ▶ Probability of the actual path = maximum
- ▶ Action of the actual path = minimum
the absolute square of the sum of probability amplitudes over all possible paths

Leibniz's Program

莱布尼茨哲学



George Boole 1815-1864

- ▶ *The Laws of Thought*
- ▶ Propositional Logic / Boolean Algebra

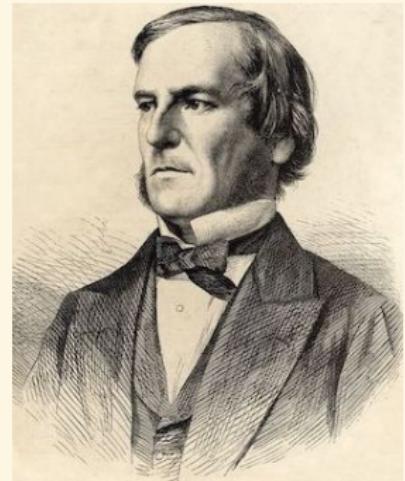
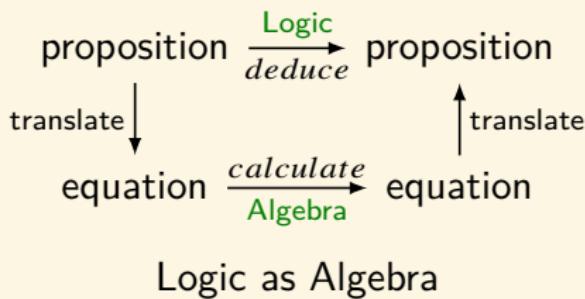
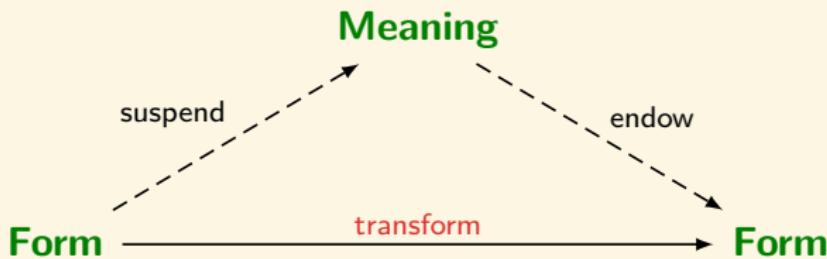


Figure: self-taught mathematician, philosopher, logician, and poet

Logic → Truth

“Truth points the way for logic, just as beauty does for aesthetics, and goodness for ethics.”

— Frege



“Mathematical logic is a science prior to all others, which contains the ideas and principles underlying all sciences.”

— Gödel

A notion is “logical” iff it is invariant under all possible one-one transformations of the universe of discourse onto itself.

— Tarski

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

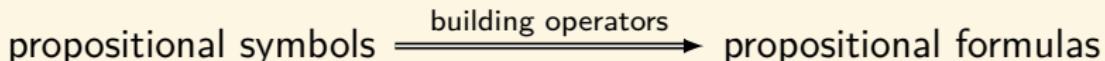
Quantum Computing

Answers to the Exercises

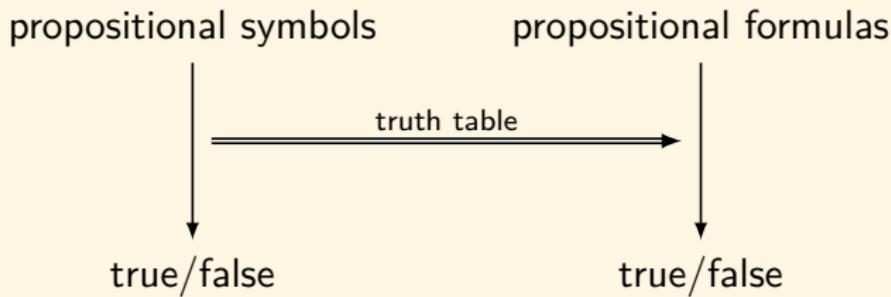
References 1436

Propositional Logic

- ▶ Language.
Building blocks of propositional logic language.
 - ▶ Syntax.



- ### ► Semantics.



- ## ► Formal System.



Syntax

Language

$$\mathcal{L}^0 := \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,), \} \cup \text{Var}$$

where $\text{Var} := \{p_1, p_2, p_3, \dots\}$.

Definition (Well-Formed Formula Wff)

- ▶ A propositional variable $p \in \text{Var}$ is a wff.
- ▶ If A is a wff, so is $(\neg A)$.
- ▶ If A and B are wffs, so are $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$.
- ▶ Nothing else is a wff.

$$A ::= p \mid (\neg A) \mid (A \wedge A) \mid (A \vee A) \mid (A \rightarrow A) \mid (A \leftrightarrow A)$$

- ▶ $\perp := (A \wedge (\neg A))$
- ▶ $\top := (\neg \perp)$

Example

Most people are so frightened of the name of mathematics that they are ready, quite unaffectedly, to exaggerate their own mathematical stupidity.

— G. H. Hardy

1. Lily is beautiful.
2. Lily is **not** beautiful.
3. Lily is beautiful **and** Lucy is smart.
4. Lily is beautiful **or** Lucy is smart.
5. **If** wishes were wings, **then** pigs would fly.
6. Lily is beautiful **if and only if** Lucy is smart.
7. 侠之大者，为国为民。
8. 只要功夫深，铁杵磨成针。 / 砍头不要紧，只要主义真。
9. 你请他才来。
10. 没有共产党，就没有新中国。
11. 不是你死，就是我亡。
12. 鱼与熊掌不可兼得。
13. 欲寄君衣君不还，不寄君衣君又寒。寄与不寄间，妾身千万难。

Well-Formed Formula

A panda eats, shoots and leaves.



Definition (Formula-Building Operators)

$$f_{\neg}(A) := (\neg A)$$

$$f_{\wedge}(A, B) := (A \wedge B)$$

$$f_{\vee}(A, B) := (A \vee B)$$

$$f_{\rightarrow}(A, B) := (A \rightarrow B)$$

$$f_{\leftrightarrow}(A, B) := (A \leftrightarrow B)$$

$$f_{\neg}(A) := \neg A$$

$$f_{\wedge}(A, B) := \wedge AB$$

$$f_{\vee}(A, B) := \vee AB$$

$$f_{\rightarrow}(A, B) := \rightarrow AB$$

$$f_{\leftrightarrow}(A, B) := \leftrightarrow AB$$

Well-Formed Formula



Definition (Construction Sequence)

A construction sequence (C_1, \dots, C_n) is a finite sequence of expressions s.t. for each $i \leq n$ we have at least one of

$$C_i = p_i \quad \text{for some } i$$

$$C_i = (\neg C_j) \quad \text{for some } j$$

$$C_i = (C_j \star C_k) \quad \text{for some } j < i, k < i, \text{ where } \star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}.$$

Definition (Well-Formed Formula)

A formula A is a well-formed formula (wff) iff there is some construction sequence (C_1, \dots, C_n) and $C_n = A$.

$$\text{Wff}_0 := \{p_1, p_2, \dots\}$$

$$\text{Wff}_{n+1} := \text{Wff}_n \cup \{(\neg A) : A \in \text{Wff}_n\} \cup \{(A \rightarrow B) : A, B \in \text{Wff}_n\}$$

$$\text{Wff}_* := \bigcup_{n \in \mathbb{N}} \text{Wff}_n$$

Generation — Bottom Up vs Top Down

Problem

Given a class \mathcal{F} of functions over U , how to **generate** a certain subset of U by starting with some initial elements $B \subset U$?

Bottom Up

$$C_0 := B$$

$$C_{n+1} := C_n \cup \bigcup_{f \in \mathcal{F}} \{f(\mathbf{x}) : \mathbf{x} \in C_n\} \quad \deg(\mathbf{x}) := \mu n \ [\mathbf{x} \in C_n]$$

$$C_* := \bigcup_{n \in \mathbb{N}} C_n$$

Top Down

- A set S is **closed under a function** f iff for all \mathbf{x} : $\mathbf{x} \in S \rightarrow f(\mathbf{x}) \in S$.
- A set S is **inductive** iff $B \subset S$ and for all $f \in \mathcal{F}$: S is closed under f .
- $C^* := \bigcap \{S : S \text{ is inductive}\}$

Bottom Up vs Top Down



How many bottles of beer can you buy with \$10?

- ▶ \$2 can buy 1 bottle of beer.
- ▶ 4 bottle caps can be exchanged for 1 bottle of beer.
- ▶ 2 empty bottles can be exchanged for 1 bottle of beer.

Generation — Bottom Up vs Top Down



Example

Let $B := \{0\}$, $\mathcal{F} := \{s, p\}$, $s(x) := x + 1$, $p(x) := x - 1$

$$C_* = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

There is more than one way of obtaining a member of C_* , e.g.

$$1 = s(0) = s(p(s(0))).$$

Theorem (Bottom up and Top down)

$$C_* = C^*$$

Proof.

$(C^* \subset C_*)$: to show C_* is inductive.

$(C_* \subset C^*)$: to show $C_n \subset C^*$ for all n by induction. Consider $x \in C_*$ and a construction sequence (x_0, \dots, x_n) for x . First $x_0 \in B \subset C^*$. If for all $i < n$ we have $x_i \in C^*$, then $x_n \in C^*$.

Induction Principle for Formulas



Theorem (Induction Principle)

Let P be a property of formulas, satisfying

- every atomic formula has property P , and
- property P is closed under all the formula-building operations,
then every formula has property P .

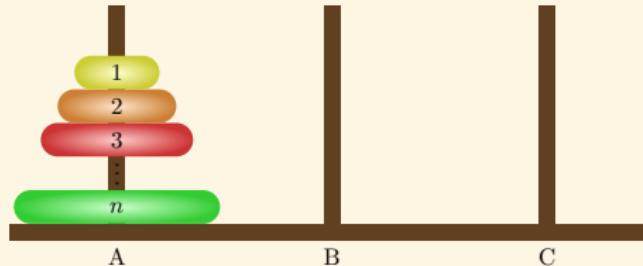
Proof.

$$\text{Wff}_* = \text{Wff}^* \subset P$$

$$P(0) \wedge \forall n(P(n) \rightarrow P(n+1)) \rightarrow \forall n \in \mathbb{N} P(n)$$

$$P(n) := P(\text{Wff}_n)$$

Induction vs Recursion



$P(n)$:= “ n rings needs $2^n - 1$ moves.”

1. If ever you leave milk one day, be sure and leave it the next day as well.
2. Leave milk today.

Leave milk today and read this note again tomorrow.

Subformula

Definition (Subformula)

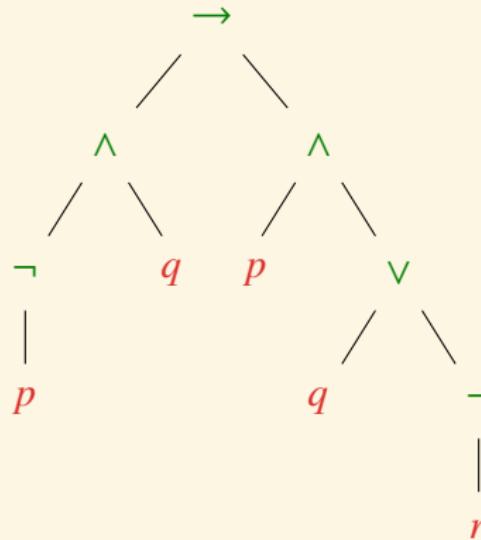
The set $\text{Sub}(A)$ of subformulas of a wff A is the smallest set Γ that satisfies

1. $A \in \Gamma$
2. $\neg B \in \Gamma \implies B \in \Gamma$
3. $B \rightarrow C \in \Gamma \implies B, C \in \Gamma$

$$\text{Sub}(A) := \begin{cases} \{A\} & \text{if } A = p \\ \{A\} \cup \text{Sub}(B) & \text{if } A = \neg B \\ \{A\} \cup \text{Sub}(B) \cup \text{Sub}(C) & \text{if } A = B \rightarrow C \end{cases}$$

Unique Readability — Unique Parse Tree

$$((\neg p) \wedge q) \rightarrow (p \wedge (q \vee (\neg r)))$$



- ▶ Principal connective: the root
- ▶ Subformula: subtree

Balanced-Parentheses



Proposition (Balanced-Parentheses)

The number of left and right parentheses in a formula are equal.

Lemma

Any proper prefix of a formula contains an excess of left parentheses.

Thus a proper prefix of a formula is not a formula.

Proof.

Consider $A = (C \wedge D)$. The proper prefix of $(C \wedge D)$:

1. ([inductive hypothesis]
2. $(C_0$ [balanced-parentheses]
3. $(C$ [balanced-parentheses]
4. $(C \wedge$ [balanced-parentheses]
5. $(C \wedge D_0$ [inductive hypothesis]
6. $(C \wedge D$ [balanced-parentheses]

Unique Readability

Theorem (Unique Readability Theorem)

The five formula-building operations, when restricted to the set of wffs,

1. *have ranges that are disjoint from each other and from the set of proposition symbols, and*
2. *are injective.*

Proof.

$$(A \star B) = (C * D)$$



$$A \star B) = C * D)$$



$$A = C$$

(Lemma)



$$\star = *$$



$$B = D$$

(Lemma)

Omitting Parentheses

1. The outermost parentheses need not be explicitly mentioned.
2. We order the boolean connectives according to decreasing binding strength: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
3. Where one connective symbol is used repeatedly, grouping is to the right.

$$1 + 2 * 3$$

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Truth Assignment

- A truth assignment for \mathcal{L}^0 is a function

$$\nu : \text{Var} \rightarrow \{0, 1\}$$

- Such a truth assignment can be uniquely extended to $\bar{\nu} : \text{Wff} \rightarrow \{0, 1\}$ satisfying the following condition³:

1. $\bar{\nu}(p) = \nu(p)$ for $p \in \text{Var}$

2. $\bar{\nu}(\neg A) = 1 - \bar{\nu}(A)$

3. $\bar{\nu}(A \wedge B) = \min\{\bar{\nu}(A), \bar{\nu}(B)\}$

4. $\bar{\nu}(A \vee B) = \max\{\bar{\nu}(A), \bar{\nu}(B)\}$

5. $\bar{\nu}(A \rightarrow B) = \max\{1 - \bar{\nu}(A), \bar{\nu}(B)\}$

6. $\bar{\nu}(A \leftrightarrow B) = 1 - |\bar{\nu}(A) - \bar{\nu}(B)|$

p	$\neg p$
0	1
1	0

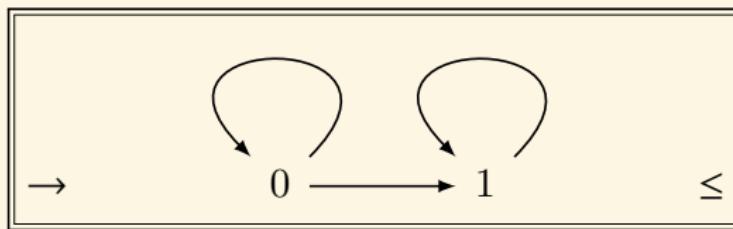
\wedge	0	1	\vee	0	1
0	0	0	0	0	1
1	0	1	1	1	1

\rightarrow	0	1	\leftrightarrow	0	1
0	1	1	0	1	0
1	0	1	1	0	1

³Some authors use $\llbracket \rrbracket_\nu$ for $\bar{\nu}$.

Truth Table & Truth/Boolean Function

p	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	1	0	0	1	1
1	0	0	1	1	0
1	1	1	1	1	1



Example

- If $0 = 1$, then Russell is God.
- Snow is white iff $1 + 1 = 2$.

Freeness vs Unique Readability

Definition

The set C is **freely generated** from B by a class of functions \mathcal{F} iff in addition to the requirements for being generated, the following conditions hold:

1. for every $f \in \mathcal{F}$: $f|_C$ is injective.
2. the range of $f|_C$ for all $f \in \mathcal{F}$, and the set B are pairwise disjoint.

Recursion Theorem



Theorem (Recursion Theorem)

Assume that C is freely generated from B by \mathcal{F} , and for every n -ary $f \in \mathcal{F}$ we have $F_f : V^n \rightarrow V$. Then for every function $h : B \rightarrow V$, there exists a unique function $\bar{h} : C \rightarrow V$ such that

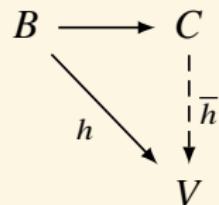
1. $\bar{h}|_B = h$
2. for all $f \in \mathcal{F}$ and all $x_1, \dots, x_n \in C$:

$$\bar{h}(f(x_1, \dots, x_n)) = F_f(\bar{h}(x_1), \dots, \bar{h}(x_n))$$

Remark:

- h tells you how to color the initial elements in B ;
- F_f tells you how to convert the color of x into the color of $f(x)$.

Danger! F_f is saying “green” but F_g is saying “red” for the same point.



Material Implication vs Cognition

Which cards must be turned over to test the idea that if a card shows an even number on one face, then its opposite face is red?



No drinking under 18!

Semantic Entailment & Validity

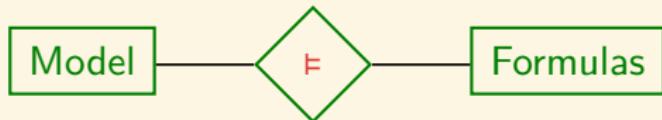
If lily is beautiful, then the fact that 2 is a prime number implies lily is beautiful.

p	q	$q \rightarrow p$	$p \rightarrow q \rightarrow p$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

There are 2^n truth assignments for a set of n propositional symbols.

- **Satisfiability:** A is *satisfiable* iff there is some truth assignment ν s.t. $\nu \models A$.
- **Semantic Entailment:** $\Gamma \models A$ iff for any truth assignment ν s.t. $(\text{for all } B \in \Gamma : \nu \models B) \implies \nu \models A$.
- **Validity / Tautology:** A is valid $\models A$ iff $\emptyset \models A$.
- **Logical Equivalence:** A and B are logically equivalent $A \equiv B$ iff for any truth assignment ν , $\nu \models A \iff \nu \models B$.

semantic entailment	validity	satisfiability	equivalence
$A \models B$	$\models A \rightarrow B$	$A \wedge \neg B$ unsatisfiable	$A \rightarrow B \equiv \top$
$\top \models A$	$\models A$	$\neg A$ unsatisfiable	$A \equiv \top$
$A \not\models \perp$	$\not\models \neg A$	A satisfiable	$\neg A \not\models \top$
$A \models B$ and $B \models A$	$\models A \leftrightarrow B$	$A \leftrightarrow \neg B$ unsatisfiable	$A \equiv B$



- ▶ **Satisfiability:** A is *satisfiable* iff there is some truth assignment ν s.t. $\nu \models A$.
- ▶ **Semantic Entailment:** $\Gamma \models A$ iff for any truth assignment ν s.t. $(\text{for all } B \in \Gamma : \nu \models B) \implies \nu \models A$.
- ▶ **Validity / Tautology:** A is valid $\models A$ iff $\emptyset \models A$.
- ▶ **Logical Equivalence:** A and B are logically equivalent $A \equiv B$ iff for any truth assignment ν , $\nu \models A \iff \nu \models B$.

Truth Assignment — set-based version

A truth assignment for \mathcal{L}^0 is a function

$$\nu : \text{Var} \rightarrow \{0, 1\}$$

- ▶ $\llbracket p \rrbracket := \{\nu : \nu(p) = 1\}$
- ▶ $\llbracket \top \rrbracket := \{0, 1\}^{\text{Var}}$
- ▶ $\llbracket \perp \rrbracket := \emptyset$
- ▶ $\llbracket \neg A \rrbracket := \{0, 1\}^{\text{Var}} \setminus \llbracket A \rrbracket$
- ▶ $\llbracket A \wedge B \rrbracket := \llbracket A \rrbracket \cap \llbracket B \rrbracket$
- ▶ $\llbracket A \vee B \rrbracket := \llbracket A \rrbracket \cup \llbracket B \rrbracket$
- ▶ $\llbracket A \rightarrow B \rrbracket := (\{0, 1\}^{\text{Var}} \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket$

$$A \models B \iff \llbracket A \rrbracket \subset \llbracket B \rrbracket$$

Valid Argument

An argument is **valid** if the set of premises semantically entails the conclusion $A_1, \dots, A_n \models B$.

$$\frac{A_1, \dots, A_n}{B}$$

- If all the premises A_1, \dots, A_n are true, so is the conclusion B .
- If the conclusion B is false, at least one premise A_i is false.

Example:

An integer x is even or odd.

If x is even, then $x + x$ is even.

If x is odd, then $x + x$ is even.

Therefore, $x + x$ is even.

$$\frac{p \vee q \\ p \rightarrow r \\ q \rightarrow r}{r}$$



$$p \vee q, p \rightarrow r, q \rightarrow r \models r$$

兴，百姓苦；亡，百姓苦。

Valid Argument — Example ☺

Kline is a professor. Therefore, either Kline is a professor or a serial killer.

$$\frac{p}{p \vee q}$$

Linda is 31 years old, single, outspoken, and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in antinuclear demonstrations.

1. Linda is a bank teller.
2. Linda is a bank teller and is active in the feminist movement.

$$\frac{p \wedge q}{p}$$

Logical Form — Ignore Irrelevant Details!

Problem (How old is my father?)

My father is twice as old as me but ten years ago he was three times as old as me.

Problem (How many apples are there?)

This bag has twice as many apples as that one but if I take ten out of each then this one has three times as many as that one.

$$x = 2y$$

$$x - 10 = 3(y - 10)$$

Remark: Abstraction — forget as many details as possible while still retaining the truth of what you are trying to study.

Logical Form

Given a logical form, a proposition is an instance of this form if it can be obtained from the form by replacing the variables in the form with propositions, according to the rule: **all occurrences of the same variable must be replaced by the same proposition.**

$$p \rightarrow p \vee q$$

$$\heartsuit \rightarrow \heartsuit \vee \text{bike}$$



$$A \rightarrow A \vee B$$

$$A \rightarrow A \vee A$$

$$A \rightarrow A \vee (A \rightarrow B)$$

$$(A \wedge B) \rightarrow (A \wedge B) \vee (A \rightarrow B)$$

Validity / Tautology — Example

$$\models (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r$$

p	q	r	$q \rightarrow r$	$p \rightarrow q \rightarrow r$	$p \rightarrow q$	$p \rightarrow r$	$(p \rightarrow q) \rightarrow p \rightarrow r$	$(p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r$
0	0	0						1
0	0	1						1
0	1	0						1
0	1	1						1
1	0	0						1
1	0	1						1
1	1	0						1
1	1	1						1

Truth Table — Simplification for Tautology

$$(p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r$$

			0								
1			0			0			0		
1	1	0	0	1	1	0	1	0	0	0	0
1	1	0	0	1	1	1	0	1	0	0	0
1	1	1	1	0	0	1	1	1	0	1	0
			×								

Translation Tactics ❤

- ▶ **Negation:** not / it is false that ...
 - ▶ Jay and Kay are married, but not to each other. $J \wedge K \wedge \neg M$
- ▶ **Conjunction:** and / moreover / furthermore / but / yet / although / though / even though / however / whereas
- ▶ **Disjunction:** or / either or / unless
- ▶ **Implies:** "if then" / provided that / in case / on the condition that
- ▶ **Neither Nor:** negation of "either or"
- ▶ **Only If:** "in order that ... it is necessary that ..."
- ▶ **Even If:**
 - ▶ I'm going to the party even if it rains. $p \wedge (q \rightarrow p) \equiv p$
 - ▶ The Allies would have won even if the U.S. had not entered the war.
 $p \wedge (\neg q \rightarrow p) \equiv p$
 - ▶ The Axis powers would have won if the U.S. had not entered the war.
 $\neg p \wedge (\neg q \rightarrow p)$
- ▶ **Unless:** if not / if and only if not
 1. I will not graduate unless I pass logic. $\neg \text{PassLogic} \rightarrow \neg \text{Graduate}$
 2. The store is open unless/except it is sunday. $\text{Open} \leftrightarrow \neg \text{Sunday}$

Example 😞

1. The programmer's wife tells him: "Run to the store and pick up a loaf of bread. If they have eggs, get a dozen."
2. The programmer comes home with 12 loaves of bread.
3. "Why did you buy 12 loaves of bread!?", his wife screamed.
4. "Because they had eggs!"

► wife.

$$q \wedge (p \rightarrow r)$$

► programmer.

$$(\neg p \rightarrow q) \wedge (p \rightarrow s)$$

Exercises — Translation — Now it's your turn ❤

1. I am **not** good at logic.
2. Either Jones is a fool **or** he is dishonest.
3. If you **can't** say it clearly, you **don't** understand it yourself. — Searle
4. You understand something **only if** you can formalize it.
5. A science becomes developed **only when** it can make use of mathematics. — Marx
6. If you work hard **only if** you are threatened, then you will not succeed.
7. Even though the dark clouds veil the sky, You are by my side.
8. You will pass **unless** you goof off, **provided that** you are intelligent.
9. If Jones will work **only if** Smith is fired, then we should fire Smith if we want the job finished.
10. In **order to** put on the show it will be **necessary** to find a substitute, if **neither** the leading lady **nor** her understudy recovers from the flu.

Exercises — Translation — Now it's your turn ❤

11. If you make an appointment and do not keep it, then I shall be angry unless you have a good excuse.
12. Getting a 100 on the exam is necessary but not sufficient for getting an A.
13. I'll play tennis unless it is raining, in which case I'll play pingpong.
14. If it is sunny and not cold, I'll play tennis; otherwise, I'll play pingpong or go swimming.
15. I will go out unless it rains.
16. You can pay by credit card or cheque, but not both.
17. Neither Sarah nor Peter was to blame for the mistake.
18. I want to buy either a new desktop computer or a laptop, but I have neither the cash nor the credit I need.

Translation — Natural language is not always precise!

1. If I get in the lift then it breaks, and if you get in then the lift breaks.
(?)
2. If we both get in the lift, then the lift breaks.(?)

$$\frac{p \vee q \rightarrow r}{(p \rightarrow r) \wedge (q \rightarrow r)}$$

$$\frac{p \wedge q \rightarrow r}{(p \rightarrow r) \vee (q \rightarrow r)}$$

- I weigh 100 pounds.
- You weigh 100 pounds.
- The maximum capacity of the lift is 150 pounds.

Translation

Philosophy is written in that great book — the universe — which ever is before our eyes, but it can't be understood unless one first learns to comprehend the mathematical language, without which one wanders in vain through a dark labyrinth.

— Galileo Galilei

$$P \wedge E \wedge (\neg C \rightarrow \neg U) \wedge (\neg C \rightarrow W)$$



Figure: Leaning Tower of Pisa

Exercises — Validity — Now it's your turn ❤

$$1. p \vee q \equiv \neg p \rightarrow q \equiv (p \rightarrow q) \rightarrow q$$

$$2. p \wedge q \equiv \neg(p \rightarrow \neg q)$$

$$3. p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

$$4. p \wedge q \equiv \neg(\neg p \vee \neg q)$$

$$5. p \rightarrow q \rightarrow r \equiv (p \wedge q) \rightarrow r$$

$$6. p \rightarrow q \equiv \neg q \rightarrow \neg p$$

$$7. p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

$$8. p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

$$9. \neg(p \vee q) \equiv \neg p \wedge \neg q$$

$$10. \neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$11. p \equiv p \vee (p \wedge q)$$

$$12. p \equiv p \wedge (p \vee q)$$

$$1. \neg\neg p \rightarrow p$$

$$2. p \rightarrow \neg\neg p$$

$$3. p \vee \neg p$$

$$4. \neg(p \wedge \neg p)$$

$$5. p \wedge \neg p \rightarrow q$$

$$6. (p \rightarrow q) \wedge (\neg p \rightarrow q) \rightarrow q$$

$$7. (p \rightarrow q) \wedge (p \rightarrow \neg q) \rightarrow \neg p$$

$$8. (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \rightarrow p$$

$$9. ((p \rightarrow q) \rightarrow p) \rightarrow p$$

$$1. \Gamma, A \models B \iff \Gamma \models A \rightarrow B$$

$$2. A \equiv B \iff \models A \leftrightarrow B$$

$$3. A \vee B, \neg A \vee C \models B \vee C$$

Invalid Argument

$$\frac{p \rightarrow q}{\frac{q}{p}}$$

$$\frac{p \rightarrow q}{\frac{\neg p}{\neg q}}$$

$$\frac{p \vee q}{\frac{p}{\neg q}}$$

I think, therefore I am
I do not think
—————
Therefore I am not

Mickey is murdered by Tom or Jerry
Tom is the killer
—————
Jerry is innocent

- ▶ 家里有一头猪和一头驴，你说我是杀猪呢，还是杀驴呢？
- ▶ 杀驴。
- ▶ 猪也是这么想的。

By all means marry; if you get a good wife, you'll be happy. If you get a bad one, you'll become a philosopher. — Socrates

梁实秋 vs 鲁迅

说我是资本家的走狗，是哪一个资本家，还是所有的资本家？我还不知道我的主子是谁。

— 梁实秋《资本家的走狗》

凡走狗，虽或为一个资本家所豢养，其实是属于所有的资本家的，所以它遇见所有的阔人都驯良，遇见所有的穷人都狂吠。不知道谁是它的主子，正是它遇见所有阔人都驯良的原因，也就是属于所有的资本家的证据。

即使无人豢养，饿的精瘦，变成野狗了，但还是遇见所有的阔人都驯良，遇见所有的穷人都狂吠的，不过这时它就愈不明白谁是主子了。

— 鲁迅《丧家的资本家的乏走狗》

主子豢养 → 是走狗
无主子豢养 → 不是走狗 ×

两小儿辩日

《列子·汤问》

孔子东游，见两小儿辩斗，问其故。

- ▶ 一儿曰：“我以日始出时去人近，而日中时远也。”
- ▶ 一儿曰：“我以日初出远，而日中时近也。”
- ▶ 一儿曰：“日初出大如车盖，及日中则如盘盂，此不为远者小而近者大乎？”
- ▶ 一儿曰：“日初出沧沧凉凉，及其日中如探汤，此不为近者热而远者凉乎？”
- ▶ 孔子不能决也。
- ▶ 两小儿笑曰：“孰为汝多知乎？”

日出 → 大， 日中 → 小
大者 → 近， 小者 → 远

日出 → 近， 日中 → 远

日出 → 凉， 日中 → 热
凉者 → 远， 热者 → 近

日出 → 远， 日中 → 近

Example

明·浮白斋主人《雅谑》

叶衡罢相归，一日病，问诸客曰：“我且死，但未知死后佳否？”一士曰：“甚佳”。叶惊问曰：“何以知之？”答曰：“使死而不佳，死者皆逃回矣。一死不返，以是知其佳也。”

好货不贱，贱货不好。

痞子蔡《第一次的亲密接触》

1. 如果把整个太平洋的水倒出，也浇不灭我爱你爱情的火焰。整个太平洋的水倒得出吗？不行。所以，我不爱你。
2. 如果把整个浴缸的水倒出，也浇不灭我爱你爱情的火焰。整个浴缸的水倒得出吗？可以。所以，是的，我爱你。

Example

- ▶ 如果你工作，就能挣钱；如果你赋闲在家，就能悠然自在。你要么工作要么赋闲，总之，你能挣钱或者能悠然自在。
- ▶ 如果你工作，就不能悠然自在；如果你赋闲在家，就不能挣钱。你要么工作要么赋闲，总之，你不能悠然自在或者不能挣钱。

$$\frac{p \rightarrow r \\ q \rightarrow s}{p \vee q \rightarrow r \vee s} \qquad \frac{p \rightarrow \neg s \\ q \rightarrow \neg r}{p \vee q \rightarrow \neg s \vee \neg r}$$

- ▶ 老婆婆有俩儿子，老大卖阳伞，老二卖雨伞，晴天雨伞不好卖，雨天阳伞不好卖.....
- ▶ 被困失火的高楼，走楼梯会被烧死，跳窗会摔死.....

蒋介石

反腐，亡党；不反，亡国。

¬ 上帝万能

上帝能否创造一块自己举不起来的石头？

Example

诉讼悖论

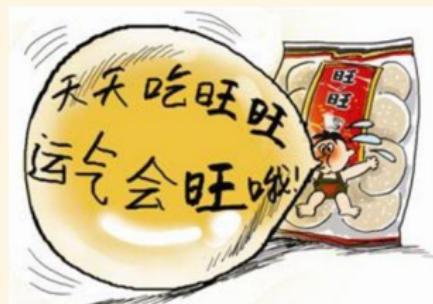
- ▶ 曾有师生签订合同：上学期间不收费，学生毕业打赢第一场官司后交学费。
- ▶ 可学生毕业后并未从事律师职业，于是老师威胁起诉学生。
- ▶ 老师说：如果我赢了，根据法庭判决，你必须交学费；如果你赢了，根据合同，你也必须交学费。要么我赢要么你赢，你都必须交学费。
- ▶ 学生说：如果我赢了，根据法庭判决，我不用交学费；如果你赢了，根据合同，我不用交学费。要么我赢要么你赢，我都不用交学费。

$$w \rightarrow p, \neg w \rightarrow p, w \vee \neg w \models p$$

$$w \wedge j \rightarrow p, \neg w \wedge c \rightarrow p, w \vee \neg w \stackrel{?}{\models} p$$

$$\neg w \wedge j \rightarrow \neg p, w \wedge c \rightarrow \neg p, w \vee \neg w \stackrel{?}{\models} \neg p$$

$$w \wedge j \rightarrow p, \neg w \wedge c \rightarrow p, (w \wedge j) \vee (\neg w \wedge c) \models p$$



The Crocodile Dilemma

The Crocodile Dilemma

I will return your child iff you can correctly predict what I will do next.

$$x =? \implies \models (x \leftrightarrow r) \rightarrow r$$

r	$(\neg r \leftrightarrow r) \rightarrow r$
0	1
1	1

$$((r \vee \neg r) \leftrightarrow r) \rightarrow r$$

怎么得大奖?

Problem (怎么得大奖?)

- ▶ 说真话得一个大奖或一个小奖。
- ▶ 说假话不得奖。
- ▶ b : 我会得大奖。
- ▶ s : 我会得小奖。

$$x =? \implies \models (\neg b \wedge \neg s \leftrightarrow b \vee s) \rightarrow b$$

b	s	$(\neg b \wedge \neg s \leftrightarrow b \vee s) \rightarrow b$	$(\neg s \leftrightarrow b \vee s) \rightarrow b$	$((s \rightarrow b) \leftrightarrow b \vee s) \rightarrow b$
0	0	1	1	1
0	1	1	1	1
1	0	1	1	1
1	1	1	1	1

Gateway to Heaven

Problem (天堂之路)

- ▶ 你面前有左右两人守卫左右两门。
- ▶ 一人只说真话，一人只说假话。
- ▶ 一门通天堂，一门通地狱。
- ▶ 你只能向其中一人提一个“是/否”的问题。
- ▶ 怎么问出去天堂的路？

$$x = ? \implies \models (p \rightarrow (x \leftrightarrow q)) \wedge (\neg p \rightarrow (x \leftrightarrow \neg q))$$

- ▶ p: 你说真话。
- ▶ q: 左门通天堂。

p	q	$(p \wedge q) \vee (\neg p \wedge \neg q)$	report	A
0	0	1	0	1
0	1	0	1	1
1	0	0	0	1
1	1	1	1	1

Valid Argument & Proof Methods

1. Direct Proof:

$$\frac{A \rightarrow B}{\frac{A}{B}}$$

Example: If n is an odd integer, then n^2 is odd.

2. Backward Reasoning: to prove B , find A and $A \rightarrow B$.

Example: If x and y are non-negative real numbers, then

$$\frac{x+y}{2} \geq \sqrt{xy}$$

3. Proof by Contraposition:

$$\frac{A \rightarrow B}{\neg B \rightarrow \neg A}$$

Example: If n is an integer and $3n + 2$ is odd, then n is odd.

Valid Argument & Proof Methods

4. Proof by Cases:

$$\frac{A \vee B \rightarrow C}{(A \rightarrow C) \wedge (B \rightarrow C)}$$

Example: If n is an integer, then $n(n + 1)$ is even.

5. Proof by Elimination:

$$\frac{A \rightarrow B \vee C}{A \wedge \neg B \rightarrow C}$$

Example: If $a + bi$ and $c + di$ are complex numbers for which $(a + bi)(c + di) = 1$, then $a \neq 0$ or $b \neq 0$.

Valid Argument & Proof Methods

6. Proof by Contradiction:

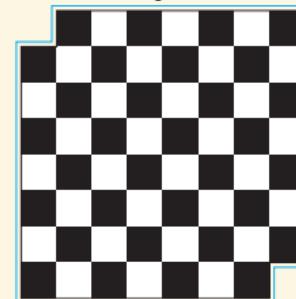
$$\frac{\neg A \rightarrow B \\ \neg A \rightarrow \neg B}{A}$$

Example: $\sqrt{2}$ is irrational.

7. Reductio Ad Absurdum:

$$\frac{A \rightarrow B \\ A \rightarrow \neg B}{\neg A}$$

Example: The following board cannot be tiled by the dominos.



Logical Equivalence

- ▶ Logical equivalence is an equivalence relation between formulas.
 1. reflexive
 2. symmetric
 3. transitive
- ▶ Logical equivalence is compatible with operators.

$$\frac{A \equiv A'}{\neg A \equiv \neg A'}$$

$$\frac{\begin{array}{c} A \equiv A' \\ B \equiv B' \end{array}}{A \star B \equiv A' \star B'}$$

where $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

- ▶ Equivalence relation + Compatible with Operators = Congruence relation

Substitution

$$p_i[C/p] := \begin{cases} C & \text{if } p_i = p \\ p_i & \text{otherwise} \end{cases}$$

$$(\neg A)[C/p] := \neg A[C/p]$$

$$(A \rightarrow B)[C/p] := A[C/p] \rightarrow B[C/p]$$

Theorem (Substitution Theorem)

$$\frac{B \leftrightarrow C}{A[B/p] \leftrightarrow A[C/p]}$$

Proof.

- $A = p_i$
- $A = \neg A_1$
- $A = A_1 \rightarrow A_2$

Substitution

$$p[C_1/p_1, \dots, C_n/p_n] := \begin{cases} C_i & \text{if } p = p_i \text{ for some } 1 \leq i \leq n \\ p & \text{otherwise} \end{cases}$$

$$(\neg A)[C_1/p_1, \dots, C_n/p_n] := \neg A[C_1/p_1, \dots, C_n/p_n]$$

$$(A \rightarrow B)[C_1/p_1, \dots, C_n/p_n] := A[C_1/p_1, \dots, C_n/p_n] \rightarrow B[C_1/p_1, \dots, C_n/p_n]$$

Theorem

Consider a wff A and a sequence C_1, \dots, C_n of wffs.

1. Let ν be a truth assignment for the set of all propositional symbols. Define μ to be the truth assignment for which $\mu(p_i) = \nu(C_i)$. Then $\mu(A) = \nu(A[C_1/p_1, \dots, C_n/p_n])$.
2. $\models A \implies \models A[C_1/p_1, \dots, C_n/p_n]$

Example

$$\models p \vee \neg p \implies \models (p \wedge \neg p) \vee \neg(p \wedge \neg p)$$

Equivalent Replacement

Theorem

Suppose $B \in \text{Sub}(A)$, and $A(C//B)$ arises from the wff A by replacing one or more occurrences of B in A by C . Then

$$\frac{B \leftrightarrow C}{A \leftrightarrow A(C//B)}$$

Proof.

Prove by induction.

Example ☺

1. A logician's wife is having a baby.
2. The doctor immediately hands the newborn to the dad.
3. His wife asks impatiently: "So, is it a boy or a girl"?
4. The logician replies: "yes".

► wife.

$p?$

► logician.

$$\frac{p \vee q \\ q \leftrightarrow \neg p}{p \vee \neg p} \quad \checkmark$$

Duality

Theorem

Let A be a wff whose only connectives are \neg, \wedge, \vee . Let A^* be the result of interchanging \wedge and \vee and replacing each propositional symbol by its negation. Then $\neg A \equiv A^*$.

Proof.

Prove by induction.

- $A = p_i$
- $A = \neg B$
- $A = B \wedge C$
- $A = B \vee C$

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

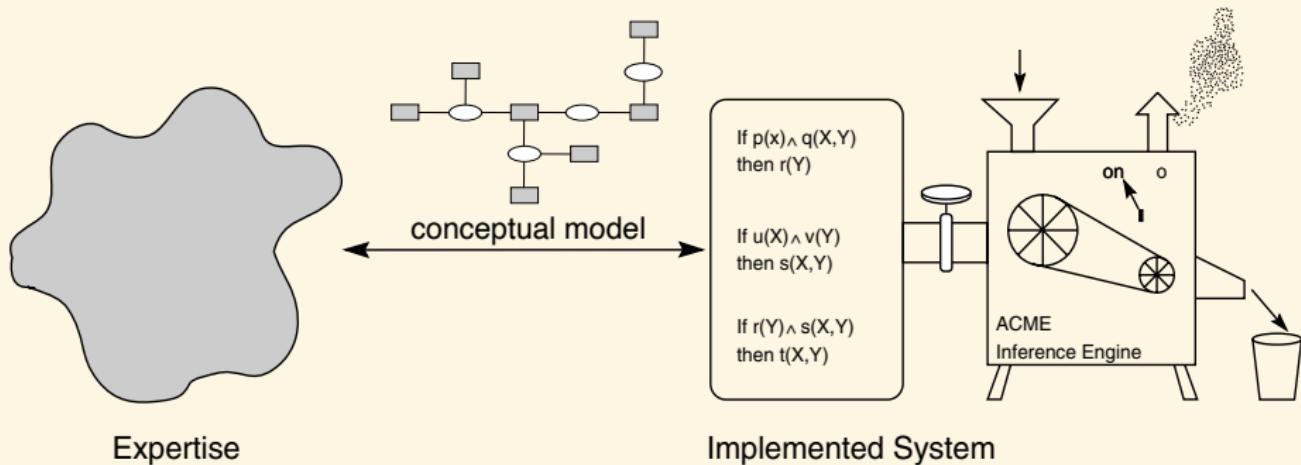
Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Formal Systems

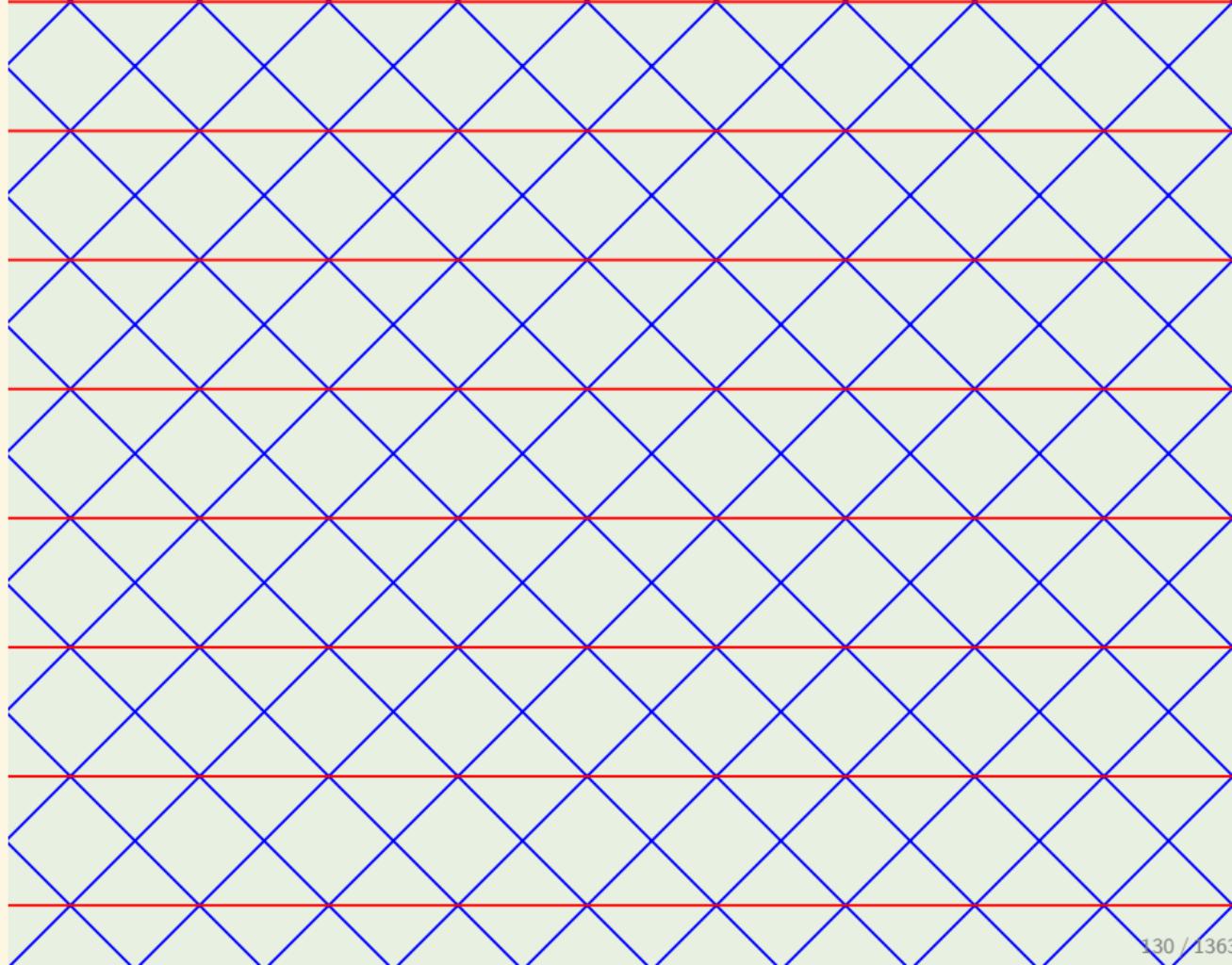


- ▶ Hilbert System
- ▶ Tree Method
- ▶ Natural Deduction
- ▶ Sequent Calculus
- ▶ Resolution
- ▶ ...

Why Study Formal System?

Why truth tables are not sufficient?

- ▶ Exponential size
 - ▶ How many **times** would you have to fold a piece of paper(0.1mm) onto itself to reach the Moon?
 - ▶ **Common Ancestors of All Humans**
 - (1) Someone alive 1000BC is an ancestor of everyone alive today;
 - (2) Everyone alive 2000BC is either an ancestor of nobody alive today or of everyone alive today;
 - (3) Most of the people you are descended from are no more genetically related to you than strangers are.
 - (4) Even if everyone alive today had exactly the same set of ancestors from 2000BC , the distribution of one's ancestors from that population could be very different.
- ▶ Inapplicability beyond Boolean connectives.



Hilbert Formal System = Axiom + Inference Rule

- ▶ which sentences are true?
- ▶ can I split them into axioms, which are evidently true, and
- ▶ a few simple inference rules, that preserve truth?

Axiom Schema

1. $A \rightarrow B \rightarrow A$
2. $(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
3. $(\neg A \rightarrow \neg B) \rightarrow (\neg A \rightarrow B) \rightarrow A$

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} [\text{MP}]$$

Lewis Carroll's Paradox: What the Tortoise Said to Achilles 😞

- A Things that are equal to the same are equal to each other.
- B The two sides of this Triangle are things that are equal to the same.
- C If A and B are true, Z must be true.
- D If A and B and C are true, Z must be true.
- ⋮
- ⋮
- ⋮
- Z The two sides of this Triangle are equal to each other.

Deduction / Proof

This sentence can never be proved.

What is “proof”?

Definition (Deduction)

A deduction from Γ is a sequence of wff (C_1, \dots, C_n) s.t. for $k \leq n$, either

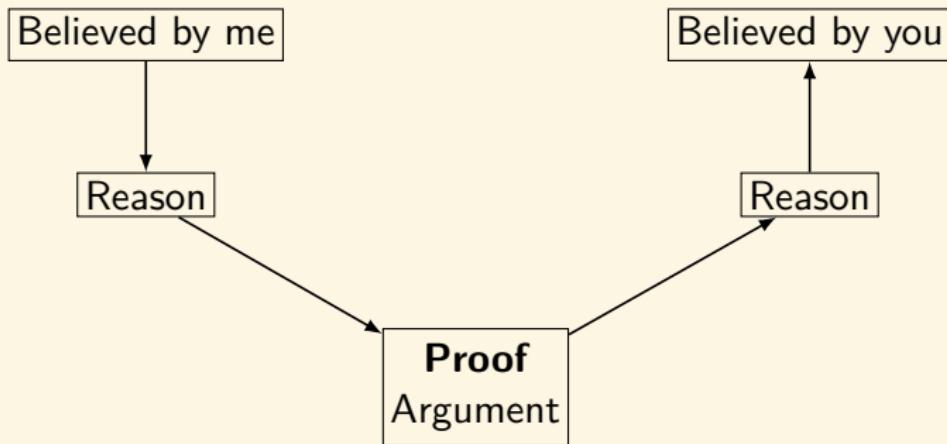
1. C_k is an axiom, or
2. $C_k \in \Gamma$, or
3. for some $i < k$ and $j < k$, $C_i = C_j \rightarrow C_k$.

- ▶ $\Gamma \vdash A$ iff A is the last member of some deduction from Γ .
- ▶ A is a theorem $\vdash A$ iff $\emptyset \vdash A$.

A Joke

A mathematician's house is on fire. His wife puts it out with a bucket of water. Then there is a gas leak. The mathematician lights it on fire.

Proof vs Belief / Knowledge / Understanding



Remark: Proof is the medium for communicating my argument to you in a way that will not be in danger of ambiguity, misunderstanding, or distortion.

Example

Theorem

$$\vdash p \rightarrow p$$

Proof.

1. $p \rightarrow (p \rightarrow p) \rightarrow p$ A1
2. $(p \rightarrow (p \rightarrow p) \rightarrow p) \rightarrow (p \rightarrow p \rightarrow p) \rightarrow p \rightarrow p$ A2
3. $(p \rightarrow p \rightarrow p) \rightarrow p \rightarrow p$ 1,2 MP
4. $p \rightarrow p \rightarrow p$ A1
5. $p \rightarrow p$ 3,4 MP

Remark: Logic is like love; a simple idea, but it can get complicated.

- 这 TM 也用证?
- 这 TM 也能证?

Example

Theorem

$$\vdash (\neg p \rightarrow p) \rightarrow p$$

Proof.

1. $(\neg p \rightarrow \neg p) \rightarrow (\neg p \rightarrow p) \rightarrow p$ A3
2. $\neg p \rightarrow \neg p$
3. $(\neg p \rightarrow p) \rightarrow p$ 1,2 MP

Example

Theorem

$$p \rightarrow q, q \rightarrow r \vdash p \rightarrow r$$

Proof.

1. $(q \rightarrow r) \rightarrow (p \rightarrow q \rightarrow r)$ A1
2. $q \rightarrow r$ Premise
3. $p \rightarrow q \rightarrow r$ 1,2 MP
4. $(p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r$ A2
5. $(p \rightarrow q) \rightarrow p \rightarrow r$ 4,3 MP
6. $p \rightarrow q$ Premise
7. $p \rightarrow r$ 5,6 MP

Example — Curry's Paradox 😐

If this sentence is true, then God exists.

$$p \leftrightarrow (p \rightarrow q) \vdash q$$

Proof.

1. $p \leftrightarrow (p \rightarrow q)$
2. $p \rightarrow p \rightarrow q$
3. $(p \rightarrow p) \rightarrow p \rightarrow q$
4. $p \rightarrow q$
5. p
6. q

1. 甲：如果我没说错，那么上帝存在。
2. 乙：**如果你没说错，那么上帝存在。**
3. 甲：你承认我没说错了？
4. 乙：当然。
5. 甲：可见我没说错。你已经承认：**如果我没说错，那么上帝存在。** 所以，上帝存在。

This sentence is false, and God does not exist.

Curry's Paradox — How to Flirt with a Beauty 😊

Smullyan

Flirts with a Beauty ❤️😊

1. "I am to make a statement. If it is true, would you give me your autograph?"
2. "I don't see why not."
3. "If it is false, do not give me your autograph."
4. "Alright."
5. Then Smullyan said such a sentence that she have to give him a kiss.

$$x =? \implies \models (a \leftrightarrow x) \rightarrow k$$

Hi 美女，问你个问题呗

如果我问你“你能做我女朋友吗”，那么你的答案能否和这个问题本身的答案一样？

Boolean Algebra



\perp	\top	\vee	\wedge	\neg
0	1	+	\cdot	$\bar{}$

- $x + (y + z) = (x + y) + z$
 $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x + y = y + x$ $x \cdot y = y \cdot x$
- $x + (x \cdot y) = x$ $x \cdot (x + y) = x$
- $x + (y \cdot z) = (x + y) \cdot (x + z)$
 $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $\bar{\bar{x}} = x$
- $\overline{x + y} = \bar{x} \cdot \bar{y}$ $\overline{x \cdot y} = \bar{x} + \bar{y}$
- $x + \bar{x} = 1$ $x \cdot \bar{x} = 0$ $0 \neq 1$
- $x + 0 = x$ $x \cdot 0 = 0$
 $x + 1 = 1$ $x \cdot 1 = x$

Theorem (General Solution of Boolean Equation)

If $f(0) \cdot f(1) = 0$, then

$$f(x) = 0 \implies x = f(0) + \theta \cdot \overline{f(1)}$$

where $\theta \in \{0, 1\}$.

Example: $x = ? \implies \models (a \leftrightarrow x) \rightarrow k$

$$(a \cdot x + \bar{a} \cdot \bar{x}) \cdot \bar{k} = 0$$

⇓

$$x = \bar{a} \cdot \bar{k} + \theta \cdot (\bar{a} + k)$$

$$x = \begin{cases} \neg a \wedge \neg k & \text{if } \theta = 0 \\ a \rightarrow k & \text{if } \theta = 1 \end{cases}$$

Deduction Theorem “ \vdash ” vs “ \rightarrow ”

Theorem (Deduction Theorem)

$$\Gamma, A \vdash B \implies \Gamma \vdash A \rightarrow B$$

Proof.

Prove by induction on the length of the deduction sequence (C_1, \dots, C_n) of B from $\Gamma \cup \{A\}$.

Base step $n = 1$:

case1. B is an axiom. (use Axiom1.)

case2. $B \in \Gamma$.

case3. $B = A$.

Inductive step $n > 1$:

case1. B is either an axiom, or $B \in \Gamma$, or $B = A$.

case2. $C_i = C_j \rightarrow B$

$$\Gamma, A \vdash C_j \implies \Gamma \vdash A \rightarrow C_j$$

$$\Gamma, A \vdash C_j \rightarrow B \implies \Gamma \vdash A \rightarrow C_j \rightarrow B$$

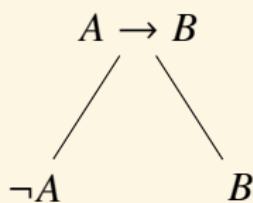
$$\Gamma \vdash A \rightarrow B$$

Tree Method for Propositional Logic ❤

$$\neg\neg A$$



$$A \rightarrow B$$



$$\neg(A \rightarrow B)$$



$$A$$



$$\neg B$$

$$A \wedge B$$



$$A$$



$$B$$

$$\neg(A \wedge B)$$



$$\neg A$$



$$\neg B$$

$$A \vee B$$



$$A$$



$$B$$

$$\neg(A \vee B)$$



$$\neg A$$



$$\neg B$$

$$A \leftrightarrow B$$



$$A$$



$$B$$

$$\neg A$$



$$\neg B$$

$$\neg(A \leftrightarrow B)$$



$$A$$



$$\neg B$$

$$\neg A$$



$$B$$

Instructions for Tree Construction

- ▶ A *literal* is an atomic formula or its negation.
- ▶ When a non-literal wff has been fully unpacked, check it with ✓
 1. Start with premises and the negation of the conclusion.
 2. Inspect each open path for an occurrence of a wff and its negation. If these occur, close the path with ✗.
 3. If there is no unchecked non-literal wff on any open path, then stop!
 4. Otherwise, unpack any unchecked non-literal wff on any open path.
 5. Goto ②.
- ▶ *Closed branch*. A branch is closed iff it contains a wff and its negation.
- ▶ *Closed tree*. A tree is closed iff all its branches are closed.
- ▶ *Open branch*. A branch is open iff it is not closed and no rule can be applied.
- ▶ *Open tree*. A tree is open iff it has at least one open branch.

Deduction & Proof Tactics

Definition (Deduction)

$A_1, \dots, A_n \vdash B$ iff there exists a *closed tree* from $\{A_1, \dots, A_n, \neg B\}$.

Proof Tactics

- ▶ Try to apply “non-branching” rules first, in order to reduce the number of branches.
- ▶ Try to close off branches as quickly as possible.

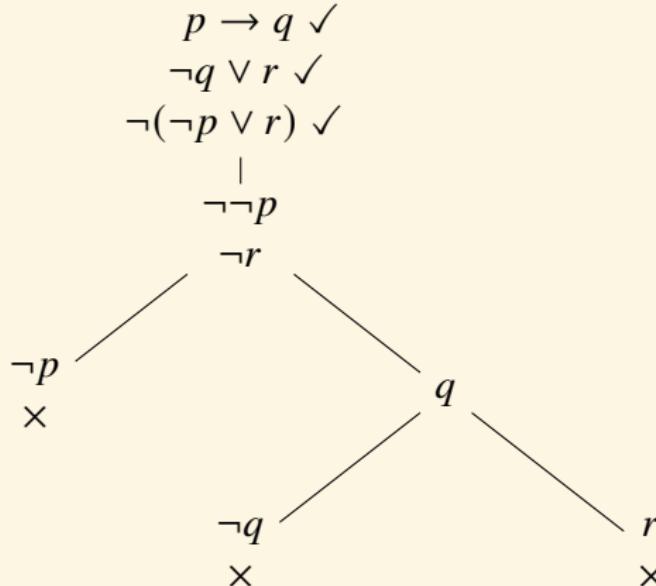
Theorem (Soundness & Completeness Theorem)

$$A_1, \dots, A_n \vdash B \iff A_1, \dots, A_n \vDash B$$

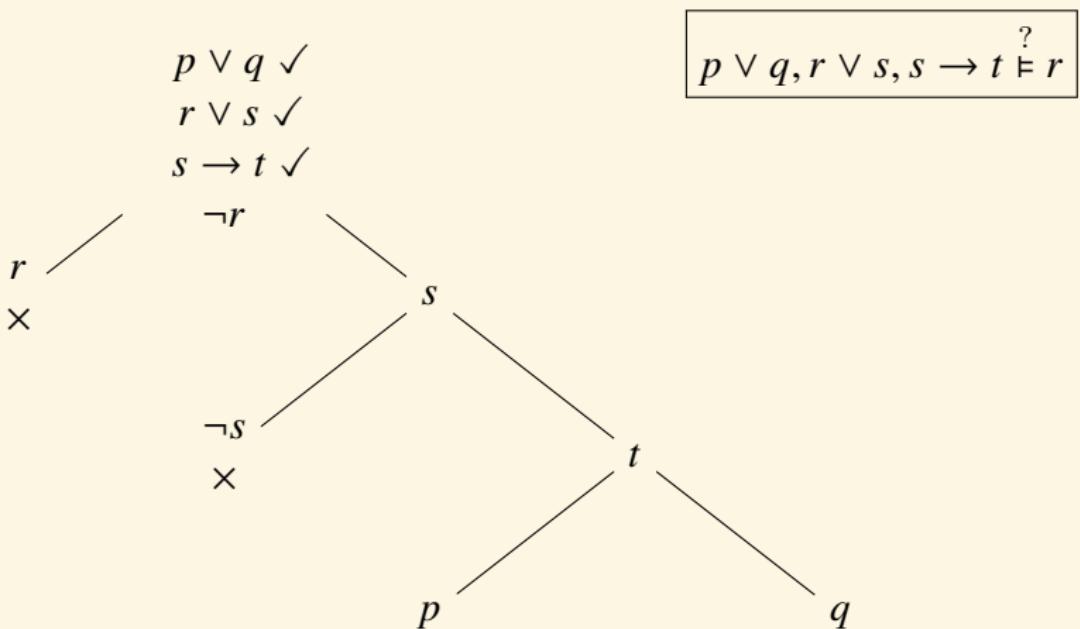
Remark: If an inference with propositional formulas is not valid, then its tree will have at least one open branch. The tree method can generate every counterexample of an invalid inference in propositional logic.

Examples — Tree Method

$$p \rightarrow q, \neg q \vee r \vdash \neg p \vee r$$



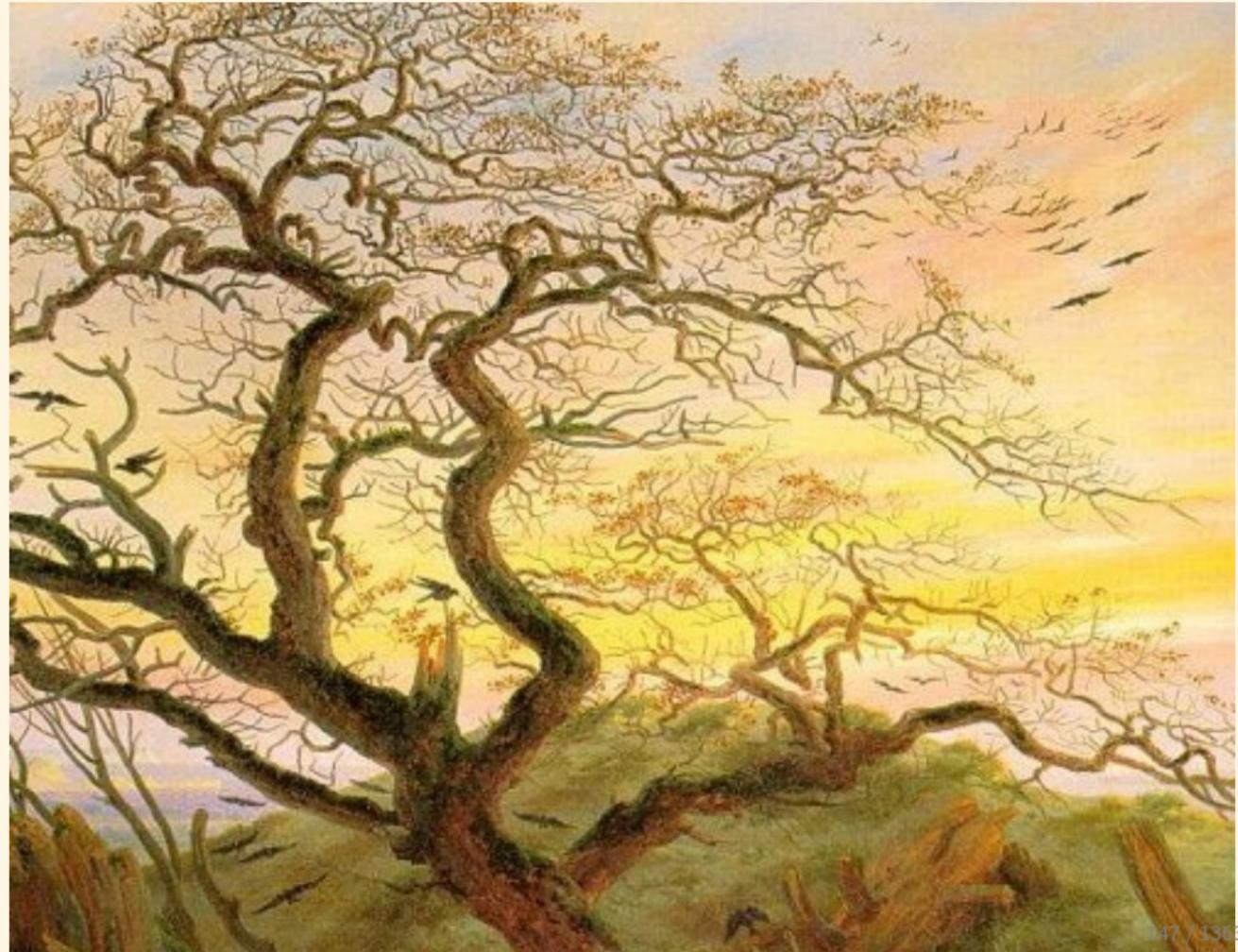
Open branches correspond to truth assignments



$$\nu(r) = 0, \quad \nu(s) = 1, \quad \nu(t) = 1 \quad \nu(p) = 1 \quad \nu(q) = 1 \text{ or } 0$$

$$\nu(r) = 0, \quad \nu(s) = 1, \quad \nu(t) = 1 \quad \nu(q) = 1 \quad \nu(p) = 1 \text{ or } 0$$

$$\nu \models p \vee q, \quad \nu \models r \vee s, \quad \nu \models s \rightarrow t, \quad \nu \not\models r$$





Don't just read it; fight it!

Ask your own questions,
look for your own examples,
discover your own proofs.
Is the hypothesis necessary?
Is the converse true?

What happens in the classical special case?
What about the degenerate cases?
Where does the proof use the hypothesis?

Exercises — Tree Method — Now it's your turn ♡

1. $p \rightarrow (\neg q \rightarrow q) \vdash p \rightarrow q$
2. $(p \rightarrow r) \wedge (q \rightarrow r) \vdash p \vee q \rightarrow r$
3. $(p \rightarrow q) \wedge (r \rightarrow s) \vdash \neg q \wedge r \rightarrow \neg q \wedge s$
4. $\left(((p \rightarrow q) \rightarrow (\neg r \rightarrow \neg s)) \rightarrow r \right) \rightarrow t \vdash (t \rightarrow p) \rightarrow s \rightarrow p$
5. $(p \rightarrow q) \vee (q \rightarrow r)$
6. $(p \rightarrow q) \rightarrow (\neg p \rightarrow q) \rightarrow q$
7. $((p \rightarrow q) \rightarrow p) \rightarrow p$
8. $(p \rightarrow q) \wedge (r \rightarrow s) \rightarrow p \vee r \rightarrow q \vee s$
9. $(p \rightarrow q) \wedge r \rightarrow \neg(p \wedge r) \vee (q \wedge r)$
10. $(p \leftrightarrow (p \rightarrow q)) \rightarrow q$
11. $\neg(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow q)$
12. $(p \leftrightarrow q) \leftrightarrow (p \vee q \rightarrow p \wedge q)$

Exercises — Tree Method — Now it's your turn ❤

Decide whether the following inferences are valid or not. If not, provide a counterexample.

1. $(p \vee q) \wedge r \stackrel{?}{\models} p \vee (q \wedge r)$
2. $p \vee (q \wedge r) \stackrel{?}{\models} (p \vee q) \wedge r$
3. $p \leftrightarrow (q \rightarrow r) \stackrel{?}{\models} (p \leftrightarrow q) \rightarrow r$
4. $(p \leftrightarrow q) \rightarrow r \stackrel{?}{\models} p \leftrightarrow (q \rightarrow r)$
5. $\neg(p \rightarrow q \wedge r), r \rightarrow p \wedge q \stackrel{?}{\models} \neg r$
6. $p \rightarrow (q \wedge r), \neg(p \vee q \rightarrow r) \stackrel{?}{\models} p$
7. $p \rightarrow q, r \rightarrow s, p \vee r, \neg(q \wedge s) \stackrel{?}{\models} (q \rightarrow p) \wedge (s \rightarrow r)$
8. If God does not exist, then it's not the case that *if I pray, my prayers will be answered*; and I don't pray; so God exists.
9. If you concentrate **only if** you are threatened, then you will not pass **unless** you are threatened — **provided that** concentrating is a necessary condition for passing.

Natural Deduction



$$\frac{A \quad B}{A \wedge B} [\wedge^+]$$

$$\frac{A \wedge B}{A} [\wedge^-]$$

$$\frac{A \wedge B}{B} [\wedge^-]$$

$$\frac{A}{A \vee B} [\vee^+]$$

$$\frac{B}{A \vee B} [\vee^+]$$

$$\frac{\begin{array}{c} [A]^n \quad [B]^n \\ \vdots \quad \vdots \\ A \vee B \quad C \end{array}}{C} [\vee^-]^n$$

$$\frac{\begin{array}{c} [A]^n \\ \vdots \\ B \end{array}}{A \rightarrow B} [\rightarrow^+]^n$$

$$\frac{A \rightarrow B \quad A}{B} [\rightarrow^-]$$

$$\frac{\begin{array}{c} [A]^n \\ \vdots \\ \perp \end{array}}{\neg A} [\neg^+]^n$$

$$\frac{\neg \neg A}{A} [\neg^-]$$

$$\frac{\neg A \quad A}{\perp} [\perp^+]$$

$$\frac{\perp}{A} [\perp^-]$$

Examples

$$A \rightarrow \neg\neg A$$

Proof.

$$\frac{\begin{array}{c} [\neg A]^1 \quad [A]^2 \\ \hline \bot \\ \hline \neg\neg A \end{array}}{A \rightarrow \neg\neg A} \quad [\rightarrow^+]^2$$

$$(\neg A \rightarrow A) \rightarrow A$$

Proof.

$$\frac{\begin{array}{c} [\neg A \rightarrow A]^1 \quad [\neg A]^2 \\ \hline A \\ \hline \begin{array}{c} \bot \\ \neg\neg A \end{array} \quad [\neg^+]^2 \\ \hline \begin{array}{c} A \\ (\neg A \rightarrow A) \rightarrow A \end{array} \quad [\rightarrow^+]^1 \end{array}}{A \rightarrow \neg\neg A} \quad [\rightarrow^-]$$

Examples

$$A \vee B \rightarrow C \vdash (A \rightarrow C) \wedge (B \rightarrow C)$$

Proof.

$$\frac{\frac{[A]^1}{A \vee B} [\vee^+] \quad A \vee B \rightarrow C \quad [\rightarrow^-] \quad \frac{[B]^2}{A \vee B} [\vee^+] \quad A \vee B \rightarrow C \quad [\rightarrow^-]}{\frac{C}{A \rightarrow C} [\rightarrow^+]^1 \quad \frac{C}{B \rightarrow C} [\rightarrow^+]^2 [\wedge^+]}{(A \rightarrow C) \wedge (B \rightarrow C)}$$

$$(A \rightarrow C) \wedge (B \rightarrow C) \vdash A \vee B \rightarrow C$$

Proof.

$$\frac{\frac{(A \rightarrow C) \wedge (B \rightarrow C)}{A \rightarrow C} [\wedge^-] \quad [A]^1 \quad [\rightarrow^-] \quad \frac{(A \rightarrow C) \wedge (B \rightarrow C)}{B \rightarrow C} [\wedge^-] \quad [B]^1 \quad [\rightarrow^-] \quad [A \vee B]^2 \quad [\vee^-]^1}{\frac{C}{A \vee B \rightarrow C} [\rightarrow^+]^2}{C}$$

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Independence

Definition (Independence)

An axiom A in Γ is independent iff $\Gamma \setminus \{A\} \not\vdash A$.

Find some property that makes the axiom false and the propositions deduced from the other axioms true.

- ▶ $\not\vdash A$
- ▶ for all B , $\Gamma \setminus \{A\} \vdash B \implies \vdash B$

Theorem

Axiom3 is independent of Axiom1 and Axiom2.

p	$\neg p$	\rightarrow	0	1
0	0	0	1	1
1	0	1	0	1

Let $v(p) = 0$ and $v(q) = 1$, then $\not\vdash (\neg p \rightarrow \neg q) \rightarrow (\neg p \rightarrow q) \rightarrow p$.

Independence

Axiom1 and Axiom2 axiomatizes the conditional (\rightarrow) fragment of intuitionistic propositional logic. To axiomatize the conditional fragment of classical logic, we also need *Peirce's law*: $((p \rightarrow q) \rightarrow p) \rightarrow p$.

Theorem

Peirce's law is independent of Axiom1 and Axiom2.

\rightarrow	0	u	1
0	1	1	1
u	0	1	1
1	0	u	1

Here we interpret 1 as “true”, 0 as “false”, and u as “maybe”. Let $v(p) = u$ and $v(q) = 0$, then $v(((p \rightarrow q) \rightarrow p) \rightarrow p) = u$.

Model & Theory & Semantic Entailment

- ▶ $\text{Mod}(A) := \{\nu : \nu \models A\}$
 - ▶ $\text{Mod}(\Gamma) := \bigcap_{A \in \Gamma} \text{Mod}(A)$
 - ▶ $\text{Th}(\nu) := \{A : \nu \models A\}$
 - ▶ $\text{Th}(\mathcal{K}) := \bigcap_{\nu \in \mathcal{K}} \text{Th}(\nu)$
 - ▶ $\text{Cn}(\Gamma) := \{A : \Gamma \models A\}$
- $A \models B \iff \text{Mod}(A) \subset \text{Mod}(B)$

What is “theory”?

- ▶ A set Γ of sentences is a **theory** iff $\Gamma = \text{Cn}(\Gamma)$.
- ▶ A theory Γ is **complete** iff for every sentence A , either $A \in \Gamma$ or $\neg A \in \Gamma$.
- ▶ A theory Γ is **axiomatizable** iff there is a decidable set Σ of sentences s.t. $\Gamma = \text{Cn}(\Sigma)$.

Consistency & Satisfiability



- ▶ Γ is **consistent** iff $\Gamma \not\vdash \perp$.
- ▶ Γ is **Post-consistent** iff there is some wff $A : \Gamma \not\vdash A$.

Γ is consistent iff it is Post-consistent.
- ▶ Γ is **maximal** iff for every wff A , either $A \in \Gamma$ or $\neg A \in \Gamma$.
- ▶ Γ is **maximal consistent** iff it is both consistent and maximal.
- ▶ Γ is **satisfiable** iff $\text{Mod}(\Gamma) \neq \emptyset$.
- ▶ Γ is **finitely satisfiable** iff every finite subset of Γ is satisfiable.

- ▶ If Γ is consistent and $\Gamma \vdash A$, then $\Gamma \cup \{A\}$ is consistent.
- ▶ $\Gamma \cup \{\neg A\}$ is inconsistent iff $\Gamma \vdash A$.
- ▶ If Γ is maximal consistent, then $A \notin \Gamma \implies \Gamma \cup \{A\}$ is inconsistent.

Soundness Theorem

Theorem (Soundness Theorem)

$$\Gamma \vdash A \implies \Gamma \vDash A$$

Proof.

Prove by induction on the length of the deduction sequence.

Case1: A is an axiom. (truth table)

Case2: $A \in \Gamma$

Case3:

$$\left. \begin{array}{l} \Gamma \vDash C_j \\ \Gamma \vDash C_j \rightarrow A \end{array} \right\} \implies \Gamma \vDash A$$

Corollary

Any *satisfiable* set of wffs is *consistent*.

Compactness Theorem

Theorem (Compactness Theorem)

A set of wffs is satisfiable iff it is finitely satisfiable.

Corollary

If $\Gamma \models A$, then there is a finite $\Gamma_0 \subset \Gamma$ s.t. $\Gamma_0 \models A$.

Proof.

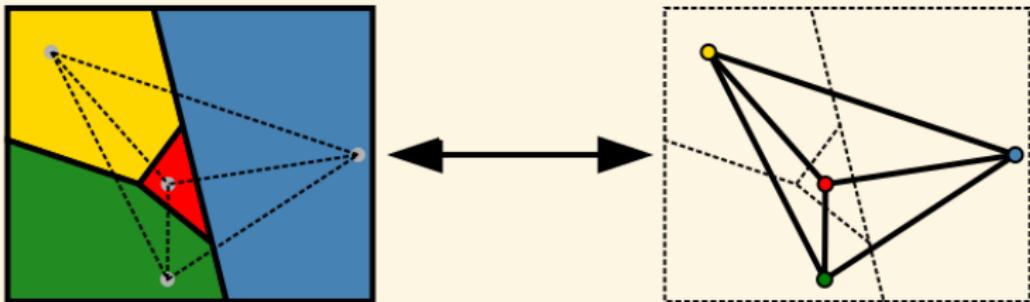
$$\begin{aligned}\Gamma_0 \not\models A \text{ for any } \Gamma_0 \subset \Gamma &\implies \Gamma_0 \cup \{\neg A\} \text{ is satisfiable for any } \Gamma_0 \subset \Gamma \\ &\implies \Gamma \cup \{\neg A\} \text{ is satisfiable} \\ &\implies \Gamma \not\models A\end{aligned}$$

Remark: Γ is consistent iff every finite subset of Γ is consistent.

Remark: Compactness does not hold in a language with infinite disjunctions.

$$\left\{ \bigvee_{i=1}^{\infty} p_i, \neg p_1, \neg p_2, \dots \right\}$$

Applications of Compactness



An infinite graph (V, E) is n -colorable iff every finite subgraph of (V, E) is n -colorable.

Proof.

Take $\{p_v^i : v \in V, 1 \leq i \leq n\}$ as the set of atoms.

$$\Gamma := \{p_v^1 \vee \dots \vee p_v^n : v \in V\} \cup \{\neg(p_v^i \wedge p_v^j) : v \in V, 1 \leq i < j \leq n\} \cup \{\neg(p_v^i \wedge p_w^i) : (v, w) \in E, 1 \leq i \leq n\}$$

Proof of Compactness Theorem



Proof.

part1. Extend the finitely satisfiable set Γ to a maximal finitely satisfiable set Δ .

Let $\langle A_i : i \in \mathbb{N} \rangle$ be a fixed enumeration of the wffs.

$$\begin{aligned}\Delta_0 &:= \Gamma \\ \Delta_{n+1} &:= \begin{cases} \Delta_n \cup \{A_n\} & \text{if } \Delta_n \cup \{A_n\} \text{ is finitely satisfiable} \\ \Delta_n \cup \{\neg A_n\} & \text{otherwise} \end{cases} \\ \Delta &:= \bigcup_{n \in \mathbb{N}} \Delta_n\end{aligned}$$

part2. Define a truth assignment that satisfies Γ .

$$v(p) := \begin{cases} 1 & \text{if } p \in \Delta \\ 0 & \text{otherwise} \end{cases} \implies (v \models A \iff A \in \Delta)$$

Compactness in Topology \iff Compactness in Logic

Compactness in Topology \implies Compactness in Logic

Let $\mathbf{2} := \{0, 1\}$ be the discrete topology.

For any wff A , let $\text{Mod}(A) := \{\nu \in \mathbf{2}^{\text{Var}} : \nu \models A\}$.

$\text{Mod}(A)$ are a basis for a topology on $\mathbf{2}^{\text{Var}}$.

Let τ be the topology on $\mathbf{2}^{\text{Var}}$ generated by $\text{Mod}(A)$. Then $(\mathbf{2}^{\text{Var}}, \tau)$ is the product topology.

By Tychonoff Theorem, $(\mathbf{2}^{\text{Var}}, \tau)$ is a compact, Hausdorff space.

It can be shown that $\text{Mod}(A)$ is clopen in $\mathbf{2}^{\text{Var}}$.

By hypothesis, for each finite $\Gamma_0 \subset \Gamma$, there is a truth assignment making Γ_0 true, i.e. $\text{Mod}(\Gamma_0) \neq \emptyset$. That is to say, $\{\text{Mod}(A) : A \in \Gamma\}$ has the Finite Intersection Property. By the compactness of $(\mathbf{2}^{\text{Var}}, \tau)$, $\text{Mod}(\Gamma) \neq \emptyset$.

Compactness in Logic \implies Compactness in Topology

Γ is unsatisfiable iff $\{\text{Mod}(\neg A) : A \in \Gamma\}$ covers $\mathbf{2}^{\text{Var}}$.

Given any cover $\{\text{Mod}(A)\}_{A \in \Gamma}$ of $\mathbf{2}^{\text{Var}}$. Then $\Gamma^* := \{\neg A : A \in \Gamma\}$ is unsatisfiable. By compactness theorem, some finite subset $\Delta \subset \Gamma^*$ is unsatisfiable. The set $\{\text{Mod}(A)\}_{\neg A \in \Delta} \subset \{\text{Mod}(A)\}_{A \in \Gamma}$ is a finite subcover for $\mathbf{2}^{\text{Var}}$. So $(\mathbf{2}^{\text{Var}}, \tau)$ is compact.

Weak Completeness Theorem

Lemma

Let A be a wff whose only propositional symbols are p_1, \dots, p_n . Let

$$p_i^\nu := \begin{cases} p_i & \text{if } \nu \models p_i \\ \neg p_i & \text{otherwise} \end{cases} \quad A^\nu := \begin{cases} A & \text{if } \nu \models A \\ \neg A & \text{otherwise} \end{cases}$$

then $p_1^\nu, \dots, p_n^\nu \vdash A^\nu$.

Weak Completeness Theorem $\models A \implies \vdash A$

$$\mu(p) := \begin{cases} 1 - \nu(p) & \text{if } p = p_n \\ \nu(p) & \text{otherwise} \end{cases}$$

$$\left. \begin{array}{l} p_1^\nu, \dots, p_{n-1}^\nu, p_n^\nu \vdash A \\ p_1^\mu, \dots, p_{n-1}^\mu, p_n^\mu \vdash A \end{array} \right\} \implies p_1^\nu, \dots, p_{n-1}^\nu \vdash A$$

$$\models A \iff \vdash A$$

+

Compactness Theorem



$$\Gamma \models A \iff \Gamma \vdash A$$

Emil Post 1897-1954



- ▶ Truth table
- ▶ Completeness of propositional logic
- ▶ Post machine
- ▶ Post canonical system
- ▶ Post correspondence problem
- ▶ Post problem

Completeness Theorem

Theorem (Completeness Theorem — Post1921)

$$\Gamma \models A \implies \Gamma \vdash A$$

Corollary

Any *consistent* set of wffs is *satisfiable*.

$$\begin{array}{ccc} \Gamma \models A & \iff & \Gamma \vdash A \\ \updownarrow & & \updownarrow \\ \Gamma \cup \{\neg A\} & \iff & \Gamma \cup \{\neg A\} \\ \text{unsatisfiable} & & \text{inconsistent} \end{array}$$

Corollary (Compactness Theorem)

A set of wffs is satisfiable iff it is finitely satisfiable.

Proof of Completeness Theorem



Proof.

step1. Extend the consistent set Γ to a maximal consistent set Δ .

Let $\langle A_i : i \in \mathbb{N} \rangle$ be a fixed enumeration of the wffs.

$$\begin{aligned}\Delta_0 &:= \Gamma \\ \Delta_{n+1} &:= \begin{cases} \Delta_n \cup \{A_n\} & \text{if } \Delta_n \cup \{A_n\} \text{ is consistent} \\ \Delta_n \cup \{\neg A_n\} & \text{otherwise} \end{cases} \\ \Delta &:= \bigcup_{n \in \mathbb{N}} \Delta_n\end{aligned}$$

step2. Define a truth assignment that satisfies Γ .

$$v(p) := \begin{cases} 1 & \text{if } p \in \Delta \\ 0 & \text{otherwise} \end{cases} \implies (v \models A \iff A \in \Delta)$$

Decidability

Theorem

There is an effective procedure that, given any expression, will decide whether or not it is a wff.

Theorem (Decidability — Post1921)

There is an effective procedure that, given a finite set $\Gamma \cup \{A\}$ of wffs, will decide whether or not $\Gamma \models A$.

Theorem

If Γ is a decidable set of wffs, then the set of logical consequences of Γ is recursively enumerable.

Model Checking & Satisfiability Checking & Validity Checking⁴

- Given a model ν and a formula A . Is $\nu \models A$?
- Given a formula A . Is there a model ν s.t. $\nu \models A$?
- Given a sentence A . Is $\models A$?

—P

—NP

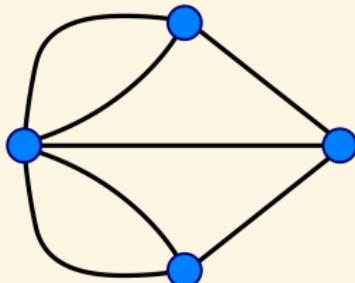
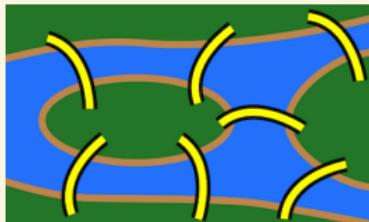


Figure: Eulerian Circle(P)

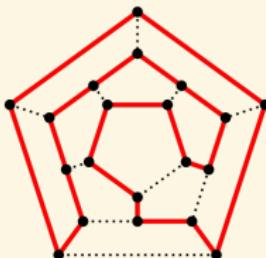


Figure: Hamiltonian Circle(NPC)

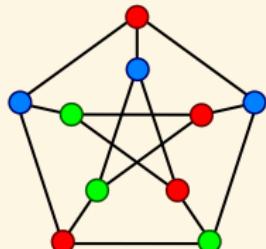
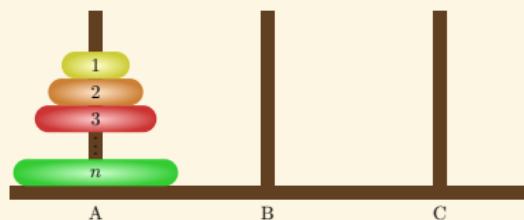


Figure: Graph Coloring(NPC)



⁴ Aaronson: Why philosophers should care about computational complexity.

Contents

Introduction

Term Logic

Propositional Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Meta-Theorems

 Application

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Party and Friends

Problem

Alice, Ben, Charlie, and Diane are considering going to a Halloween party.

1. *If Alice goes then Ben won't go and Charlie will.*
2. *If Ben and Diane go, then either Alice or Charlie (but not both) will go.*
3. *If Charlie goes and Ben does not, then Diane will go but Alice will not.*

Solution

1. $A \rightarrow \neg B \wedge C$
2. $B \wedge D \rightarrow (A \wedge \neg C) \vee (\neg A \wedge C)$
3. $C \wedge \neg B \rightarrow D \wedge \neg A$

Which road will lead you to the center?

Problem (Which road will lead you to the center?)

You are in front of three roads: the gold road, the marble road, and the stone road. Each road is protected by a *lying* guardian.

1. The guardian of the gold road: "This road will bring you to the center. Moreover, if the stones take you to the center, then also the marble takes you to the center."
2. The guardian of the marble road: "Neither the gold nor the stones will take you to the center."
3. The guardian of the stone road: "Follow the gold and you'll reach the center, follow the marble and you will be lost."

Solution

1. $\neg(g \wedge (s \rightarrow m))$
2. $\neg(\neg g \wedge \neg s)$
3. $\neg(g \wedge \neg m)$

Self-reference Puzzle

Alice: Bob is a liar.

Bob: Alice tells the truth.

$$A \leftrightarrow \neg B, B \leftrightarrow A \vdash \perp$$

Problem (Which answer is the correct answer to this question?)

1. *All of the below.*
2. *None of the below.*
3. *All of the above.*
4. *One of the above.*
5. *None of the above.*
6. *None of the above.*

$$1. p_1 \leftrightarrow p_2 \wedge p_3 \wedge p_4 \wedge p_5 \wedge p_6$$

$$2. p_2 \leftrightarrow \neg p_3 \wedge \neg p_4 \wedge \neg p_5 \wedge \neg p_6$$

$$3. p_3 \leftrightarrow p_1 \wedge p_2$$

$$4. p_4 \leftrightarrow (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge p_2 \wedge \neg p_3) \vee (\neg p_1 \wedge \neg p_2 \wedge p_3)$$

$$5. p_5 \leftrightarrow \neg p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge \neg p_4$$

$$6. p_6 \leftrightarrow \neg p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge \neg p_4 \wedge \neg p_5$$

$$1 \wedge 2 \wedge 3 \wedge 4 \wedge 5 \wedge 6 \vdash \neg p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge \neg p_4 \wedge p_5 \wedge \neg p_6$$

Sudoku

	8	6				2	9	
4			1	5				8
7			9					4
1								9
	5						1	
		8			3			
		5	9					
			2					

$p(i, j, n) \coloneqq$ the cell in row i
and column j contains the
number n

- Every row/column contains every number.

$$\bigwedge_{i=1}^9 \bigwedge_{n=1}^9 \bigvee_{j=1}^9 p(i, j, n) \quad \bigwedge_{j=1}^9 \bigwedge_{n=1}^9 \bigvee_{i=1}^9 p(i, j, n)$$

- Every 3×3 block contains every number.

$$\bigwedge_{r=0}^2 \bigwedge_{s=0}^2 \bigwedge_{n=1}^9 \bigvee_{i=1}^3 \bigvee_{j=1}^3 p(3r + i, 3s + j, n)$$

- No cell contains more than one number.
for all $1 \leq i, j, n, n' \leq 9$ and $n \neq n'$:

$$p(i, j, n) \rightarrow \neg p(i, j, n')$$

Example: The Wumpus World

			PIT
	 Gold	PIT	
		PIT	

- squares adjacent to wumpus are smelly
- squares adjacent to pit are breezy
- glitter iff gold is in the same square
- shooting kills wumpus if you are facing it
- shooting uses up the only arrow
- grabbing picks up gold if in same square
- releasing drops the gold in same square

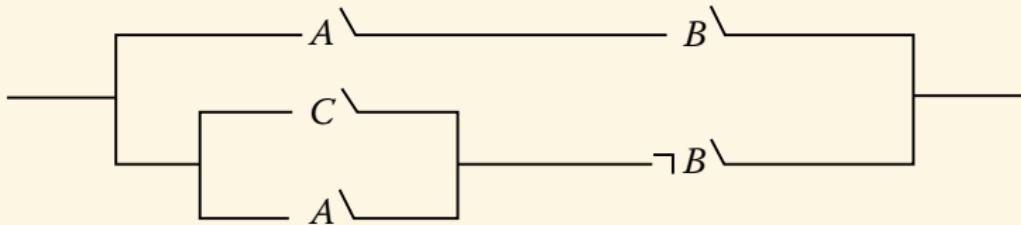
KB = wumpus-world rules + observations

Example: $B_{21} \leftrightarrow P_{11} \vee P_{22} \vee P_{31}$

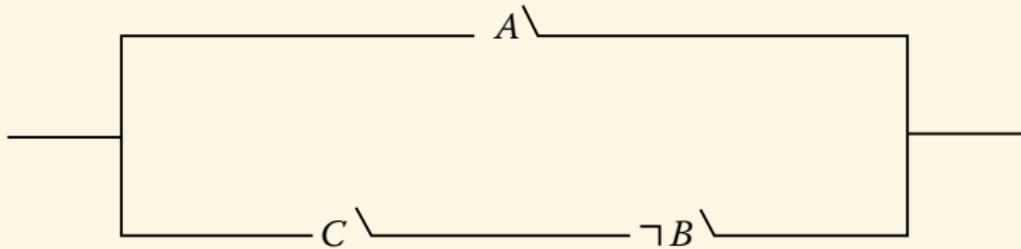
Automated Theorem Prover: [Prover9](#) is an automated theorem prover for first-order and equational logic, and [Mace4](#) searches for finite models and counterexamples.⁵

⁵Adrian Groza: Modelling Puzzles in First Order Logic.

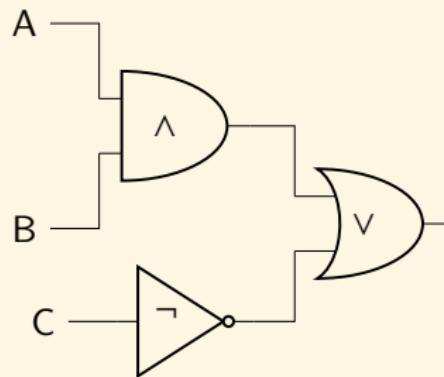
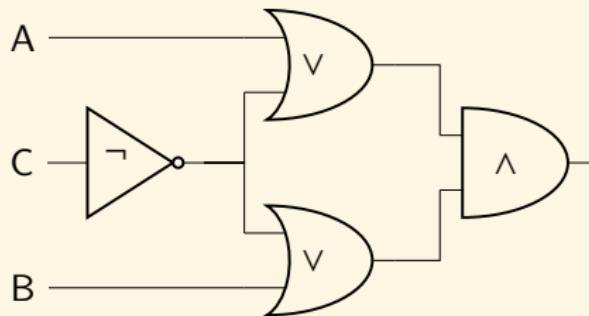
Shannon — Digital Circuit Design



$$\frac{(A \wedge B) \vee ((C \vee A) \wedge \neg B)}{A \vee (C \wedge \neg B)}$$

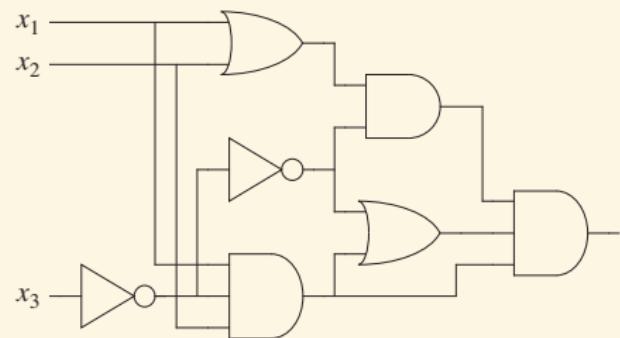
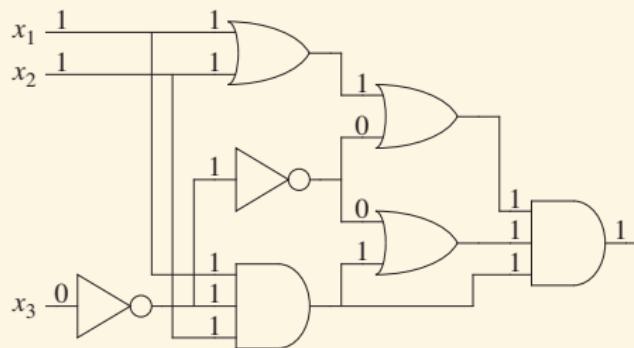


Shannon — Digital Circuit Design



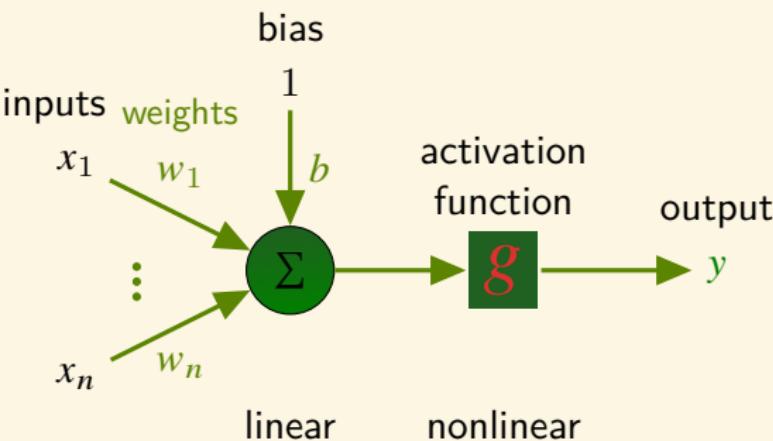
$$\frac{(A \vee \neg C) \wedge (B \vee \neg C)}{(A \wedge B) \vee \neg C}$$

Circuit-Satisfiability Problem

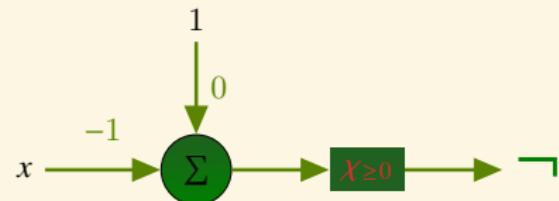
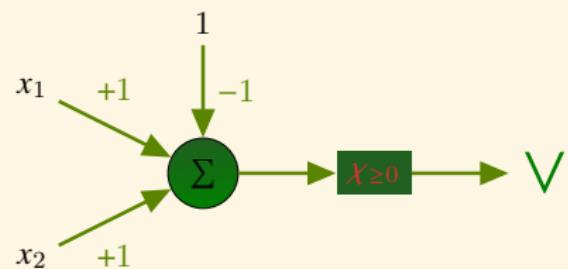
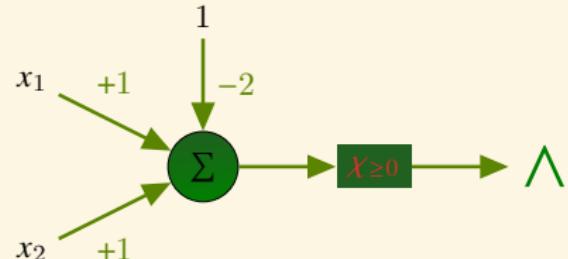


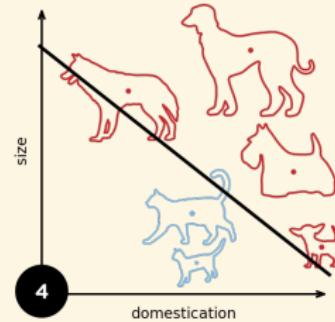
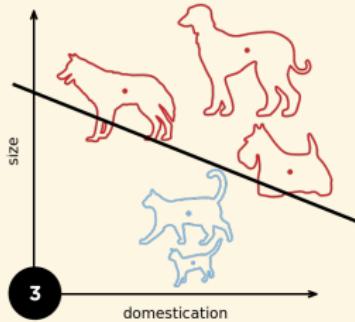
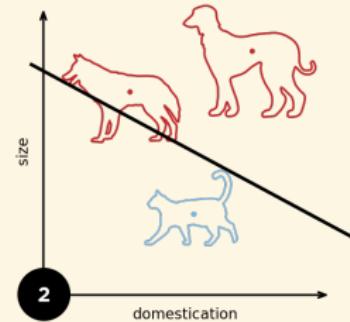
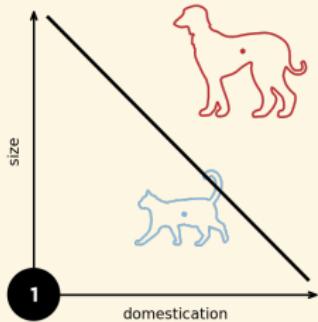
A one-output boolean combinational circuit is **satisfiable** if it has a truth assignment that causes the output of the circuit to be 1.

McCulloch-Pitts Artificial Neural Network



$$y = g \left(\sum_{i=1}^n w_i x_i + b \right)$$





1-layer NN

$$y = \begin{cases} 1 & \text{if } \sum_{i=1}^n w_i x_i + b \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

Linearly Separable

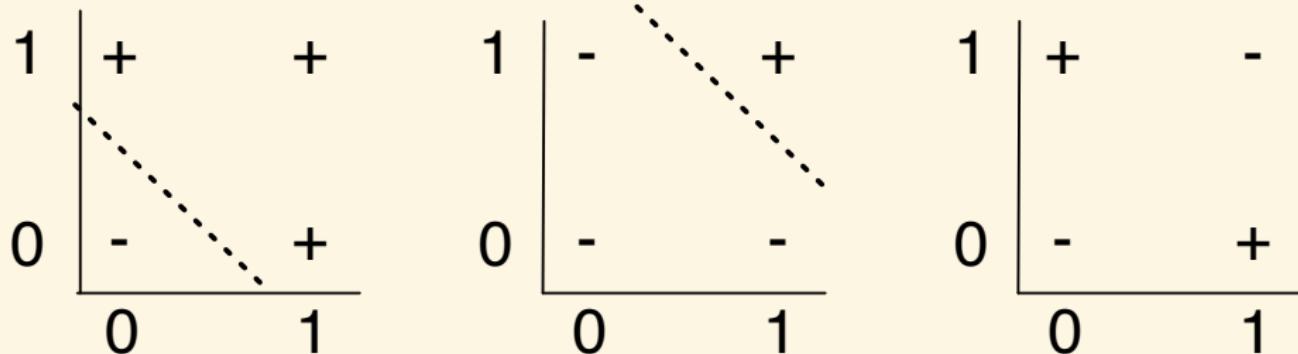


Figure: \vee, \wedge, \oplus

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

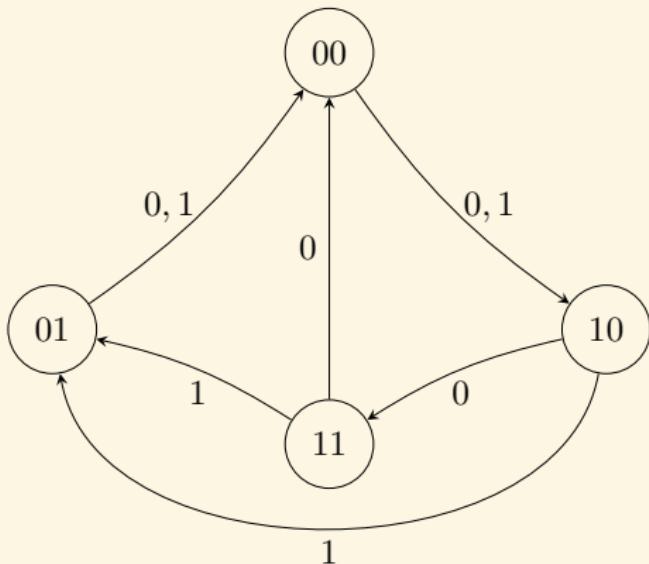
$$\begin{array}{lll} w_1 \cdot 0 + w_2 \cdot 0 + b < 0 & & b < 0 \\ w_1 \cdot 0 + w_2 \cdot 1 + b \geq 0 & & w_2 + b \geq 0 \\ w_1 \cdot 1 + w_2 \cdot 0 + b \geq 0 & & w_1 + b \geq 0 \\ w_1 \cdot 1 + w_2 \cdot 1 + b < 0 & & w_1 + w_2 + b < 0 \end{array}$$

A simple single-layer perception can't solve nonlinearly separable problems.

《三体》

- ▶ 秦始皇：朕当然需要预测太阳的运行，但你们让我集结三千万大军，至少要首先向朕演示一下这种计算如何进行吧？
- ▶ 冯诺依曼：陛下，请给我三个士兵，我将为您演示。
- ▶ 秦始皇：三个？只要三个吗，朕可以轻易给你三千个。
- ▶ 冯诺依曼：伟大的陛下，您刚提到东方人在科学思维上的缺陷，就是因为你们没有意识到，复杂的宇宙万物其实是由最简单的单元构成的。我只要三个，陛下。……
- ▶ 秦始皇：他们不需要学更多的东西了吗？
- ▶ 冯诺依曼：不需要，我们组建一千万个这样的门部件，再将这些部件组合成一个系统，这个系统就能进行我们所需要的运算，解出那些预测太阳运行的微分方程。

Finite State Automaton



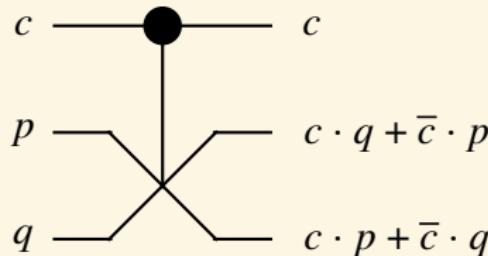
y_1	y_2	x	y_1^+	y_2^+
0	0	0	1	0
0	0	1	1	0
0	1	0	0	0
0	1	1	0	0
1	0	0	1	1
1	0	1	0	1
1	1	0	0	0
1	1	1	0	1

$$y_1^+ = \bar{y}_1 \bar{y}_2 + \bar{x} \bar{y}_2$$

$$y_2^+ = y_1 \bar{y}_2 + x y_1$$

Reversible Computing — Fredkin Gate: CSWAP

c	p	q	x	y	z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1



transmit the first bit unchanged and
swap the last two bits iff the first bit is 1.
 $f : (c, p, q) \mapsto (c, c \cdot q + \bar{c} \cdot p, c \cdot p + \bar{c} \cdot q)$

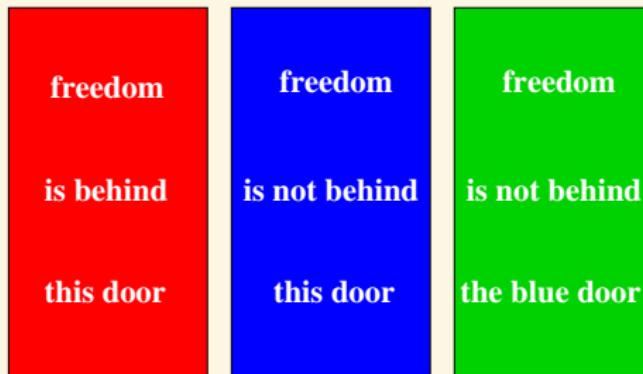
$$\neg p = 0 \ \& \ q = 1 \implies z = \bar{c}$$

$$\wedge q = 0 \implies z = c \cdot p$$

Remark: no entropy changes occur and no heat dissipation is involved.

Exercise

1. Behind one of the door is a path to freedom, behind the other two doors is an evil dragon.
2. At least one of the three statements is true.
3. At least one of the three statements is false.



1. $(r \wedge \neg b \wedge \neg g) \vee (\neg r \wedge b \wedge \neg g) \vee (\neg r \wedge \neg b \wedge g)$
2. $r \vee \neg b \vee \neg b$
3. $\neg r \vee \neg \neg b \vee \neg \neg b$

Solution

r	b	g	1	2	3
0	0	0	0	1	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	0	0	1
1	0	0	1	1	0
1	0	1	0	1	0
1	1	0	0	1	1
1	1	1	0	1	1

r	b	g	
0	0	0	1×
0	0	1	
0	1	0	2×
0	1	1	1×
1	0	0	3×
1	0	1	1×
1	1	0	1×
1	1	1	1×

$$(r \wedge \neg b \wedge \neg g) \vee (\neg r \wedge b \wedge \neg g) \vee (\neg r \wedge \neg b \wedge g), r \vee \neg b, \neg r \vee b \vdash g$$

Exercise

宝藏在哪里？

你面前有三扇门，只有一扇门后是宝藏。门上各有一句话，只有一扇门上的是真话。

- ① 宝藏不在这儿。
- ② 宝藏不在这儿。
- ③ 宝藏在②号门。

Solution

- ① $\neg t_1$; ② $\neg t_2$; ③ t_2 .
- 只有一扇门上的是真话。
$$(\neg t_1 \wedge \neg \neg t_2 \wedge \neg t_2) \vee (\neg \neg t_1 \wedge \neg t_2 \wedge \neg t_2) \vee (\neg \neg t_1 \wedge \neg \neg t_2 \wedge t_2)$$
- 只有一扇门后是宝藏。
$$(t_1 \wedge \neg t_2 \wedge \neg t_3) \vee (\neg t_1 \wedge t_2 \wedge \neg t_3) \vee (\neg t_1 \wedge \neg t_2 \wedge t_3)$$

Exercise — Now it's your turn ❤

谁是凶手？

一起凶杀案有三个嫌疑人：小白、大黄和老王。

1. 至少有一人是凶手，但不可能三人同时犯罪。
2. 如果小白是凶手，那么老王是同犯。
3. 如果大黄不是凶手，那么老王也不是。

谁是盗贼？

1. 《白玉美人》是白展堂或楚留香偷的。
2. 如果是白展堂偷的，则偷窃时间不会在午夜前。
3. 如果楚留香的证词正确，则午夜时烛光未灭。
4. 如果楚留香的证词不正确，则偷窃发生在午夜前。
5. 午夜时没有烛光。

Exercise — Now it's your turn ❤

哪个部落的？

一个岛上有 T、F 两个部落，T 部落的居民只说真话，F 部落的居民只说谎。你在岛上遇到了小白、大黄、老王三个土著。

1. 小白：“如果老王说谎，我或大黄说的就是真话”。
2. 大黄：“如果小白或老王说真话，那么，我们三人中有且只有一人说真话是不可能的”。
3. 老王：“小白或大黄说谎当且仅当小白或我说真话”。

What am I doing?

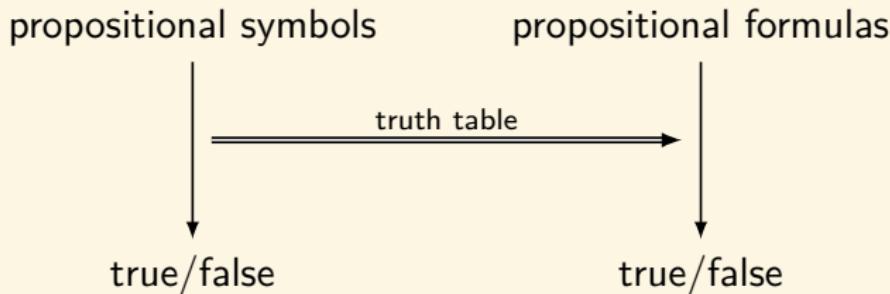
1. If I'm not playing tennis, I'm watching tennis.
2. If I'm not watching tennis, I'm reading about tennis.
3. I cannot do more than one of these activities at a time.

Summary

- ## ► Syntax.



- ## ► Semantics.



- ## ► Formal System.



- ▶ Expressiveness / Succinctness
 - ▶ Satisfiability / Validity
 - ▶ Soundness / Completeness / Compactness
 - ▶ Decidability / Computational Complexity

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References

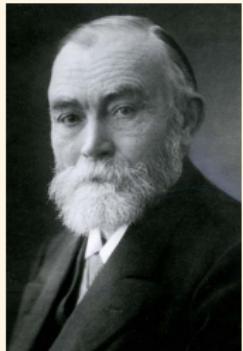
1436

Gottlob Frege 1848-1925 (+Charles Peirce 1839-1914)

- ▶ *Begriffsschrift, a formal language of pure thought modelled upon that of arithmetic.*
- ▶ Predicate Logic. (Relations & Quantifiers)
(Every boy loves some girl.)

$$\frac{\text{subject}}{\text{predicate}} \approx \frac{\text{argument}}{\text{function}}$$

- ▶ Philosophy of Language.
The evening star is the morning star. (venus)



Logicism

Mathematics \leadsto Logic.⁶

⁶ Frege: The Foundations of Arithmetic.

Why Study Predicate Logic?

- ▶ Propositional logic assumes the world contains **facts**.
- ▶ Predicate logic assumes the world contains
 - ▶ **Objects**: people, houses, numbers, colors, baseball games, wars, ...
 - ▶ **Relations**: red, round, prime, brother of, bigger than, part of, between, fall in love with, ...
 - ▶ **Functions**: father of, best friend, one more than, plus, ...
- ▶ Expressive power.

Language	Ontological Commitment	Epistemological Commitment
Propositional Logic	facts	true/false/unknown
Predicate Logic	facts, objects, relations	true/false/unknown
Temporal Logic	facts, objects, relations, times	true/false/unknown
Probability Theory	facts	degree of belief [0, 1]
Fuzzy Logic	facts with degree of truth [0, 1]	known interval value

Example 😞

What will a logician choose: an egg or eternal bliss?

An egg! Because nothing is better than eternal bliss, and an egg is better than nothing.

$$e > 0 > b \implies e > b$$

$$\neg \exists x(x > b) \implies 0 \not> b$$

“*The Nothing itself nothings.*”

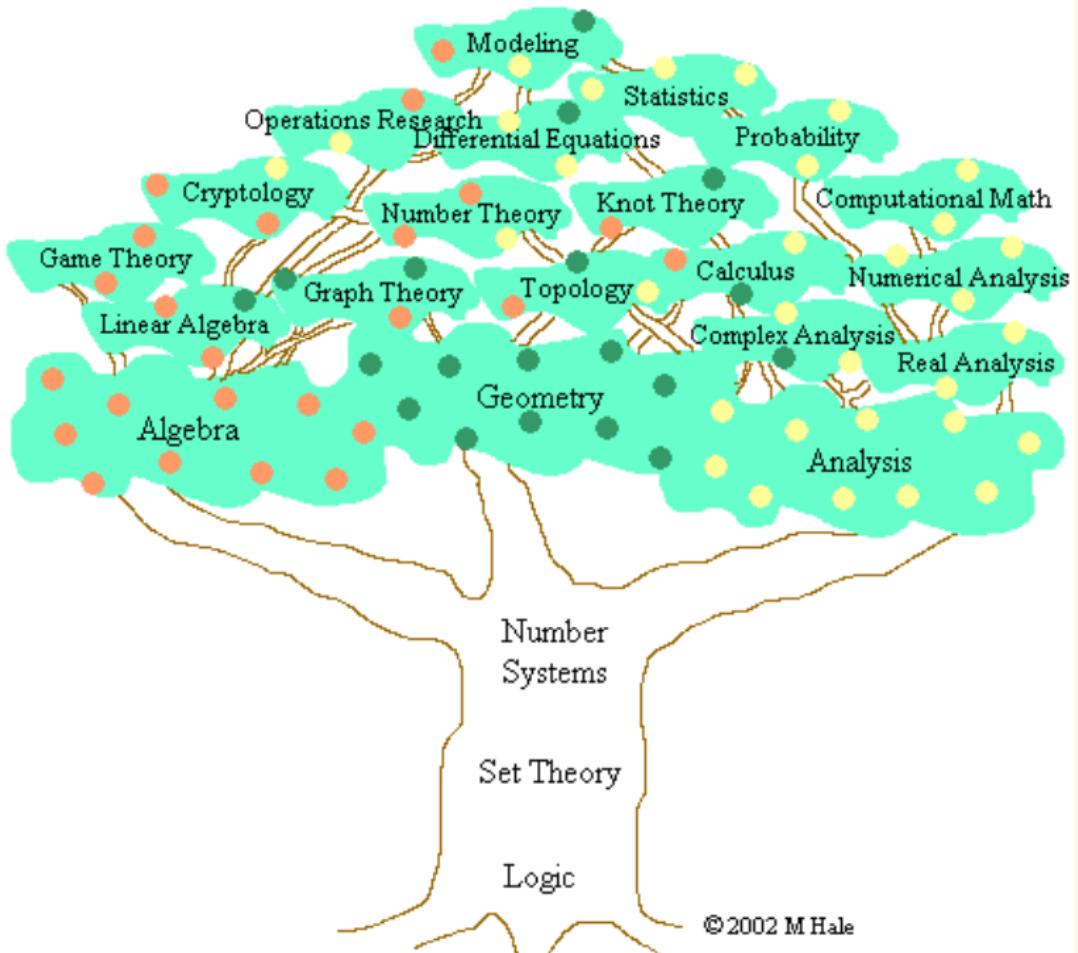
— Heidegger

A cat has nine lives 😞

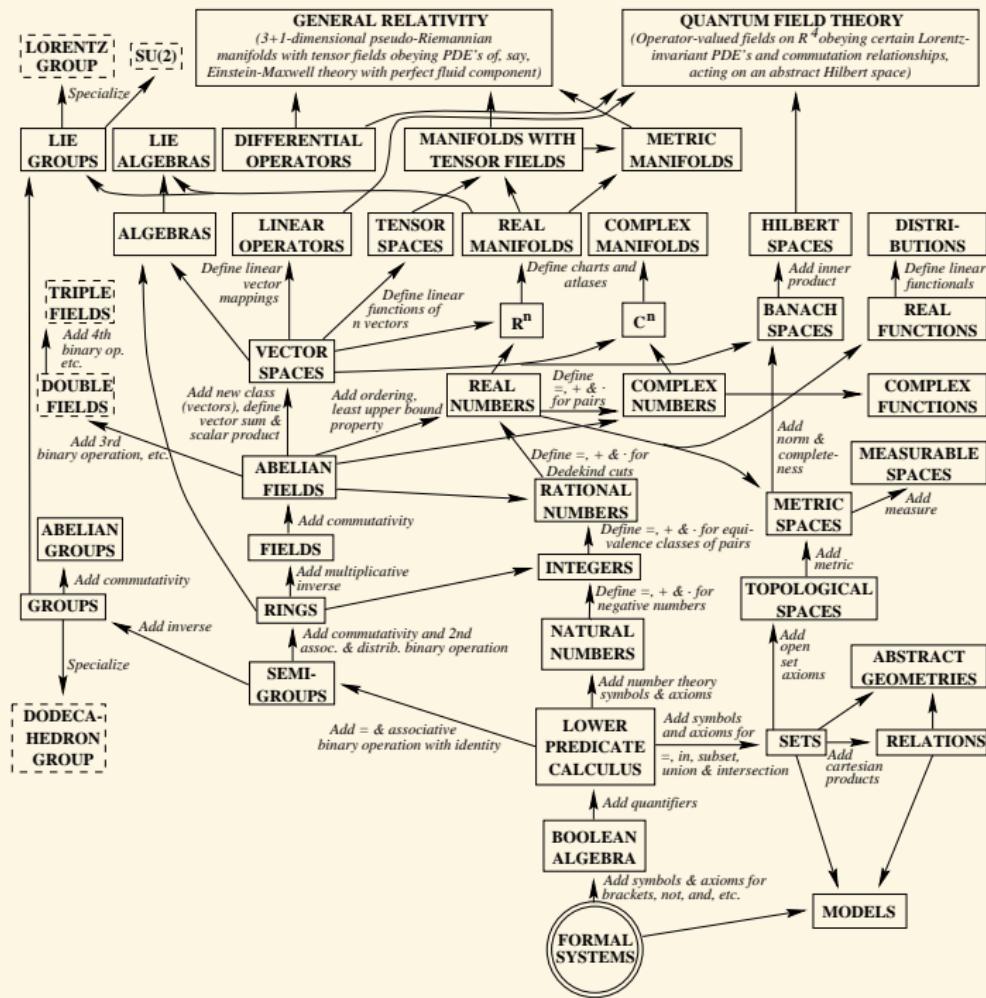
No cat has eight lives. A cat has one more life than no cat.

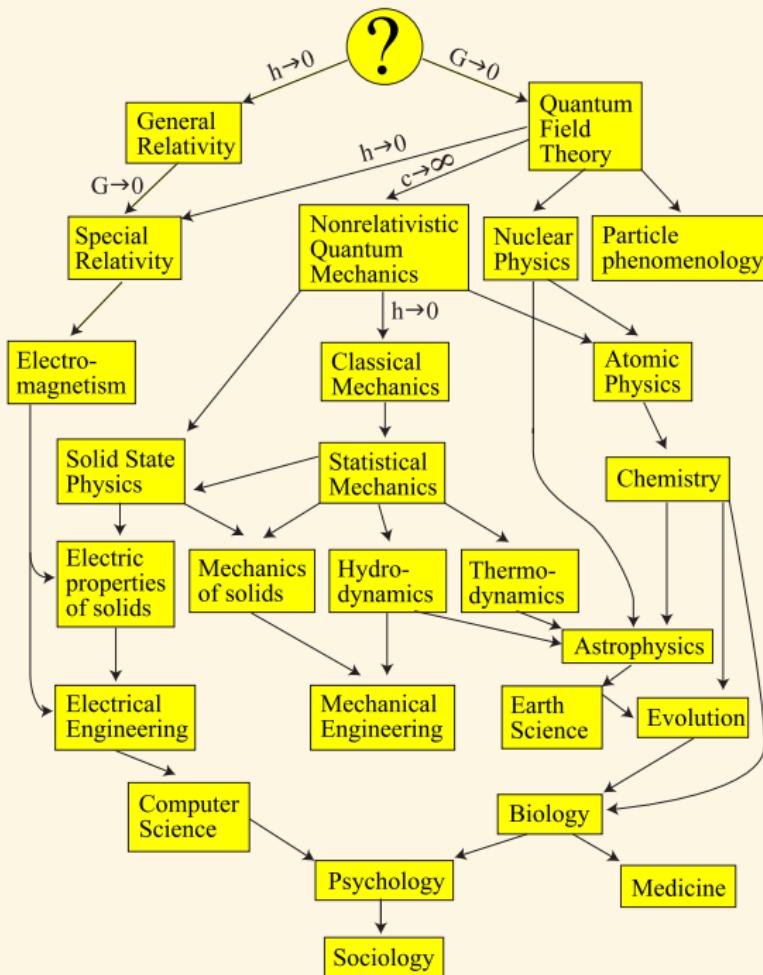
Lewis Carroll — Through the Looking-Glass

- ▶ “I see nobody on the road.” said Alice.
- ▶ “I only wish I had such eyes,” the King remarked in a fretful tone. “To be able to see Nobody! And at that distance too!”
- ▶
- ▶ “Who did you pass on the road?” the King went on, holding out his hand to the Messenger for some more hay.
- ▶ “Nobody,” said the Messenger.
- ▶ “Quite right,” said the King; “this young lady saw him too. So of course Nobody walks slower than you.”
- ▶ “I do my best,” the Messenger said in a sullen tone. “I’m sure nobody walks much faster than I do!”
- ▶ “He can’t do that,” said the King, “or else he’d have been here first.”

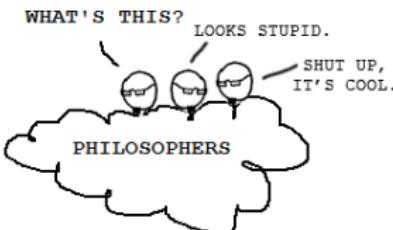


© 2002 M Hale



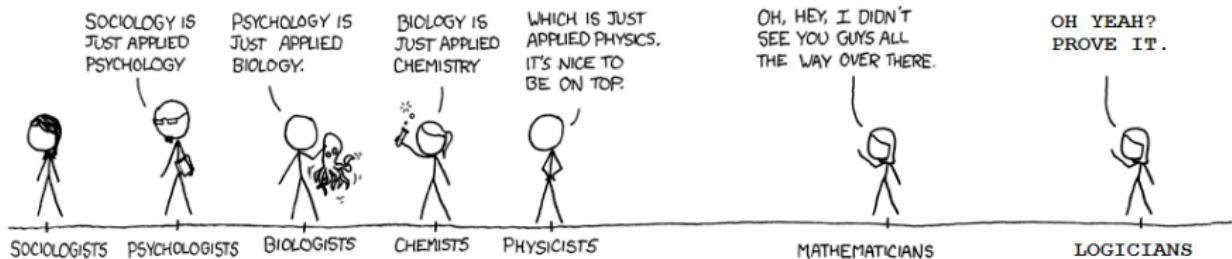


Emergentism ≠ Reductionism



FIELDS ARRANGED BY PURITY

→ MORE PURE



Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

What are quantifiers?

- ▶ All students work hard.
- ▶ Some students are asleep.
- ▶ At least six students are awake.
- ▶ Eight out of ten students are good at logic.
- ▶ Nobody knows logic better than Donald Trump.
- ▶ Most students love logic.
- ▶ There are infinitely many prime numbers.
- ▶ There are more PCs than there are Macs.

Syntax

Language

$$\mathcal{L}^1 := \{\textcolor{green}{\neg}, \wedge, \vee, \rightarrow, \leftrightarrow, \textcolor{green}{\forall}, \exists, =, (,)\} \cup \text{Var} \cup \overbrace{\text{Fun} \cup \text{Pred}}^{\text{signature}}$$

where

$$\text{Var} := \{x_i : i \in \mathbb{N}\}$$

$$\text{Fun} := \bigcup_{n \in \mathbb{N}} \text{Fun}^n \quad \text{Fun}^n := \{f_1^n, f_2^n, f_3^n, \dots\}$$

$$\text{Pred} := \bigcup_{n \in \mathbb{N}} \text{Pred}^n \quad \text{Pred}^n := \{P_1^n, P_2^n, P_3^n, \dots\}$$

f^n is an n -place function symbol.

P^n is an n -place predicate symbol.

A 0-place function symbol f^0 is called constant.

A 0-place predicate symbol P^0 is called atomic proposition.

Term & Formula

Definition (Term)

$$t ::= x \mid c \mid f(t, \dots, t)$$

where $x \in \text{Var}$ and $f \in \text{Fun}$.

- Term is freely generated from Var by Fun.

Definition (Well-Formed Formula Wff)

$$A ::= \overbrace{t = t \mid P(t, \dots, t)}^{\text{atomic formula}} \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid A \leftrightarrow A \mid \forall x A \mid \exists x A$$

where $t \in \text{Term}$ and $P \in \text{Pred}$.

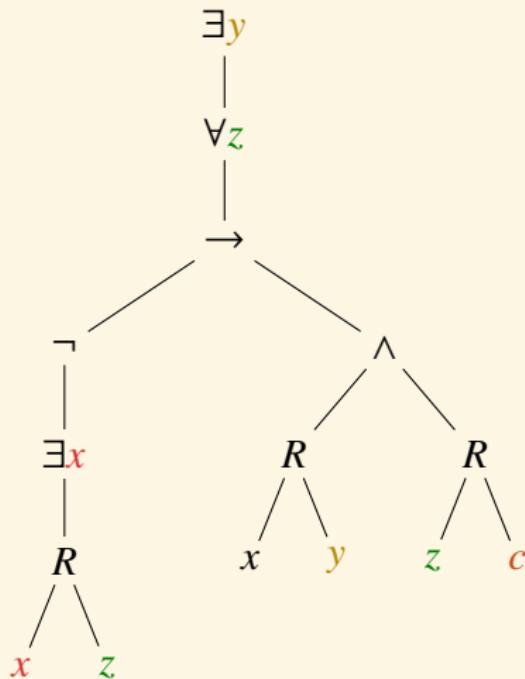
- Wff is freely generated from atomic formulas by connective and quantifier operators.

Syntax

- $A \wedge B := \neg(A \rightarrow \neg B)$
- $A \vee B := \neg A \rightarrow B$
- $A \leftrightarrow B := (A \rightarrow B) \wedge (B \rightarrow A)$
- $\exists x A := \neg \forall x \neg A$
- $\perp := A \wedge \neg A$
- $\top := \neg \perp$
- Bottom up and Top down definitions of terms, subterms, wffs and subformulas.
- Induction Principle for terms and wffs.
- Unique readability theorem for terms and wffs.
- Omitting Parenthesis.
 - 1). outermost parentheses.
 - 2). $\neg, \forall, \exists, \wedge, \vee, \rightarrow, \leftrightarrow$
 - 3). group to the right.

Freedom & Bondage

$$\exists y \forall z (\neg \exists x R x z \rightarrow Rx y \wedge R z c)$$



$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$$

$$e^{i\theta} = \cos \theta + i \sin \theta$$

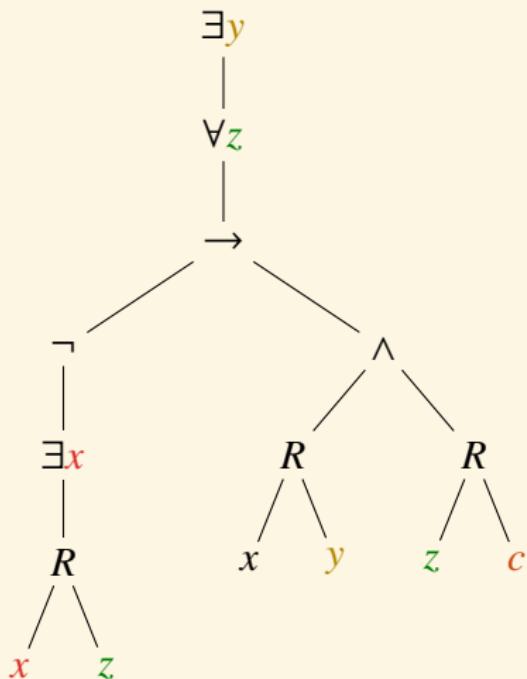
$$\frac{d}{dx} \int_a^x f(t) dt = f(x)$$

$$P_k(x) = \sum_{n=0}^k \frac{f^{(n)}(a)}{n!} (x-a)^n$$

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$$

Freedom & Bondage

$$\exists y \forall z (\neg \exists x Rxz \rightarrow Rxy \wedge Rzc)$$



- ▶ In the wff $\forall x A$, we say that the **scope** of this quantifier \forall is A .
- ▶ An occurrence of a variable x is **bound** if it occurs within the scope of $\forall x$, or it is the x in $\forall x$.
- ▶ An occurrence of a variable is **free** if it is not bound.
- ▶ The term t is a **ground term** iff $\text{Var}(t) = \emptyset$.
- ▶ A is a **sentence** iff $\text{Fv}(A) = \emptyset$.
- ▶ A is an **open formula** iff $\text{Bv}(A) = \emptyset$.

Example: $c = d$ is clopen.

Variable of a Term, Free / Bound Variable of a wff

$$\text{Var}(t) := \begin{cases} \{x\} & \text{if } t = x \\ \emptyset & \text{if } t = c \\ \text{Var}(t_1) \cup \dots \cup \text{Var}(t_n) & \text{if } t = f(t_1, \dots, t_n) \end{cases}$$

$$\text{Fv}(A) := \begin{cases} \text{Var}(t_1) \cup \text{Var}(t_2) & \text{if } A = t_1 = t_2 \\ \text{Var}(t_1) \cup \dots \cup \text{Var}(t_n) & \text{if } A = P(t_1, \dots, t_n) \\ \text{Fv}(B) & \text{if } A = \neg B \\ \text{Fv}(B) \cup \text{Fv}(C) & \text{if } A = B \rightarrow C \\ \text{Fv}(B) \setminus \{x\} & \text{if } A = \forall x B \end{cases}$$

$$\text{Bv}(A) := \begin{cases} \emptyset & \text{if } A = t_1 = t_2 \\ \emptyset & \text{if } A = P(t_1, \dots, t_n) \\ \text{Bv}(B) & \text{if } A = \neg B \\ \text{Bv}(B) \cup \text{Bv}(C) & \text{if } A = B \rightarrow C \\ \text{Bv}(B) \cup \{x\} & \text{if } A = \forall x B \end{cases}$$

Translation — How to ‘speak’ the language of FOL?

- | | | |
|----------|------------------------|-------------------------------------|
| A | All S are P . | $\forall x(Sx \rightarrow Px)$ |
| E | No S are P . | $\forall x(Sx \rightarrow \neg Px)$ |
| I | Some S are P . | $\exists x(Sx \wedge Px)$ |
| O | Some S are not P . | $\exists x(Sx \wedge \neg Px)$ |

1. Every boy loves some girl.

$$\forall x(Bx \rightarrow \exists y(Gy \wedge Lxy))$$

2. Whoever has a father has a mother.

$$\forall x(\exists yFyx \rightarrow \exists yMyx)$$

3. Grandmother is mother's mother.

$$\forall x\forall y(Gxy \leftrightarrow \exists z(Mxz \wedge Mzy))$$

$$\forall x\forall y(x = Gy \leftrightarrow \exists z(x = Mz \wedge z = My))$$

4. No man loves children unless he has his own.

$$\forall x(Mx \wedge \exists y\exists z(Cyz \wedge Lxy) \rightarrow \exists yCyx)$$

Translation — How to ‘speak’ the language of FOL?

1. If bad things happen to good people, then God is either not omnipotent or not benevolent.

$$\exists x \exists y (\text{Bad}(x) \wedge \text{Good}(y) \wedge \text{Happen}(x, y)) \rightarrow \neg \text{Omnip}(g) \vee \neg \text{Benev}(y)$$

2. Every book that Alice lends to Bob she steals from Chris.

$$\forall x (Bx \wedge Laxb \rightarrow Saxc)$$

3. For every professor, there is a student who likes every book the professor recommends to the student.

$$\forall x (Px \rightarrow \exists y (Sy \wedge \forall z (Bz \wedge Rxzy \rightarrow Lyz)))$$

4. Anyone who befriends any enemy of yours is an enemy of mine.

$$\forall x \forall y (Eyu \wedge Bxy \rightarrow Exam)$$

5. When a mathematical or philosophical author writes with a misty profundity, he is talking nonsense.
— Alfred Whitehead

$$\forall x ((\text{Math}(x) \vee \text{Pilo}(x)) \wedge \text{Write}(x) \rightarrow \text{TalkNonsense}(x))$$

Translation — How to ‘speak’ the language of FOL?

1. If all dancers have knee injuries, then *they* will be frustrated.

$$\forall x \left(\text{Dancer}(x) \rightarrow \text{Knee}(x) \right) \rightarrow \forall y \left(\text{Dancer}(y) \rightarrow \text{Frustrated}(y) \right)$$

2. If all dancers have knee injuries, then *some of them* will be frustrated.

$$\forall x \left(\text{Dancer}(x) \rightarrow \text{Knee}(x) \right) \rightarrow \exists y \left(\text{Dancer}(y) \wedge \text{Knee}(y) \wedge \text{Frustrated}(y) \right)$$

3. No dolphin sings unless it jumps.

$$\forall x \left(\text{Dolphin}(x) \rightarrow \neg \text{Jumps}(x) \rightarrow \neg \text{Sings}(x) \right)$$

4. Alice is the first to have completed the test.

$$Cat \wedge \forall x (Cxt \wedge x \neq a \rightarrow Baxt)$$

Alice is the oldest daughter of the King.

5. Alice is the second to have completed the test.

$$Cat \wedge \exists x (Cxt \wedge x \neq a \wedge Bxat \wedge \forall y (Cyt \wedge y \neq a \wedge y \neq x \rightarrow Bayt))$$

1. There are at most 1 elements.

$$\forall x \forall y (x = y)$$

2. There are at least 2 elements.

$$\exists x \exists y (x \neq y)$$

3. There are exactly 2 elements.

$$\exists x \exists y (x \neq y \wedge \forall z (z = x \vee z = y))$$

4. There are exactly n elements.

$$\exists x_1 \dots \exists x_n \left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left(\bigvee_{i=1}^n y = x_i \right) \right)$$

5. There exists a unique element such that P .

$$\exists x Px \wedge \forall y \forall z (Py \wedge Pz \rightarrow y = z)$$

$$\exists x (Px \wedge \forall y (Py \rightarrow y = x))$$

$$\exists x \forall y (Py \leftrightarrow y = x)$$

$$\exists !x Px$$

Example — How Many Gods?

- Theism: there is at least one god

$$\exists x Gx$$

- Atheism: there are no gods

$$\neg \exists x Gx$$

- Pantheism: everything is god

$$\forall x Gx$$

- Agnosticism: there is at most one god

$$\forall x(Gx \rightarrow \forall y(Gy \rightarrow y = x))$$

- Monotheism: there is exactly one god

$$\exists x(Gx \wedge \forall y(Gy \rightarrow y = x))$$

- Gnosticism: there are exactly two gods

$$\exists x(Gx \wedge \exists y(Gy \wedge x \neq y) \wedge \forall z(Gz \rightarrow z = x \vee z = y))$$

Translation — How to ‘speak’ the language of FOL?

1. 敌人的敌人是朋友。

$$\forall x \forall y \forall z (Exy \wedge Eyz \rightarrow Fxz)$$

2. 朋友之间要么都吸烟要么都不吸烟。

$$\forall x \forall y (Fxy \rightarrow (Sx \leftrightarrow Sy))$$

3. 既没有朋友又没有敌人是寂寞的。

$$\forall x (\neg \exists y Fxy \wedge \neg \exists z Exz \rightarrow Lx)$$

4. 最可怕的敌人是最亲密的朋友。

$$\forall x \forall y (Exy \wedge \forall z (Exz \rightarrow Tyz) \rightarrow Fxy \wedge \forall z (Fxz \rightarrow Cyz))$$

5. 如果大鱼比小鱼游得快，那么，有最大的鱼就有游得最快的鱼。

$$\forall x \forall y (Fx \wedge Fy \wedge Bxy \rightarrow Sxy) \rightarrow$$

$$\exists x (Fx \wedge \forall y (Fy \rightarrow Bxy)) \rightarrow \exists x (Fx \wedge \forall y (Fy \rightarrow Sxy))$$

6. 名，可名，非常名。

$$\forall x \left(\exists y \text{Name}(x, y) \wedge \exists z \text{Name}(z, x) \rightarrow \neg \text{Unchanging}(x) \right) ?$$

1. No dogs must be brought to this Park except on a lead.

$$\forall d \forall t (Bdt \rightarrow Ldt)$$

Objection: this is consistent with $\exists d \exists t (Pdt \wedge \neg Ldt)$.

2. Dogs are not allowed in this Park without leads.

$$\forall d \forall t (Pdt \rightarrow Ldt)$$

Objection? The order should be addressed to the owners, not to the dogs.

3. Owners of dogs are not allowed in this Park unless they keep them on leads.

$$\forall p \forall d \forall t (Opd \wedge Ppt \rightarrow Lpdt)$$

Objection: doesn't allow $\exists t \exists p \exists d (Opd \wedge Ppt \wedge \neg Pdt \wedge \neg Lpdt)$.

4. Nobody without his dog on a lead is allowed in this Park.

$$\forall p \forall t (Ppt \rightarrow \exists d (Opd \wedge Lpdt))$$

Objection: doesn't allow $\exists p \exists t (Ppt \wedge \neg \exists d Opd)$.

5. Dogs must be led in this Park.

$$\forall d \forall t (Ldt \wedge Pdt) \quad \forall d \forall t (Ldt \rightarrow Pdt)$$

6. All dogs in this Park must be kept on the lead.

$$\forall d \forall t (Pdt \rightarrow Ldt)$$

$$\forall d \forall t \forall p (Pdt \wedge Opd \rightarrow Lpdt)$$

Translation — How to ‘speak’ the language of FOL?

1. He who learns but does not think, is lost. He who thinks but does not learn is in danger. — *Confucius*

$$\forall x(\text{Learn}(x) \wedge \neg \text{Think}(x) \rightarrow \text{Lost}(x)) \wedge$$

$$\forall x(\text{Think}(x) \wedge \neg \text{Learn}(x) \rightarrow \text{InDanger}(x))$$

2. He who can, does. He who cannot, teaches. — *Bernard Shaw*

$$\forall xy(\text{Can}(x, y) \rightarrow \text{Does}(x, y)) \wedge \forall xy(\neg \text{Can}(x, y) \rightarrow \text{Teaches}(x, y))$$

3. Don’t interrupt me, while I’m interrupting. — *Churchill*

$$\exists x \text{Interrupt}(i, x) \rightarrow \forall y \neg \text{Interrupt}(y, i)$$

4. There are no shortcuts to any place worth going. — *Beverly Sills*

$$\forall x(\text{Place}(x) \wedge \text{WorthGo}(x) \rightarrow \neg \exists y \text{ Shortcut}(y, x))$$

5. The old believe everything; the middle-aged suspect everything; the young know everything. — *Oscar Wilde*

$$\forall x(\text{Old}(x) \rightarrow \forall y \text{ Believe}(x, y)) \wedge$$

$$\forall x(\text{Middle}(x) \rightarrow \forall y \text{ Suspect}(x, y)) \wedge \forall x(\text{Young}(x) \rightarrow \forall y \text{ Know}(x, y))$$

6. No married man is ever attractive except to his wife. — *Oscar Wilde*

$$\forall x(\text{Man}(x) \wedge \text{Married}(x) \rightarrow \forall y(\text{Attractive}(x, y) \leftrightarrow y = \text{wife}(x)))$$

Translation — How to ‘speak’ the language of FOL?

7. Always two there are: a Master and an Apprentice. — *Yoda*

$$\exists xy(x \neq y \wedge \forall z(z = x \vee z = y) \wedge \text{Master}(x) \wedge \text{Apprentice}(y))$$

8. There are two ways to live your life. One is as though nothing is a miracle. The other is as though everything is a miracle. — *Einstein*

$$\exists xy(x \neq y \wedge \forall z(\text{WayLive}(z) \leftrightarrow z = x \vee z = y) \wedge$$
$$(\text{WayLive}(x) \rightarrow \neg \exists z \text{ Miracle}(z)) \wedge (\text{WayLive}(y) \rightarrow \forall z \text{ Miracle}(z)))$$

9. The weakest link in a chain is the strongest because it can break it.

— *Stanislaw J. Lec*

$$\forall xy((\text{Link}(x) \wedge \text{Chain}(y) \wedge \text{In}(x, y) \wedge \text{Weakest}(x) \rightarrow \text{Break}(x, y))$$
$$\rightarrow \text{Strongest}(x))$$

10. To a man who only has a hammer, everything looks like a nail.

— *Maslow*

$$\forall x(\text{Man}(x) \wedge \exists !y(\text{Hammer}(y) \wedge \text{Has}(x, y)) \rightarrow$$
$$\forall z \exists n(\text{Nail}(n) \wedge \text{LooksLike}(z, n, x)))$$

11. He who refuses to do arithmetic is doomed to talk nonsense.

— *John McCarthy*

$$\forall x(\text{Refuse}(x, \text{arithmetic}) \rightarrow \square \text{TalkNonsense}(x))$$

1. $\text{Think}(i) \rightarrow \exists x(x = i)$ *Descartes*
2. $\exists x(x = i) \vee \neg \exists x(x = i)$ *Shakespeare*
3. $\forall x(\text{Month}(x) \rightarrow \text{Crueler}(\text{april}, x))$ *Eliot*
4. $\forall x(\neg \text{Weep}(x) \rightarrow \neg \text{See}(x))$ *Hugo*
5. $\forall x(\text{Time}(x) \rightarrow \text{Better}(t, x)) \wedge \forall x(\text{Time}(x) \rightarrow \text{Better}(x, t))$ *Dickens*
6. $\exists x(\text{Child}(x) \wedge \neg \text{Growup}(x) \wedge \forall y(\text{Child}(y) \wedge y \neq x \rightarrow \text{Growup}(y)))$ *Barrie*
7. $\forall x \forall y(Fx \wedge Fy \rightarrow (Hx \wedge Hy \rightarrow Axy) \wedge (\neg Hx \wedge \neg Hy \rightarrow \neg Axy))$ *Tolstoi*
8. $\forall x(Px \rightarrow \exists y(Ty \wedge Fxy)) \wedge \exists x(Px \wedge \forall y(Ty \rightarrow Fxy)) \wedge \neg \forall x(Px \rightarrow \forall y(Ty \rightarrow Fxy))$ *Lincoln*
9. $\forall x(\text{Problem}(x) \wedge \text{Philo}(x) \wedge \text{Serious}(x) \leftrightarrow x = \text{suicide})$ *Camus*
10. $\forall x(\text{Feather}(x) \wedge \text{Perch}(x, \text{soul}) \leftrightarrow x = \text{hope})$ *Dickinson*
11. $\forall x(\text{Enter}(x) \rightarrow \forall y(\text{Hope}(y) \rightarrow \text{Abandon}(x, y)))$ *Dante*
12. $\exists x \forall y(\text{For}(y, x) \wedge \text{For}(x, y))?$ $\forall x \forall y(\text{For}(y, x) \leftrightarrow \text{For}(x, y))?$ *Dumas*
13. $\exists x(\text{Fear}(\text{we}, x) \leftrightarrow x = \text{fear})?$ *Roosevelt*
14. $\forall x \forall y(Ax \wedge Ay \rightarrow Exy) \wedge \exists x \exists y(Ax \wedge Ay \wedge [\![Exx]\!] > [\![Eyy]\!])?$ *Orwell*

Translation — Logic to Natural Language

1. $\forall x (\text{Buy}(\text{susan}, x) \rightarrow \text{Buy}(\text{alice}, x))$
 2. $\forall x (\exists y \text{Buy}(y, x) \vee \exists z \text{Sell}(z, x) \rightarrow \neg \text{Human}(x))$
 3. $\forall x ((\text{Petted}(x) \rightarrow \text{Jump}(x)) \rightarrow \text{Dog}(x) \vee \text{Dolphin}(x))$
 4. $\forall x (\text{Girl}(x) \wedge \text{Love}(\text{bob}, x) \rightarrow \forall y (\text{PhilosophyBook}(y) \rightarrow \text{Read}(x, y)))$
- ▶ $\forall x (\text{Minute}(x) \rightarrow \exists y (\text{Driver}(y) \wedge \text{Die}(y, x)))$
 - ▶ $\exists x (\text{Driver}(x) \wedge \forall y (\text{Minite}(y) \rightarrow \text{Die}(x, y)))$
 - ▶ Every minute one driver dies in car accident.
 - ▶ One driver dies in car accident every minute.

Translation — Logic to Natural Language

1. $\exists x \left(Gx \wedge \forall y \left(By \wedge \forall z (Gz \wedge z \neq x \rightarrow \neg Lzy) \rightarrow Lxy \right) \right) \rightarrow \forall x \left(Bx \rightarrow \exists y (Gy \wedge Lyx) \right)$
2. $\forall x \forall y \left((Gx \wedge \forall y (By \rightarrow \neg Lxy)) \wedge (Gy \wedge \exists x (Bx \wedge Lyx)) \rightarrow \neg Lxy \right)$

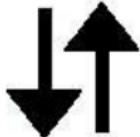
Translation — Logic to Natural Language

- $\exists x \left(Gx \wedge \forall y (By \wedge \forall z (Gz \wedge z \neq x \rightarrow \neg Lzy) \rightarrow Lxy) \right) \rightarrow \forall x (Bx \rightarrow \exists y (Gy \wedge Lyx))$
- $\forall x \forall y ((Gx \wedge \forall y (By \rightarrow \neg Lxy)) \wedge (Gy \wedge \exists x (Bx \wedge Lyx)) \rightarrow \neg Lxy)$

安得圣母爱渣男，大庇天下雄性有红颜！

相信我，我肯定能找到一种你
不屑于理解的语言来试图跟你
对 (zhuang) 话 (B) 的。

No girl who does not
love a boy loves
a girl who
loves a
boy.



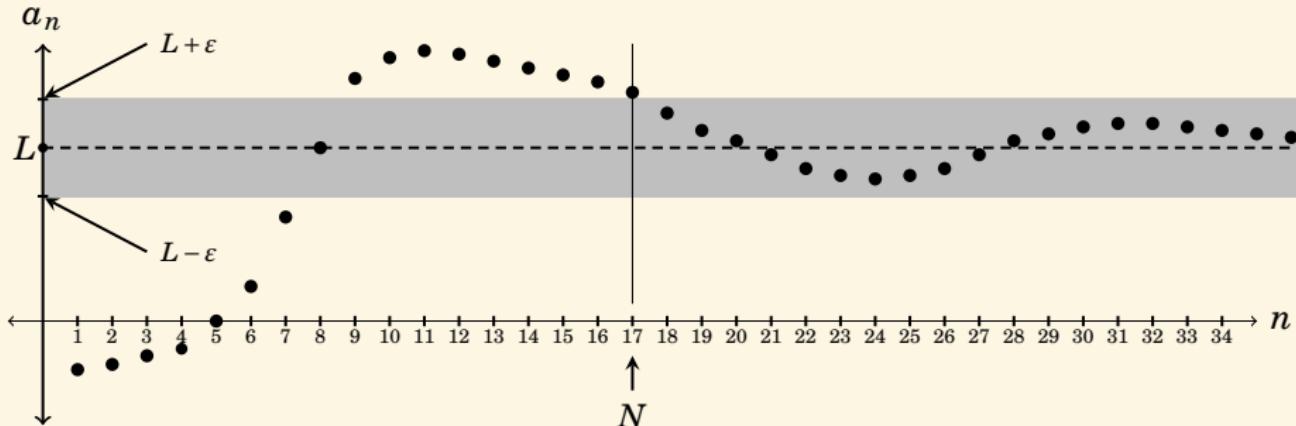
女同不爱女异。

某女没
个孩有
男会一
孩爱的上
一个不
女爱一
孩。爱男
孩着的



$$\forall x \forall y (((Gx \wedge \forall v (Bv \rightarrow \neg Lxv)) \wedge (Gy \wedge \exists z (Bz \wedge Lyz))) \rightarrow \neg Lxy).$$

Translation — Natural Language to Logic



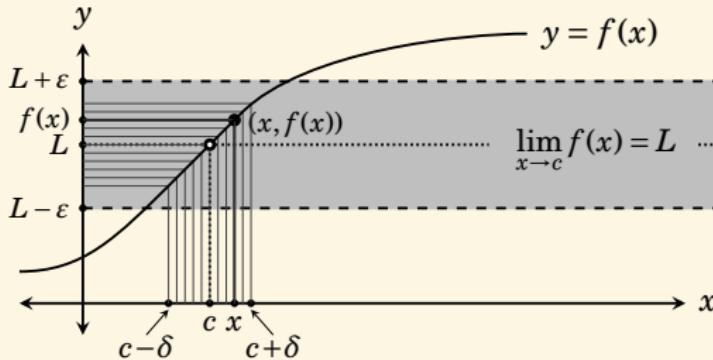
Definition (Convergence)

A sequence $\{a_n\}$ converges to a number $L \in \mathbb{R}$ provided that for any real number $\varepsilon > 0$ there is an $N \in \mathbb{N}$ for which $n > N$ implies $|a_n - L| < \varepsilon$.

$$\lim_{n \rightarrow \infty} a_n = L \iff \forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \geq N (|a_n - L| < \varepsilon)$$

$$\lim_{n \rightarrow \infty} a_n = \infty \iff \forall L \in \mathbb{R} \exists N \in \mathbb{N} \forall n \geq N (a_n > L)$$

Translation — Natural Language to Logic



- ▶ Informal definition of a **limit**: $f(x)$ is arbitrarily close to L provided that x is sufficiently close to c .
- ▶ Precise definition: for any real number $\varepsilon > 0$, there is a real number $\delta > 0$ for which $|f(x) - L| < \varepsilon$ provided that $0 < |x - c| < \delta$.
- ▶ Formal definition:

$$\forall \varepsilon > 0 \exists \delta > 0 (0 < |x - c| < \delta \rightarrow |f(x) - L| < \varepsilon)$$

- ▶ **Divergence**

$$\lim_{x \rightarrow c} f(x) \uparrow \iff \forall L \in \mathbb{R} \exists \varepsilon > 0 \forall \delta > 0 (0 < |x - c| < \delta \wedge |f(x) - L| \geq \varepsilon)$$

Translation — Natural Language to Logic

- Continuity

$$\forall x \in I \forall \varepsilon > 0 \exists \delta > 0 \forall y \in I (|x - y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon)$$

$$\forall (x_n)_{n \in \mathbb{N}} \subset I : \lim_{n \rightarrow \infty} f(x_n) = f(\lim_{n \rightarrow \infty} x_n)$$

- Uniform Continuity

$$\forall \varepsilon > 0 \exists \delta > 0 \forall xy \in I (|x - y| < \delta \rightarrow |f(x) - f(y)| < \varepsilon)$$

- Any two distinct points determine a unique line.

$$\forall x \forall y \left(\text{Point}(x) \wedge \text{Point}(y) \wedge x \neq y \rightarrow \exists !z \text{Line}(z) \wedge \text{On}(x, z) \wedge \text{On}(y, z) \right)$$

Exercises — Translation — Now it's your turn ❤

1. If you can't solve a problem, then there is an easier problem that you can't solve.
— Polya
2. Men *and* women are welcome to apply.
3. *None but* ripe bananas are edible.
4. *Only* Socrates and Plato are human.
5. *All but* Socrates and Plato are human.
6. Every boy loves *at least* two girls.
7. Adams can't do *every* job right.
8. Adams can't do *any* job right.
9. *Not all* that glitters are gold.
10. Everyone's zipcode within a city has the same first digit.
11. Every farmer who owns a donkey is happy.
12. Every farmer who owns a donkey beats it.
13. All even numbers are divisible by 2, but *only some* are divisible by 4.

Exercises — Translation — Now it's your turn ❤

14. Behind every great fortune there is a crime. — Balzac
15. If a clown enters the room, then it will be displeased if no person is surprised.
16. Everyone alive 2000BC is either an ancestor of nobody alive today or of everyone alive today.
17. John hates all people who do not hate themselves.
18. No barber shaves exactly those who do not shave themselves.
19. Andy and Bob have the same maternal grandmother. *mother(x, y)*
20. Anyone who loves two different girls is Tony.
21. Socrates' wife *has* a face that *only* her mother could love.
22. If dogs are animals, every head of a dog is the head of an animal.
23. *The* detective is *never* happy.
24. Someone *other than the girl* who loves Bob is stupid.
25. Morris *only* loves *the girl* who loves him.
26. *The one* who loves Alice is *the one* she loves.
27. *The shortest* English speaker loves *the tallest* English speaker.

Translation

1. Only the bishop gave the monkey the banana.
2. The only bishop gave the monkey the banana.
3. The bishop only gave the monkey the banana.
4. The bishop gave only the monkey the banana.
5. The bishop gave the only monkey the banana.
6. The bishop gave the monkey only the banana.
7. The bishop gave the monkey the only banana.
8. The bishop gave the monkey the banana only.

Substitution

Definition (Substitution in a term)

$$s[t/x] := \begin{cases} c & \text{if } s = c \\ t & \text{if } s = x \\ y & \text{if } s = y \& y \neq x \\ f(t_1[t/x], \dots, t_n[t/x]) & \text{if } s = f(t_1, \dots, t_n) \end{cases}$$

Definition (Substitution in a formula)

$=, P, \neg, \rightarrow \dots$

$$(\forall y B)[t/x] := \begin{cases} \forall y B[t/x] & \text{if } y \neq x \\ \forall y B & \text{if } y = x \end{cases}$$

Substitutable

Definition (Substitutable)

A term t is substitutable for x in A iff none of the free occurrences of x in A occur in the scope of a quantifier that binds a variable in t .

Variables in t don't become bound in A .

- ▶ For atomic A , t is always substitutable for x in A .
- ▶ t is substitutable for x in $\neg A$ iff it is substitutable for x in A .
- ▶ t is substitutable for x in $A \rightarrow B$ iff it is substitutable for x in A and B .
- ▶ t is substitutable for x in $\forall y A$ iff either
 1. $x \notin \text{Fv}(A)$ or
 2. $y \notin \text{Var}(t)$ and t is substitutable for x in A .

Counterexample: $A = \exists y(x \neq y) \quad t = y \quad A[t/x]?$

Contents

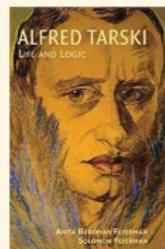
	Modal Logic
Introduction	
Term Logic	Set Theory
Propositional Logic	Recursion Theory
Predicate Logic	Equational Logic
Introduction	Homotopy Type Theory
Syntax	
Semantics	Category Theory
Formal System	
Definability & Isomorphism	Quantum Computing
What is Logic?	
Connectives	Answers to the Exercises
Normal Forms	References
Meta-Theorems	1436

Philosophy

- ▶ No entity without identity. — Quine's standards of ontological admissibility
- ▶ To be is to be the value of a bound variable. — Quine's criterion of ontological commitments
- ▶ To be is to be constructed by intuition. — Brouwer
- ▶ To be true is to be provable. — Kolmogorov
- ▶ " p " is true iff p . — Tarski's " T -schema"

What is “truth” — Are all truths knowable?

1. *formally correct* $\forall x(T(x) \leftrightarrow A(x))$
2. *materially adequate* $A(s) \leftrightarrow p$
where ‘ s ’ is the name of a sentence of \mathcal{L} , and ‘ p ’ is the translation of this sentence in \mathcal{L}' .



Alfred Tarski 1901-1983

“snow is white” is true iff snow is white.

“I am false.”⁷

Model Theory

Undefinability of truth Theorem

Arithmetical truth can't be defined in arithmetic.

The theory of real closed fields / elementary geometry is complete and decidable.

Banach-Tarski Paradox

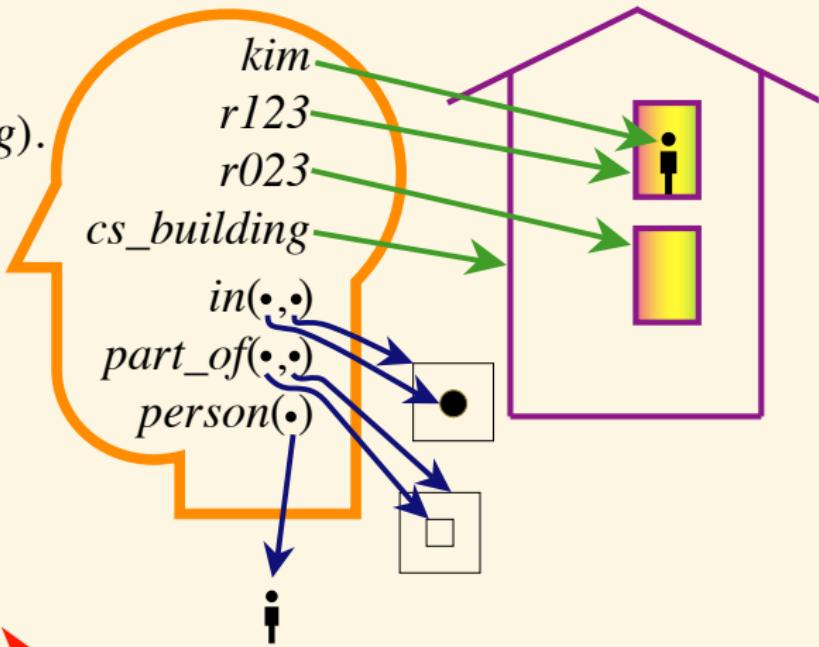
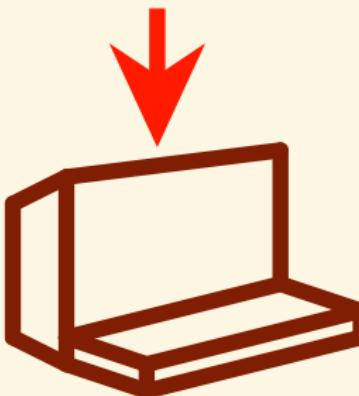


⁷

Tarski: On the Concept of Truth in Formalized Languages.
Tarski: The Semantic Conception of Truth and the Foundations of Semantics.

Syntax and Semantics

```
in(kim,r123).  
part_of(r123,cs_building).  
in(X,Y) ←  
    part_of(Z,Y) ∧  
    in(X,Z).
```



`in(kim,cs_building)`

Language — Mind — World

- ▶ What is the meaning of 'meaning'? (symbol grounding problem)
- ▶ How do words relate to objects?
- ▶ How do words relate to thought?
- ▶ What makes a sentence true/false?

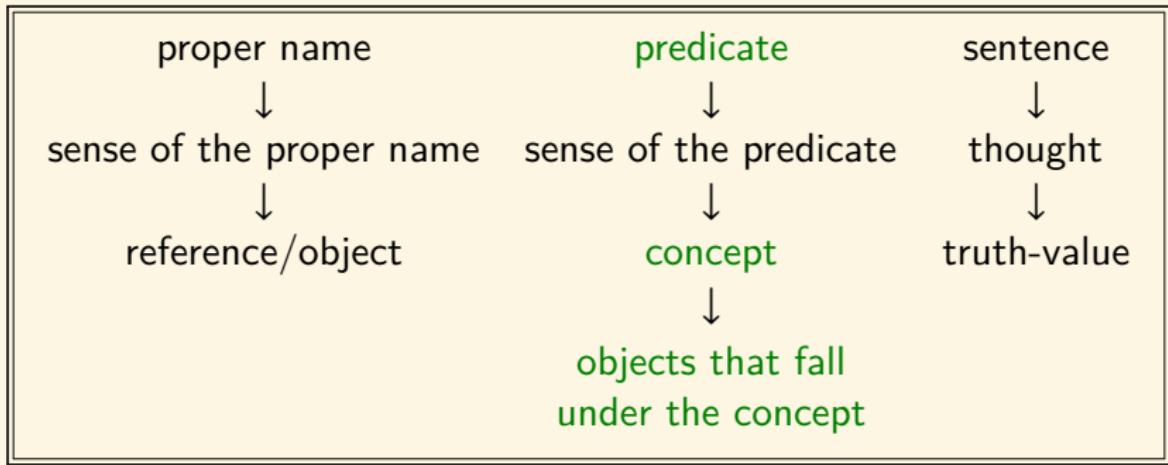


Table: Frege: sense & reference

The intension of an expression is a function from each possible world to the extension of the expression.

Wittgenstein: The limits of my language means the limits of my world.

Structure

A **structure** over the signature is a pair $\mathcal{M} := (M, \llbracket \rrbracket)$, where M is a non-empty set, and $\llbracket \rrbracket$ is a mapping which

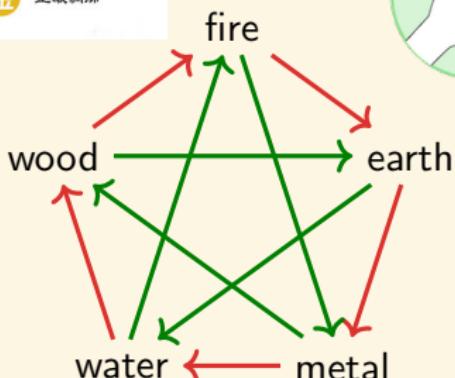
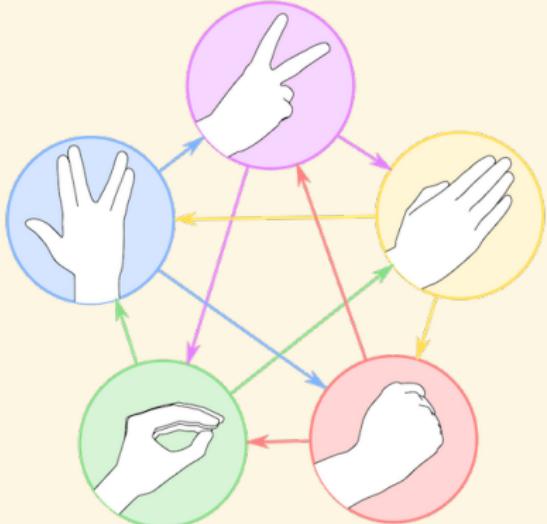
- ▶ assigns to each constant symbol c an element $\llbracket c \rrbracket \in M$,
- ▶ assigns to each function symbol f an n -ary function $\llbracket f \rrbracket : M^n \rightarrow M$,
- ▶ assigns to each predicate symbol P an n -ary relation $\llbracket P \rrbracket \subset M^n$.

We write $\mathcal{M} = (M, \llbracket c \rrbracket, \llbracket f \rrbracket, \llbracket P \rrbracket)$ or $(M, c^{\mathcal{M}}, f^{\mathcal{M}}, P^{\mathcal{M}})$ for convenience.

The ‘elements’ of the structure have no properties other than those relating them to other ‘elements’ of the same structure.



Structure



Interpretation

Definition (Interpretation of Terms)

An interpretation (\mathcal{M}, ν) is a structure \mathcal{M} with a variable assignment $\nu : \text{Var} \rightarrow M$.

We extend ν to $\bar{\nu} : \text{Term} \rightarrow M$ by recursion as follows:

- ▶ $\bar{\nu}(x) := \nu(x)$
- ▶ $\bar{\nu}(c) := \llbracket c \rrbracket$
- ▶ $\bar{\nu}(f(t_1, \dots, t_n)) := \llbracket f \rrbracket(\bar{\nu}(t_1), \dots, \bar{\nu}(t_n))$

$$\begin{array}{ccc} \text{Term} & \xrightarrow{\bar{\nu}} & M \\ f \downarrow & & \downarrow \llbracket f \rrbracket \\ \text{Term} & \xrightarrow{\bar{\nu}} & M \end{array}$$

Tarski's Definition of Truth

Definition (Interpretation of Formulas $\mathcal{M}, v \models A$)

- ▶ $\mathcal{M}, v \models t_1 = t_2$ iff $\bar{v}(t_1) = \bar{v}(t_2)$
- ▶ $\mathcal{M}, v \models P(t_1, \dots, t_n)$ iff $(\bar{v}(t_1), \dots, \bar{v}(t_n)) \in \llbracket P \rrbracket$
- ▶ $\mathcal{M}, v \models \neg A$ iff $\mathcal{M}, v \not\models A$
- ▶ $\mathcal{M}, v \models A \rightarrow B$ iff $\mathcal{M}, v \not\models A$ or $\mathcal{M}, v \models B$
- ▶ $\mathcal{M}, v \models \forall x A$ iff for every $a \in M : \mathcal{M}, v(a/x) \models A$
where

$$v(a/x)(y) := \begin{cases} v(y) & \text{if } y \neq x \\ a & \text{otherwise} \end{cases}$$

or, $\mathcal{M}, v \models \forall x A$ iff for all $v' \sim_x v : \mathcal{M}, v' \models A$.

where $v' \sim_x v$ iff for all $y \neq x : v'(y) = v(y)$.

*To say of what is that it is not, or of what is not that it is, is false,
while to say of what is that it is, or of what is not that it is not, is
true.*

— Aristotle

Tarski's Definition of Truth — another version



An **interpretation** (\mathcal{M}, ν) is a structure \mathcal{M} with $\nu : \text{Var} \rightarrow M$.

We extend ν to $\llbracket \cdot \rrbracket_\nu$ by recursion as follows:

Interpretation of Terms

- $\llbracket x \rrbracket_\nu := \nu(x)$
- $\llbracket c \rrbracket_\nu := \llbracket c \rrbracket$
- $\llbracket f(t_1, \dots, t_n) \rrbracket_\nu := \llbracket f \rrbracket(\llbracket t_1 \rrbracket_\nu, \dots, \llbracket t_n \rrbracket_\nu)$

Remark: Whenever there is no confusion we omit explicit mention of ν .

Interpretation of Formulas

- $\llbracket t_1 = t_2 \rrbracket := \begin{cases} 1 & \text{if } \llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket \\ 0 & \text{otherwise} \end{cases}$
- $\llbracket P(t_1, \dots, t_n) \rrbracket := \begin{cases} 1 & \text{if } (\llbracket t_1 \rrbracket, \dots, \llbracket t_n \rrbracket) \in \llbracket P \rrbracket \\ 0 & \text{otherwise} \end{cases}$
- $\llbracket \neg A \rrbracket := 1 - \llbracket A \rrbracket$
- $\llbracket A \wedge B \rrbracket := \min \{\llbracket A \rrbracket, \llbracket B \rrbracket\}$
- $\llbracket A \vee B \rrbracket := \max \{\llbracket A \rrbracket, \llbracket B \rrbracket\}$
- $\llbracket A \rightarrow B \rrbracket := \max \{1 - \llbracket A \rrbracket, \llbracket B \rrbracket\}$
- $\llbracket A \leftrightarrow B \rrbracket := 1 - |\llbracket A \rrbracket - \llbracket B \rrbracket|$
- $\llbracket \forall x A \rrbracket_\nu := \min_{a \in M} \{\llbracket A \rrbracket_{\nu(a/x)}\}$
- $\llbracket \exists x A \rrbracket_\nu := \max_{a \in M} \{\llbracket A \rrbracket_{\nu(a/x)}\}$

Remark: Whenever there is no confusion we omit explicit mention of ν .

$$\mathcal{M}, \nu \models A \iff \llbracket A \rrbracket_\nu = 1$$

Tarski's Definition of Truth — set-based version

Let $\llbracket \cdot \rrbracket$ map atomic formulas to variable assignments $P(M^{\text{Var}})$.

- $\llbracket t_1 = t_2 \rrbracket := \{v : \llbracket t_1 \rrbracket_v = \llbracket t_2 \rrbracket_v\}$
- $\llbracket P(t_1, \dots, t_k) \rrbracket := \{v : (\llbracket t_1 \rrbracket_v, \dots, \llbracket t_n \rrbracket_v) \in \llbracket P \rrbracket\}$

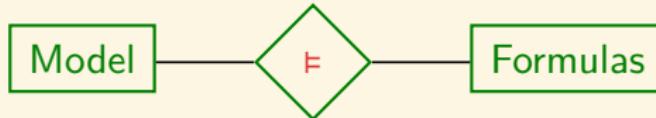
We extend $\llbracket \cdot \rrbracket$ to all wffs by recursion as follows:

1. $\llbracket \neg A \rrbracket := M^{\text{Var}} \setminus \llbracket A \rrbracket$
2. $\llbracket A \wedge B \rrbracket := \llbracket A \rrbracket \cap \llbracket B \rrbracket$
3. $\llbracket A \vee B \rrbracket := \llbracket A \rrbracket \cup \llbracket B \rrbracket$
4. $\llbracket A \rightarrow B \rrbracket := (M^{\text{Var}} \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket$
5. $\llbracket \forall x A \rrbracket := \bigcap_{a \in M} \{v : v(a/x) \in \llbracket A \rrbracket\}$
6. $\llbracket \exists x A \rrbracket := \bigcup_{a \in M} \{v : v(a/x) \in \llbracket A \rrbracket\}$

$$\mathcal{M}, v \models A \iff v \in \llbracket A \rrbracket$$

Tarski's Definition of Truth

- $\mathcal{M}, \nu \models \Gamma$ iff for all $A \in \Gamma : \mathcal{M}, \nu \models A.$
- Γ is **satisfiable** iff there exists \mathcal{M}, ν s.t. $\mathcal{M}, \nu \models \Gamma.$ (Satisfiable)
- $\mathcal{M} \models A$ iff for every variable assignment $\nu : \mathcal{M}, \nu \models A.$ (True)
- $\mathcal{M} \models \Gamma$ iff for all $A \in \Gamma : \mathcal{M} \models A.$
- A structure \mathcal{M} is called a **model** of Γ iff $\mathcal{M} \models \Gamma.$
- $\Gamma \models A$ iff for all $\mathcal{M}, \nu : \mathcal{M}, \nu \models \Gamma \implies \mathcal{M}, \nu \models A.$ (Semantic Entailment)
- $\Gamma \models^* A$ iff for all $\mathcal{M} : \mathcal{M} \models \Gamma \implies \mathcal{M} \models A.$
- A is **valid** $\models A$ iff $\emptyset \models A.$ (Valid)



$$Px \stackrel{?}{\models} \forall x Px$$

$$Px \models^* \forall x Px$$

Natural Language

represents

Formal Language (Syntax)

expresses

Theory (calculus \vdash)

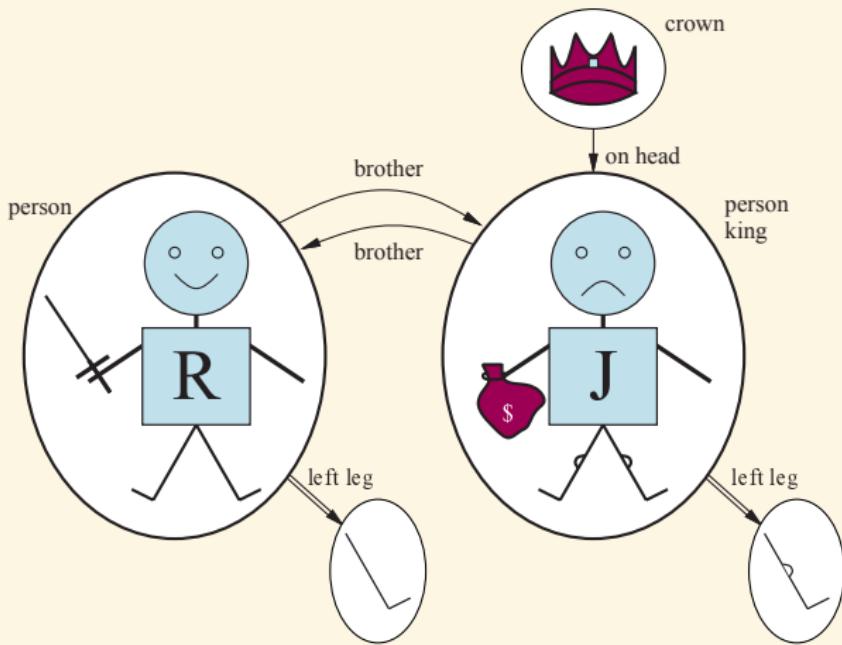
interprets characterizes

Models (semantics \models)

represents

..... semantic gap

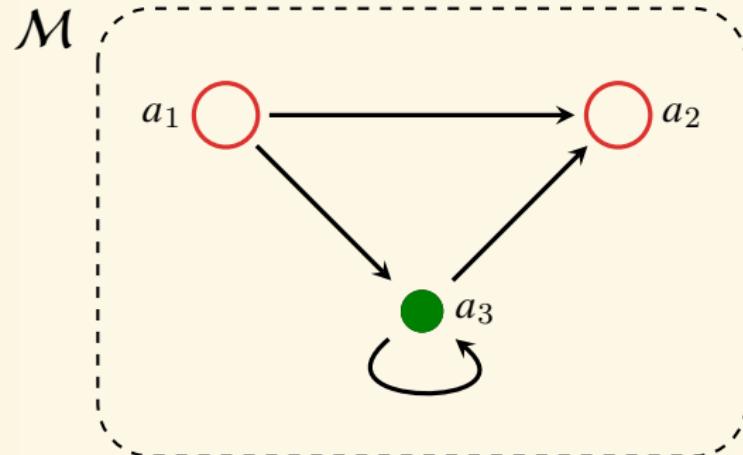
Real World



1. Brother(Richard, John)
2. $\neg \text{King}(\text{Richard}) \rightarrow \text{King}(\text{John})$
3. $\text{King}(\text{John}) \wedge \exists x (\text{Crown}(x) \wedge \text{OnHead}(x, \text{John}))$
4. $\neg \text{Brother}(\text{leftLeg}(\text{Richard}), \text{John})$
5. $\forall x (\text{King}(x) \rightarrow \text{Person}(x))$
6. $\text{length}(\text{leftLeg}(\text{Richard})) > \text{length}(\text{leftLeg}(\text{John}))$

Example

Example



- $M = \{a_1, a_2, a_3\}$
- $\llbracket c \rrbracket = a_3$
- $\llbracket P \rrbracket = \{a_1, a_2\}$
- $\llbracket R \rrbracket = \{(a_1, a_2), (a_1, a_3), (a_3, a_2), (a_3, a_3)\}$

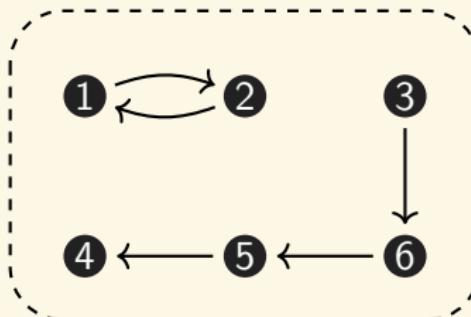
- $\llbracket c \rrbracket$: green point
 - $\llbracket P \rrbracket$: red circles
 - $\llbracket R \rrbracket$: arrows
1. $\mathcal{M} \models^? P c$
 2. $\mathcal{M} \models^? P c \vee Rcc$
 3. $\mathcal{M} \models^? \forall x(Px \vee Rxx)$
 4. $\mathcal{M} \models^? \exists x \forall y(y = x \vee Rxy)$
 5. $\mathcal{M}, v \models^? Rxy \rightarrow Rcy$
where $v(x) = a_1, v(y) = a_3$.

Example

Example

$$\forall xyz(Rxy \wedge Ry\bar{z} \rightarrow Rxz)$$

What arrows are missing to make the following a model?



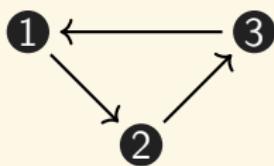
(Add only those arrows that are really needed.)

Counter-Model

A counter-model to $A \models B$ is a model \mathcal{M} such that $\mathcal{M} \models A$, but $\mathcal{M} \not\models B$.

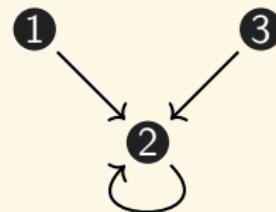
Counter-Model

$$\frac{\forall x \exists y Rxy}{\exists x \forall y Rxy} \times$$



$$\frac{\forall x \exists y Rxy}{\exists y \forall x Rxy} \times$$

$$\frac{\exists y \forall x Rxy}{\forall y \exists x Rxy} \times$$

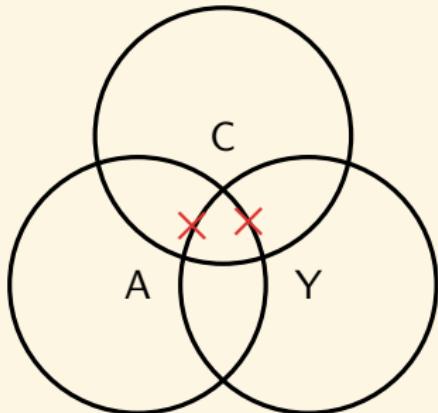


Counter-Model

有些动物是猫
有些猫是黄色的

有些动物是黄色的

$$\frac{\exists x(Ax \wedge Cx) \quad \exists x(Cx \wedge Yx)}{\exists x(Ax \wedge Yx)}$$



$$M = \left\{ \begin{array}{c} \text{A bowl of oranges with one orange peeled open, revealing its segments.} \\ , \\ \text{A white cat wearing glasses and a bow tie, sitting at a lab bench with chemistry glassware and equations in the background.} \\ , \\ \text{A blue donkey standing upright.} \end{array} \right\}$$

A collage of three images. On the left, a fluffy orange cat sits in a white bowl filled with ripe oranges. In the center, a white cat with black-rimmed glasses and a red bow tie sits on a surface, looking slightly to the side. On the right, a chalkboard displays mathematical notation related to category theory, specifically monads, including terms like "MONADS ARE JUST MONOIDS IN THE CATEGORY OF ENDOFUNCTORS", "H", "F", "G", "P", and "CH'".

$$[Y] = \left\{ \begin{array}{c} \text{orange slices} \\ \text{cat} \end{array} \right\}$$

Is there a finite counter-model?

Everybody loves somebody

Everybody loves all persons who are loved by his loved ones

There is at least a pair of persons who love each other

Exercise (Counter-Model)

Give a counter-model for

$$\frac{\forall x \exists y Rxy \quad \forall xyz(Rxy \wedge Ryx \rightarrow Rxz)}{\exists xy(Rxy \wedge Ryx)} \times$$

$$\frac{\forall x \exists y Rxy \quad \forall xyz(Rxy \wedge Ryx \rightarrow Rxz)}{\exists x Rxx} \times$$

$(\mathbb{Z}, <)$

Lewis Carroll — Alice's Adventures in Wonderland



- ▶ The March Hare: You should say what you mean.
- ▶ Alice: I mean what I say — that's the same thing.
- ▶ The Mad Hatter: Not the same thing a bit! You might just as well say that "I see what I eat" is the same thing as "I eat what I see"!
- ▶ The March Hare: You might just as well say that "I like what I get" is the same thing as "I get what I like"!

$$\forall x(P \rightarrow Q) \not\equiv \forall x(Q \rightarrow P)$$

Mistakes to Avoid

$$\forall x(Bx \rightarrow Sx)$$

$$\exists x(Bx \wedge Sx)$$

- ▶ $\forall x(Bx \wedge Sx)$
Everyone is a boy and everyone is smart.
- ▶ $\exists x(Bx \rightarrow Sx)$
It is true if there is anyone who is not a boy.

Coincidence Lemma

Lemma (Coincidence Lemma)

Assume $\nu_1, \nu_2 : \text{Var} \rightarrow M$, and for all $x \in \text{Fv}(A) : \nu_1(x) = \nu_2(x)$. Then

$$\mathcal{M}, \nu_1 \models A \iff \mathcal{M}, \nu_2 \models A$$

- ▶ If A is a sentence, then either $\mathcal{M} \models A$ or $\mathcal{M} \models \neg A$.
- ▶ $\mathcal{M} \models A \implies \mathcal{M} \models \forall x A$
- ▶ **Notation:** If $\text{Fv}(A) \subset \{x_1, \dots, x_n\}$, then we write $\mathcal{M} \models A[a_1, \dots, a_n]$ to mean $\mathcal{M}, \nu \models A$ for some (equivalently any) assignment ν s.t. $\nu(x_i) = a_i$ for $1 \leq i \leq n$.

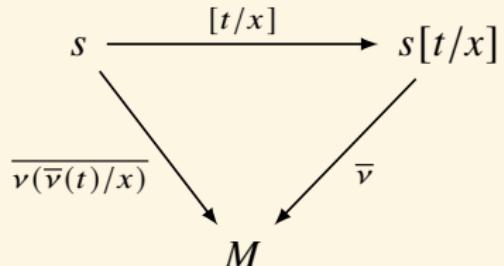
Substitution Lemma



Lemma (Substitution Lemma)

- $v(s[t/x]) = v(v(t)/x)(s)$
- If the term t is substitutable for the variable x in the wff A , then

$$\mathcal{M}, v \models A[t/x] \iff \mathcal{M}, v(v(t)/x) \models A$$



$$\mathcal{L}_M := \mathcal{L} \cup C_M \text{ where } C_M := \{c_a : a \in M\}$$

$$\mathcal{M}, v \models A[c_a/x] \iff \mathcal{M}, v(a/x) \models A$$

We abbreviate $\mathcal{M}, v \models A[c_a/x]$ by $\mathcal{M}, v \models A[a]$.

$$\mathcal{M}, v \models \forall x A \iff \text{for every } a \in M : \mathcal{M}, v \models A[a]$$

Equivalent Replacement

Lemma

Suppose $B \in \text{Sub}(A)$, and $A(C//B)$ arises from A by replacing one or more occurrences of B by C . Then

$$\frac{B \leftrightarrow C}{A \leftrightarrow A(C//B)}$$

Alphabetic Variant



Definition (Alphabetic Variant)

If $y \notin \text{Fv}(A)$, and y is substitutable for x in A , we say that $\forall y A[y/x]$ is an alphabetic variant of $\forall x A$.

Theorem

If $\forall y A[y/x]$ is an alphabetic variant of $\forall x A$, then

$$\models \forall x A \leftrightarrow \forall y A[y/x]$$

If $y \notin \text{Fv}(A)$, then $A[y/x][x/y] = A$.

- **Convention:** When we write $A[t/x]$ we assume that t is substitutable for x in A . — *For any formula A and a finite number of variables y_1, \dots, y_n (occurring in t), we can always find a logically equivalent alphabetic variant A^* of A s.t. y_1, \dots, y_n do not occur bound in A^* .*

Equality & Equivalence

Lemma

Suppose $\text{Var}(t) \cup \text{Var}(s) \subset \{x_1, \dots, x_n\}$, and A^* arises from the wff A by replacing one occurrence of t in A by s . Then

$$\vdash \forall x_1 \dots x_n (t = s) \rightarrow (A \leftrightarrow A^*)$$
$$\mathcal{M} \models t = s \implies \mathcal{M} \models A \leftrightarrow A^*$$

Lemma

Suppose $\text{Fv}(B) \cup \text{Fv}(C) \subset \{x_1, \dots, x_n\}$, and A^* arises from the wff A by replacing one occurrence of B in A by C . Then

$$\vdash \forall x_1 \dots x_n (B \leftrightarrow C) \rightarrow (A \leftrightarrow A^*)$$
$$\mathcal{M} \models B \leftrightarrow C \implies \mathcal{M} \models A \leftrightarrow A^*$$

Remark:

- $\vdash \forall x (Px \leftrightarrow Qx) \rightarrow (\forall x Px \leftrightarrow \forall x Qx)$
- ✗ $(Px \leftrightarrow Qx) \rightarrow (\forall x Px \leftrightarrow \forall x Qx)$
- $\mathcal{M}, \nu \models t = s \not\Rightarrow \mathcal{M}, \nu \models A \leftrightarrow A^*$
- $\mathcal{M}, \nu \models B \leftrightarrow C \not\Rightarrow \mathcal{M}, \nu \models A \leftrightarrow A^*$

$$B = Px, \quad C = Py, \quad A = \forall x Px, \quad A^* = \forall x Py$$

How to Check Validity? — Example

$$\models \exists x \forall y Rxy \rightarrow \forall y \exists x Rxy$$

Proof.

Assume $\mathcal{M}, \nu \models \exists x \forall y Rxy$.

Then there exists $a \in M$ s.t.

$$\mathcal{M}, \nu(a/x) \models \forall y Rxy$$

For all $b \in M$,

$$\mathcal{M}, \nu(a/x)(b/y) \models Rxy$$

Since

$$\nu(a/x)(b/y) = \nu(b/y)(a/x)$$

it follows that

$$\mathcal{M}, \nu(b/y) \models \exists x Rxy$$

Therefore $\mathcal{M}, \nu \models \forall y \exists x Rxy$.

How to Check Validity? — Example



$$\boxed{\forall x A \rightarrow A[t/x]}$$

$\mathcal{M}, \nu \models \forall x A \implies \text{for all } a \in M : \mathcal{M}, \nu(a/x) \models A \implies \mathcal{M}, \nu(\nu(t)/x) \models A$
According to Substitution Lemma, $\mathcal{M}, \nu \models A[t/x]$.

$$\boxed{\forall x(B \rightarrow A) \rightarrow (\exists x B \rightarrow A) \quad \text{where } x \notin \text{Fv}(A)}$$

Assume $\mathcal{M}, \nu \models \exists x B$ and $\mathcal{M}, \nu \not\models A$. Then there exists $a \in M$ s.t. $\mathcal{M}, \nu(a/x) \models B$. According to Coincidence Lemma and $x \notin \text{Fv}(A)$, we have $\mathcal{M}, \nu(a/x) \not\models A$. Therefore $\mathcal{M}, \nu(a/x) \not\models B \rightarrow A$. This contradicts $\mathcal{M}, \nu \models \forall x(B \rightarrow A)$.

$$\boxed{(\exists x B \rightarrow A) \rightarrow \forall x(B \rightarrow A) \quad \text{where } x \notin \text{Fv}(A)}$$

$\mathcal{M}, \nu \models \exists x B \rightarrow A \implies \mathcal{M}, \nu \not\models \exists x B \text{ or } \mathcal{M}, \nu \models A$.

If $\mathcal{M}, \nu \not\models \exists x B$, then for all $a \in M$, $\mathcal{M}, \nu(a/x) \not\models B$. It follows that $\mathcal{M}, \nu(a/x) \models B \rightarrow A$. Therefore $\mathcal{M}, \nu \models \forall x(B \rightarrow A)$.

If $\mathcal{M}, \nu \models A$, then according to Coincidence Lemma and $x \notin \text{Fv}(A)$, for all $a \in M$, $\mathcal{M}, \nu(a/x) \models A$. It follows that $\mathcal{M}, \nu(a/x) \models B \rightarrow A$.
Therefore $\mathcal{M}, \nu \models \forall x(B \rightarrow A)$.

How to Check Validity? — Example

$$A[t/x] \leftrightarrow \forall x(x = t \rightarrow A) \quad \text{where } x \notin \text{Var}(t)$$

$$A[t/x] \rightarrow \forall x(x = t \rightarrow A) \quad \text{where } x \notin \text{Var}(t)$$

$$\mathcal{M}, \nu \models A[t/x] \implies \mathcal{M}, \nu(\nu(t)/x) \models A$$

Assume $\nu(t) = b$. Then for all $a \in M$, either $a = b$ or $a \neq b$.

If $a = b$, then $\mathcal{M}, \nu(a/x) \models A$.

If $a \neq b$, then $\nu(a/x)(x) = a \neq b = \nu(t) = \nu(a/x)(t)$. So $\mathcal{M}, \nu(a/x) \not\models x = t$.

Therefore we have $\mathcal{M}, \nu(a/x) \models x = t \rightarrow A$ for all $a \in M$.

$$\forall x(x = t \rightarrow A) \rightarrow A[t/x] \quad \text{where } x \notin \text{Var}(t)$$

$$\mathcal{M}, \nu \models \forall x(x = t \rightarrow A) \implies \text{for all } a \in M : \mathcal{M}, \nu(a/x) \models x = t \rightarrow A$$

Let $\nu(t) = b$. Then $\mathcal{M}, \nu(b/x) \models x = t \rightarrow A$.

$$\nu(b/x)(x) = b = \nu(t) = \nu(b/x)(t) \implies \mathcal{M}, \nu(b/x) \models x = t$$

Therefore $\mathcal{M}, \nu(b/x) \models A$. By Substitution Lemma, $\mathcal{M}, \nu \models A[t/x]$.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

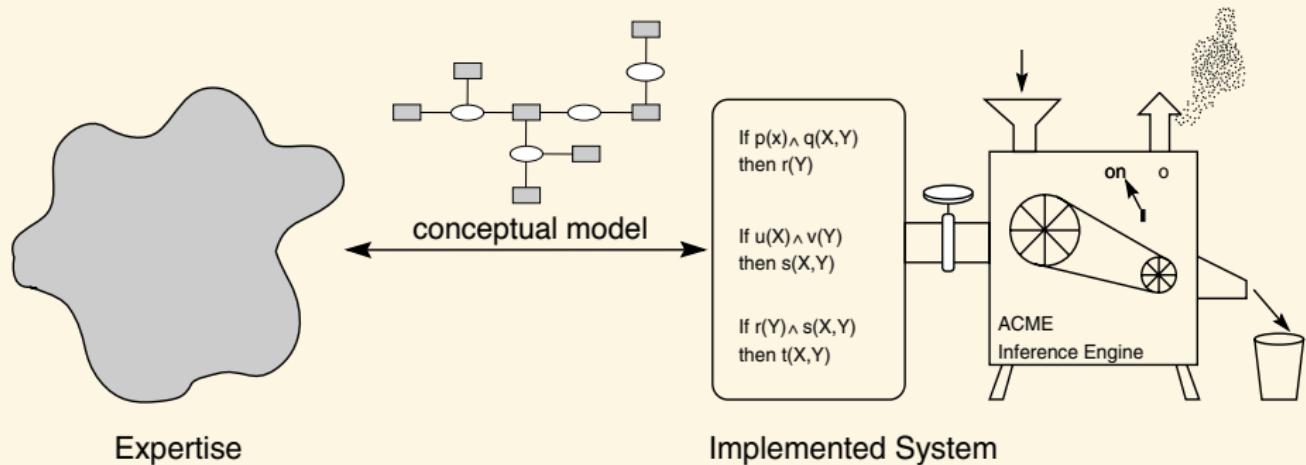
Quantum Computing

Answers to the Exercises

References

1436

Formal Systems



- ▶ Hilbert System
- ▶ Tree Method
- ▶ Natural Deduction
- ▶ Sequent Calculus
- ▶ Resolution
- ▶ ...

Hilbert System = Axiom + Inference Rule

Axiom Schema

1. $A \rightarrow B \rightarrow A$
2. $(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
3. $(\neg A \rightarrow \neg B) \rightarrow (\neg A \rightarrow B) \rightarrow A$
4. $\forall x(A \rightarrow B) \rightarrow \forall x A \rightarrow \forall x B$
5. $\forall x A \rightarrow A[t/x]$ where t is substitutable for x in A .
6. $A \rightarrow \forall x A$ where $x \notin \text{Fv}(A)$.
7. $x = x$
8. $x = y \rightarrow A \rightarrow A(y//x)$ where A is atomic and $A(y//x)$ is obtained from A by replacing x in one or more places by y .
9. $\forall x_1 \dots x_n A$ where $n \geq 0$ and A is any axiom of the preceding groups.

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} [\text{MP}]$$

Example

Theorem

$$A \vdash \exists x A$$

Proof.

1. $(\forall x \neg A \rightarrow \neg A) \rightarrow A \rightarrow \neg \forall x \neg A$ Tautology
2. $\forall x \neg A \rightarrow \neg A$ A5
3. $A \rightarrow \neg \forall x \neg A$ 1,2 MP
4. A Premise
5. $\neg \forall x \neg A$ 3,4 MP
6. $\exists x A$ Definition of \exists

Deduction Theorem



Theorem (Deduction Theorem1)

$$\Gamma, A \vdash B \implies \Gamma \vdash A \rightarrow B$$

Inference Rule

$$\frac{A}{\forall x A} [G]$$

What if we remove Axiom9 and add the rule of generalization [G] to Hilbert System?

Theorem (Deduction Theorem2)

If $\Gamma, A \vdash B$, where the rule of generalization is not applied to the free variables of A, then $\Gamma \vdash A \rightarrow B$.

Meta-properties

- $\models A[B_1/p_1, \dots, B_n/p_n]$ where $A \in \mathcal{L}^0$, $B_1, \dots, B_n \in \mathcal{L}^1$. tautology
- reductio ad absurdum / proof by contradiction

$$\frac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$$
$$\frac{\Gamma, \neg A \vdash B \quad \Gamma, \neg A \vdash \neg B}{\Gamma \vdash A}$$

- contraposition

$$\frac{\Gamma, A \vdash \neg B}{\Gamma, B \vdash \neg A}$$

- substitution

$$\frac{t = s}{r[t/x] = r[s/x]}$$
$$\frac{t = s}{A[t/x] \leftrightarrow A[s/x]}$$

- equivalent replacement

$$\frac{B \leftrightarrow C}{A \leftrightarrow A(C // B)}$$

where $A(C // B)$ arises from A by replacing one or more occurrences of B in A by C .

Meta-properties

$$\frac{\Gamma, A[t/x] \vdash B}{\Gamma, \forall x A \vdash B} \forall L$$

$$\frac{\Gamma, A \vdash B \quad x \notin \text{Fv}(\Gamma, B)}{\Gamma, \exists x A \vdash B} \exists L$$

$$\frac{\Gamma, A[y/x] \vdash B \quad y \notin \text{Fv}(\Gamma, \exists x A, B)}{\Gamma, \exists x A \vdash B} \exists L$$

$$\frac{\Gamma, A[a/x] \vdash B \quad a \notin \text{Cst}(\Gamma, \exists x A, B)}{\Gamma, \exists x A \vdash B} \exists L$$

$$\frac{\forall x A}{\forall y A[y/x]} \text{ alphabetic variant}$$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A} \exists R$$

$$\frac{\Gamma \vdash A \quad x \notin \text{Fv}(\Gamma)}{\Gamma \vdash \forall x A} \forall R$$

$$\frac{\Gamma \vdash A[y/x] \quad y \notin \text{Fv}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A} \forall R$$

$$\frac{\Gamma \vdash A[a/x] \quad a \notin \text{Cst}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A} \forall R$$

Theorem (Existence of Alphabetic Variants)

Let A be a formula, t a term, and x a variable. Then we can find a formula A^* which differs from A only in the choice of quantified variables s.t.

1. $\vdash A \leftrightarrow A^*$
2. t is substitutable for x in A^* .

Proof Tactics



- ► $\Gamma \vdash A \rightarrow B \iff \Gamma, A \vdash B$
- ∀
 - 1. if $x \notin \text{Fv}(\Gamma)$, $\Gamma \vdash \forall x A \iff \Gamma \vdash A$
 - 2. if $x \in \text{Fv}(\Gamma)$,
 $\Gamma \vdash \forall x A \iff \Gamma \vdash \forall y A[y/x] \iff \Gamma \vdash A[y/x]$ for some new y .
- ¬
 - 1. ($\neg \rightarrow$) $\Gamma \vdash \neg(A \rightarrow B) \iff \Gamma \vdash A \ \& \ \Gamma \vdash \neg B$
 - 2. ($\neg\neg$) $\Gamma \vdash \neg\neg A \iff \Gamma \vdash A$
 - 3. ($\neg\forall$) $\Gamma \vdash \neg\forall x A \iff \Gamma \vdash \neg A[t/x]$
Unfortunately this is not always possible. Try contraposition, reductio ad absurdum or prove by contradiction...

Existence Proofs — Constructive vs Nonconstructive

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A}$$

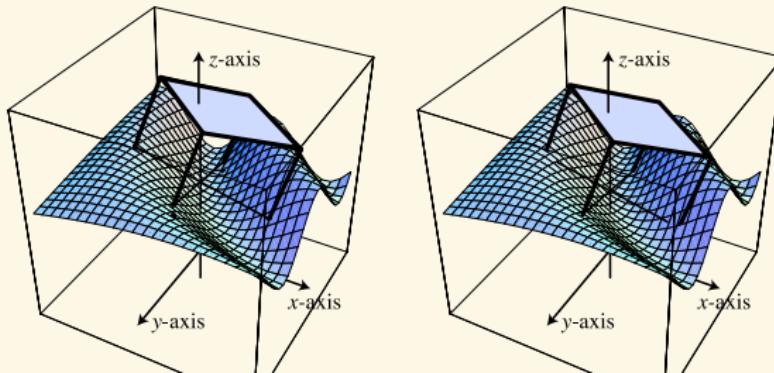
$$\frac{\Gamma, \forall x \neg A \vdash \perp}{\Gamma \vdash \exists x A}$$

Example (There exist two irrational numbers x, y s.t. x^y is rational.)

$$x := \sqrt{2}$$

$$y := \log_2 9$$

Example (The wobbly table problem)

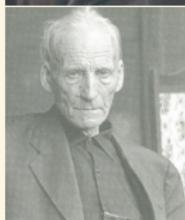


Intuitionism

- ▶ Impredicativism. (*Poincaré, Russell*)
Vicious circle principle: No entity can be defined only in terms of a totality to which this entity belongs.



- ▶ **Intuitionism** Logic \leadsto Mathematics \leadsto Mental construction.
(Kronecker, *Brouwer, Heyting, Kolmogorov, Weyl*)
 - ▶ Potential infinity vs actual infinity.
 - ▶ To be is to be constructed by intuition.
 - ▶ Law of excluded middle. \times
 - ▶ Non-constructive proof. \times



(There exist two irrational numbers x and y s.t. x^y is rational.)

$$\sqrt{2} \quad \log_2 9$$



"God created the integers, all the rest is the work of man."

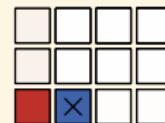
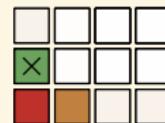
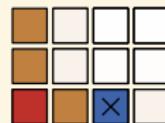
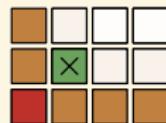
- ▶ **Constructive Mathematics.** (Bishop, *Martin-Löf*)



Existence Proofs — Constructive vs Nonconstructive

The Chomp Game

The chocolate at the bottom left is poisoned. Two players take turns choosing a square and eating the chosen square and all the squares to the right and above it.



Theorem

The player 1 has a winning strategy.

Proof.

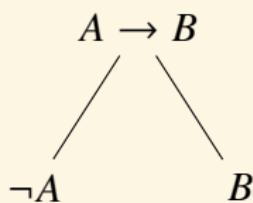
Suppose that player 2 has a winning strategy. Let player 1 start by selecting the top right corner. By assumption, player 2 has a strategy, and therefore a move, that is winning. But player 1 could just as well have started with that move.

Tree Method for Propositional Logic ❤

$$\neg\neg A$$



$$A \rightarrow B$$



$$\neg(A \rightarrow B)$$



$$A$$

$$\neg B$$

$$A \wedge B$$



$$A$$

$$B$$

$$\neg(A \wedge B)$$



$$A \vee B$$



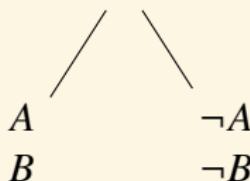
$$\neg(A \vee B)$$



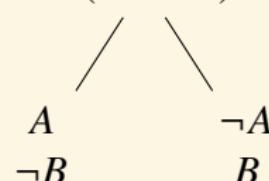
$$\neg A$$

$$\neg B$$

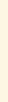
$$A \leftrightarrow B$$



$$\neg(A \leftrightarrow B)$$

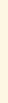
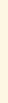


Tree Method for Predicate Logic — Ground Tree ❤

 $\forall x A$  $A[t/x]$ $\exists x A \checkmark$ $A(a)$

where t is a ground term.

where a is a new constant.

 $\neg \forall x A \checkmark$  $\exists x \neg A$ $\neg \exists x A \checkmark$  $\forall x \neg A$

Tree Method for Predicate Logic ❤

$$\begin{array}{c} A(x) \\ x = y \\ | \\ A(y//x) \end{array}$$

$$\begin{array}{c} A(x) \\ y = x \\ | \\ A(y//x) \end{array}$$

where $A(y//x)$ arises from the wff $A(x)$ by replacing one or more occurrences of x by y .

$$\begin{array}{c} x \neq x \\ \times \end{array}$$

Deduction & Proof Tactics

Definition (Deduction)

$A_1, \dots, A_n \vdash B$ iff there exists a closed tree from $\{A_1, \dots, A_n, \neg B\}$.

Proof Tactics

- ▶ Try to apply “non-branching” rules first, in order to reduce the number of branches.
- ▶ Try to close off branches as quickly as possible.
- ▶ Deal with negated quantifiers first.
- ▶ Instantiate existentials before universals.

Soundness & Completeness

Theorem (Soundness Theorem)

If the tree closes, the set is unsatisfiable.

Theorem (Completeness Theorem)

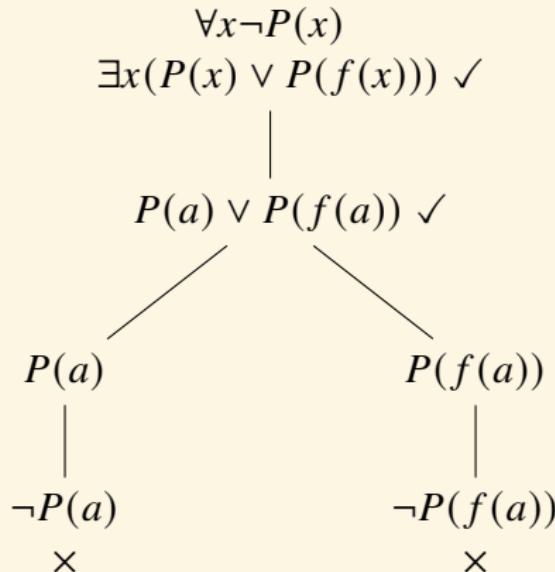
If a set is unsatisfiable, there exists a closed tree from it.

$$A_1, \dots, A_n \vdash B \iff A_1, \dots, A_n \vDash B$$

Remark: If an inference with predicate formulas is not valid and its counterexample is an infinite model, the tree will not find it. The tree method can't generate every counterexample of an invalid inference in predicate logic.

Example — Ground Tree

$\{\forall x \neg P(x), \exists x (P(x) \vee P(f(x)))\}$ is unsatisfiable.



Example — Ground Tree

There is someone such that if he is drinking, then everyone is drinking.

$$\vdash \exists x(A(x) \rightarrow \forall x A(x))$$

$$\neg \exists x(A(x) \rightarrow \forall x A(x))$$



$$\neg(A(a) \rightarrow \forall x A(x)) \checkmark$$

$$A(a)$$

$$\neg \forall x A(x) \checkmark$$

$$\neg A(b)$$



$$\neg(A(b) \rightarrow \forall x A(x)) \checkmark$$

$$A(b)$$

$$\neg \forall x A(x)$$

X

Theorems / Valid Formulas ♡

$$\forall x A \rightarrow A[t/x]$$

$$\neg \forall x A \leftrightarrow \exists x \neg A$$

$$\forall x(A \wedge B) \leftrightarrow \forall x A \wedge \forall x B$$

$$\exists x(A \vee B) \leftrightarrow \exists x A \vee \exists x B$$

$$\forall x(A \rightarrow B) \rightarrow \forall x A \rightarrow \forall x B$$

$$\forall x(A \leftrightarrow B) \rightarrow (\forall x A \leftrightarrow \forall x B)$$

$$\forall x \forall y A \leftrightarrow \forall y \forall x A$$

$$\exists x \forall y A \rightarrow \forall y \exists x A$$

$$(\forall x A \rightarrow \exists x B) \leftrightarrow \exists x(A \rightarrow B)$$

$$\exists x(A \rightarrow \forall x A)$$

$$A[t/x] \rightarrow \exists x A$$

$$\neg \exists x A \leftrightarrow \forall x \neg A$$

$$\forall x A \vee \forall x B \rightarrow \forall x(A \vee B)$$

$$\exists x(A \wedge B) \rightarrow \exists x A \wedge \exists x B$$

$$\forall x(A \rightarrow B) \rightarrow \exists x A \rightarrow \exists x B$$

$$\exists x \exists y A \leftrightarrow \exists y \exists x A$$

$$(\exists x A \rightarrow \forall x B) \leftrightarrow \forall x(A \rightarrow B)$$

Theorems / Valid Formulas ❤

$x \notin \text{Fv}(A)$:

$$A \leftrightarrow \forall x A$$

$$\forall x(A \vee B) \leftrightarrow A \vee \forall x B$$

$$\forall x(A \wedge B) \leftrightarrow A \wedge \forall x B$$

$$\forall x(A \rightarrow B) \leftrightarrow (A \rightarrow \forall x B)$$

$$\forall x(B \rightarrow A) \leftrightarrow (\exists x B \rightarrow A)$$

$$A \leftrightarrow \exists x A$$

$$\exists x(A \vee B) \leftrightarrow A \vee \exists x B$$

$$\exists x(A \wedge B) \leftrightarrow A \wedge \exists x B$$

$$\exists x(A \rightarrow B) \leftrightarrow (A \rightarrow \exists x B)$$

$$\exists x(B \rightarrow A) \leftrightarrow (\forall x B \rightarrow A)$$

Remark

$$(\forall x B \rightarrow A) \leftrightarrow \exists x (B \rightarrow A)$$

$$\text{diam}(X) := \sup \{|x - y| : x, y \in X\}$$

$$(\forall x \in X |x| \leq 1) \rightarrow \text{diam}(X) \leq 2$$

↑?

$$\exists x \in X (|x| \leq 1 \rightarrow \text{diam}(X) \leq 2) ?$$

Theorems / Valid Formulas ❤

$$t = t$$

$$t = s \rightarrow s = t$$

$$t = s \rightarrow s = r \rightarrow t = r$$

$$t_1 = s_1 \rightarrow \dots \rightarrow t_n = s_n \rightarrow f(t_1, \dots, t_n) = f(s_1, \dots, s_n)$$

$$t_1 = s_1 \rightarrow \dots \rightarrow t_n = s_n \rightarrow (P(t_1, \dots, t_n) \leftrightarrow P(s_1, \dots, s_n))$$

$$t = s \rightarrow r[t/x] = r[s/x]$$

$$t = s \rightarrow (A[t/x] \leftrightarrow A[s/x])$$

Theorems / Valid Formulas ♡

$x \notin \text{Var}(t)$:

$$\exists x(x = t)$$

$$A[t/x] \leftrightarrow \exists x(x = t \wedge A)$$

$$A[t/x] \leftrightarrow \forall x(x = t \rightarrow A)$$

$y \notin \text{Var}(A)$:

$$\forall x(A \leftrightarrow \exists y(y = x \wedge A[y/x]))$$

$$\forall x(A \leftrightarrow \forall y(y = x \rightarrow A[y/x]))$$

Exercises — Tree Method — Now it's your turn ♡

1. $\neg \exists x Px \vdash \forall x Px \rightarrow Qx$
2. $\exists x \forall y (P(y) \rightarrow y = x), \forall x P(f(x)) \vdash \exists x (x = f(x))$
3. $\exists x (Px \wedge \forall y (Py \rightarrow y = x) \wedge Qx) \leftrightarrow \exists x \forall y ((Py \leftrightarrow y = x) \wedge Qx)$
4. $\exists x (Px \wedge \forall y (Py \rightarrow y = x)), \exists x (Qx \wedge \forall y (Qy \rightarrow y = x)), \neg \exists x (Px \wedge Qx) \vdash \exists xy (x \neq y \wedge (Px \vee Qx) \wedge (Py \vee Qy) \wedge \forall z (Pz \vee Qz \rightarrow z = x \vee z = y))$

*54 · 43. $\vdash .\alpha, \beta \in 1. \supset: \alpha \cap \beta = \Lambda. \equiv .\alpha \cup \beta \in 2$

Dem.

$$\vdash . * 54 \cdot 26. \supset \vdash .\alpha = t'x.\beta = t'y. \supset: \alpha \cup \beta \in 2. \equiv x \neq y.$$

$$[*51 \cdot 231] \quad \equiv .t'x \cap t'y = \Lambda.$$

$$[*13 \cdot 12] \quad \equiv .\alpha \cap \beta = \Lambda \quad (1)$$

$$\vdash .(1). * 11 \cdot 11 \cdot 35. \supset$$

$$\vdash .(\exists x, y).\alpha = t'x.\beta = t'y. \supset: \alpha \cup \beta \in 2. \equiv .\alpha \cap \beta = \Lambda \quad (2)$$

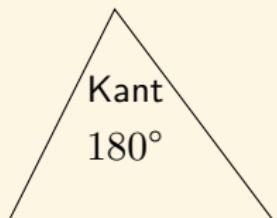
$$\vdash .(2). * 11 \cdot 54. * 52 \cdot 1. \supset \vdash .Prop$$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

$$\exists_1 x Px \wedge \exists_1 x Qx \wedge \neg \exists x (Px \wedge Qx) \rightarrow \exists_2 x (Px \vee Qx)$$

Philosophy of Math: is math synthetic a priori?

- ▶ Descartes: we can be certain about how things seem to us from the inside; but how to build up to the external world?
- ▶ Hume: we can't. (i) Knowledge of the external world requires knowledge of causation. (ii) Causal statements are synthetic, and so can be known only a posteriori. (iii) Causal statements can't be known a posteriori, because we don't perceive causation itself and can't noncircularly argue that the future will resemble the past.
- ▶ Kant: we can know facts about causation a priori, even though they are synthetic, because facts about causation are constituted partly by how the world is in itself, and partly by our minds' operation; and we can know a priori the rules by which our mind operates.



- ▶ Geometry — pure intuition of space
- ▶ Arithmetic — pure intuition of time $1 + 1 = 2$

Kant Mathematics is synthetic a priori.
Frege Mathematics is analytic.

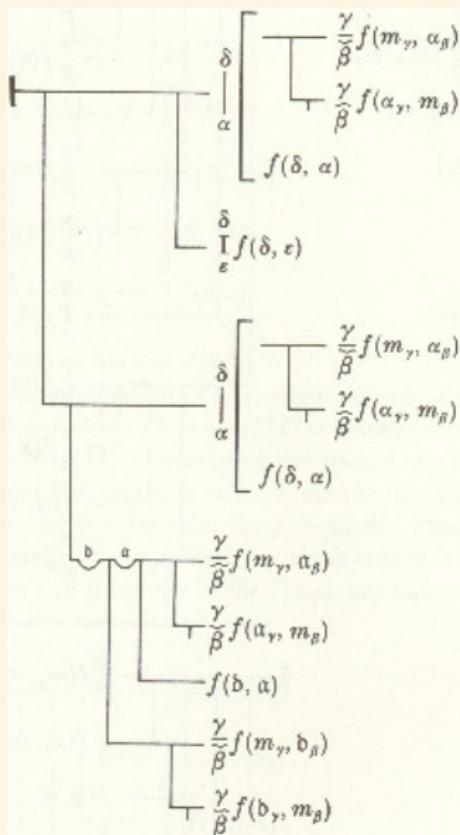
- ▶ The proof that all pure mathematics, including Geometry, is nothing but formal logic, is a fatal blow to the Kantian philosophy.
- ▶ Kant, rightly perceiving that Euclid's propositions could not be deduced from Euclid's axioms without the help of the figures, invented a theory of knowledge to account for this fact.
- ▶ Kant invented the synthetic *a priori* only in order to compensate for a deficient logic.
- ▶ For it is not true, as Kant urged, that intuition is a pure *a priori* means of knowledge, but rather that it is force of habit rooted in psychological inertia.
- ▶ Obviousness is always the enemy to correctness. Hence we invent some new and difficult symbolism.⁸

— Bertrand Russell

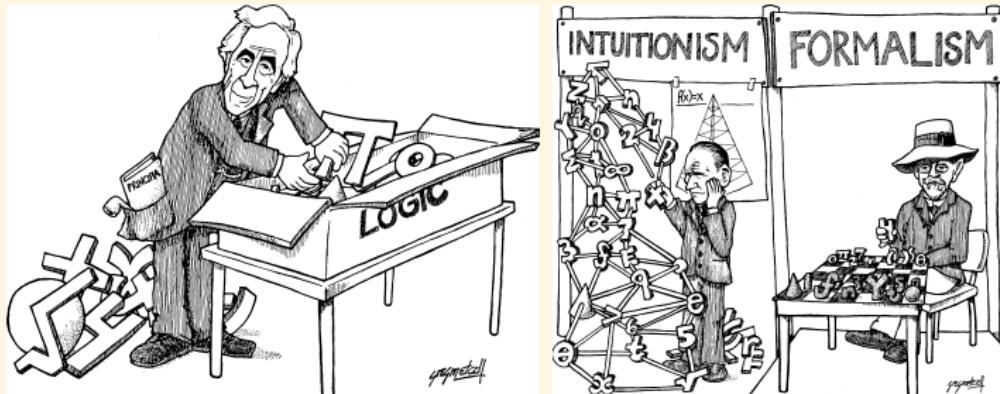
⁸Bertrand Russell: "Mathematics and the Metaphysicians". Reprinted in *Mysticism and Logic, and Other Essays*.

Frege

- ▶ Arithmetic laws are analytic judgements, and hence a priori. Arithmetic is a developed logic. The application of arithmetic to natural science is logical processing of observed facts; calculation is deduction.
- ▶ If the task of philosophy is to break the domination of words over the human mind by freeing thought from the mask of existing means of expression, then my ideography would become a useful instrument in the hands of philosophers.
- ▶ Every good mathematician is at least half a philosopher, and every good philosopher is at least half a mathematician.



Philosophy of Math: Logicism/Intuitionism/Formalism



Logicism	Intuitionism	Formalism
<u>Mathematics</u> Logic	Logic <u>Mathematics</u> Mind	<u>Mathematics</u> Game
Realism	Conceptualism	Nominalism

David Hilbert 1862-1943

- **Formal Axiomatization** of Geometry.

The consistency of geometry relative to arithmetic.

(Klein: Non-Euclidean relative to Euclidean)

(natural/integer/rational/real/complex)

- Hilbert's 23/24 problems. (1st, 2nd, 10th, 24th)

- Meta-mathematics — Proof Theory.

- **Formalism** Mathematics \leadsto Symbolic Game.

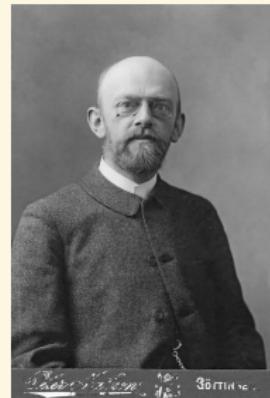
- Axioms are the implicit definitions of the concepts.

- One must be able to say 'table, chair, beer-mug' each time in place of 'point, line, plane'.

- Mathematics is a game played according to certain rules with meaningless marks on paper.

- We hear within us the perpetual call: There is the problem. Seek its solution.
You can find it by pure reason, for in mathematics there is *no ignorabimus*.

- We must know; We will know.



Formal Axiomatization

One of the goals of all scientific inquiry is to achieve precision and clarity of a body of knowledge. This “precision and clarity” means:

- ▶ all assumptions of a given theory are stated explicitly;
- ▶ the language is designed carefully by choosing some basic notions and defining others in terms of these ones;
- ▶ the theory contains some axioms — all other claims of the theory follow from the axioms.

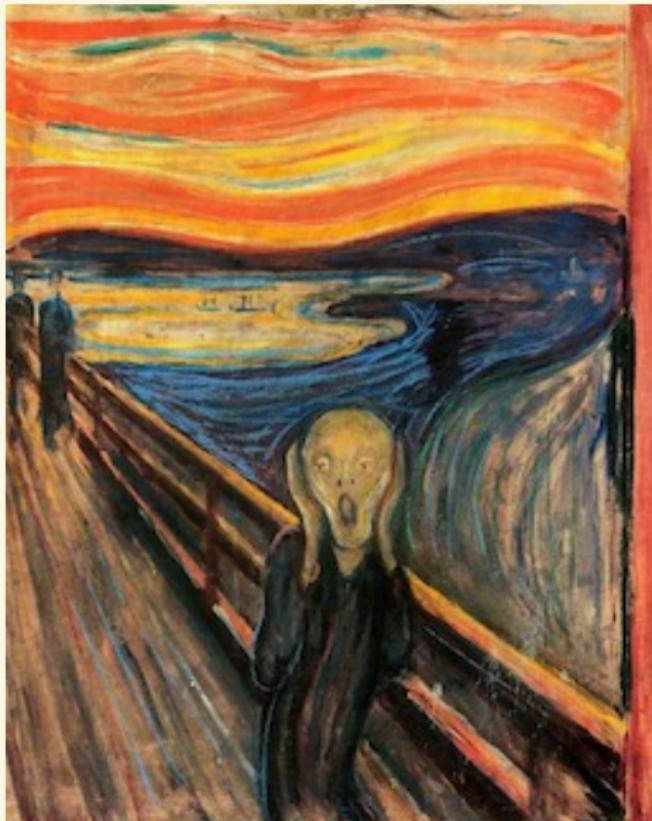
1. 我是一个神 $0 \in \mathbb{N}$
2. 每个神的兽也是一个神 $\forall n \in \mathbb{N} : s(n) \in \mathbb{N}$
3. 我不是任何神的兽 $\forall n \in \mathbb{N} : s(n) \neq 0$
4. 不同的神有不同的兽 $\forall mn \in \mathbb{N} : s(m) = s(n) \rightarrow m = n$
5. 如果我有 X , 且每个神都把 X 递送给它的兽, 那么所有的神都有 X

$$\forall X [0 \in X \wedge \forall n (n \in X \rightarrow s(n) \in X) \rightarrow \forall n \in \mathbb{N} (n \in X)]$$

— acquire knowledge about the actual world via
a detour through the ideal world

1. Formalization & Axiomatization (Richness): Formalize and axiomatize (recursively) the elementary logic L, the “finitistic” mathematics F (which is concerned with the ‘actual world’) and the “infinitistic” mathematics T (which is concerned with the ‘ideal world’).
2. Independence: the axioms should be “independent” of one another.
3. Completeness: (1) all valid logical statements can be proved in L; (2) all true mathematical statements can be proved in T.
4. **Consistency:** a finitistic proof that no contradiction can be proved in T.
5. Conservation(Consequence of Consistency $\forall A \in \Pi_1 : T \vdash A \implies F, \text{Con}_T \vdash A$): any statement about ‘real objects’ provable in T can be proved in F.
6. Decidability (Effectiveness): a mechanical procedure for deciding the validity of any logical statement and the truth of any mathematical statement.
7. Simplicity: a criteria of simplicity, or proof of the greatest simplicity of certain proofs.
8. Categoricity? T characterizes exactly one model up to isomorphism.

Leibniz & Hilbert — Dream Shattered...



数学哲学

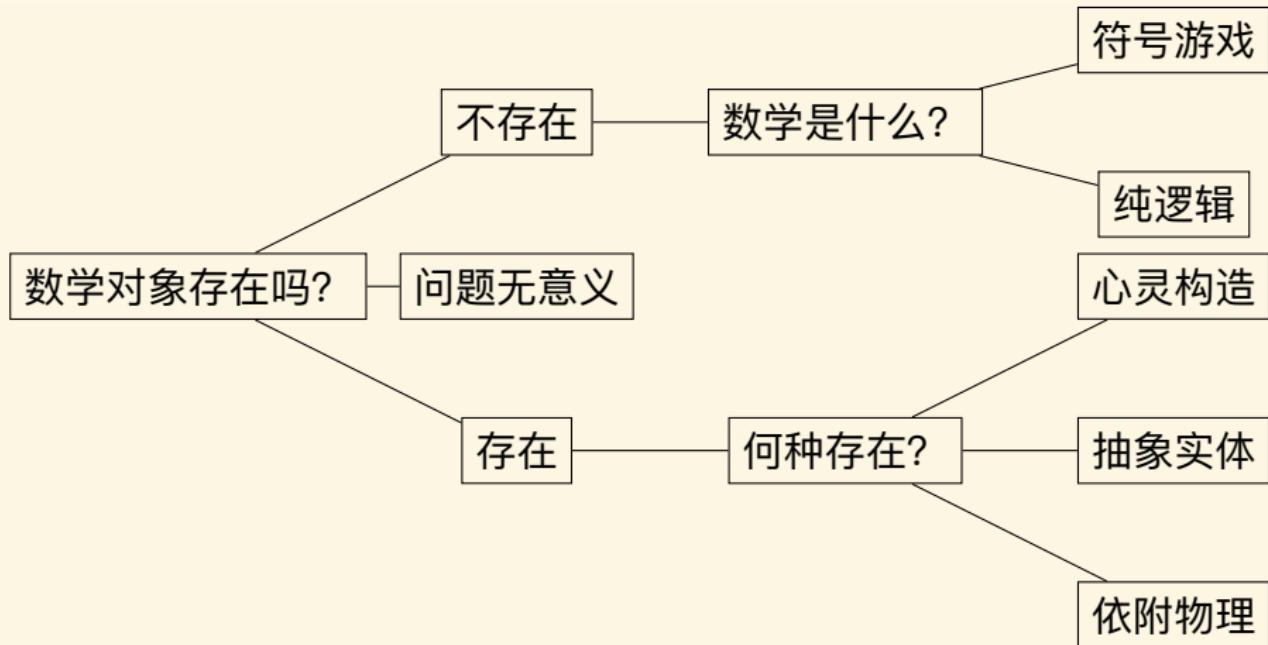


Figure: 形式主义/逻辑主义/直觉主义/柏拉图主义/物理主义

Is there more than one mathematical universe?⁹

⁹ Penelope Maddy: What Do We Want a Foundation to Do?

Valid Argument — Example

1. Whatever begins to exist, has a cause of its existence. The universe began to exist. Therefore, the universe has a cause of its existence.

$$\frac{\forall x(Bx \rightarrow \exists yCyx) \\ Bu}{\exists yCyu}$$

2. Alice is looking at Bob, but Bob is looking at Carl. Alice is married, but Carl is not. Is a married person looking at an unmarried person?

$$\frac{Lab \\ Lbc \\ Ma \\ \neg Mc}{\exists xy(Mx \wedge \neg My \wedge Lxy)}$$

Valid Argument — Example

1. If God exists and a person does not believe sincerely in its existence then that person will not be saved.
2. If God does not exist then nobody will be saved.
3. If a person believes that God exists and his/her belief is motivated only by Pascal's wager then that person does not believe sincerely.
4. Pascal believes that God exists but his belief is motivated by his own wager only. Therefore, Pascal will not be saved.

$$\forall x(Eg \wedge \neg Bx \rightarrow \neg Sx)$$

$$\neg Eg \rightarrow \neg \exists x Sx$$

$$\forall x(Wx \rightarrow \neg Bx)$$

$$Wp \rightarrow \neg Sp$$

Everybody loves my baby

My baby loves nobody but me

Everybody loves me

$\forall x Lxb$

$\forall x(Lbx \rightarrow x = m)$

$\forall x Lxm$

Valid Argument — Example

1. If radiation in the 2 slit experiment consists of a beam of particles, then the impact pattern on the photographic plate consists of a series of successive flashes and the pattern has at most two local maxima.
2. If radiation in the 2 slit experiment is a wave, then the impact pattern on the photographic plate is not a series of successive flashes and the pattern has more than two local maxima.
3. If in the 2 slit experiment the impact consists of a series of successive flashes and the impact pattern has more than two local maxima, then in this experiment radiation is neither a beam of particles nor a wave.

$$\frac{\begin{array}{c} \forall x(Px \rightarrow Fx \wedge Mx) \\ \forall x(Wx \rightarrow \neg Fx \wedge \neg Mx) \end{array}}{\forall x(Fx \wedge \neg Mx \rightarrow \neg Px \wedge \neg Wx)}$$

Valid Argument — Example

- ▶ Bob stakes himself in a gamble and he loses himself; then he stakes his wife Alice and loses her too. Alice objects by saying that Bob could not have staked her because he did not own her anymore after losing himself.
- ▶ For all x, y, z if x owns y and y owns z then x owns z .
- ▶ For all y there exists x such that x owns y .
- ▶ For all x, y, z if y owns x and z owns x then $y = z$.

$$\frac{\begin{array}{c} \forall xyz(Oxy \wedge Oyz \rightarrow Oxz) \\ \forall y \exists x Oxy \\ \forall xyz(Oyx \wedge Ozx \rightarrow y = z) \end{array}}{\forall x(\neg Oxx \rightarrow \neg \exists y Oxy)}$$

Valid Argument — Example

It is a crime for an American to sell weapons to hostile nations. The country Nono, an enemy of America, has some missiles, and all of its missiles were sold to it by Colonel West, who is American. Therefore, Colonel West is a criminal.

1. $\forall xyz(\text{American}(x) \wedge \text{Weapon}(y) \wedge \text{Hostile}(z) \wedge \text{Sell}(x, y, z) \rightarrow \text{Criminal}(x))$
2. $\exists x(\text{Own}(\text{nono}, x) \wedge \text{Missile}(x))$
3. $\forall x(\text{Missile}(x) \wedge \text{Own}(\text{nono}, x) \rightarrow \text{Sell}(\text{west}, x, \text{nono}))$
4. $\forall x(\text{Missile}(x) \rightarrow \text{Weapon}(x))$
5. $\forall x(\text{Enemy}(x, \text{america}) \rightarrow \text{Hostile}(x))$
6. $\text{American}(\text{west})$
7. $\text{Enemy}(\text{nono}, \text{america})$
8. $\text{Criminal}(\text{west})$

1. 所有中国学生和所有日本学生都爱 Gakki。中南大学只有中国学生和日本学生。因此，中南大学的学生都爱 Gakki。

$$\frac{\begin{array}{c} \forall x(Cx \vee Jx \rightarrow Lxg) \\ \forall x(Zx \rightarrow Cx \vee Jx) \end{array}}{\forall x(Zx \rightarrow Lxg)}$$

2. 如果所有的思想都清楚，那么没有思想需要解释；如果所有的思想都不清楚，那么没有思想能够解释清楚。因此，如果有的思想既需要解释又能够解释清楚，那么说明有的思想清楚、有的思想不清楚。

$$\frac{\begin{array}{c} \forall xCx \rightarrow \neg \exists xNx \\ \forall x \neg Cx \rightarrow \neg \exists xEx \end{array}}{\exists x(Nx \wedge Ex) \rightarrow \exists xCx \wedge \exists x \neg Cx}$$

3. 一个系统是完全的当且仅当所有它能表达的真命题在该系统中都可证。一个系统是一致的当且仅当，存在一个真命题，它在该系统中虽然能表达但不可证。因此，所有不一致的系统都是完全的。

$$\frac{\begin{array}{c} \forall x(Cx \leftrightarrow \forall y(Eyx \wedge Ty \rightarrow Pyx)) \\ \forall x(Sx \leftrightarrow \exists y(Ty \wedge Eyx \wedge \neg Pyx)) \end{array}}{\forall x(\neg Sx \rightarrow Cx)}$$

Valid Argument — Example “人有来生”

1. 人的一生有太多可能性没有实现。
2. 如果只有一生没有来生，没有实现的可能性将永远不可实现。
3. 永远不可实现的可能性没有意义。
4. 如果宇宙是有意义的，那么其包含的事物的可能性都是有意义的。
5. 可被学习理解的东西是有意义的。
6. 有序的东西是可被学习理解的。
7. 宇宙是有秩序的。

1. $\forall xy(\text{Man}(x) \wedge \text{Life}(y, x) \rightarrow \exists z(\text{Possible}(z, x, y) \wedge \neg \text{Realize}(z)))$
2. $\forall xy(\text{Man}(x) \wedge \text{Life}(y, x) \wedge \neg \exists y'(\text{Life}(y', x) \wedge y' \neq y) \rightarrow \forall z(\text{Possible}(z, x, y) \wedge \neg \text{Realize}(z) \rightarrow \text{UnRealizable}(z)))$
3. $\forall x(\text{UnRealizable}(x) \rightarrow \neg \text{Meaning}(x))$
4. $\text{Meaning}(u) \rightarrow \forall xyz(\text{Contain}(u, x) \wedge \text{Possible}(z, x, y) \rightarrow \text{Meaning}(z))$
5. $\forall x(\text{Learnable}(x) \rightarrow \text{Meaning}(x))$
6. $\forall x(\text{Ordered}(x) \rightarrow \text{Learnable}(x))$
7. $\text{Ordered}(u)$
8. $\forall x(\text{Man}(x) \rightarrow \text{Contain}(u, x))$
9. $\forall xy(\text{Man}(x) \wedge \text{Life}(y, x) \rightarrow \exists y'(\text{Life}(y', x) \wedge y' \neq y))$

Exercises — Tree Method — Now it's your turn ❤

1. Nobody trusts *exactly* those who have no mutual trust with anybody.
2. If dogs are animals, every head of a dog is the head of an animal.
3. Every non-analytic, meaningful proposition is either verifiable or falsifiable. Philosophical propositions are neither analytic nor verifiable or falsifiable. Therefore, they are meaningless.
4. Some wars are just. No war of aggression is just. Therefore, there are wars that are not wars of aggression.
5. *The present King of France is bald. Bald men are sexy. Hence whoever is a present King of France is sexy.*
6. *Only Russell is a great philosopher. Wittgenstein is a great philosopher who smokes. So Russell smokes.*
7. Everyone is afraid of Dracula. Dracula is afraid *only* of me. Therefore, I am Dracula.
8. Everyone loves a “*lover*”(*anyone who loves somebody*). Romeo loves Juliet. Therefore, I love you.
9. Everyone loves a “*lover*”(*anyone who loves somebody*); hence if someone is a “*lover*”, everyone loves everyone!

10. No girl loves any sexist pig. Caroline is a girl who loves whoever loves her. Henry loves Caroline. Thus Henry isn't a sexist pig.
11. I am a philosopher. A philosopher can *only* be appreciated by philosophers. No philosopher is without some eccentricity. I sing rock. Every eccentric rock singer is appreciated by some girl. Eccentrics are conceited. Therefore, some girl is conceited.
12. Any philosopher admires some logician. Some students admire *only* film stars. No film stars are logicians. Therefore not all students are philosophers.
13. If anyone speaks to anyone, then someone introduces them; no one introduces anyone to anyone unless he knows them both; everyone speaks to Frank; therefore everyone is introduced to Frank by someone who knows him.
14. Whoever stole the goods, knew the safe combination. Someone stole the goods, and *only* Jack knew the safe combination. Hence Jack stole the goods.
15. *No one but Alice and Bette (who are different people)* admires Carl. All and only those who admire Carl love him. Hence *exactly* two people love Carl.

Application — Minesweeper



- ▶ There are exactly n mines in the game.
- ▶ If a cell contains the number 1, then there is exactly one mine in the adjacent cells.

$\forall x(\text{Contain}(x, 1) \rightarrow$

$\exists y(\text{Adj}(x, y) \wedge \text{Mine}(y) \wedge \forall z(\text{Adj}(x, z) \wedge \text{Mine}(z) \rightarrow z = y)))$

- ▶ ...

Application — Example

Problem

A man goes to the brook with two measures of 15 pints and 16 pints. How is he to measure 8 pints of water?

States (x, y) : x is the content of the first vessel, y the second.

Initial State $(15, 16)$

Goal State $\exists x[(8, x) \vee (x, 8)]$

There are 8 possible actions:

Fill 1 $(x, y) \rightarrow (15, y)$

Empty 1 $(x, y) \rightarrow (0, y)$

Fill 2 $(x, y) \rightarrow (x, 16)$

Empty 2 $(x, y) \rightarrow (x, 0)$

Empty 1 into 2 $(x, y) \wedge x + y \leq 16 \rightarrow (0, y + x)$

Pour 1 into 2 $(x, y) \wedge x + y > 16 \rightarrow (x - (16 - y), 16)$

Empty 2 into 1 $(x, y) \wedge x + y \leq 15 \rightarrow (x + y, 0)$

Pour 2 into 1 $(x, y) \wedge x + y > 15 \rightarrow (15, y - (15 - x))$

Application in Game Theory

Theorem (Zermelo's Theorem 1913)

Every finite game of perfect information with no tie is determined.

Proof.

$$\exists x_1 \forall y_1 \dots \exists x_n \forall y_n A \vee \forall x_1 \exists y_1 \dots \forall x_n \exists y_n \neg A$$

where A states that a final position is reached where player 1 wins.

Proof.

First, color those end nodes black that are wins for player 1, and color the other end nodes white, being the wins for player 2. Then

- ▶ if player 1 is to move, and at least one child is black, color it black; if all children are white, color it white.
- ▶ if player 2 is to move, and at least one child is white, color it white; if all children are black, color it black.

Russell's Theory of Descriptions

1. The substitution of identicals.

"The morning star is the evening star."

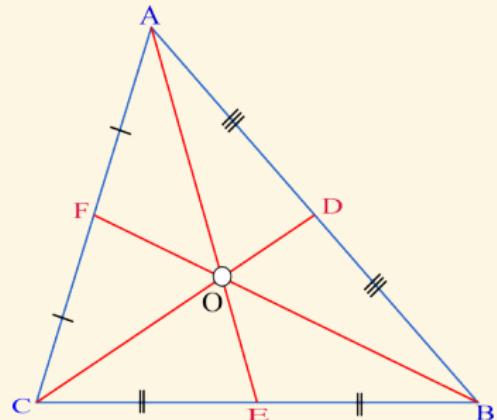
2. The law of the excluded middle.

"The present King of France is bald." or

"The present King of France is not bald."

3. The problem of negative existentials.

"The flying horse does not exist."



flying horse →



$$B(\iota_x A) := \exists x(Ax \wedge \forall y(Ay \rightarrow y = x) \wedge Bx)$$

- I don't know the author of Sherlock Holmes is Conan Doyle.

$$\neg K(\iota_x A = c) ? \quad \iota_x A = c \rightarrow K(c = c) \rightarrow K(\iota_x A = c) ?$$

$$\exists x(Ax \wedge \forall y(Ay \rightarrow y = x) \wedge \neg K(x = c))$$

$$\neg K[\exists x(Ax \wedge \forall y(Ay \rightarrow y = x) \wedge x = c)]$$

- The present King of France is bald. $B(\iota_x K) \vee (\neg B)(\iota_x K) ?$

$$\exists x(Kx \wedge \forall y(Ky \rightarrow y = x) \wedge \neg Bx) \quad (\neg B)(\iota_x K)$$

$$\neg \exists x(Kx \wedge \forall y(Ky \rightarrow y = x) \wedge Bx) \quad \neg B(\iota_x K)$$

- The flying horse does not exist. $\neg E(\iota_x Fx)$

$$\exists x(Fx \wedge \forall y(Fy \rightarrow y = x) \wedge \neg Ex) ?$$

$$\neg \exists x(Fx \wedge \forall y(Fy \rightarrow y = x))$$

$$Ex := \exists P(Px \wedge \exists y \neg Py)$$

- Get rid of function symbols.

$$\text{Bald}(\iota_x \text{Father}(x, \text{alice})) \quad vs \quad \text{Bald}(\text{father}(\text{alice}))$$

- Universal Instantiation. $\forall x B \rightarrow B(\iota_x A) ?$

$$B(\iota_x^y A) := (\exists !xA \rightarrow \exists x(A \wedge B)) \wedge (\neg \exists !xA \rightarrow B[y/x])$$

$$\vdash \forall x B \rightarrow B(\iota_x^y A)$$

Translation

1. Every citizen of every country respects the King of that country.

$$\forall xy(Cy \wedge Zxy \rightarrow Rx\iota_z Kzy)$$

2. The daughter of the King of China is the person everyone respects.

$$\iota_y Dyi_x Kxc = \iota_x(Px \wedge \forall y(Py \rightarrow Ryx))$$

3. The person everyone respects is a citizen of the country everyone respects.

$$Z\iota_x(Px \wedge \forall y(Py \rightarrow Ryx))\iota_x(Cx \wedge \forall y(Py \rightarrow Ryx))$$

Bertrand Russell 1872-1970

- ▶ Russell Paradox.
(3^{ed} crisis of the Foundations of Mathematics)
- ▶ Theory of Descriptions.
(The present King of France is not bald.)
- ▶ Type Theory.
- ▶ *Principia Mathematica*.



No barber shaves exactly those who do not shave themselves.¹⁰

¹⁰Russell: On denoting.

- ▶ The **logical form** of a statement may differ from its **grammatical form**.
- ▶ **Contextuality Principle:** Never ask for the meaning of a phrase in isolation, but only in the context of some meaningful fragment of a text.
- ▶ The method of contextual definition, which the theory of descriptions exemplifies, was inspired by the nineteenth-century rigorization of analysis.

Berkeley: 2nd crisis of the Foundations of Mathematics

For $f(x) = x^2$,

$$\frac{df(x)}{dx} = \frac{f(x + dx) - f(x)}{dx} = \frac{(x + dx)^2 - x^2}{dx} = \frac{2x dx + (dx)^2}{dx} = 2x + \cancel{dx} = 2x$$

$\frac{d}{dx}$ should be explained as a whole.

$$\frac{df(x)}{dx} = \frac{d}{dx} f(x) = \lim_{\Delta x \rightarrow 0} \frac{f(x + \Delta x) - f(x)}{\Delta x}$$

Logicism & Logical Positivism

- ▶ Mathematics could be reduced to logic.
- ▶ Science could be reduced to logical compounds of statements about sense data.
- ▶ Only statements verifiable through observation or logical proof are meaningful.
- ▶ The new logical resources provided by Frege and Russell had both tempted the positivists to conjecture more than they could prove and made it clear to them that proof of their conjecture was impossible.
- ▶ Few if any philosophical schools before the positivists had even stated their aims with sufficient clarity to make it possible to see that they were unachievable.

卡尔纳普《通过语言的逻辑分析清除形而上学》

一个陈述的意义在于它的**证实方法**。形而上学陈述不能被证实，毫无意义。那么留给哲学的还有什么呢？一种方法：逻辑分析法。逻辑分析的消极应用是清除无意义的词和陈述，积极应用是澄清有意义的概念和命题，为经验科学和数学奠基。形而上学家相信自己是在攸关**真假**的领域里前行，却未断言任何东西。他们只是试图表达一点儿人生态度。艺术是表达人生态度的恰当手段。抒情诗人并不企图在自己的诗里驳倒其他抒情诗人诗里的陈述，但形而上学家却用论证维护他的陈述。形而上学家是没有艺术才能的艺术家，有的是在理论环境里工作的爱好，却既不在科学领域里发挥这种爱好，又不能满足艺术表达的要求，倒是混淆了这两个方面，创造出一种对知识既无贡献、对人生态度的表达又不相宜的东西。

"If we take in our hand any volume; of divinity or school metaphysics, for instance; let us ask, Does it contain any abstract reasoning concerning quantity or number? No. Does it contain any experimental reasoning concerning matter of fact and existence? No. Commit it then to the flames: For it can contain nothing but sophistry and illusion."

— David Hume: *An Enquiry Concerning Human Understanding*

Russell's Theory of Descriptions & Church's λ -Abstraction

$$\nu(\iota_x A) = \begin{cases} a & \text{if there is a unique } a \in M : \mathcal{M}, \nu(a/x) \models A \\ \uparrow & \text{otherwise} \end{cases}$$
$$\begin{cases} \mathcal{M}, \nu \models (\lambda x. A)t \iff \mathcal{M}, \nu \models A[t/x] & \text{if } \nu(t) \downarrow \\ \mathcal{M}, \nu \not\models (\lambda x. A)t & \text{if } \nu(t) \uparrow \end{cases}$$

The present King of France is not bald.

$$(\lambda x. \neg Bx)\iota_x Kx$$

It's not the case that the present King of France is bald.

$$\neg(\lambda x. Bx)\iota_x Kx$$

Crossing the street without looking is dangerous.

$$\mathbf{D}(\lambda x(Cx \wedge \neg Lx))$$

Expressive Limitation of First Order Language

- ▶ Most boys are funny.
- ▶ Some critics admire only one another.

$$\exists X \left(\exists x Xx \wedge \forall x (Xx \rightarrow Cx) \wedge \forall x \forall y (Xx \wedge A(x, y) \rightarrow Xy \wedge x \neq y) \right)$$

- ▶ There are some gunslingers each of whom has shot the right foot of at least one of the others.

$$\exists X \left(\exists x Xx \wedge \forall x (Xx \rightarrow Gx) \wedge \forall x (Xx \rightarrow \exists y (Xy \wedge y \neq x \wedge Sxy)) \right)$$

- ▶ Least Number Principle.

$$\forall X \left(\exists x Xx \wedge \forall x (Xx \rightarrow Nx) \rightarrow \exists x (Xx \wedge \forall y (Xy \wedge y \neq x \rightarrow x < y)) \right)$$

- ▶ A linear order $(P, <)$ is *complete* iff every non-empty subset of P that is bounded above has a supremum in P .

$$\forall X \left(\exists x Xx \wedge \exists y \forall x (Xx \rightarrow x \leq y) \rightarrow \right.$$

$$\left. \exists y \left(\forall x (Xx \rightarrow x \leq y) \wedge \forall z (\forall x (Xx \rightarrow x \leq z) \rightarrow y \leq z) \right) \right)$$

Hilbert's Epsilon Calculus

$$\nu(\varepsilon_x A) = \Phi(\{a \in M : \mathcal{M}, \nu(a/x) \models A\})$$

where $\Phi : P(M) \rightarrow M :: \Phi(X) \in X$ whenever $X \neq \emptyset$ and $\Phi(\emptyset) \in M$.

Axiom ε

$$A(t) \rightarrow A(\varepsilon_x A)$$

where t is an arbitrary term.

ε -Extensionality Axiom

$$\forall x(A(x) \leftrightarrow B(x)) \rightarrow \varepsilon_x A = \varepsilon_x B$$

Hilbert's epsilon calculus is quantifier-free.

Predicate logic can be embedded in epsilon calculus.

Quantifiers can be defined as follows:

$$\exists x A(x) \equiv A(\varepsilon_x A)$$

$$\forall x A(x) \equiv A(\varepsilon_x \neg A)$$

Hilbert's Epsilon Calculus

- ▶ First ε -theorem: Suppose A is a quantifier-free and ε -free wff. Then $\vdash_{\varepsilon} A \implies \vdash_{\text{QF}} A$ in quantifier-free predicate logic.
- ▶ Extended first ε -theorem: Suppose $\exists x_1 \dots \exists x_n A(x_1, \dots, x_n)$ is a purely existential formula containing only the bound variables x_1, \dots, x_n . Then $\vdash_{\varepsilon} \exists x_1 \dots \exists x_n A(x_1, \dots, x_n) \implies \vdash \bigvee_i A(t_{i1}, \dots, t_{in})$ for some terms t_{ij} .
- ▶ Second ε -theorem: Suppose A is an ε -free wff. Then $\vdash_{\varepsilon} A \implies \vdash A$.

Herbrand's Theorem is a corollary of the extended first ε -theorem.

Tree Method with Unification

$$\forall x A \checkmark$$

|

$$A[x_i/x]$$

$$\exists x A \checkmark$$

|

$$A[f(x_1, \dots, x_m)/x]$$

where x_i is a new variable.

where f is a new function and
 $\{x_1, \dots, x_m\} = \text{Fv}(\exists x A)$.

$$\neg \forall x A \checkmark$$

|

$$\exists x \neg A$$

$$\neg \exists x A \checkmark$$

|

$$\forall x \neg A$$

Tree Method with Unification



- ▶ when expanding a universally quantified formula, do not choose a specific term but a rigid variable as a placeholder.
- ▶ choose the term only when it is clear it allows closing a branch.

rigid variable=same value in the whole tree

- ▶ variables can be assigned to closed terms, like $x_1 = a$.
- ▶ can also be assigned to unclosed terms, like $x_1 = f(x_2)$.
- ▶ make literals one the opposite of the other.
- ▶ using terms as unspecified as possible — Given literals A and $\neg B$ on the same branch, take the most general unifier of A and B .

Unifier

- ▶ A substitution σ is a *unifier* for a set Γ of formulas iff for every $A, B \in \Gamma : A\sigma = B\sigma$.
- ▶ A unifier σ is a *most general unifier* for Γ iff for each unifier θ there exists a substitution λ s.t. $\theta = \sigma\lambda$.

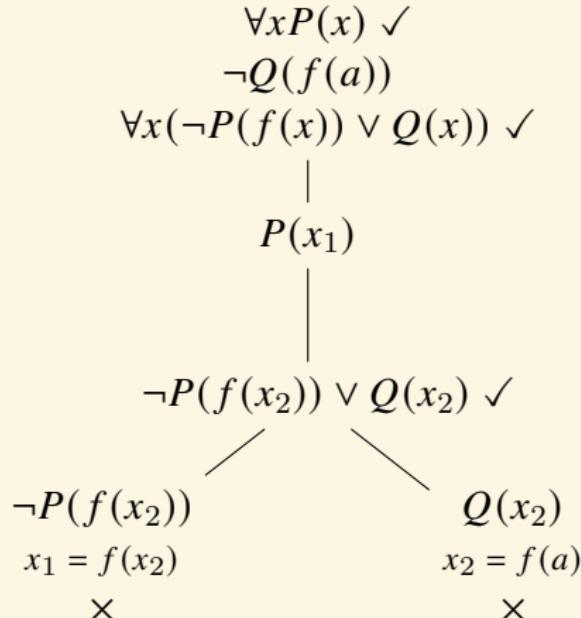
$$\sigma := \{t_1/x_1, \dots, t_m/x_m\} \quad \lambda := \{s_1/y_1, \dots, s_n/y_n\}$$

$$\sigma\lambda = \{t_1\lambda/x_1, \dots, t_m\lambda/x_m, s_1/y_1, \dots, s_n/y_n\} \setminus \{s_i/y_i : y_i \in \{x_1, \dots, x_m\}\}$$

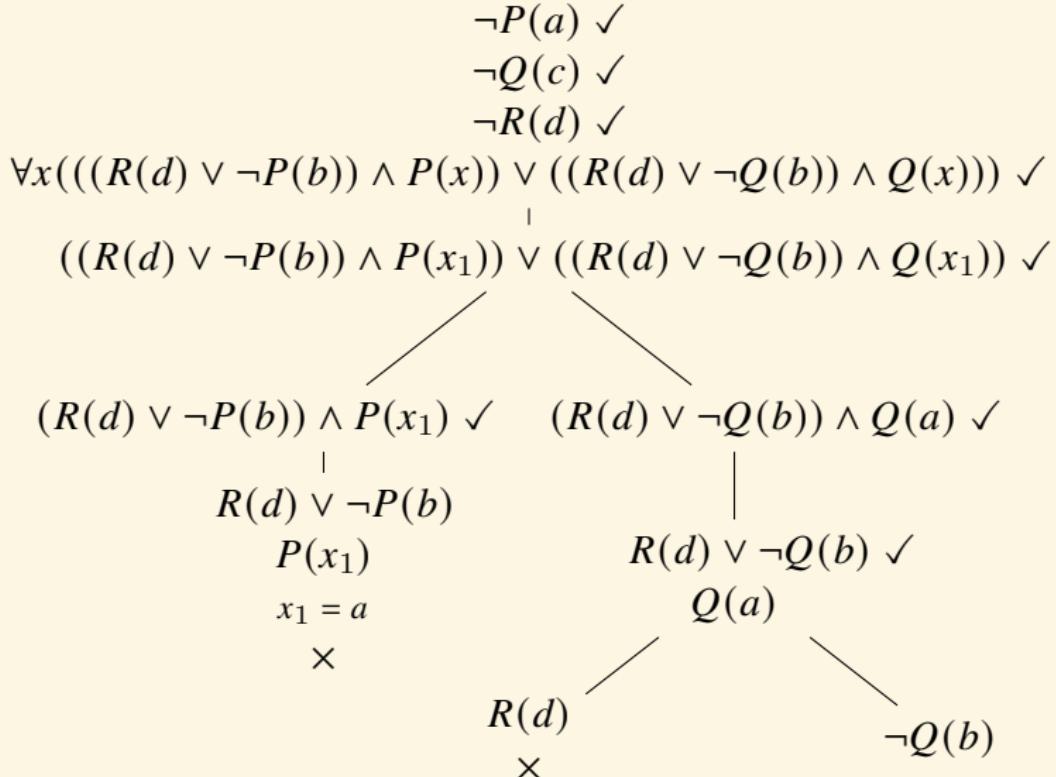
- ▶ $(A\sigma)\lambda = A(\sigma\lambda)$ and $(t\sigma)\lambda = t(\sigma\lambda)$
- ▶ $(\sigma\lambda)\theta = \sigma(\lambda\theta)$

Example — Tree Method with Unification

$\{\forall x P(x), \neg Q(f(a)), \forall x (\neg P(f(x)) \vee Q(x))\}$ is unsatisfiable.



Unification — Greedy Unification (incomplete)



Applying unification as soon as a branch can be closed by lead to incompleteness.

Unification — Final Closure

$\neg P(a) \checkmark$

$\neg Q(c)$ ✓

$\neg R(d)$ ✓

$$\forall x(((R(d) \vee \neg P(b)) \wedge P(x)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x))) \checkmark$$

$$((R(d) \vee \neg P(b)) \wedge P(x_1)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x_1)) \vee$$

$$(R(d) \vee \neg P(b)) \wedge P(x_1) \checkmark \quad (R(d) \vee \neg Q(b)) \wedge Q(x_1) \checkmark$$

1

$$R(d) \vee \neg P(b) \vee$$

$$R(d) \vee \neg Q(b) \checkmark$$

$$P(x_1)$$

$$Q(x_1)$$

$$R(d)$$

$\neg P(b)$

$$R(d)$$

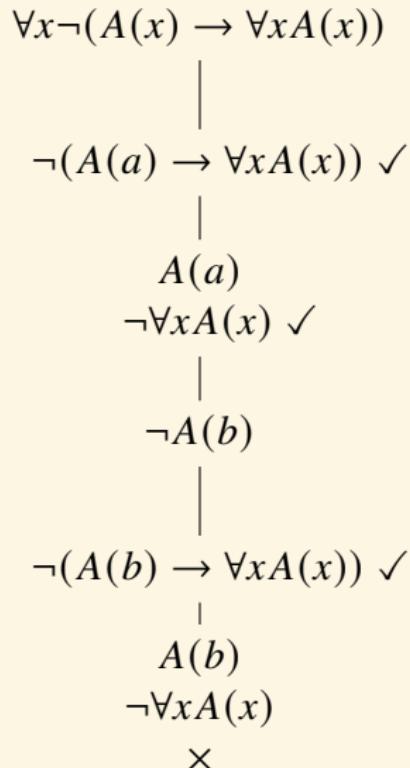
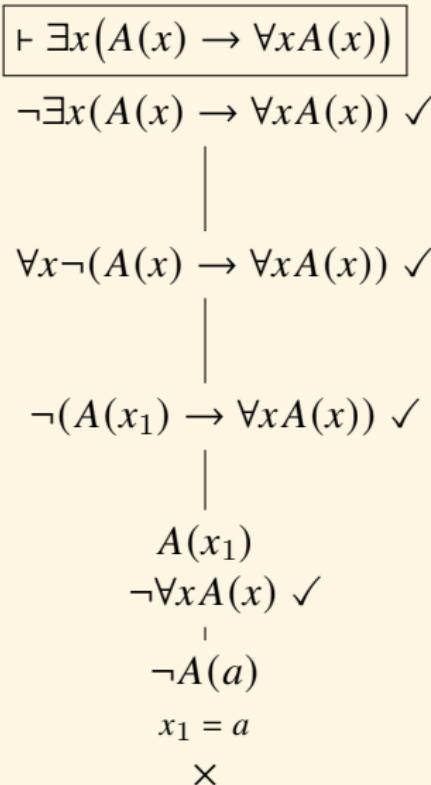
$$x_1 = b$$

X

Unification is applied only when it closes all open branches at the same time.

Example — Unification vs Ground Tree

There is someone such that if he is drinking, then everyone is drinking.



Gentzen



Figure: Gentzen 1909-1945

- ▶ Natural Deduction: one proposition on the right.
- ▶ Sequent Calculus: zero or more propositions on the right.

$$\Gamma \vdash \Delta \iff \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$$

- ▶ Consistency of PA
(proof-theoretical strength of PA)

Natural Deduction

$$\frac{A \quad B}{A \wedge B} [\wedge^+]$$

$$\frac{A \wedge B}{A} [\wedge^-]$$

$$\frac{A \wedge B}{B} [\wedge^-]$$

$$\frac{A}{A \vee B} [v^+]$$

$$\frac{B}{A \vee B} [v^+]$$

$$\frac{\begin{array}{c} [A]^n \quad [B]^n \\ \vdots \quad \vdots \\ A \vee B \quad C \end{array}}{C} [v^-]^n$$

$$\frac{\begin{array}{c} [A]^n \\ \vdots \\ B \end{array}}{A \rightarrow B} [\rightarrow^+]^n$$

$$\frac{A \rightarrow B \quad A}{B} [\rightarrow^-]$$

$$\frac{\begin{array}{c} [A]^n \\ \vdots \\ \perp \end{array}}{\neg A} [\neg^+]^n$$

$$\frac{\neg \neg A}{A} [\neg^-]$$

$$\frac{\neg A \quad A}{\perp} [\perp^+]$$

$$\frac{\perp}{A} [\perp^-]$$

Natural Deduction

$$\frac{A(a)}{\forall x A} [\forall^+]$$

$$\frac{\forall x A}{A(t)} [\forall^-]$$

where $a \notin \text{Cst}(\forall x A)$, and a is not in any assumption which is undischarged in the derivation ending with $A(a)$.

$$\frac{A(t)}{\exists x A} [\exists^+]$$

$$\frac{\begin{array}{c} [A(a)]^n \\ \vdots \\ \exists x A \end{array}}{\frac{B}{B}} [\exists^-]^n$$

where $a \notin \text{Cst}(\exists x A, B)$, and a is not in any assumption which is undischarged in the derivations ending with $\exists x A, B$ except in $A(a)$.

$$\frac{}{t = t} [=^+]$$

$$\frac{s = t \quad A(s)}{A(t)} [=^-]$$

Remark: How do we prove universal statements?

- ▶ Choose an arbitrary object from a given set and show that this object has the desired property.

$$\frac{A(a)}{\forall x A} [\forall^+]$$

where $a \notin \text{Cst}(\forall x A)$, and a is not in any assumption which is undischarged in the derivation ending with $A(a)$.

- ▶ “**random**” \neq “**arbitrary**”.

If we choose an item randomly, it means that the probability of choosing it is equal to that of choosing any other element. An arbitrary element is a placeholder that acts as a representative of any of the other elements.

Examples

$$\boxed{\neg A \rightarrow \perp \vdash A}$$

Proof.

$$\frac{\frac{\neg A \rightarrow \perp \quad [\neg A]^1}{\perp} \text{ [}\rightarrow^-\text{]} }{\frac{\perp \quad [\neg^+]^1}{\frac{\neg \neg A \quad [\neg^-]^1}{A}}} \text{ [}\rightarrow^-\text{]}$$

$$\boxed{\text{If } x \notin \text{Fv}(A), \text{ then } \vdash \forall x(A \rightarrow B) \rightarrow A \rightarrow \forall x B}$$

Proof.

$$\frac{\frac{\frac{[\forall x(A \rightarrow B)]^2}{A \rightarrow Ba} \text{ [}\forall^-\text{]} \quad [A]^1 \text{ [}\rightarrow^-\text{]}}{\frac{Ba}{\frac{\forall xB \quad [\forall^+]^1}{\frac{A \rightarrow \forall xB \quad [\rightarrow^+]^1}{\forall x(A \rightarrow B) \rightarrow A \rightarrow \forall x B}}} \text{ [}\rightarrow^+\text{]}^2$$

Natural Deduction — another version

$$\frac{A \in \Gamma}{\Gamma \vdash A} [\text{I}]$$

$$\frac{\Gamma \vdash A \quad \Gamma \subset \Gamma'}{\Gamma' \vdash A} [\text{M}]$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} [\wedge^+]$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} [\wedge^-]$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} [\wedge^-]$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} [\vee^+]$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash B \vee A} [\vee^+]$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} [\vee^-]$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} [\rightarrow^+]$$

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} [\rightarrow^-]$$

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} [\neg^+]$$

$$\frac{\Gamma \vdash \neg \neg A}{\Gamma \vdash A} [\neg^-]$$

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \perp} [\perp^+]$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} [\perp^-]$$

Natural Deduction — another version

$$\frac{\Gamma \vdash A(a) \quad a \notin \text{Cst}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A} [\forall^+]$$

$$\frac{\Gamma \vdash \forall x A}{\Gamma \vdash A(t)} [\forall^-]$$

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A} [\exists^+]$$

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A(a) \vdash B \quad a \notin \text{Cst}(\Gamma, \exists x A, B)}{\Gamma \vdash B} [\exists^-]$$

$$\frac{}{\Gamma \vdash t = t} [=^+]$$

$$\frac{\Gamma \vdash s = t \quad \Gamma \vdash A(s)}{\Gamma \vdash A(t)} [=^-]$$

Examples

$$\neg A \rightarrow \perp \vdash A$$

$$\frac{\neg A \rightarrow \perp, \neg A \vdash \neg A \rightarrow \perp}{\neg A \rightarrow \perp, \neg A \vdash \perp} [I] \quad \frac{\neg A \rightarrow \perp, \neg A \vdash \neg A}{\neg A \rightarrow \perp, \neg A \vdash \neg\neg A} [I]$$
$$\frac{\neg A \rightarrow \perp, \neg A \vdash \perp}{\neg A \rightarrow \perp \vdash \neg\neg A} [\neg^+]$$
$$\frac{\neg A \rightarrow \perp \vdash \neg\neg A}{\neg A \rightarrow \perp \vdash A} [\neg^-]$$

$$\boxed{\text{If } x \notin \text{Fv}(A), \text{ then } \vdash \forall x(A \rightarrow B) \rightarrow A \rightarrow \forall x B}$$

$$\frac{\forall x(A \rightarrow B) \vdash \forall x(A \rightarrow B)}{\forall x(A \rightarrow B) \vdash A \rightarrow Ba} [I]$$
$$\frac{\forall x(A \rightarrow B) \vdash A \rightarrow Ba}{\forall x(A \rightarrow B), A \vdash Ba} [\forall^-]$$
$$\frac{\forall x(A \rightarrow B), A \vdash Ba}{\forall x(A \rightarrow B), A \vdash \forall x B} [\forall^+]$$
$$\frac{\forall x(A \rightarrow B), A \vdash \forall x B}{\forall x(A \rightarrow B) \vdash A \rightarrow \forall x B} [\rightarrow^+]$$
$$\vdash \forall x(A \rightarrow B) \rightarrow A \rightarrow \forall x B [\rightarrow^+]$$

Sequent Calculus

Axiom

Cut

$$\frac{}{A \vdash A} [I]$$

$$\frac{\Gamma \vdash \Delta, A \quad \Sigma, A \vdash \Theta}{\Gamma, \Sigma \vdash \Delta, \Theta} [\text{Cut}]$$

Left structural rules

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} [\text{WL}]$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} [\text{CL}]$$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta} [\text{PL}]$$

Right structural rules

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta} [\text{WR}]$$

$$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta} [\text{CR}]$$

$$\frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2} [\text{PR}]$$

Sequent Calculus

Left logical rules:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} [\wedge L_1]$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} [\wedge L_2]$$

$$\frac{\Gamma, A \vdash \Delta \quad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \vee B \vdash \Delta, \Theta} [\vee L]$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \rightarrow B \vdash \Delta, \Theta} [\rightarrow L]$$

Right logical rules:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta} [\vee R_1]$$

$$\frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta} [\vee R_2]$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Theta}{\Gamma, \Sigma \vdash A \wedge B, \Delta, \Theta} [\wedge R]$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} [\rightarrow R]$$

Sequent Calculus

Left logical rules:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} [\neg L]$$

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x A \vdash \Delta} [\forall L]$$

$$\frac{\Gamma, A(a) \vdash \Delta \quad a \notin \text{Cst}(\Gamma, \exists x A, \Delta)}{\Gamma, \exists x A \vdash \Delta} [\exists L]$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} [\neg R]$$

$$\frac{\Gamma \vdash A(a), \Delta \quad a \notin \text{Cst}(\Gamma, \forall x A, \Delta)}{\Gamma \vdash \forall x A, \Delta} [\forall R]$$

$$\frac{\Gamma \vdash A(t), \Delta}{\Gamma \vdash \exists x A, \Delta} [\exists R]$$

$$\frac{}{A \vdash A} [I]$$

$$\frac{\vdash \neg A, A}{\vdash \neg A \vee A, A} [\vee R_2]$$

$$\frac{\vdash A, A \vee \neg A}{\vdash A \vee \neg A, A \vee \neg A} [PR]$$

$$\frac{\vdash A \vee \neg A, A \vee \neg A}{\vdash A \vee \neg A} [\vee R_1]$$

$$\frac{\vdash A \vee \neg A}{\vdash A \vee \neg A} [CR]$$

$$\frac{}{A \vdash A} [I]$$

$$\frac{A \vdash B, A}{A \vdash B, A} [WR]$$

$$\frac{B \vdash B}{A, B \vdash B} [I]$$

$$\frac{A, \neg A \vdash B}{A, \neg A \vee B \vdash B} [\neg L]$$

$$\frac{B \vdash B}{A, B \vdash B} [WL]$$

$$\frac{A, \neg A \vee B \vdash B}{\neg A \vee B \vdash A \rightarrow B} [\rightarrow R]$$

$$\frac{}{Aa \vdash Aa} [I]$$

$$\frac{\forall x A \vdash Aa}{\forall x A \vdash Aa} [\forall L]$$

$$\frac{\forall x A, \neg Aa \vdash}{\neg Aa \vdash \neg \forall x A} [\neg L]$$

$$\frac{\neg Aa \vdash \neg \forall x A}{\exists x \neg A \vdash \neg \forall x A} [\neg R]$$

$$\frac{\forall x A, \neg Aa \vdash}{\exists x \neg A \vdash \neg \forall x A} [\exists L]$$

$$\frac{A \vdash A}{A \wedge B \vdash A} [I]$$

$$\frac{A \wedge B \vdash A}{A \wedge B, \neg A \vdash} [\neg L]$$

$$\frac{B \vdash B}{A \wedge B \vdash B} [I]$$

$$\frac{A \wedge B \vdash B}{A \wedge B, \neg B \vdash} [\neg L]$$

$$\frac{A \wedge B, \neg A \vee \neg B \vdash}{\neg A \vee \neg B \vdash \neg(A \wedge B)} [\neg R]$$

$$\frac{}{A \wedge B, \neg A \vee \neg B \vdash} [\vee L]$$

$$\frac{A(a, b) \vdash A(a, b)}{\forall x A(x, b) \vdash A(a, b)} [I]$$

$$\frac{\forall x A(x, b) \vdash A(a, b)}{\forall x A(x, b) \vdash \exists y A(a, y)} [\forall L]$$

$$\frac{\exists y A(a, y)}{\forall x A(x, y) \vdash \exists y A(a, y)} [\exists R]$$

$$\frac{\exists y \forall x A(x, y) \vdash \exists y A(a, y)}{\exists y \forall x A(x, y) \vdash \forall x \exists y A(x, y)} [\exists L]$$

$$\frac{\exists y \forall x A(x, y) \vdash \forall x \exists y A(x, y)}{\exists y \forall x A(x, y) \vdash} [\forall R]$$

Natural Deduction — constant vs variable

$$\frac{\Gamma \vdash A(a) \quad a \notin \text{Cst}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A} [\forall^+]$$

$$\frac{\Gamma \vdash A[y/x] \quad y \notin \text{Fv}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A} [\forall^+]$$

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A(a) \vdash B \quad a \notin \text{Cst}(\Gamma, \exists x A, B)}{\Gamma \vdash B} [\exists^-]$$

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A[y/x] \vdash B \quad y \notin \text{Fv}(\Gamma, \exists x A, B)}{\Gamma \vdash B} [\exists^-]$$

Natural Deduction — another version — constant vs variable

$$\frac{A(a)}{\forall x A} [\forall^+]$$

$$\frac{A[y/x]}{\forall x A} [\forall^+]$$

where $a \notin \text{Cst}(\forall x A)$, and a is not in any assumption which is undischarged in the derivation ending with $A(a)$.

where $y \notin \text{Fv}(\forall x A)$, and y is not free in any assumption which is undischarged in the derivation ending with $A[y/x]$.

$$\begin{array}{c} [A(a)]^n \\ \vdots \\ \exists x A \quad B \quad [\exists^-]^n \\ \hline B \end{array}$$

$$\begin{array}{c} [A[y/x]]^n \\ \vdots \\ \exists x A \quad B \quad [\exists^-]^n \\ \hline B \end{array}$$

where $a \notin \text{Cst}(\exists x A, B)$, and a is not in any assumption which is undischarged in the derivations ending with $\exists x A, B$ except in $A(a)$.

where $y \notin \text{Fv}(\exists x A, B)$, and y is not free in any assumption which is undischarged in the derivations ending with $\exists x A, B$ except in $A[y/x]$.

Sequent Calculus — constant vs variable

$$\frac{\Gamma \vdash A(a), \Delta \quad a \notin \text{Cst}(\Gamma, \forall x A, \Delta)}{\Gamma \vdash \forall x A, \Delta} [\forall R]$$

$$\frac{\Gamma \vdash A[y/x], \Delta \quad y \notin \text{Fv}(\Gamma, \forall x A, \Delta)}{\Gamma \vdash \forall x A, \Delta} [\forall R]$$

$$\frac{\Gamma, A(a) \vdash \Delta \quad a \notin \text{Cst}(\Gamma, \exists x A, \Delta)}{\Gamma, \exists x A \vdash \Delta} [\exists L]$$

$$\frac{\Gamma, A[y/x] \vdash \Delta \quad y \notin \text{Fv}(\Gamma, \exists x A, \Delta)}{\Gamma, \exists x A \vdash \Delta} [\exists L]$$

Cut-Elimination Theorem

Theorem (Cut-Elimination Theorem — Gentzen1934)

If $\Gamma \vdash \Delta$ is provable, then it is provable without use of the *Cut Rule*.

Corollary (The Subformula Property)

If $\Gamma \vdash \Delta$ is provable, then it has a deduction all of whose formulas are subformulas of Γ and Δ .

Corollary (Consistency)

A contradiction, i.e. the empty sequent $\emptyset \vdash \emptyset$, is not deducible.

Corollary (Conservation)

Predicate logic is conservative over propositional logic.

Theorem (Cut-free Completeness Theorem)

Let Θ be a set of sentences. If Θ logically implies $\Gamma \vdash \Delta$, then there is a finite subset $\Sigma \subset \Theta$ s.t. $\Sigma, \Gamma \vdash \Delta$ has a cut-free proof.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

Definability & Isomorphism

What is Logic?

Connectives

Normal Forms

Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References

1436

Definability

What is “definability”?

Berry Paradox

The smallest positive integer not definable in fewer than twelve words.

Definition (Definability)

- $X \subset M^n$ is Y -definable over \mathcal{M} (denoted by $X \in \text{Def}(\mathcal{M}, Y)$) iff there is a wff A and $b_1, \dots, b_m \in Y^m$ s.t.

$$X = \{(a_1, \dots, a_n) : \mathcal{M} \models A[a_1, \dots, a_n, b_1, \dots, b_m]\}$$

- X is definable in \mathcal{M} iff it is \emptyset -definable in \mathcal{M} .

A definition is acceptable only on condition that it implies no contradiction.

— Poincaré

Representability

What is “representability”?

Definition (Representable Functions)

A n -ary function $f : \mathbb{N}^n \rightarrow \mathbb{N}$ is representable in the theory T iff there is a wff $A(x_1, \dots, x_n, y)$ s.t. for all a_1, \dots, a_n ,

$$T \vdash \forall y \left(A(\underline{a_1}, \dots, \underline{a_n}, y) \leftrightarrow y = \underline{f(a_1, \dots, a_n)} \right)$$

Definition (Representable Relations)

A n -ary relation $R \subset \mathbb{N}^n$ is representable in the theory T iff there is a wff A s.t. for all a_1, \dots, a_n ,

$$(a_1, \dots, a_n) \in R \implies T \vdash A[a_1, \dots, a_n]$$

$$(a_1, \dots, a_n) \notin R \implies T \vdash \neg A[a_1, \dots, a_n]$$

A function/relation is representable in Robinson Q iff it is computable.

Example

- The interval $[0, \infty)$ is definable in $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$, where the language is $\mathcal{L} = \{0, 1, +, \cdot\}$.

$$x \geq 0 \iff \mathcal{R} \models \exists y(x = y \cdot y)$$

- The ordering relation $<$ is definable in $\mathcal{N} = (\mathbb{N}, 0, s, +, \cdot)$, where the language is $\mathcal{L} = \{0, s, +, \cdot\}$.

$$\exists z(x + s(z) = y)$$

- The set of primes is definable in \mathcal{N} by the formula

$$\exists y(x = s(0) + s(y)) \wedge \forall yz(x = y \cdot z \rightarrow y = s(0) \vee z = s(0))$$

- Exponentiation $\{(m, n, p) : p = m^n\}$ is definable in \mathcal{N} . (use the Chinese remainder theorem)

Example

- The number 0 is definable in $(\mathbb{Z}, +)$, since

$$x = 0 \iff (\mathbb{Z}, +) \models x + x = x$$

No other elements are definable, because negation $x \mapsto -x$ is an automorphism.

- The number 1 is definable in $(\mathbb{Z}, +, \cdot)$, since

$$x = 1 \iff (\mathbb{Z}, +, \cdot) \models x \cdot x = x$$

- \mathbb{N} is definable in $(\mathbb{Z}, +, \cdot)$ by

$$\exists y_1 y_2 y_3 y_4 (x = y_1^2 + y_2^2 + y_3^2 + y_4^2) \quad (\text{Lagrange four-square theorem})$$

Example

- ▶ No point is definable in $(\mathbb{R}, <)$, since any two real numbers are automorphic by translation.
- ▶ The ordering relation $<$ is definable in $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$.

$$x < y \iff \mathcal{R} \models \exists z(x + z \cdot z = y)$$

Every individual integer is definable.

Every rational number is definable.

Every algebraic number is definable.

But only algebraic numbers are definable.

Theorem (Tarski)

In $(\mathbb{R}, 0, 1, +, \cdot)$, every formula $A(x)$ is equivalent to a quantifier-free formula.

- ▶ π is definable in $(\mathbb{R}, 0, 1, +, \cdot, \sin)$.
 \mathbb{Z} is definable.
Every computable real number is definable.
Every arithmetic real & every projective real is definable.

Example

- A model \mathcal{M} is *Leibnizian* if any two distinct objects have different properties: if $a \neq b$, then there is some wff A such that

$$\mathcal{M} \models A(a) \wedge \neg A(b)$$

- A model \mathcal{M} is *pointwise definable* if every object of \mathcal{M} is definable in \mathcal{M} without parameters.

$$\mathcal{M} \models A(x) \leftrightarrow x = a$$

- Are these notions the same?
- $(\mathbb{R}, 0, 1, +, \cdot)$ is Leibnizian, because any two reals have a rational number between them. Being larger or smaller than a specific rational number is expressible.
- But $(\mathbb{R}, 0, 1, +, \cdot)$ is not pointwise definable, because it is uncountable, and there are only countably many definitions.

Homomorphism & Isomorphism

Definition (Homomorphism)

A homomorphism h of \mathcal{M} into \mathcal{N} is a function $h : M \rightarrow N$ s.t.

- ▶ For each n -place predicate symbol P and each n -tuple

$$(a_1, \dots, a_n) \in M^n,$$

$$(a_1, \dots, a_n) \in P^M \iff (h(a_1), \dots, h(a_n)) \in P^N$$

- ▶ For each n -place function symbol f and each n -tuple

$$(a_1, \dots, a_n) \in M^n,$$

$$h : f^M(a_1, \dots, a_n) \mapsto f^N(h(a_1), \dots, h(a_n))$$

In the case of a constant symbol c this becomes $h : c^M \mapsto c^N$.

- ▶ An isomorphism (monomorphism/epimorphism) is a bijective (injective/surjective) homomorphism. $\mathcal{M} \cong \mathcal{N}$

- ▶ An automorphism (endomorphism) is an isomorphism (homomorphism) from \mathcal{M} to itself.

- ▶ A structure \mathcal{M} is rigid iff it has no automorphisms other than 1_M .

Homomorphism Theorem

Theorem (Homomorphism Theorem)

Let h be a homomorphism of \mathcal{M} into \mathcal{N} , and $\nu : \text{Var} \rightarrow M$.

1. For any term t , $h(\bar{\nu}(t)) = \overline{h \circ \nu}(t)$
2. For any open formula A not containing $=$, $\mathcal{M}, \nu \models A \iff \mathcal{N}, h \circ \nu \models A$
3. If $h : M \rightarrow N$, we may delete the restriction "not containing $=$ ".
4. If $h : M \rightarrow N$, we may delete the restriction "open".

Definition (Elementary Equivalence)

$\mathcal{M} \equiv \mathcal{N}$ iff for any sentence $A : \mathcal{M} \models A \iff \mathcal{N} \models A$

$$\mathcal{M} \cong \mathcal{N} \implies \mathcal{M} \equiv \mathcal{N}$$

Theorem

$$\mathcal{M} \equiv \mathcal{N} \text{ } \& \text{ } |M| < \infty \implies \mathcal{M} \cong \mathcal{N}$$

Proof.

Suppose $|M| = n$. Then $|N| = n$.

There are only finitely many functions $f_1, \dots, f_m : M \rightarrow N$. Assume none of $f : M \rightarrow N$ is an isomorphism. For each $f_i, 1 \leq i \leq m$, there is a formula A_i s.t. $\mathcal{M} \models A_i(a_1, \dots, a_n)$ but $\mathcal{N} \not\models A_i(f_i(a_1), \dots, f_i(a_n))$. Then we have

$$\mathcal{M} \models \bigwedge_{i=1}^m A_i(a_1, \dots, a_n) \quad \& \quad \mathcal{M} \models \exists x_1 \dots x_n \bigwedge_{i=1}^m A_i(x_1, \dots, x_n)$$

Since $\mathcal{M} \equiv \mathcal{N}$, then $\mathcal{N} \models \exists x_1 \dots x_n \bigwedge_{i=1}^m A_i(x_1, \dots, x_n)$, and

$$\mathcal{N} \models \bigwedge_{i=1}^m A_i(b_1, \dots, b_n) \text{ for some } b_1, \dots, b_n \in N.$$

Let $f_j : a_i \mapsto b_i$. But $\mathcal{N} \not\models A_j(b_1, \dots, b_n)$.

Substructure

Definition (Substructure)

\mathcal{M} is called a *substructure* of \mathcal{N} ($\mathcal{M} \subset \mathcal{N}$) iff

- ▶ $M \subset N$
- ▶ 1. $P^{\mathcal{M}} = P^{\mathcal{N}} \cap M^n$ for any n -ary predicate symbol P .
2. $f^{\mathcal{M}} = f^{\mathcal{N}}|_{M^n}$ for any n -ary function symbol f .

Suppose $\mathcal{M} \subset \mathcal{N}$. Then

- ▶ for any term $t(x_1, \dots, x_n)$, and any $a_1, \dots, a_n \in M$,

$$t^{\mathcal{M}}[a_1, \dots, a_n] = t^{\mathcal{N}}[a_1, \dots, a_n]$$

- ▶ for any open formula $A(x_1, \dots, x_n)$, and any $a_1, \dots, a_n \in M$,

$$\mathcal{M} \models A[a_1, \dots, a_n] \iff \mathcal{N} \models A[a_1, \dots, a_n]$$

Example

- $\mathcal{L} = \{0, 1, +, \cdot\}, \mathcal{N} = (\mathbb{N}, 0, 1, +, \cdot), \mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$

$$\mathcal{N} \subset \mathcal{R}$$

- $\mathcal{L} = \{<\}, \mathcal{M} = (\mathbb{N}, <), \mathcal{N} = (\{2n : n \in \mathbb{N}\}, <)$

$$h : n \mapsto 2n, \quad h : \mathcal{M} \cong \mathcal{N}, \quad \text{but} \quad \mathcal{M} \not\subset \mathcal{N}$$

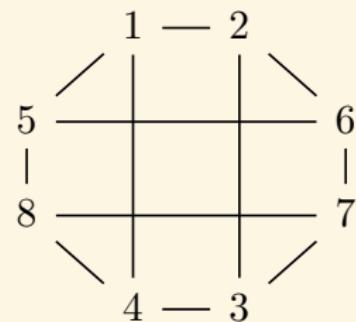
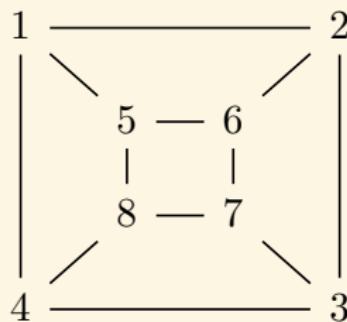
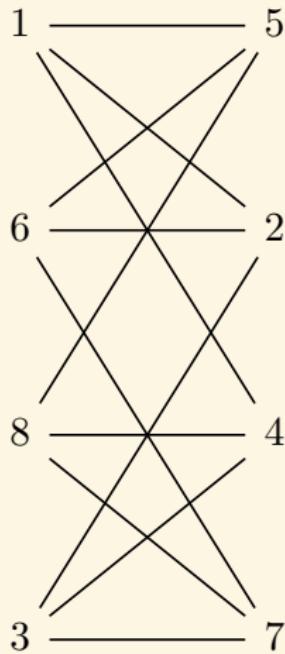
- $\mathcal{L} = \{0, +\}$

$$\mathcal{M} = (\mathbb{N}, 0^{\mathcal{M}}, +^{\mathcal{M}}), \quad \text{where} \quad 0^{\mathcal{M}} = 0, \quad +^{\mathcal{M}}(a, b) = a + b$$

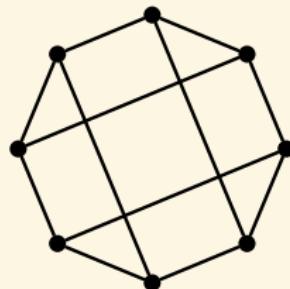
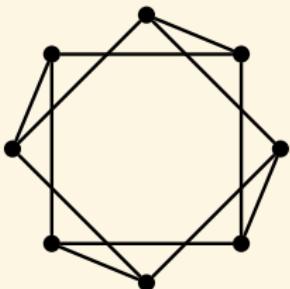
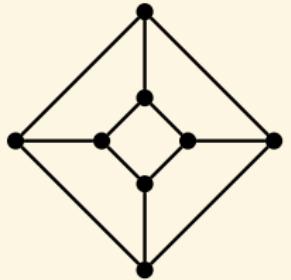
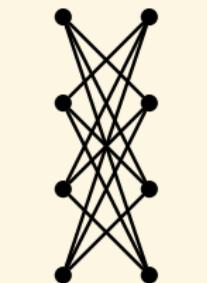
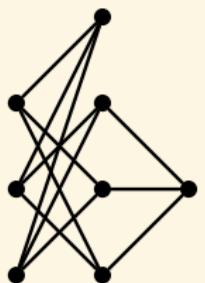
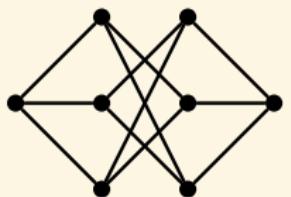
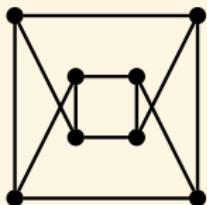
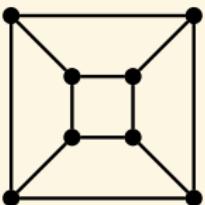
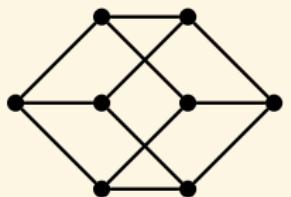
$$\mathcal{N} = (\{2^n : n \in \mathbb{N}\}, 0^{\mathcal{N}}, +^{\mathcal{N}}), \quad \text{where} \quad 0^{\mathcal{N}} = 1, \quad +^{\mathcal{N}}(a, b) = a \cdot b$$

$$h : n \mapsto 2^n, \quad h : \mathcal{M} \cong \mathcal{N} \quad \text{but} \quad \mathcal{M} \not\subset \mathcal{N}.$$

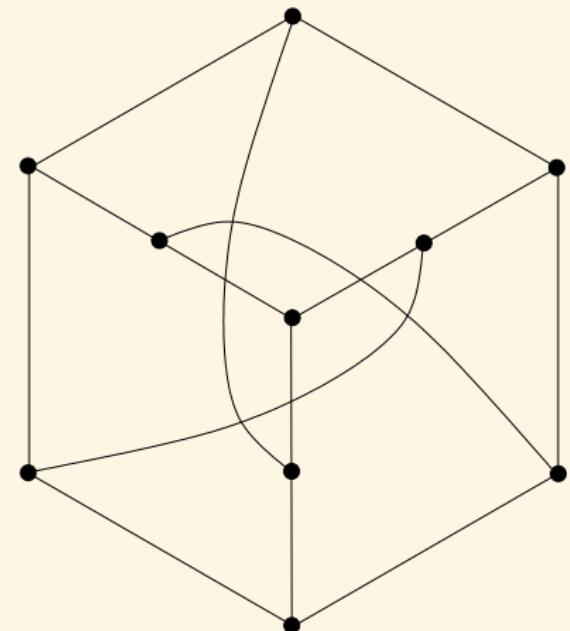
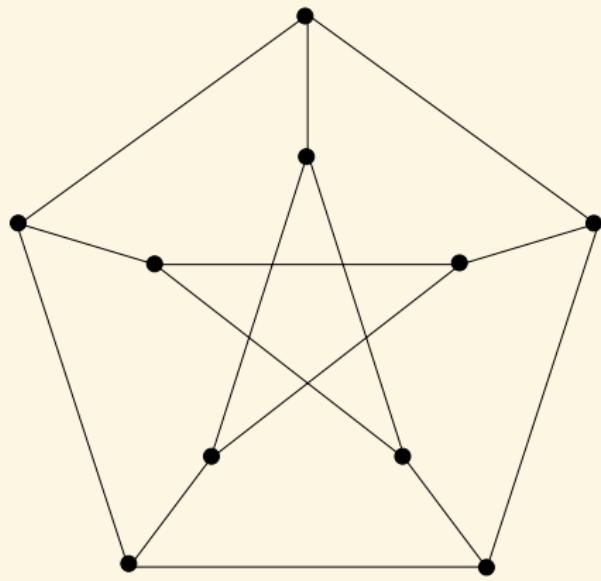
Example



quasipolynomial $2^{O((\log n)^c)}$



Example



A Joke

"Let G_1 be the group ..., and G_2 be the group ... Prove that G_1 and G_2 are isomorphic."

One of the papers submitted had an answer "We will show that G_1 is isomorphic..." and some nonsense, followed by "Now we'll show that G_2 is isomorphic..." and more nonsense.

share cite

answered Jan 31 '11 at 18:53

community wiki
[Asaf Karagila](#)

-
- 86 I gave a homework problem, "Let G_1 be the group ..., let G_2 be the group Are G_1 and G_2 isomorphic?" and was astonished to get the response, " G_1 is, but G_2 isn't." Are Asaf's story and mine isomorphic? – [Gerry Myerson](#) Jan 31 '11 at 22:39
- 165 @Gerry: Asaf's is, but yours isn't. – [Nate Eldredge](#) Feb 1 '11 at 1:20

Automorphism & Undefinability

Corollary

Let h be an automorphism $h : M \rightarrow M$, and $R \subset M^n$ definable in M . Then for any $a_1, \dots, a_n \in M$,

$$(a_1, \dots, a_n) \in R \iff (h(a_1), \dots, h(a_n)) \in R$$

Remark: This corollary is sometimes useful in showing that a given relation is not definable.

The set \mathbb{N} is not definable in $(\mathbb{R}, <)$ where $\mathcal{L} = \{<\}$.

$h : a \mapsto a^3$ is an automorphism of \mathbb{R} .

It maps points outside of \mathbb{N} into \mathbb{N} .

\mathbb{N} is not definable in $(\mathbb{R}, 0, 1, +, \cdot, <)$

Natural numbers are not definable over the theory of real-closed fields.

Example

Example

The structure $\mathcal{M} := (\{a, b, c\}, \{(a, b), (a, c)\})$
where the language is $\mathcal{L} = \{E\}$.

$$b \bullet \leftarrow \overset{a}{\bullet} \rightarrow \bullet c$$

- ▶ $\{b, c\}$ is definable in \mathcal{M} : $\exists y E(y, x)$
- ▶ $\{b\}$ is not definable in \mathcal{M} .

Example

Consider the vector space $\mathcal{E} := (E, +, f_r)_{r \in \mathbb{R}}$, where E is the universe, f_r is the scalar multiplication by r .

- ▶ $U := \{x \in E : |x| = 1\}$ is not definable in \mathcal{E} .
- ▶ $h : x \mapsto 2x$ is an automorphism but it does not preserve U .

Ehrenfeucht-Fraïssé Game (EF Game)

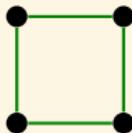
Spoiler and *Duplicator*, played on two structures \mathcal{M} and \mathcal{N} .
Each run of the game has n moves. In each move,

- ▶ *Spoiler* picks an element from \mathcal{M} or from \mathcal{N} .
- ▶ *Duplicator* picks an element from \mathcal{N} or from \mathcal{M} .
- ▶ *Duplicator* wins the run if $(a_i, b_i)_{i=1}^n$ is a partial isomorphism from \mathcal{M} to \mathcal{N} .
- ▶ *Spoiler* wins the run otherwise.
- ▶ $\mathcal{M} \sim_n \mathcal{N}$ iff *Duplicator* has a winning strategy in the n -move game.
- ▶ $\mathcal{M} \equiv_n \mathcal{N}$ iff $\mathcal{M} \models A \iff \mathcal{N} \models A$ for all sentences up to *quantifier depth* n .

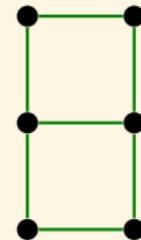
Theorem

$$\mathcal{M} \sim_n \mathcal{N} \iff \mathcal{M} \equiv_n \mathcal{N}$$

Ehrenfeucht-Fraïssé Game (EF Game)



$$\mathcal{M} \sim_2 \mathcal{N}$$



$$\mathcal{M} \not\sim_3 \mathcal{N}$$

$$\forall xy \exists z (\neg Exy \rightarrow Exz \wedge Eyz)$$

Isomorphic Embedding, Elementary Embedding

Definition

- ▶ Isomorphic embedding $f : \mathcal{M} \subset \mathcal{N}$ iff there is $\mathcal{A} \subset \mathcal{N}$ s.t. $f : \mathcal{M} \cong \mathcal{A}$.
- ▶ Elementary embedding $f : \mathcal{M} \prec \mathcal{N}$ iff for any wff $A(x_1, \dots, x_n)$ and any $a_1, \dots, a_n \in M$,
$$\mathcal{M} \models A[a_1, \dots, a_n] \iff \mathcal{N} \models A[f(a_1), \dots, f(a_n)]$$
- ▶ Elementary substructure $\mathcal{M} \prec \mathcal{N}$ iff $M \subset N$ & $1_M : \mathcal{M} \prec \mathcal{N}$.

Example

- ▶ $(\mathbb{N} \setminus \{0\}, \leq) \subset (\mathbb{N}, \leq)$ $(\mathbb{N} \setminus \{0\}, \leq) \cong (\mathbb{N}, \leq)$ $(\mathbb{N} \setminus \{0\}, \leq) \not\prec (\mathbb{N}, \leq)$
 $A(x) := \exists y(y \leq x \wedge \neg y = x)$ $(\mathbb{N}, \leq) \models A[1]$ $(\mathbb{N} \setminus \{0\}, \leq) \not\models A[1]$
- ▶ $(2\mathbb{Z}, <) \subset (\mathbb{Z}, <)$ $(2\mathbb{Z}, <) \cong (\mathbb{Z}, <)$ $(2\mathbb{Z}, <) \not\prec (\mathbb{Z}, <)$
 $A(x, y) := \exists z(x < z < y)$ $(\mathbb{Z}, <) \models A[0, 2]$ $(2\mathbb{Z}, <) \not\models A[0, 2]$

$$f : \mathcal{M} \prec \mathcal{N} \iff \exists \mathcal{A}(f : \mathcal{M} \cong \mathcal{A} \prec \mathcal{N}) \iff \exists \mathcal{A}(\mathcal{M} \prec \mathcal{A} \cong \mathcal{N})$$

Isomorphic Embedding, Elementary Embedding

$$(\mathbb{N}, <) \subset (\mathbb{Z}, <) \subset (\mathbb{Q}, <)$$

$$(\mathbb{N}, <) \not\prec (\mathbb{Z}, <) \not\prec (\mathbb{Q}, <)$$

$$(\mathbb{Q}, 0, 1, +, \cdot) \subset (\mathbb{R}, 0, 1, +, \cdot) \subset (\mathbb{C}, 0, 1, +, \cdot)$$

$$(\mathbb{Q}, 0, 1, +, \cdot) \not\prec (\mathbb{R}, 0, 1, +, \cdot) \not\prec (\mathbb{C}, 0, 1, +, \cdot)$$

$$(\mathbb{N}, 0, 1, +, \cdot, <) \subset (\mathbb{Z}, 0, 1, +, \cdot, <) \subset (\mathbb{Q}, 0, 1, +, \cdot, <) \subset (\mathbb{R}, 0, 1, +, \cdot, <)$$

$$(\mathbb{N}, 0, 1, +, \cdot, <) \not\prec (\mathbb{Z}, 0, 1, +, \cdot, <) \not\prec (\mathbb{Q}, 0, 1, +, \cdot, <) \not\prec (\mathbb{R}, 0, 1, +, \cdot, <)$$

$$(\mathbb{Q}, <) \prec (\mathbb{R}, <)$$

$$(2\mathbb{Z}, 0, +, -, <) \subset (\mathbb{Z}, 0, +, -, <)$$

$$(2\mathbb{Z}, 0, +, -, <) \equiv (\mathbb{Z}, 0, +, -, <)$$

$$(2\mathbb{Z}, 0, +, -, <) \not\prec (\mathbb{Z}, 0, +, -, <)$$

Isomorphic Embedding, Elementary Embedding

- If $f : \mathcal{M} \cong \mathcal{N}$, then for any term $t(x_1, \dots, x_n)$, any wff $A(x_1, \dots, x_n)$, and any $a_1, \dots, a_n \in M$,

$$f(t^{\mathcal{M}}[a_1, \dots, a_n]) = t^{\mathcal{N}}[f(a_1), \dots, f(a_n)]$$

$$\mathcal{M} \models A[a_1, \dots, a_n] \iff \mathcal{N} \models A[f(a_1), \dots, f(a_n)]$$

- $f : \mathcal{M} < \mathcal{N}$ iff $f : \mathcal{M} \subset \mathcal{N}$ and for any wff $\exists x A(x_1, \dots, x_n, x)$ and any $a_1, \dots, a_n \in M$,

$$\mathcal{N} \models \exists x A[f(a_1), \dots, f(a_n), x] \implies \exists a \in M : \mathcal{N} \models A[f(a_1), \dots, f(a_n), f(a)]$$

$$\mathcal{M} < \mathcal{N} \iff \mathcal{M} \subset \mathcal{N} \ \& \ \forall X \in \text{Def}(\mathcal{N}, M) : X \cap M \neq \emptyset$$

Let $M \subset \mathbb{R}$. $(M, <) < (\mathbb{R}, <)$ iff $(M, <)$ is a dense linear ordering without endpoints.

Isomorphic Embedding, Elementary Embedding

- ▶ Let \mathcal{M} be a \mathcal{L} -structure. $\mathcal{M}_M := (\mathcal{M}, a)_{a \in M}$ is a \mathcal{L}_M -structure by interpreting c_a by a .
- ▶ Let \mathcal{N} be a \mathcal{L} -structure, and $X \subset M$ & $f : X \rightarrow N$. $(\mathcal{N}, f(a))_{a \in X}$ is a \mathcal{L}_X -structure by interpreting c_a by $f(a)$.

$\text{diag}(\mathcal{M}) := \{A : A \text{ is an atomic or negated atomic sentence of } \mathcal{L}_M \text{ and } \mathcal{M}_M \models A\}$

- ▶ $f : \mathcal{M} \subset \mathcal{N} \iff (\mathcal{N}, f(a))_{a \in M} \models \text{diag}(\mathcal{M})$
- ▶ $f : \mathcal{M} \prec \mathcal{N} \iff (\mathcal{N}, f(a))_{a \in M} \models \text{Th}(\mathcal{M}_M)$

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References

1436

What is Logic?

- ▶ Arithmetic — the study of numbers.
- ▶ Geometry — the study of figures.
- ▶ Algebra — the study of mathematical symbols.
- ▶ Set Theory — the study of sets.
- ▶ Logic — the study of logical notions.
- ▶ What is a number?
- ▶ What is a line?
- ▶ What is a set?
- ▶ What is a logical notion?

What is Mathematics?

Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true.

— Bertrand Russell

Mathematics is the art of giving the same name to different things.

— Henri Poincaré

Not substance but invariant form is the carrier of the relevant mathematical information.

— F. William Lawvere

Mathematics is the analysis of invariants and of the transformations that preserve them (including the analysis of non-preserved, deformations and symmetry breakings).

What is Geometry? — Klein's Erlangen Program

What is Geometry?

The study of *invariants* under a group of transformations.

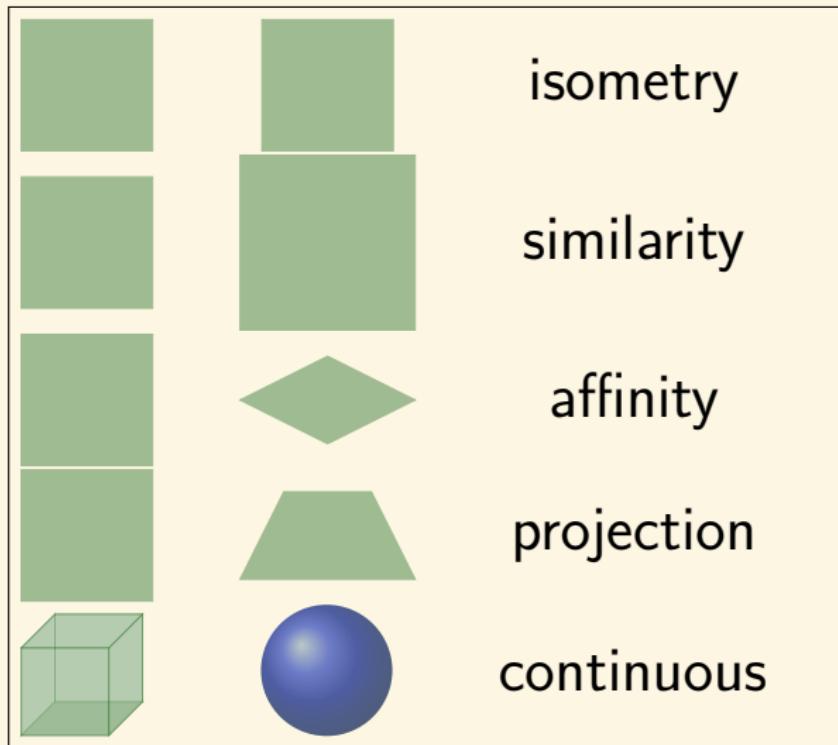
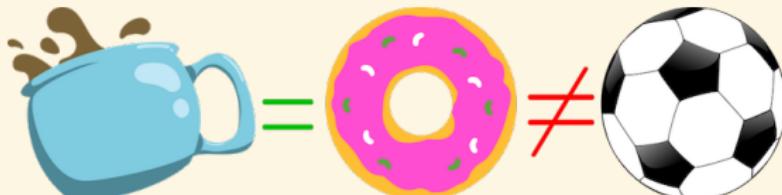


Figure: Felix Klein

What is Geometry? — Klein's Erlangen Program



	isometry	similarity	affine	projective	continuous
location					
length	✓				
area	✓				
perpendicularity	✓	✓			
parallelism	✓	✓	✓		
collinearity	✓	✓	✓	✓	
concurrence	✓	✓	✓	✓	
connectedness	✓	✓	✓	✓	✓

Given a manifold, and a transformation group acting on it, to study its invariants.

— Felix Klein

Klein's Erlangen Program vs Logic

What is Logic?¹¹

Logic is the science that investigates the principles of **valid** reasoning.

what follows from what

The art of thinking and reasoning in strict accordance with the limitations and incapacities of the human understanding. ☺ô☺

— *The Devil's Dictionary*

The study of **invariants** under all automorphisms (**symmetries**).

¹¹Tarski: What are logical notions?

Logic as permutation-invariant theory

Logic as permutation-invariant theory.

The study of **invariants under all automorphisms (symmetries)**.

A notion is “logical” iff it is invariant under all possible one-one transformations of the universe of discourse onto itself.

— Tarski

Logic analyzes the meaning of the concepts common to all the sciences, and establishes the general laws governing the concepts.

— Tarski

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

Connectives

Normal Forms

Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References

1436

Would we gain anything by adding more connectives to the language?

Exclusive Disjunction

$$\nu(p \oplus q) = \nu(p) + \nu(q) \bmod 2$$

⇓

$$\begin{aligned} p \oplus q &\equiv (\neg p \wedge q) \vee (p \wedge \neg q) \\ &\equiv (p \vee q) \wedge (\neg p \vee \neg q) \\ &\equiv \neg(p \leftrightarrow q) \end{aligned}$$

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

$$\frac{p \oplus q}{\neg q}$$

$$\frac{p \oplus q}{\neg p}$$

$$\frac{p}{p \oplus q} ?$$

Nim Game

Nim Game

Given several piles of stones. Two players take turns moving. Each move consists of selecting one of the piles and removing any positive number of stones from it. The winner is the player who removes the last stone.

$$\begin{array}{cccc} & \star & \star & \star \\ & \star & \star & \star \\ & \star & \star & \star \\ \star & \star & \star & \star \\ 3 & 0 & 1 & 1 \\ 4 & 1 & 0 & 0 \\ 5 & 1 & 0 & 1 \\ \hline 2 & 0 & 1 & 0 \end{array} \quad \begin{array}{c} x \\ \oplus \\ y \\ = \\ z \end{array} \quad \begin{array}{ccccc} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \\ c_1 & \cdots & c_n \end{array} \quad \begin{array}{l} x \oplus (y \oplus z) = (x \oplus y) \oplus z \\ x \oplus y = y \oplus x \\ x \oplus 0 = x \\ x \oplus x = 0 \\ x \oplus y = x \oplus z \implies y = z \end{array}$$

where $c_i := a_i \oplus b_i$

Nim Game

Theorem (Bouton Theorem)

In a Nim game with piles of size x_1, \dots, x_n , the first player has a winning strategy iff $\bigoplus_{i=1}^n x_i \neq 0$.

1. If $\bigoplus_{i=1}^n x_i \neq 0$, it is possible to make a move $x_k - x'_k$ so that

$$x_1 \oplus \cdots \oplus x'_k \cdots \oplus x_n = 0, \text{ where } x'_k := x_k \oplus \bigoplus_{i=1}^n x_i.$$

Here's how we construct such a move. Form the nim-sum as a column addition, and look at the leftmost column with an odd number of 1's. Choose the pile that have a 1 in that column.

2. If $\bigoplus_{i=1}^n y_i = 0$, and y_k is changed to $y'_k < y_k$, then
 $y_1 \oplus \cdots \oplus y'_k \cdots \oplus y_n \neq 0$, because otherwise the cancellation law would imply that $y_k = y'_k$.

Example

Example

Let $\#$ be a three-place proposition connective.

The interpretation of $\#$ is given by

$$v(\#(p, q, r)) = \left\lfloor \frac{v(p) + v(q) + v(r)}{2} \right\rfloor$$

then

$$\#(p, q, r) \equiv (p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$$

p	q	r	$\#(p, q, r)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Truth Table & Truth/Boolean Function

A truth assignment for \mathcal{L}^0 is a function $v : \text{Var} \rightarrow \{0, 1\}$.

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$	\dots
p	$\neg p$	0	0	1	1	\dots
0	1	0	1	1	0	\dots
1	0	0	1	0	0	\dots
1	1	1	1	1	1	\dots

A n -place truth/Boolean function is a function $F : \{0, 1\}^n \rightarrow \{0, 1\}$.

x	y	$F_{\wedge}(x, y)$	$F_{\vee}(x, y)$	$F_{\rightarrow}(x, y)$	$F_{\leftrightarrow}(x, y)$	\dots
x	$F_{\neg}(x)$	0	0	1	1	\dots
0	1	0	1	1	0	\dots
1	0	0	1	0	0	\dots
1	1	1	1	1	1	\dots

There are 2^{2^n} distinct truth functions with n places.

Truth Table & Truth/Boolean Function

$$\nu : \text{Var} \rightarrow \{0, 1\}$$

$$F : \{0, 1\}^n \rightarrow \{0, 1\}$$

$\nu(p_1), \dots, \nu(p_n)$	x_1, \dots, x_n	$F_A(x_1, \dots, x_n)$	$\nu(A)$
$\nu_1(p_1), \dots, \nu_1(p_n)$	$=$	$0, \dots, 0$	$F_A(0, \dots, 0)$
\vdots	\vdots	\vdots	\vdots
$\nu_{2^n}(p_1), \dots, \nu_{2^n}(p_n)$	$=$	$1, \dots, 1$	$F_A(1, \dots, 1)$

Definition

Suppose A is a wff whose propositional symbols are p_1, \dots, p_n .
A truth function $F : \{0, 1\}^n \rightarrow \{0, 1\}$ represented by A is

$$F_A(\nu(p_1), \dots, \nu(p_n)) = \nu(A)$$

$$A \equiv B \iff F_A = F_B$$

Theorem (Post1921)

Every truth function $F : \{0, 1\}^n \rightarrow \{0, 1\}$ can be represented by some wff whose only connectives are \neg, \wedge, \vee .

Proof.

$$p_i^{x_i} := \begin{cases} p_i & \text{if } x_i = 1 \\ \neg p_i & \text{otherwise} \end{cases}$$

Case1: $F(\mathbf{x}) = 0$ for all $\mathbf{x} \in \{0, 1\}^n$.

Let $A := p \wedge \neg p$.

Case2:

$$A := \bigvee_{\mathbf{x}: F(\mathbf{x})=1} \bigwedge_{i=1}^n p_i^{x_i}$$

Case1: $F(\mathbf{x}) = 1$ for all $\mathbf{x} \in \{0, 1\}^n$.

Let $B := p \vee \neg p$.

Case2:

$$B := \bigwedge_{\mathbf{x}: F(\mathbf{x})=0} \bigvee_{i=1}^n p_i^{1-x_i}$$

Normal Form

Corollary

Every wff which is not a contradiction is logically equivalent to a formula of disjunctive normal form (DNF):

$$\bigvee_{i=1}^m \bigwedge_{j=1}^n \pm p_{ij}$$

Corollary

Every wff which is not a tautology is logically equivalent to a formula of conjunctive normal form (CNF):

$$\bigwedge_{i=1}^m \bigvee_{j=1}^n \pm p_{ij}$$

Proof.

$$\neg A \equiv \bigvee_{i=1}^m \bigwedge_{j=1}^n \pm p_{ij} \implies A \equiv \neg \left(\bigvee_{i=1}^m \bigwedge_{j=1}^n \pm p_{ij} \right) \equiv \bigwedge_{i=1}^m \bigvee_{j=1}^n \mp p_{ij}$$

CNF Transformation

subformula	replaced by
$A \leftrightarrow B$	$(\neg A \vee B) \wedge (\neg B \vee A)$
$A \rightarrow B$	$\neg A \vee B$
$\neg(A \wedge B)$	$\neg A \vee \neg B$
$\neg(A \vee B)$	$\neg A \wedge \neg B$
$\neg\neg A$	A
$(A_1 \wedge \cdots \wedge A_n) \vee B$	$(A_1 \vee B) \wedge \cdots \wedge (A_n \vee B)$

How many connectives are really necessary?

Definition (Adequate Sets of Connectives)

A set of connectives is **adequate** iff every truth function can be represented by a wff containing only connectives from that set.

- ▶ $\{\neg, \wedge, \vee\}$
- ▶ $\{\neg, \wedge\}; \{\neg, \vee\}; \{\neg, \rightarrow\}; \{\perp, \rightarrow\}$
- ▶ $\{\uparrow\}; \{\downarrow\}$
- ▶ $\{\wedge, \vee, \rightarrow, \leftrightarrow\}; \{\neg, \leftrightarrow\}$ not adequate.

p	\perp
0	0
1	0

$$\perp := p \wedge \neg p$$

$$p \uparrow q := \neg(p \wedge q)$$

$$p \downarrow q := \neg(p \vee q)$$

$$\neg p := p \uparrow p$$

$$p \wedge q := (p \uparrow q) \uparrow (p \uparrow q)$$

$$p \vee q := (p \uparrow p) \uparrow (q \uparrow q)$$

p	q	$p \uparrow q$	$p \downarrow q$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

3-valued Logics

p	$\neg p$	\wedge	0	u	1	\vee	0	u	1	\rightarrow	0	u	1	\leftrightarrow	0	u	1
0	1	0	0	u	0	0	0	u	1	0	1	u	1	0	1	u	0
u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u	u
1	0	1	0	u	1	1	1	u	1	1	0	u	1	1	0	u	1

Table: Bochvar: u as “meaningless”

p	$\neg p$	\wedge	0	u	1	\vee	0	u	1	\rightarrow	0	u	1	\leftrightarrow	0	u	1
0	1	0	0	0	0	0	0	u	1	0	1	1	1	0	1	u	0
u	u	u	0	u	u	u	u	u	u	u	u	u	u	u	u	u	u
1	0	1	0	u	1	1	1	1	1	1	0	u	1	1	0	u	1

Table: Kleene: u as “undefined”

p	$\neg p$	\wedge	0	u	1	\vee	0	u	1	\rightarrow	0	u	1	\leftrightarrow	0	u	1
0	1	0	0	0	0	0	0	u	1	0	1	1	1	0	1	u	0
u	u	u	0	u	u	u	u	u	u	u	u	u	u	u	u	u	u
1	0	1	0	u	1	1	1	1	1	1	0	u	1	1	0	u	1

Table: Lukasiewicz: u as “possible”

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

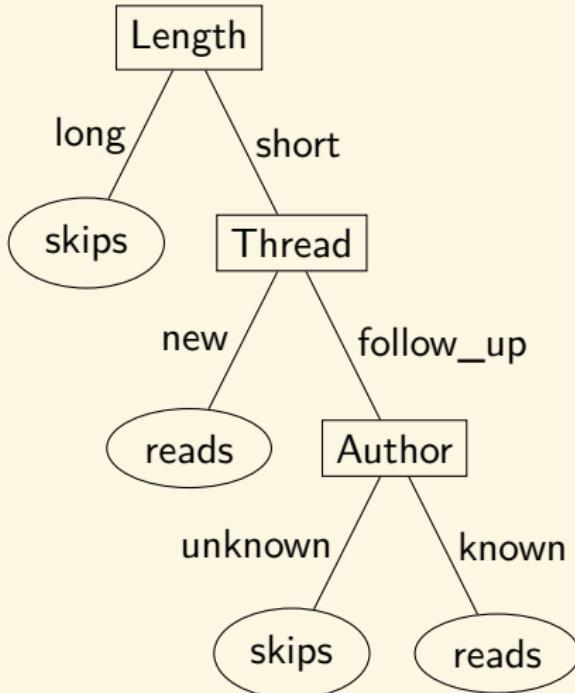
References

1436

Normal Form

- ▶ A *literal* is an atomic formula or its negation.
- ▶ A formula is in negation normal form (NNF) iff it contains no other connectives than \neg , \wedge , \vee , and the negation sign \neg appears in literals only.
- ▶ A clause is any formula of the form: $A_1 \vee A_2 \vee \dots \vee A_n$, where $n \geq 1$ and A_1, A_2, \dots, A_n are literals.
- ▶ A Horn clause is a clause in which at most one literal is positive.
- ▶ An open formula is in conjunctive normal form (CNF) iff it is a conjunction of clauses.
- ▶ An open formula is in disjunctive normal form (DNF) iff it is a disjunction of one or more conjunctions of one or more literals.
- ▶ A CNF formula is in full conjunctive normal form (FCNF) iff each of its variables appears exactly once in every clause. (similarly, full disjunctive normal form)

Decision Tree vs Horn Clause



skips \leftarrow long
reads \leftarrow short \wedge new
reads \leftarrow short \wedge follow_up \wedge known
skips \leftarrow short \wedge follow_up \wedge unknown

- We want a small and efficient tree
- Ask the question which is most informative

NNF/CNF/DNF

subformula	replaced by
$A \leftrightarrow B$	$(\neg A \vee B) \wedge (A \vee \neg B)$
$A \rightarrow B$	$\neg A \vee B$
$\neg\neg A$	A
$\neg(A \vee B)$	$\neg A \wedge \neg B$
$\neg(A \wedge B)$	$\neg A \vee \neg B$
$\neg\forall x A$	$\exists x \neg A$
$\neg\exists x A$	$\forall x \neg A$

subformula	replaced by
$(A \wedge B) \vee C$	$(A \vee C) \wedge (B \vee C)$
$C \vee (A \wedge B)$	$(C \vee A) \wedge (C \vee B)$

subformula	replaced by
$(A \vee B) \wedge C$	$(A \wedge C) \vee (B \wedge C)$
$C \wedge (A \vee B)$	$(C \wedge A) \vee (C \wedge B)$

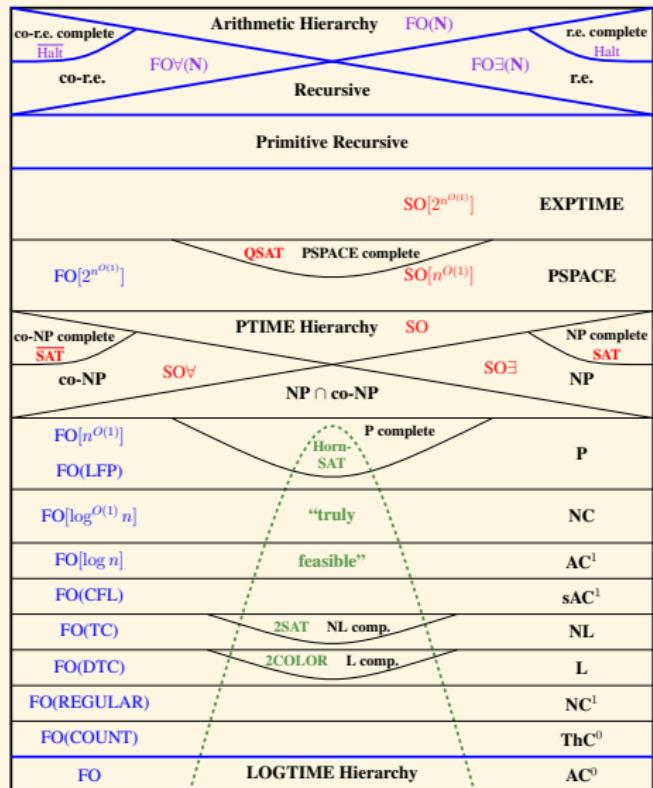
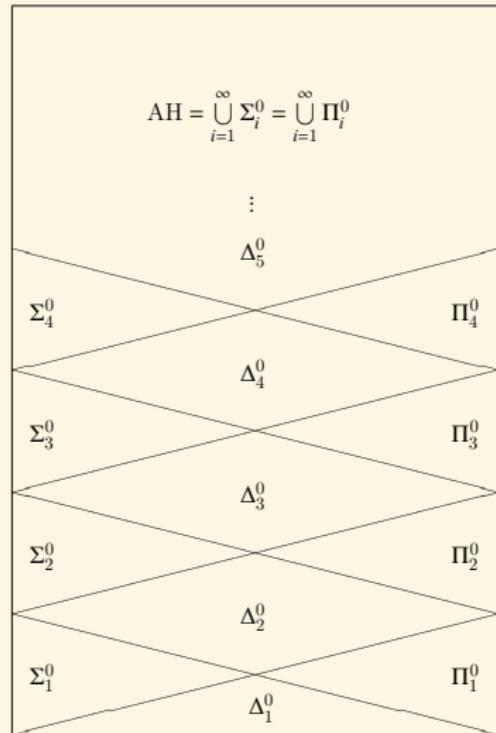
- ▶ Any formula can be equivalently transformed into NNF.
- ▶ Any open formula can be equivalently transformed into CNF/DNF.

PNF

- ▶ A formula is in prenex normal form (PNF) iff all its quantifiers (if any) are in its prefix. (PCNF)
- ▶ Any formula can be equivalently transformed into PNF/PCNF.

subformula	replaced by	
$\neg \forall x A$	$\exists x \neg A$	
$\neg \exists x A$	$\forall x \neg A$	
$\forall x A(x) \wedge \forall x B(x)$	$\forall x(A(x) \wedge B(x))$	
$\exists x A(x) \vee \exists x B(x)$	$\exists x(A(x) \vee B(x))$	
$\forall x A(x)$	$\forall y A[y/x]$	where $y \notin \text{Fv}(A) \cup \text{Bv}(A)$
$A \vee Qx B$	$Qx(A \vee B)$	where $x \notin \text{Fv}(A)$
$A \wedge Qx B$	$Qx(A \wedge B)$	where $x \notin \text{Fv}(A)$
$A \rightarrow \forall x B$	$\forall x(A \rightarrow B)$	where $x \notin \text{Fv}(A)$
$A \rightarrow \exists x B$	$\exists x(A \rightarrow B)$	where $x \notin \text{Fv}(A)$
$\forall x A \rightarrow B$	$\exists x(A \rightarrow B)$	where $x \notin \text{Fv}(A)$
$\exists x A \rightarrow B$	$\forall x(A \rightarrow B)$	where $x \notin \text{Fv}(A)$

PNF & Arithmetical Hierarchy



Skolem Normal Form

- ▶ A formula is in *Skolem normal form* (SNF) iff it is in PNF (PCNF) without existential quantifiers.
- ▶ Skolemization: Replace $\forall x_1 \dots \forall x_n \exists y A$ by $\forall x_1 \dots \forall x_n A[f(x_1, \dots, x_n)/y]$, where f is a new function symbol. If there are no universal quantifiers preceding \exists , replace $\exists x A$ by $A[c/x]$, where c is a new constant. Given A , in finitely many steps we can obtain its *Skolem normal form* A^{SNF} without existential quantifiers.
- ▶ Any formula can be *equisatisfiably* transformed into SNF.

Warning: $A^{\text{SNF}} \models A$ but the converse is not true in general.

Exercise (Transform the following sentence into SNF)

Who loves all animals, is in turn loved by someone.

Herbrand Normal Form

A is satisfiable iff A^{SNF} is satisfiable.

$$A^{\text{HNF}} := \left(\neg(\neg A)^{\text{SNF}} \right)^{\text{NNF}}$$

$$\models A \iff \models A^{\text{HNF}}$$

Example:

$$(\forall x \exists y \forall z A(x, y, z))^{\text{SNF}} = \forall x z A(x, f(x), z)$$

$$(\forall x \exists y \forall z A(x, y, z))^{\text{HNF}} = \exists y A(a, y, f(y))$$

Herbrand Universe

Definition (Herbrand Universe)

Given a sentence A in Skolem normal form,

- ▶ $H_0 := \{\text{all constants in } A\}$. If no constant in A then $H_0 := \{a\}$ for a new constant a .
- ▶ $H_{i+1} := \{f(t_1, \dots, t_n) : f \text{ in } A \text{ and } t_j \in H_i, j = 1, \dots, n\}$
- ▶ $H_A := \bigcup_{i \in \omega} H_i$

The Herbrand universe of a language \mathcal{L} is the set of all ground terms of \mathcal{L} . If no constant in \mathcal{L} , then add a new constant to \mathcal{L} .

Herbrand Structure

Definition (Herbrand Structure)

A Herbrand structure for \mathcal{L} is (H, I) s.t.

- ▶ H is the Herbrand universe of \mathcal{L} .
- ▶ for every ground term t , $I(t) = t$.

Theorem

A formula A is satisfiable iff there is a Herbrand structure satisfying it.

Proof.

Assume A is in Skolem normal form, and it is satisfied by some structure (M, I) . Then Herbrand structure $(H_A, J) \models A$, where for each ground term $t : J(t) = t$, and for each predicate symbol P ,

$$J(P) = \{(t_1, \dots, t_n) \in H_A : M, I \models P(t_1, \dots, t_n)\}.$$

Herbrand's Theorem

For a quantifier-free wff $A(x_1, \dots, x_n)$, the Herbrand expansion over a set D of ground terms is $\mathcal{E}(A, D) := \{A(t_1, \dots, t_n) : t_i \in D\}$.

Theorem (Herbrand's Theorem)

A sentence $\forall x A(x)$ in Skolem normal form is unsatisfiable iff some finite subset $K \subset \mathcal{E}(A, H_A)$ is unsatisfiable.

Theorem (Herbrand's Theorem)

Suppose A is a sentence. Then

$$\vdash A \iff \vdash \bigvee_{i=1}^m A'(t_{i1}, \dots, t_{in})$$

for some $m > 0$ and a finite sequence of terms t_{ij} with $1 \leq i \leq m$ and $1 \leq j \leq n$, where A' is obtained from A^{HNF} by dropping the quantifiers.

Remark: If a sentence is entailed by an FOL KB, it is entailed by a finite subset of the propositional KB.

Resolution — Example

Given clauses $A = P(f(x)) \vee Q(x)$ and $B = \neg P(x) \vee \neg P(y)$.

1. Separate their variables by standard substitutions $\{x_1/x\}$ and $\{y_1/x, y_2/y\}$.

$$A' = \{P(f(x_1)), Q(x_1)\} \quad B' = \{\neg P(y_1), \neg P(y_2)\}$$

2. Pick a subset $C \subset A'$ containing literals all of the same sign, and a subset $D \subset B'$ containing literals all of the opposite sign of C such that $|C \cup D|$ is unifiable.

$$C = \{P(f(x_1))\} \quad D = \{\neg P(y_1), \neg P(y_2)\}$$

$$|C \cup D| = \{P(f(x_1)), P(y_1), P(y_2)\}$$

3. A most general unifier for $|C \cup D|$ is

$$\sigma = \{f(x_1)/y_1, f(x_1)/y_2\}$$

4. A resolvent for A and B is:

$$R = (A'\sigma \setminus C\sigma) \cup (B'\sigma \setminus D\sigma) = \{Q(x_1)\}$$

Resolution

Theorem (Soundness)

If R is a resolvent of A and B , then any model satisfying both A and B will also satisfy R .

- ▶ For a wff A , $\mathcal{R}(A)$ is A extended with all resolvents to clauses of A .
- ▶ The successive application of the resolution rule yields a complete proof procedure.

Theorem (Completeness)

If A is unsatisfiable, then $\mathcal{R}^n(A)$ will contain the empty clause for some n .

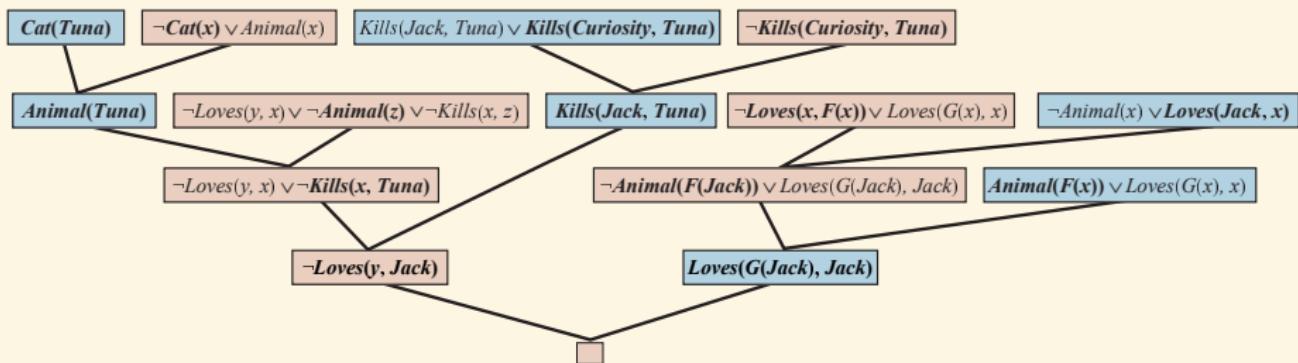
Resolution — Example

- ▶ Everyone who loves all animals is loved by someone.
- ▶ Anyone who kills an animal is loved by no one.
- ▶ Jack loves all animals.
- ▶ Either Jack or Curiosity killed the cat, who is named Tuna.
- ▶ Did Curiosity kill the cat?

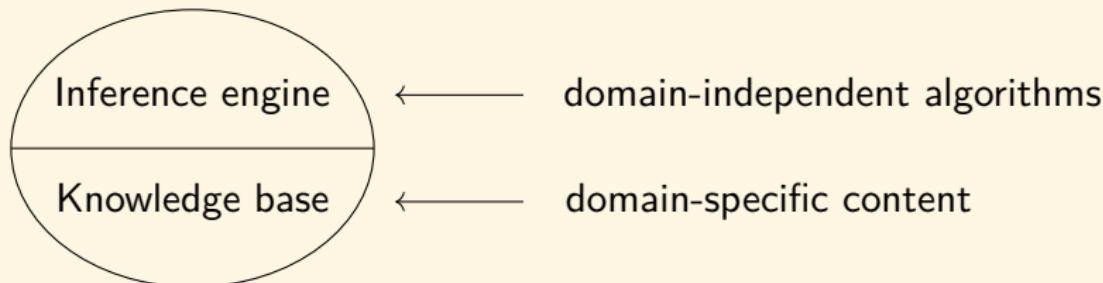
1. $\forall x(\forall y(\text{Animal}(y) \rightarrow \text{Loves}(x, y)) \rightarrow \exists z \text{ Loves}(z, x))$
2. $\forall x((\exists z \text{ Animal}(z) \wedge \text{Kills}(x, z)) \rightarrow \forall y \neg \text{Loves}(y, x))$
3. $\forall x(\text{Animal}(x) \rightarrow \text{Loves}(\text{Jack}, x))$
4. $\text{Kills}(\text{Jack}, \text{Tuna}) \vee \text{Kills}(\text{Curiosity}, \text{Tuna})$
5. $\text{Cat}(\text{Tuna})$
6. $\forall x(\text{Cat}(x) \rightarrow \text{Animal}(x))$
7. $\neg \text{Kills}(\text{Curiosity}, \text{Tuna})$

Resolution — Example

1. $\left(\text{Animal}(F(x)) \vee \text{Loves}(G(x), x) \right) \wedge \left(\neg \text{Loves}(x, F(x)) \vee \text{Loves}(G(x), x) \right)$
2. $\neg \text{Loves}(y, x) \vee \neg \text{Animal}(z) \vee \neg \text{Kills}(x, z)$
3. $\neg \text{Animal}(x) \vee \text{Loves}(\text{Jack}, x)$
4. $\text{Kills}(\text{Jack}, \text{Tuna}) \vee \text{Kills}(\text{Curiosity}, \text{Tuna})$
5. $\text{Cat}(\text{Tuna})$
6. $\neg \text{Cat}(x) \vee \text{Animal}(x)$
7. $\neg \text{Kills}(\text{Curiosity}, \text{Tuna})$



Logical Agent: Knowledge-Based Agent



A knowledge-based agent uses its knowledge base to

- ▶ represent its background knowledge: states, actions, etc.
- ▶ incorporate new percepts
- ▶ update internal representations of the world
- ▶ deduce hidden properties of the world
- ▶ deduce appropriate actions

Reducing First Order Inference to Propositional Inference

- ▶ Universal Instantiation

$$\frac{\forall x A}{A[t/x]} \text{ where } t \text{ is a ground term}$$

- ▶ can be applied several times to add new sentences
- ▶ the new KB is logically equivalent to the old
- ▶ Existential Instantiation

$$\frac{\exists x A}{A(a)} \text{ where } a \text{ is a new constant}$$

- ▶ can be applied once to replace the existential sentence
- ▶ the new KB is not equivalent to the old
- ▶ but is satisfiable iff the old KB was satisfiable

Reducing First Order Inference to Propositional Inference

- ▶ Claim: a sentence is entailed by the new KB iff it is entailed by the original KB
- ▶ Claim: every FOL KB can be propositionalized so as to preserve entailment

Theorem (Herbrand's Theorem)

If a sentence A is entailed by an FOL KB, it is entailed by a finite subset of the propositional KB.

- ▶ Idea: propositionalize KB and query, apply resolution, return result
 - for $n = 0$ to ∞ do
 - create a propositional KB by instantiating with depth- n terms see if A is entailed by this KB
- ▶ Problem: works if A is entailed, loops if A is not entailed
- ▶ Theorem (Turing, Church): entailment in FOL is semidecidable.

GNF & Self-reference Paradox

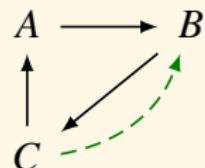
Example

- A. The next statement is false.
- B. The next statement is false.
- C. The first statement is false.

$$A \leftrightarrow \neg B$$

$$B \leftrightarrow \neg C$$

$$C \leftrightarrow \neg A$$



- The above odd cycle is a generalization of the liar paradox • ↗
- To remove the paradox, we can add the edge C to B , i.e., $C \leftrightarrow \neg A \wedge \neg B$.
- Then $A = C = 0, B = 1$.

Definition (Graph Normal Form)

- A *basic formula*, over alphabet Σ , is an equivalence $x \leftrightarrow \bigwedge_{i \in I} \neg x_i$.
- A *theory in GNF* is a set of basic formulas with each $x \in \Sigma$ occurs exactly once on the left of such an equivalence.

- ▶ For a theory Δ in GNF, we form a graph $G(\Delta) = (W, R)$, with the vertex set W and an edge from each variable occurring on the left of \leftrightarrow in a basic formula to all the variables occurring on the right of \leftrightarrow .
- ▶ Conversely, given a directed graph $F = (W, R)$, we can form a theory in GNF $D(F) := \left\{ x \leftrightarrow \bigwedge_{y:Rxy} \neg y : x \in W \right\}$.
- ▶ Obviously, we have $D(G(\Delta)) = \Delta$ and $G(D(F)) = F$.
- ▶ We say that $\nu \models (W, R)$ iff ν assigns truth-values to W so that

$$\nu(x) = 1 \iff \forall y : Rxy \rightarrow \nu(y) = 0$$

- ▶ Obviously, for a graph F : $\nu \models F \iff \nu \models D(F)$. For a theory Δ in GNF: $\nu \models \Delta \iff \nu \models G(\Delta)$.

A directed graph (W, R) is *finitary* iff $|\{y : Rxy\}| < \infty$ for all $x \in W$.

Theorem (Richardson's Theorem)

- ▶ A finitary graph with no odd cycle is satisfiable.
- ▶ If every odd cycle has at least two symmetrical arcs, then the graph is satisfiable.

Remark: Sinks (vertices with no outgoing edges) must be assigned 1.

Vertices with edges to sinks must be assigned 0 . . .

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

 Introduction

 Syntax

 Semantics

 Formal System

 Definability & Isomorphism

 What is Logic?

 Connectives

 Normal Forms

 Meta-Theorems

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References

1436

Model & Theory & Semantic Entailment

- $\text{Mod}(A) := \{\mathcal{M} : \mathcal{M} \models A\}$
- $\text{Mod}(\Gamma) := \bigcap_{A \in \Gamma} \text{Mod}(A)$
- $\text{Th}(\mathcal{M}) := \{A : \mathcal{M} \models A\}$
- $\text{Th}(\mathcal{K}) := \bigcap_{\mathcal{M} \in \mathcal{K}} \text{Th}(\mathcal{M})$
- $\text{Cn}(\Gamma) := \{A : \Gamma \models A\}$

- $\Gamma \subset \Gamma' \implies \text{Mod}(\Gamma') \subset \text{Mod}(\Gamma)$
- $\mathcal{K} \subset \mathcal{K}' \implies \text{Th}(\mathcal{K}') \subset \text{Th}(\mathcal{K})$
- $\Gamma \subset \text{Th}(\text{Mod}(\Gamma))$
- $\mathcal{K} \subset \text{Mod}(\text{Th}(\mathcal{K}))$
- $\text{Mod}(\Gamma) = \text{Mod}(\text{Th}(\text{Mod}(\Gamma)))$
- $\text{Th}(\mathcal{K}) = \text{Th}(\text{Mod}(\text{Th}(\mathcal{K})))$
- $\text{Cn}(\Gamma) = \text{Th}(\text{Mod}(\Gamma))$
- $\Gamma \subset \Gamma' \implies \text{Cn}(\Gamma) \subset \text{Cn}(\Gamma')$
- $\text{Cn}(\text{Cn}(\Gamma)) = \text{Cn}(\Gamma)$

Theory & Axiomatization

- ▶ A set Γ of sentences is a **theory** iff $\Gamma = \text{Cn}(\Gamma)$.
- ▶ A theory Γ is **complete** iff for every sentence A , either $A \in \Gamma$ or $\neg A \in \Gamma$.
- ▶ A theory Γ is **finitely axiomatizable** iff $\Gamma = \text{Cn}(\Sigma)$ for some finite set Σ of sentences.
- ▶ A theory Γ is **axiomatizable** iff there is a decidable set Σ of sentences s.t. $\Gamma = \text{Cn}(\Sigma)$.
- ▶ A class \mathcal{K} of structures is an **elementary class (EC)** iff $\mathcal{K} = \text{Mod}(A)$ for some sentence A .
- ▶ A class \mathcal{K} of structures is an **elementary class in wider sense (EC_Δ)** iff $\mathcal{K} = \text{Mod}(\Sigma)$ for some set Σ of sentences.

Definitional Extension

Definition (Definitional Extension)

\mathcal{L} is a first order language, and T is a \mathcal{L} theory.

- ▶ An explicit definition of a predicate symbol $P \in \mathcal{L}^+$ in \mathcal{L} is a sentence $\forall x(P(x) \leftrightarrow A(x))$, where $A(x)$ is a \mathcal{L} -formula.
- ▶ An explicit definition of an n -ary function symbol $f \in \mathcal{L}^+$ in \mathcal{L} is a sentence $\forall x(f(x) = y \leftrightarrow A(x, y))$, where $A(x, y)$ is a \mathcal{L} -formula and $T \vdash \forall x \exists! y A(x, y)$.
- ▶ An explicit definition of a constant symbol $c \in \mathcal{L}^+$ in \mathcal{L} is a sentence $\forall x(x = c \leftrightarrow A(x))$, where $A(x)$ is a \mathcal{L} -formula and $T \vdash \exists! x A(x)$.

A *definitional extension* of a \mathcal{L} -theory T to \mathcal{L}^+ is a T^+ -theory

$$T^+ = T \cup \{\delta_s : s \in \mathcal{L}^+ \setminus \mathcal{L}\}$$

where the sentence δ_s is an explicit definition of s in \mathcal{L} .

Definitionally Equivalent

Let T^+ be a definitional extension of T . Define the inclusion translation map $I : T \rightarrow T^+$ and the reduction map $R : T^+ \rightarrow T$: for each symbol $s \in \mathcal{L}^+ \setminus \mathcal{L}$, let $Rs = \delta_s$, where δ_s is the explicit definition of s . For $s \in \mathcal{L}$, $Rs = s$.

Theorem

If T^+ is a definitional extension of T , then

- ▶ $T \vdash A \leftrightarrow RIA$ for any \mathcal{L} -formula A .
- ▶ $T^+ \vdash A \leftrightarrow IRA$ for any \mathcal{L}^+ -formula A .
- ▶ T^+ is a conservative extension of T .

Definition (Definitionally Equivalent)

Let T_1 be a \mathcal{L}_1 -theory and T_2 be a \mathcal{L}_2 -theory. Then T_1 and T_2 are said to be *definitionally equivalent* if there is a definitional extension T_1^+ of T_1 to $\mathcal{L}_1 \cup \mathcal{L}_2$ and a definitional extension T_2^+ of T_2 to $\mathcal{L}_1 \cup \mathcal{L}_2$ such that $Cn(T_1^+) = Cn(T_2^+)$.

Consistency & Satisfiability

- ▶ Γ is **consistent** iff $\Gamma \not\vdash \perp$.
- ▶ Γ is **maximal** iff for every wff A , either $A \in \Gamma$ or $\neg A \in \Gamma$.
- ▶ Γ is **maximal consistent** iff it is both consistent and maximal.
- ▶ Γ is **satisfiable** iff $\text{Mod}(\Gamma) \neq \emptyset$.
- ▶ Γ is **finitely satisfiable** iff every finite subset of Γ is satisfiable.

Soundness Theorem

Theorem (Soundness Theorem)

$$\Gamma \vdash A \implies \Gamma \vDash A$$

Proof.

by induction on derivation lengths.

Truth in a model is preserved under making deductions.

Kurt Gödel 1906-1978

“I am unprovable.”¹²

- Completeness.

I think (consistently), therefore I am.

(Consistency implies existence.)

- Incompleteness.

1. provable < true
2. un-self-aware

- Consistency of AC and CH.



¹² Gödel: On formally undecidable propositions of Principia Mathematica and related systems.

Completeness Theorem

Theorem (Completeness Theorem — Gödel 1930)

$$\Gamma \vDash A \implies \Gamma \vdash A$$

Corollary

Any *consistent* set of wffs is *satisfiable*.

$$\begin{array}{ccc} \Gamma \vDash A & \iff & \Gamma \vdash A \\ \Updownarrow & & \Updownarrow \\ \Gamma \cup \{\neg A\} & \iff & \Gamma \cup \{\neg A\} \\ \text{unsatisfiable} & & \text{inconsistent} \end{array}$$

Proof of Completeness Theorem — step1

Lemma (Lindenbaum Lemma)

Any consistent set Θ of sentences can be extended to a maximal consistent set Δ of sentences of the same language.

Proof.

Arrange all the sentences in a sequence $\langle A_\xi : \xi < \kappa \rangle$.

$$\begin{aligned}\Theta_0 &:= \Theta \\ \Theta_{\xi+1} &:= \begin{cases} \Theta_\xi \cup \{A_\xi\} & \text{if } \Theta_\xi \cup \{A_\xi\} \text{ is consistent} \\ \Theta_\xi \cup \{\neg A_\xi\} & \text{otherwise} \end{cases} \\ \Theta_\xi &:= \bigcup_{\alpha < \xi} \Theta_\alpha \quad \text{if } \xi \text{ is a limit ordinal} \\ \Delta := \bigcup_{\xi < \kappa} \Theta_\xi &\text{ is maximal consistent.}\end{aligned}$$

Proof of Completeness Theorem — step2

A set Δ is Henkin iff Δ is maximally consistent and for any formula of the form $\exists x A$ there exists a closed term t s.t. $\exists x A \rightarrow A[t/x] \in \Delta$.

Lemma (Closure Lemma)

If Γ is consistent, then there is a Henkin set $\Delta \supset \Gamma$.

Proof.

Let C be a set of new constants. $\mathcal{L}^+ := \mathcal{L} \cup C$, $\mathcal{L} \cap C = \emptyset$, $|C| = |\mathcal{L}|$.

Assume $|C| = \kappa$, and $C = \{c_\xi : \xi < \kappa\}$. Arrange all formulas of \mathcal{L}^+ with at most one free variable in a sequence $\langle A_\xi : \xi < \kappa \rangle$. Let

$$\Gamma_0 := \Gamma$$

$$\Gamma_{\xi+1} := \Gamma_\xi \cup \{\exists x A_\xi(x) \rightarrow A_\xi[c_\beta/x]\}$$

where c_β is the first new constant not occurring in $\Gamma_\xi \cup \{A_\xi\}$.

$$\Gamma_\xi := \bigcup_{\alpha < \xi} \Gamma_\alpha \quad \text{if } \xi \text{ is a limit ordinal}$$

Then $\Theta := \bigcup_{\xi < \kappa} \Gamma_\xi$ is consistent, and we can extend Θ to a maximal consistent set $\Delta \supset \Theta$ by Lindenbaum lemma.

Proof of Completeness Theorem — step3

Lemma (Term Models Lemma)

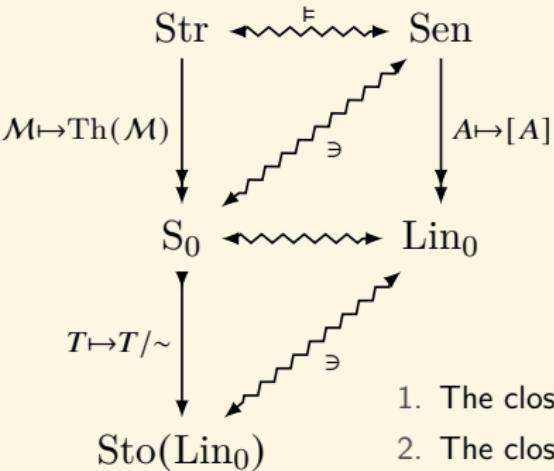
If Δ is maximal consistent, then there is an interpretation \mathcal{M}, ν s.t.

$$\mathcal{M}, \nu \models A \iff A \in \Delta$$

Proof.

- $M := \{[t] : t \in \text{Term}\}$ where Term is the set of terms of \mathcal{L}^+ ,
 $[t] := \{s : s \sim t\}$, $s \sim t := s = t \in \Delta$
- $([t_1], \dots, [t_n]) \in P^{\mathcal{M}} := P(t_1, \dots, t_n) \in \Delta$
- $f^{\mathcal{M}}([t_1], \dots, [t_n]) := [f(t_1, \dots, t_n)]$
- $c^{\mathcal{M}} = [c]$
- $\nu(x) := [x]$

Stone Space of Lindenbaum Algebra



- Str: the class of structures.
- Sen: the set of sentences.
- S₀: the set of complete theories.
- Lin₀ = Sen/∼
- Sto(M): the set of ultrafilters of M.

1. The closed subsets of Sen are precisely the theories.
2. The closed subsets of S₀ compose a Hausdorff topology.
3. $M \mapsto \text{Th}(M) : \text{Str} \rightarrow S_0$ is continuous, and $[M] \mapsto \text{Th}(M)$ is a homomorphism, S₀ is a Kolmogorov quotient Str/\equiv .
4. For every theory T , T/\sim is a filter of Lin₀.
5. For every complete theory T , T/\sim is an ultrafilter of Lin₀.
6. $T \mapsto T/\sim : S_0 \rightarrow \text{Sto}(\text{Lin}_0)$ is a homomorphism.
7. The image is dense in Sto(Lin₀).
8. The image is a closed subspace of Sto(Lin₀).
9. $T \mapsto T/\sim : S_0 \rightarrow \text{Sto}(\text{Lin}_0)$ iff the topology on S₀ is compact.

Compactness Theorem

Theorem (Compactness Theorem)

A set of wffs is satisfiable iff it is finitely satisfiable.

Corollary

If $\Gamma \models A$, then there is a finite $\Gamma_0 \subset \Gamma$ s.t. $\Gamma_0 \models A$.

Corollary

If a set Γ of sentences has arbitrarily large finite models, then it has an infinite model.

Corollary

There is a countable structure $M \equiv N$ but $M \not\cong N$.

Ultraproduct & Łoś Theorem

Definition (Ultraproduct)

Suppose $\{\mathcal{M}_i : i \in I\}$ is a set of structures, and U is an ultrafilter on I . Define $\mathcal{N} := \prod_{i \in I} \mathcal{M}_i / U$ as follows:

- ▶ $N := \prod_{i \in I} M_i / \sim = \left\{ [f] : f \in \prod_{i \in I} M_i \right\}$ where
 $f \sim g := \{i \in I : f(i) = g(i)\} \in U$
- ▶ $P^N([f_1], \dots, [f_n]) := \{i \in I : P^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))\} \in U$
- ▶ $F^N([f_1], \dots, [f_n]) := [f]$ where $f(i) := F^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))$

Theorem (Łoś Theorem)

$$\prod_{i \in I} \mathcal{M}_i / U \models A([f_1], \dots, [f_n]) \iff \{i \in I : \mathcal{M}_i \models A(f_1(i), \dots, f_n(i))\} \in U$$

Ultrapower

Let $j : a \mapsto [f_a]$, where $f_a(i) = a$ for $i \in I$. Then

$$j : \mathcal{M} \prec \prod_{i \in I} \mathcal{M}/U$$

Theorem (Kiesler-Shelah)

$\mathcal{M} \equiv \mathcal{N}$ iff for some I and an ultrafilter U on I , $\prod_{i \in I} \mathcal{M}/U \cong \prod_{i \in I} \mathcal{N}/U$.

Compactness Theorem

Corollary (Compactness Theorem)

A set Γ of wffs is satisfiable iff it is finitely satisfiable.

Proof.

Let $I := \{\Delta \subset \Gamma : |\Delta| < \infty\}$.

Then $\forall \Delta \in I \exists M_\Delta : M_\Delta \models \Delta$.

Let $\hat{A} := \{\Delta \in I : A \in \Delta\}$.

Then $F := \{\hat{A} : A \in \Gamma\}$ has the finite intersection property because

$$\{A_1, \dots, A_n\} \in \hat{A}_1 \cap \dots \cap \hat{A}_n$$

By the ultrafilter theorem, F can be extended to an ultrafilter U on I .

For $A \in \Gamma$,

$$\begin{aligned}\hat{A} \in U \quad \& \quad \hat{A} \subset \{\Delta \in I : M_\Delta \models A\} &\implies \{\Delta \in I : M_\Delta \models A\} \in U \\ &\implies \prod_{\Delta \in I} M_\Delta / U \models A\end{aligned}$$

Compactness and Compactification

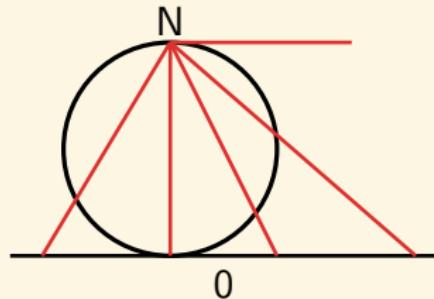
- ▶ Extreme value theorem: A continuous real-valued function on a compact space is bounded and attains its maximum and minimum values.
- ▶ A subset of a topological space is *compact* iff every open cover of it has a finite subcover.
- ▶ Heine-Borel Theorem: A subset of \mathbb{R} is compact iff it is closed and bounded.
- ▶ Cantor's Intersection Theorem: A decreasing nested sequence of non-empty, closed and bounded subsets of \mathbb{R} has a non-empty intersection.
- ▶ Bolzano-Weierstrass Theorem: Every bounded sequence of real numbers has a convergent subsequence.

Compactness

finite \implies infinite
local \implies global

Compactification

$$\mathbb{R} \implies \mathbb{R} \cup \{-\infty, +\infty\}$$



$$x \mapsto \left(\frac{x}{1+x^2}, \frac{x^2}{1+x^2} \right)$$

Nonstandard Analysis

Theorem

There is a structure \mathcal{R}^ s.t.*

$$\mathcal{R} \equiv \mathcal{R}^* \quad \mathcal{R} \subset \mathcal{R}^*$$

Proof.

$$\text{Th}(\mathcal{R}) \cup \{x > c_r : r \in \mathbb{R}\}$$



Figure: Robinson

Nonstandard Analysis

Let U be a nonprinciple ultrafilter on \mathbb{N} .

$$\prod_{i \in \mathbb{N}} \mathcal{R}/U \models \text{Th}(\mathcal{R})$$

Let $\varepsilon := \left[(1, \frac{1}{2}, \frac{1}{3}, \dots) \right] \in \mathbb{R}$.

For any $n \in \mathbb{N}$,

$$\prod_{i \in \mathbb{N}} \mathcal{R}/U \models \varepsilon < \frac{1}{n}$$

Theorem

- ▶ \mathcal{K} is EC_{Δ} iff \mathcal{K} is closed under ultraproducts and elementary equivalence.
- ▶ \mathcal{K} is EC iff both \mathcal{K} and the complement of \mathcal{K} are closed under ultraproducts and elementary equivalence.

Application of Compactness — Limitation of FOL

Theorem

If a set Γ of sentences has arbitrarily large finite models, then it has an infinite model.

Proof.

Consider the set $\Gamma \cup \{\exists^{\geq 2}, \exists^{\geq 3}, \dots\}$, where $\exists^{\geq k}$ says “there exists at least k distinct elements”. By hypothesis any finite subset has a model. By Compactness Theorem the entire set has a model, which is infinite.

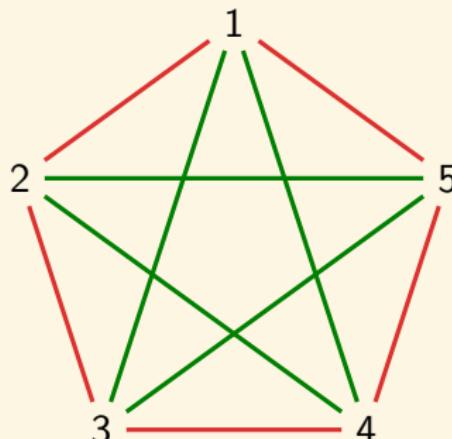
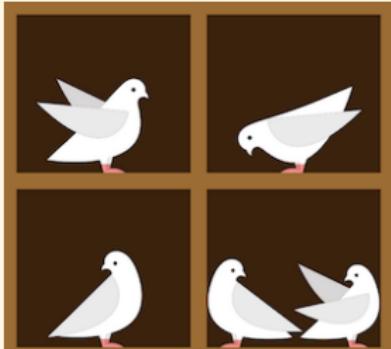
Applications of Compactness

- ▶ The class of all finite structures is not EC_{Δ} . (Model finiteness is undefinable even by a set of formulas.)
- ▶ The class of all infinite structures is EC_{Δ} but not EC . (Model infiniteness is definable by a set of formulas but undefinable by a single formula.)
- ▶ The class of graphs / groups / rings / fields / ordered fields / n -dimensional vector spaces / fields of characteristic p is EC ; the class of infinite groups / divisible groups / torsion-free groups / infinite rings / infinite-dimensional vector spaces / fields of characteristic 0 is EC_{Δ} but not EC ; the class of all connected graphs / finite graphs / finite groups / finite rings / finite fields / algebraically closed fields / torsion groups / finite-dimensional vector spaces / noetherian commutative rings is not EC_{Δ} .

Ramsey in the Dining Room

Problem (Complete Disorder is Impossible!)

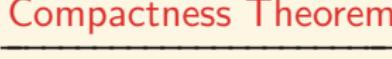
- ▶ How many people do you need to invite in a party in order to have that either at least n of them are mutual strangers or at least n of them are mutual acquaintances?
- ▶ How may we know that such number exists for any n ?



Complete Disorder is Impossible!

Theorem (Infinite Ramsey Theorem)

If (V, E) is a graph with infinitely many vertices, then it has an infinite clique or an infinite independent set.

Infinite Ramsey Theorem  Compactness Theorem → Finite Ramsey Theorem

Theorem (Finite Ramsey Theorem)

For every $m, n \geq 1$ there is an integer $R(m, n)$ s.t. any graph with at least $R(m, n)$ vertices has a clique with m vertices or an independent set with n vertices.

$$R(m, n) \leq R(m - 1, n) + R(m, n - 1)$$

$$R(m, n) \leq \binom{m + n - 2}{m - 1}$$

Ramsey Number

m, n	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	9	14	18	23	28	36	40 – 42
4	1	4	9	18	25	36 – 41	49 – 61	59 – 84	73 – 115	92 – 149
5	1	5	14	25	43 – 48	58 – 87	80 – 143	101 – 216	133 – 316	149 – 442
6	1	6	18	36 – 41	58 – 87	102 – 165	115 – 298	134 – 495	183 – 780	204 – 1171
7	1	7	23	49 – 61	80 – 143	115 – 298	205 – 540	217 – 1031	252 – 1713	292 – 2826
8	1	8	28	59 – 84	101 – 216	134 – 495	217 – 1031	282 – 1870	329 – 3583	343 – 6090
9	1	9	36	73 – 115	133 – 316	183 – 780	252 – 1713	329 – 3583	565 – 6588	581 – 12677
10	1	10	40 – 42	92 – 149	149 – 442	204 – 1171	292 – 2826	343 – 6090	581 – 12677	798 – 23556



Figure: Ramsey 1903–1930



Figure: Erdős 1913–1996

Ramsey Number — Probabilistic Method

Theorem

$$\forall k \geq 2 : R(k, k) \geq 2^{\frac{k}{2}}$$

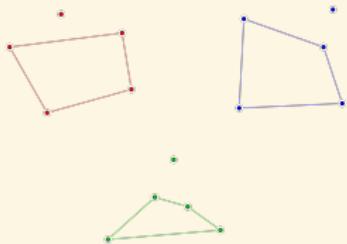
Proof.

$R(2, 2) = 2, R(3, 3) = 6$. Assume $k \geq 4$. Suppose $N < 2^{\frac{k}{2}}$, and consider all random red-blue colorings. Let A be a set of vertices of size k . The probability of the event A_R that the edges in A are all colored red is then $2^{-\binom{k}{2}}$. Hence the probability p_R for some k -set to be colored all red is bounded by

$$p_R = P\left(\bigcup_{|A|=k} A_R\right) \leq \sum_{|A|=k} P(A_R) = \binom{N}{k} 2^{-\binom{k}{2}} < \frac{1}{2}$$

By symmetry, $p_B < \frac{1}{2}$. So $p_R + p_B < 1$ for $N < 2^{\frac{k}{2}}$.

Happy Ending Problem



Any set of 5 points in the plane in general position has a subset of 4 points that form the vertices of a convex quadrilateral, where general position means that no two points coincide and no three points are collinear.

Theorem (Erdős & Szekeres 1935)

For $N \in \mathbb{N}$, any sufficiently large finite set of points in the plane in general position has a subset of N points that form the vertices of a convex polygon.

Let $f(N)$ denote the minimum M for which any set of M points in general position must contain a convex N -gon. It is known that

- $f(3) = 3$
- $f(4) = 5$
- $f(5) = 9$
- $f(6) = 17$
- $1 + 2^{N-2} \leq f(N) \leq 2^{N+o(N)}$

Complete Disorder is Impossible!

Theorem (Hales-Jewett Theorem)

For every $k, n \in \mathbb{N}^+$, there is $d \in \mathbb{N}^+$ s.t. if the unit hypercubes in a d -dimensional hypercube n^d are colored in k colors, then there exists at least one row, column or diagonal of n squares, all of the same color.

Theorem (van der Waerden Theorem)

For every $k, m \in \mathbb{N}^+$, there is $n \in \mathbb{N}^+$ s.t. if the numbers from 1 to n are colored in k colors, then there exists at least m numbers in arithmetic progression, all of the same color.

Theorem (Green-Tao Theorem)

A subset of prime numbers A with $\limsup_{n \rightarrow \infty} \frac{|A \cap [1, n]|}{\pi(n)} > 0$ contains arbitrarily long arithmetic progressions, where $\pi(n)$ is the number of primes $\leq n$.

Complete Disorder is Impossible!

Theorem (Szemerédi Theorem)

A set $A \subset \mathbb{N}$ with $\limsup_{n \rightarrow \infty} \frac{|A \cap [1, n]|}{n} > 0$ contains arbitrarily long arithmetic progressions.

Theorem (Furstenberg Multiple Recurrence Theorem)

Let (X, \mathcal{B}, μ, T) be a measure-preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Then,

$$\forall k \in \mathbb{N} : \liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \mu \left(\bigcap_{j=0}^k T^{-jn} A \right) > 0$$

Szemerédi Theorem \iff Furstenberg Multiple Recurrence Theorem

Complete Disorder is Impossible!

Theorem (Poincaré Recurrence Theorem)

Let (X, \mathcal{B}, μ, T) be a measure-preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Then almost every $x \in A$ returns infinitely often to A .

$$\mu(\{x \in A : \exists N \forall n > N : T^n x \notin A\}) = 0$$

Lemma (Kac's Lemma)

Let (X, \mathcal{B}, μ, T) be a measure-preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Then the recurrence time $\tau_A(x) := \min \{k \geq 1 : T^k x \in A\}$ satisfies

$$\int_A \tau_A(x) d\mu(x) = 1$$

Equivalently, the mean recurrence time $\langle \tau_A \rangle := \frac{1}{\mu(A)} \int_A \tau_A(x) d\mu(x) = \frac{1}{\mu(A)}$.

Correlation Supersedes Causation?

- ▶ The average recurrence time to a subset A in Poincaré recurrence theorem is the inverse of the probability of A . The probability decrease exponentially with the size (dimension) of the phase space (observables and parameters) and the recurrence time increases exponentially with that size. One can't reliably predict by "analogy" with the past, even in deterministic systems, chaotic or not.
- ▶ Given any arbitrary correlation on sets of data, there exists a large enough number such that any data set larger than that size realizes that type of correlation. Every large set of numbers, points or objects necessarily contains a highly regular pattern.
- ▶ There is no true randomness. Randomness means unpredictability with respect to some fixed theory.

Correlation Supersedes Causation?

- ▶ How to distinguish correlation from causation?
- ▶ How to distinguish content-correlations from Ramsey-type correlations?
- ▶ Ramsey-type correlations appear in all large enough databases.
- ▶ A correlation is *spurious* iff it appears in a “randomly” generated database.
- ▶ How “large” is the set of spurious correlations?
- ▶ Most strings are algorithmically random.

$$P\left(\left\{x \in \mathcal{X}^n : \frac{K(x)}{n} < 1 - \delta\right\}\right) < 2^{-\delta n}$$

- ▶ Most correlations are spurious.
- ▶ It may be the case that our part of the universe is an oasis of regularity in a maximally random universe.

Complete Disorder is Impossible!

For sufficiently large n and any $x \in \mathcal{X}^n$, if $C(x) \geq n - \delta(n)$, then each block of length $\log n - \log \log n - \log(\delta(n) + \log n) - O(1)$ occurs at least once in x .

Löwenheim-Skolem Theorem

Theorem (Downward Löwenheim-Skolem Theorem)

A consistent set of sentences in a language of cardinality λ has a model of cardinality $\leq \lambda$.

Theorem (Upward Löwenheim-Skolem Theorem)

If a set of sentences in a language of cardinality λ has an infinite model, then it has models of every cardinality $\geq \lambda$.

Proof.

Add $\{c_\xi\}_{\xi < \lambda}$ to \mathcal{L} . Let $T' := T \cup \{c_\xi \neq c_\eta : \xi < \eta < \lambda\}$.

Every finite subset $\Sigma \subset T'$ will involve at most a finite number of c_ξ .

Hence any infinite model of T can be expanded to a model of Σ .

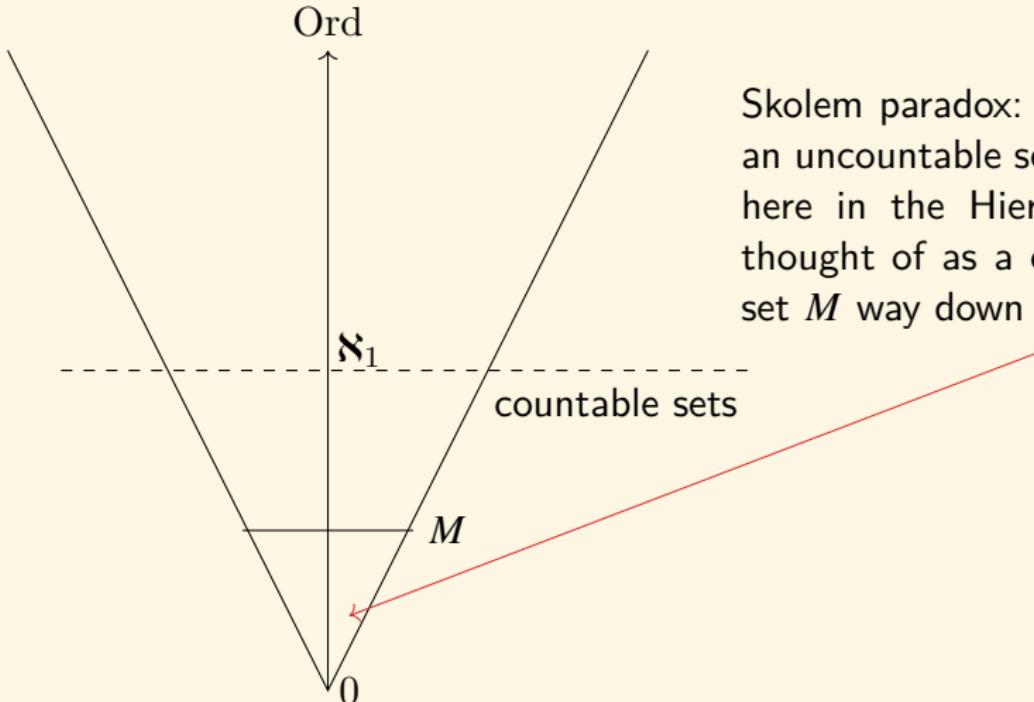
By compactness and the downward Löwenheim-Skolem theorem, T' has a model \mathcal{M} of cardinality $\leq \lambda$.

On the other hand, the interpretations of c_ξ in \mathcal{M} must give different elements. So $\lambda \leq |\mathcal{M}| \leq \lambda$.

Skolem Paradox? — Models and Reality

- ▶ Cantor: $P(\mathbb{N})$ is uncountable.
- ▶ There is a countable model $\mathcal{M} \models \text{ZF} \vdash "P(\mathbb{N}) \text{ is uncountable}"$.
- ▶ The statement “ $P(\mathbb{N})$ is uncountable” is interpreted in \mathcal{M} as — within \mathcal{M} , there is a set M_1 that looks like $P(\mathbb{N})$ and M_2 that looks like \mathbb{N} , but there is no set corresponding to the set of pairs of members of M_1 and M_2 .”
- ▶ Outside of \mathcal{M} , we can see that all \mathcal{M} -sets are really only countable. The \mathcal{M} -set M_1 that \mathcal{M} says is $P(\mathbb{N})$ really isn't — outside \mathcal{M} , M_1 and \mathbb{N} can be paired, but this requires the existence of a “pairing” set that isn't in \mathcal{M} .
- ▶ What we think are uncountable sets in our hierarchy may really be countable \mathcal{M}' -sets in the larger hierarchy.
- ▶ There is no absolute notion of countability. A set can only be said to be countable or uncountable relative to an interpretation of ZF.

Skolem Paradox? — Models and Reality



Skolem paradox: How can an uncountable set way up here in the Hierarchy be thought of as a countable set M way down here?

Craig's Interpolation Theorem

Theorem (Craig's Interpolation Theorem)

If $\models A \rightarrow B$, then there is a sentence C s.t. $\models A \rightarrow C$ and $\models C \rightarrow B$, and C contains no non-logical symbols except such as are both in A and in B .

Beth's Definability Theorem

Definition (Explicit Definition)

Suppose \mathcal{L} is a language not containing the predicate symbol P . A set $\Sigma(P)$ of sentences of $\mathcal{L} \cup \{P\}$ *explicitly defines* P iff there is a wff $A(x_1, \dots, x_n)$ of \mathcal{L} s.t.

$$\Sigma(P) \models \forall x_1 \dots \forall x_n (P(x_1, \dots, x_n) \leftrightarrow A(x_1, \dots, x_n))$$

Definition (Implicit Definition)

Suppose \mathcal{L} is a language not containing the predicate symbol P and P' . A set $\Sigma(P)$ of sentences of $\mathcal{L} \cup \{P\}$ *implicitly defines* P iff

$$\Sigma(P) \cup \Sigma(P') \models \forall x_1 \dots \forall x_n (P(x_1, \dots, x_n) \leftrightarrow P'(x_1, \dots, x_n))$$

where $\Sigma(P')$ is the result of uniformly replacing P with P' in $\Sigma(P)$.

Theorem (Beth's Definability Theorem)

$\Sigma(P)$ *implicitly defines* P iff $\Sigma(P)$ *explicitly defines* P .

Philosophy question: Is supervenience equivalent to reducibility?

Proof.

Assume that $\Sigma(P)$ implicitly defines P . First, we add constant c_1, \dots, c_n to \mathcal{L} . Then $\Sigma(P) \cup \Sigma(P') \models P(c_1, \dots, c_n) \rightarrow P'(c_1, \dots, c_n)$. By compactness, there are $A_1(P), \dots, A_m(P) \in \Sigma(P)$ and $B_1(P'), \dots, B_n(P') \in \Sigma(P')$ s.t.

$$A_1(P) \wedge \cdots \wedge A_m(P) \wedge B_1(P') \wedge \cdots \wedge B_n(P') \models P(c_1, \dots, c_n) \rightarrow P'(c_1, \dots, c_n).$$

Let $\varphi(P) := A_1(P) \wedge \cdots \wedge A_m(P) \wedge B_1(P) \wedge \cdots \wedge B_n(P)$. Then

$$\varphi(P) \wedge \varphi(P') \models P(c_1, \dots, c_n) \rightarrow P'(c_1, \dots, c_n), \text{ from which}$$

$$\varphi(P) \wedge P(c_1, \dots, c_n) \models \varphi(P') \rightarrow P'(c_1, \dots, c_n).$$

By Craig's Interpolation theorem there is a sentence $C(c_1, \dots, c_n)$ not containing P or P' such that:

$$\varphi(P) \wedge P(c_1, \dots, c_n) \models C(c_1, \dots, c_n)$$

$$C(c_1, \dots, c_n) \models \varphi(P') \rightarrow P'(c_1, \dots, c_n)$$

Since an $\mathcal{L} \cup \{P\}$ -model $\mathcal{M} \models A(P)$ iff the corresponding $\mathcal{L} \cup \{P'\}$ -model $\mathcal{M} \models A(P')$, we have $C(c_1, \dots, c_n) \models \varphi(P) \rightarrow P(c_1, \dots, c_n)$.

Putting them together, $\varphi(P) \models P(c_1, \dots, c_n) \leftrightarrow C(c_1, \dots, c_n)$.

Therefore $\Sigma(P) \models \forall x_1 \dots \forall x_n (P(x_1, \dots, x_n) \leftrightarrow C(x_1, \dots, x_n))$.

Robinson's Joint Consistency Theorem

Theorem (Robinson's Joint Consistency Theorem)

Let $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2$ be languages, with $\mathcal{L}_0 = \mathcal{L}_1 \cap \mathcal{L}_2$. Let T_i be a theory in \mathcal{L}_i for $i = 1, 2$. If T_1 and T_2 are consistent and if there is no formula A of \mathcal{L}_0 s.t. $T_1 \vdash A$ and $T_2 \vdash \neg A$, then the union $T_1 \cup T_2$ is consistent.

Proof.

Suppose $T_1 \cup T_2$ is inconsistent.

Then there exists finite subsets $\Sigma_1 \subset T_1$ and $\Sigma_2 \subset T_2$ such that $\Sigma_1 \cup \Sigma_2$ is inconsistent.

Let $A := \bigwedge \Sigma_1$ and $B := \bigwedge \Sigma_2$.

It follows that $A \models \neg B$.

By Craig's interpolation theorem, there is a sentence C of \mathcal{L}_0 such that $A \models C$ and $C \models \neg B$.

Then we have $T_1 \vdash C$ and $T_2 \vdash \neg C$. Contradiction.

Abstract Logics

Definition (Abstract Logic)

An *abstract logic* is a pair $\mathcal{L} := (\mathcal{S}, \models_{\mathcal{L}})$, where $\mathcal{S} : \text{signatures} \rightarrow \text{sets}$ assigns to signature τ a set $\mathcal{S}(\tau)$ of sentences, and $\models_{\mathcal{L}}$ is a relation between τ -structures and elements of $\mathcal{S}(\tau)$ s.t.

1. (*Monotony*) $\tau \subset \tau' \implies \mathcal{S}(\tau) \subset \mathcal{S}(\tau')$
2. (*Isomorphism*) $\mathcal{M} \models_{\mathcal{L}} A \& \mathcal{M} \cong \mathcal{N} \implies \mathcal{N} \models_{\mathcal{L}} A$
3. (*Expansion*) If $\tau \subset \tau'$, $A \in \mathcal{S}(\tau)$, and \mathcal{M} is an τ' -structure, then
 $\mathcal{M} \models_{\mathcal{L}} A \iff \mathcal{M} \upharpoonright_{\tau} \models_{\mathcal{L}} A$

$$\text{Mod}_{\mathcal{L}}^{\tau}(A) := \{\mathcal{M} \in \tau\text{-structures} : \mathcal{M} \models_{\mathcal{L}} A\}$$

Example — $\mathcal{L}_{\kappa\lambda}$

For $\kappa \geq \lambda$, define the $\mathcal{L}_{\kappa\lambda}$ formulas as for first order logic, plus:

- ▶ Given a set of formulas $\{A_i : i \in I\}$, $|I| < \kappa$, then $\bigwedge_{i \in I} A_i$ and $\bigvee_{i \in I} A_i$ are formulas.
- ▶ Given a set of variables $\{x_i : i \in J\}$, $|J| < \lambda$ and a formula A , then $\exists(x_i : i \in J)A$ and $\forall(x_i : i \in J)A$ are formulas.

Satisfaction relation:

- ▶ $\mathcal{M} \models_{\mathcal{L}_{\kappa\lambda}} \bigwedge_{i \in I} A_i$ iff $\mathcal{M} \models_{\mathcal{L}_{\kappa\lambda}} A_i$ for all $i \in I$.
- ▶ $\mathcal{M} \models_{\mathcal{L}_{\kappa\lambda}} \exists(x_i : i \in J)A$ iff $\mathcal{M} \models_{\mathcal{L}_{\kappa\lambda}} A[a_i : i \in J]$ for some $\{a_i : i \in J\} \subset M$.

Note: $\mathcal{L}_{\omega\omega}$ is classical first order logic.

Definition (Regular Abstract Logic)

An abstract logic \mathcal{L} is *regular* iff it satisfies:

1. (*Bool*) For $A \in \mathcal{S}(\tau)$ there is $B \in \mathcal{S}(\tau)$ s.t. $\mathcal{M} \models_{\mathcal{L}} B \iff \mathcal{M} \not\models_{\mathcal{L}} A$; and $\forall A, B \in \mathcal{S}(\tau) \exists C \in \mathcal{S}(\tau) : \mathcal{M} \models_{\mathcal{L}} C \iff \mathcal{M} \models_{\mathcal{L}} A \& \mathcal{M} \models_{\mathcal{L}} B$.
2. (*Quantifier*) $\forall c \in \tau \forall A \in \mathcal{S}(\tau) \exists B \in \mathcal{S}(\tau) :$

$$\text{Mod}_{\mathcal{L}}^{\tau \setminus \{c\}}(B) = \{\mathcal{M} : (\mathcal{M}, a) \in \text{Mod}_{\mathcal{L}}^\tau(A) \text{ for some } a \in M\}$$

where (\mathcal{M}, a) is the expansion of \mathcal{M} to τ assigning a to c .

3. (*Renaming*) Let $\pi : \tau \rightarrow \tau'$ be a bijection which respects arity, and we extend π in a canonical way to $\hat{\pi} : \tau\text{-structures} \rightarrow \tau'\text{-structures}$. Then

$$\forall A \in \mathcal{S}(\tau) \exists A' \in \mathcal{S}(\tau') : \mathcal{M} \models_{\mathcal{L}} A \iff \hat{\pi}(\mathcal{M}) \models_{\mathcal{L}} A'$$

4. (*Relativization*) Given $A \in \mathcal{S}(\tau)$ and symbols $R, c_1, \dots, c_n \notin \tau$, there is $B \in \mathcal{S}(\tau \cup \{R, c_1, \dots, c_n\})$ called the *relativization* of A to $R(x, c_1, \dots, c_n)$, s.t. for $\mathcal{M} : (\mathcal{M}, X, b_1, \dots, b_n) \models_{\mathcal{L}} B \iff \mathcal{N} \models_{\mathcal{L}} A$ where $\mathcal{N} \subset \mathcal{M}$ with $\mathcal{N} = \{a \in M : R^{\mathcal{M}}(a, b_1, \dots, b_n)\}$, and $(\mathcal{M}, X, b_1, \dots, b_n)$ is the expansion of \mathcal{M} interpreting R, c_1, \dots, c_n by X, b_1, \dots, b_n (with $X \subset M^{n+1}$).

Lindström's Theorem

Definition (Expressive Power)

\mathcal{L}_2 is *at least as expressive* as \mathcal{L}_1 ($\mathcal{L}_1 \leq \mathcal{L}_2$) iff for each signature τ and $A \in \mathcal{S}_1(\tau)$ there is $B \in \mathcal{S}_2(\tau)$ s.t.

$$\text{Mod}_{\mathcal{L}_1}^\tau(A) = \text{Mod}_{\mathcal{L}_2}^\tau(B)$$

$$\mathcal{L}_1 \sim \mathcal{L}_2 \coloneqq \mathcal{L}_1 \leq \mathcal{L}_2 \ \& \ \mathcal{L}_2 \leq \mathcal{L}_1$$

Theorem (Lindström's Theorem)

If a regular abstract logic \mathcal{L} has the Countable Compactness and the Downward Löwenheim-Skolem Properties, then $\mathcal{L} \sim \mathcal{L}_{\omega\omega}$.

1. The set of *Horn formulas* is the smallest set containing the set of atomic formulas and closed under \top, \wedge .
2. The set of *regular formulas* is the smallest set containing the set of atomic formulas and closed under \top, \wedge, \exists .
3. The set of *coherent formulas* is the smallest set containing the set of atomic formulas and closed under $\top, \perp, \wedge, \vee, \exists$.
4. The set of *first order formulas* is the smallest set containing the set of atomic formulas and closed under $\top, \perp, \neg, \wedge, \vee, \rightarrow, \exists, \forall$.
5. The class of *geometric formulas* over is the smallest class containing the class of atomic formulas and closed under $\top, \perp, \wedge, \vee, \exists$ and infinitary disjunction.
6. The class of *infinitary first order formulas* is the smallest class containing the class of atomic formulas and closed under $\top, \perp, \neg, \wedge, \vee, \rightarrow, \exists, \forall$ and infinitary conjunction and infinitary disjunction.

- ▶ T is an algebraic theory iff its signature has no relation symbols and its axioms are all of the form $T \vdash_x A$ where A is an atomic formula of the form $s = t$ and x its canonical context.
- ▶ T is a Horn (resp. regular, coherent, geometric) theory iff all the sequents in T are Horn (resp. regular, coherent, geometric).
- ▶ T is a universal Horn theory iff its axioms are all of the form $A \vdash_x B$, where A is a finite conjunction of atomic formulas and B is an atomic formula or the formula \perp .
- ▶ T is a propositional theory iff it only consists of 0-ary relation symbols.

Identity Axiom $A \vdash_x A$

Equality $\top \vdash_x x = x$ and $x = y \wedge A \vdash_z A[y/x]$ where $\text{Fv}(x, y, A) \subset z$.

$$A \vdash_x B$$

Substitution $\frac{A[t/x] \vdash_y B[t/x]}{A \vdash_x B} \quad \text{where } \text{Var}(t) \subset y.$

$$\frac{\begin{array}{c} A \vdash_x B \\ B \vdash_x C \end{array}}{A \vdash_x C}$$

Conjunction $A \vdash_x \top \quad A \wedge B \vdash_x A \quad A \wedge B \vdash_x B$

$$\frac{\begin{array}{c} C \vdash_x A \quad C \vdash_x B \\ \hline C \vdash_x A \wedge B \end{array}}{\begin{array}{c} A \vdash_x C \quad B \vdash_x C \\ \hline A \vee B \vdash_x C \end{array}}$$

Disjunction $\perp \vdash_x A \quad A \vdash_x A \vee B \quad B \vdash_x A \vee B$

$$A \wedge B \vdash_x C$$

Implication $\frac{A \vdash_x B \rightarrow C}{A \vdash_x B}$

$$A \vdash_{xy} B$$

Existential Quantification $\frac{\exists y A \vdash_x B}{A \vdash_{xy} B}$

$$A \vdash_{xy} B$$

Universal Quantification $\frac{A \vdash_x \forall y B}{A \vdash_x B}$

Distributive Axiom $A \wedge (B \vee C) \vdash_x (A \wedge B) \vee (A \wedge C)$

Frobenius Axiom $A \wedge \exists y B \vdash_x \exists y(A \wedge B)$ where $y \notin x$.

Law of Excluded Middle $\top \vdash_x A \vee \neg A$

Fragments of First Order Logic

In addition to the usual structural rules (Identity axiom, Equality rules, Substitution rule and Cut rule), our deduction systems consist of the following rules:

Algebraic logic	No additional rule
Horn logic	Finite conjunction
Regular logic	Finite conjunction, existential quantification and Frobenius axiom
Coherent logic	Finite conjunction, finite disjunction, existential quantification, distributive axiom and Frobenius axiom
Geometric logic	Finite conjunction, infinitary disjunction, existential quantification, 'infinitary' distributive axiom, Frobenius axiom
Intuitionistic FOL	All the finitary rules except for the law of excluded middle
Classical FOL	All the finitary rules

Intuitionistic Propositional Logic vs Heyting Algebra

A Heyting algebra $(H, \perp, \top, \wedge, \vee, \rightarrow, \leq)$ is a bounded lattice $(H, \perp, \top, \wedge, \vee, \leq)$ equipped with \rightarrow s.t. for all $a, b, c \in H$:

1. $a \leq \top$
2. $a \wedge b \leq a$
3. $a \wedge b \leq b$
4. $c \leq a \ \& \ c \leq b \implies c \leq a \wedge b$
5. $\perp \leq a$
6. $a \leq a \vee b$
7. $b \leq a \vee b$
8. $a \leq c \ \& \ b \leq c \implies a \vee b \leq c$
9. $a \leq b \rightarrow c \iff a \wedge b \leq c$

Define $\neg a := a \rightarrow \perp$.

- ▶ There is no proof of \perp .
- ▶ A proof of $A \wedge B$ is a pair $\langle m, n \rangle$ where m is a proof of A and n is a proof of B .
- ▶ A proof of $A \vee B$ is a pair $\langle m, n \rangle$ where m is 0 and n is a proof of A , or m is 1 and n is a proof of B .
- ▶ A proof of $A \rightarrow B$ is a function f that converts a proof m of A into a proof $f(m)$ of B .
- ▶ A proof of $\forall x A(x)$ is a function f that converts an element a of the domain of definition into a proof $f(a)$ of $A(a)$.
- ▶ A proof of $\exists x A(x)$ is a pair $\langle a, n \rangle$ where a is an element of the domain of definition, and n is a proof of $A(a)$.

Kleene's Realizability Interpretation

- An *assembly* $\mathbf{M} = (M, \Vdash_{\mathbf{M}})$ is a set M with a *realizability* relation $\Vdash_{\mathbf{M}} \subset \mathbb{N} \times M$ such that $\forall x \in M \exists n \in \mathbb{N} : n \Vdash_{\mathbf{M}} x$.
- An *assembly morphism* $f : \mathbf{X} \rightarrow \mathbf{Y}$ is a function $f : X \rightarrow Y$ for which
$$\exists n \in \mathbb{N} \forall x \in X \forall m \in \mathbb{N} : m \Vdash_{\mathbf{X}} x \implies \varphi_n(m) \downarrow \& \varphi_n(m) \Vdash_{\mathbf{Y}} f(x)$$

$$n \Vdash \top \quad \text{for every } n \in \mathbb{N}$$

$$n \Vdash \perp \quad \text{for no } n \in \mathbb{N}$$

$$\langle m, n \rangle \Vdash x = y \quad \text{if } \llbracket x \rrbracket = \llbracket y \rrbracket \text{ and } m \Vdash x \text{ and } n \Vdash y$$

$$\langle m, n \rangle \Vdash A \wedge B \quad \text{if } m \Vdash A \text{ and } n \Vdash B$$

$$\langle m, n \rangle \Vdash A \vee B \quad \text{if } m = 0 \text{ and } n \Vdash A, \text{ or } m = 1 \text{ and } n \Vdash B$$

$$n \Vdash A \rightarrow B \quad \text{if } m \Vdash A \text{ implies } \varphi_n(m) \Vdash B$$

$$n \Vdash \forall x A \quad \text{if } a \in M \text{ and } m \Vdash a \text{ implies } \varphi_n(m) \Vdash A(a)$$

$$\langle m, n \rangle \Vdash \exists x A \quad \text{if there is } a \in M \text{ such that } m \Vdash a \text{ and } n \Vdash A(a)$$

Kripke Semantics for Intuitionistic Logic

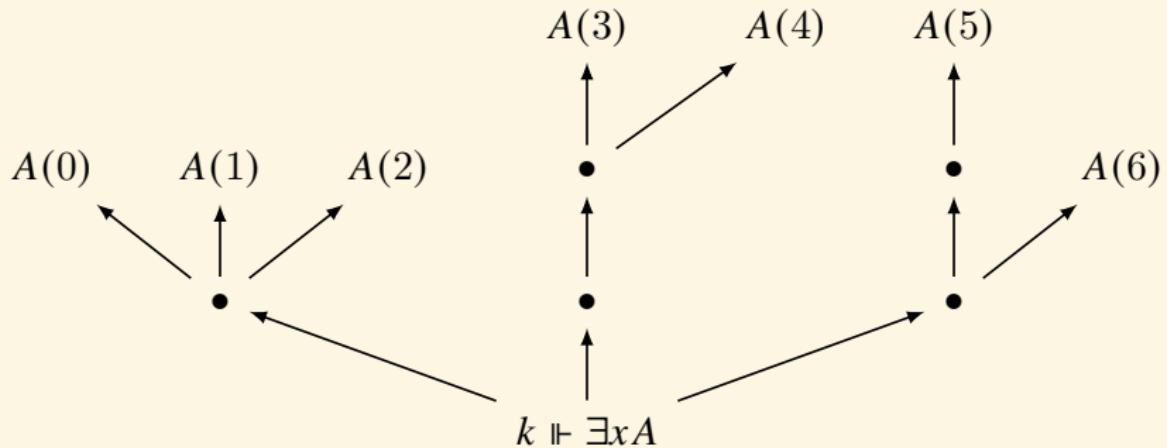
Definition (Kripke Model)

A Kripke model $\mathcal{M} = (\mathcal{I}, M, V, \Vdash)$ consists of a partially ordered set \mathcal{I} , a domain function M assigning to $k \in \mathcal{I}$ a nonempty set M_k of closed terms s.t. $k \leq l \implies M_k \subset M_l$, and a valuation function V assigning to $k \in \mathcal{I}$ a set $V(k)$ of atomic sentences s.t. $k \leq l \implies V(k) \subset V(l)$.

- ▶ $k \Vdash A$ for atomic A iff there is a bar \mathcal{B} for k s.t. for all $l \in \mathcal{B}$, $A \in V(l)$
- ▶ $k \Vdash A \wedge B$ iff $k \Vdash A$ and $k \Vdash B$
- ▶ $k \Vdash A \vee B$ iff there is a bar \mathcal{B} for k s.t. for all $l \in \mathcal{B}$, $l \Vdash A$ or $l \Vdash B$
- ▶ $k \Vdash A \rightarrow B$ iff for all $l \geq k$, if $l \Vdash A$ then $l \Vdash B$
- ▶ $k \Vdash \neg A$ iff for all $l \geq k$, $l \not\Vdash A$
- ▶ $k \Vdash \forall x A$ iff for all $l \geq k$ and all $t \in M_l$, $l \Vdash A(t/x)$
- ▶ $k \Vdash \exists x A$ iff there is a bar \mathcal{B} for k s.t. for all $l \in \mathcal{B}$, there exists $t \in M_k$, $k \Vdash A(t/x)$

where a bar for k is a subset $\mathcal{B} \subset \mathcal{I}$ s.t. each path through k intersects \mathcal{B} .

Example



Theorem (Soundness and Completeness)

$$\Gamma \vdash A \iff \Gamma \Vdash A$$

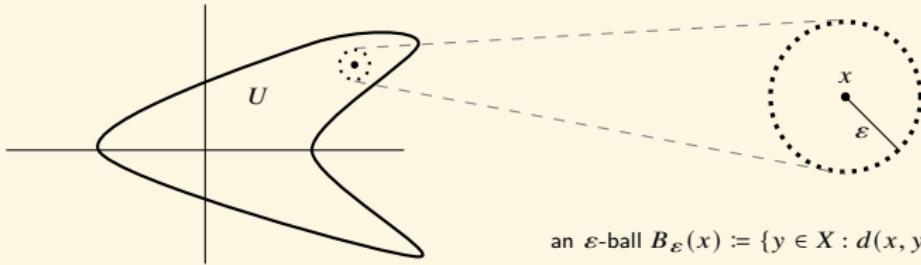
Continuity, Metric and Topology

- ▶ A function $f : X \rightarrow Y$ between metric spaces is *continuous* at point $a \in X$ iff $\forall \varepsilon > 0 \exists \delta > 0 \forall x \in X : d_X(x, a) < \delta \rightarrow d_Y(f(x), f(a)) < \varepsilon$.
- ▶ A *metric space* (X, d) is a set X with a metric $d : X \times X \rightarrow \mathbb{R}$ s.t. for all $x, y, z \in X$:
 1. $d(x, y) = 0 \leftrightarrow x = y$
 2. $d(x, y) = d(y, x)$
 3. $d(x, z) \leq d(x, y) + d(y, z)$

e.g.
$$d(x, y) = \left(\sum_{i=1}^n |x_i - y_i|^p \right)^{\frac{1}{p}}$$

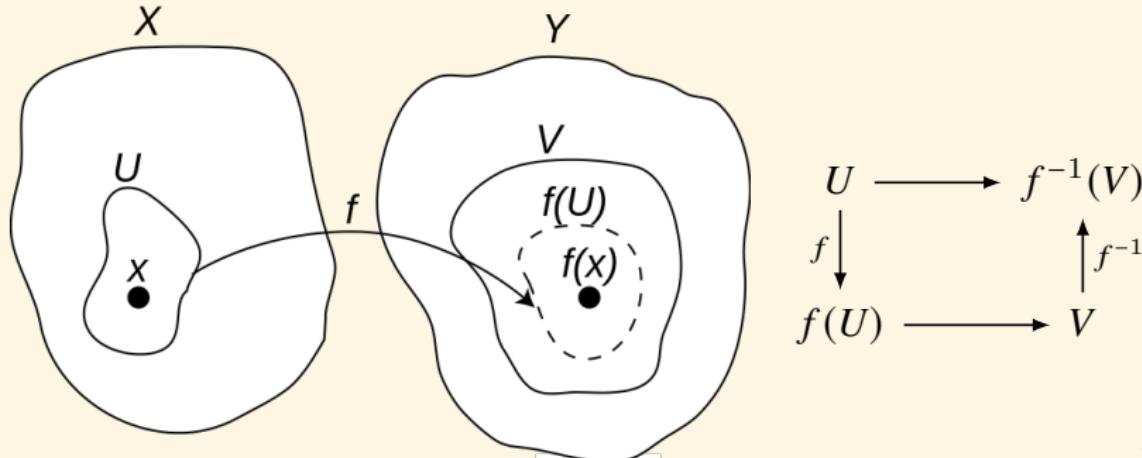
$$d(x, y) = \max_{1 \leq i \leq n} |x_i - y_i|$$

- ▶ A set $U \subset X$ is *open* iff $\forall x \in U \exists \varepsilon > 0 : B_\varepsilon(x) \subset U$.



Continuity, Metric and Topology

- ▶ For the definition of continuity (“nearby” points in U go into nearby points in V), the notion of ‘open set’ is more **intrinsic** than that of **distance**.
- ▶ A function $f : X \rightarrow Y$ between topological spaces is *continuous* iff the inverse image $f^{-1}(V)$ of any open subset $V \subset Y$ is an open subset of X .
- ▶ Equivalently, f is *continuous* at point $x \in X$ iff to each neighborhood V of $f(x)$ there is a neighborhood U of x for which $f(U) \subset V$.



Intrinsic vs. Extrinsic Properties of Functions

A property of functions $f : A \rightarrow B$ is *intrinsic* if it can be defined purely in terms of f (as a set of input-output pairs) and any structure pertaining to A and B (using only bounded quantification over the structures A and B .).

Example:

- G and H are groups. $f : G \rightarrow H$ is a group homomorphism if

$$f(x \cdot_G y) = f(x) \cdot_H f(y) \quad f(e_G) = e_H$$

- X and Y are topological spaces. $f : X \rightarrow Y$ is continuous if $f^{-1}(U)$ is open in the topology on X for every open subset U of Y .
- Computability is not an intrinsic property of partial functions $f : \mathbb{N} \rightarrow \mathbb{N}$. To say f is computable we need to refer to some external algorithmic process which computes f .

Topological Semantics of Intuitionistic Propositional Logic

- ▶ A *topological space* $(X, \mathcal{O}(X))$ is a set X with a family $\mathcal{O}(X) \subset \mathcal{P}(X)$ of subsets of X which contains \emptyset and X , and is closed under finite intersections and arbitrary unions.
- ▶ The topological *interior* of a subset $S \subset X$ is

$$S^\circ := \bigcup \{U \in \mathcal{O}(X) : U \subset S\}$$

- ▶ Define for $A, B \in \mathcal{O}(X)$ the open set

$$A \rightarrow B := ((X \setminus A) \cup B)^\circ = \bigcup \{U \in \mathcal{O}(X) : U \cap A \subset B\}$$

by definition, for all $U \in \mathcal{O}(X)$,

$$U \subset A \rightarrow B \iff U \cap A \subset B$$

Define $\neg A := A \rightarrow \perp$. Thus

$$\neg A = (X \setminus A)^\circ \quad \text{and} \quad A \vee \neg A = A \cup (X \setminus A)^\circ = X \setminus \partial A$$

- ▶ $A := (0, 1) \cup (1, \infty)$, $\neg A = (-\infty, 0)$, $\neg\neg A = (0, \infty)$, $A \cup \neg A \neq \mathbb{R}$, $A \subsetneq \neg\neg A$.
- ▶ A topological model of intuitionistic propositional logic is $(X, \mathcal{O}(X), [\![\]\!])$ where $[\![\]\!] : \text{Var} \rightarrow \mathcal{O}(X)$.

Topological Semantics of Intuitionistic Logic

$$\llbracket A \wedge B \rrbracket := \llbracket A \rrbracket \cap \llbracket B \rrbracket$$

$$\llbracket A \vee B \rrbracket := \llbracket A \rrbracket \cup \llbracket B \rrbracket$$

$$\llbracket A \rightarrow B \rrbracket := \left((X \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket \right)^\circ$$

$$\llbracket \perp \rrbracket := \emptyset$$

$$\llbracket \neg A \rrbracket := (X \setminus \llbracket A \rrbracket)^\circ$$

$$\llbracket \exists x A \rrbracket := \bigcup_{a \in M} \llbracket A[a] \rrbracket$$

$$\llbracket \forall x A \rrbracket := \left(\bigcap_{a \in M} \llbracket A[a] \rrbracket \right)^\circ$$

$$O(X) \Vdash A := \llbracket A \rrbracket = X$$

$$\Gamma \Vdash A := \left(\bigcap_{B \in \Gamma} \llbracket B \rrbracket \right)^\circ \subset \llbracket A \rrbracket$$

Remark: Classical logic appears as a special case when $O(X) = P(X)$.

Remark: The algebra of open subsets of a topological space is a special case of a Heyting algebra.

Formal Systems

Axiom Schema

1. $A \rightarrow B \rightarrow A$
2. $(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
3. $A \wedge B \rightarrow A$
4. $A \wedge B \rightarrow B$
5. $(C \rightarrow A) \rightarrow (C \rightarrow B) \rightarrow C \rightarrow A \wedge B$
6. $A \rightarrow A \vee B$
7. $B \rightarrow A \vee B$
8. $(A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow A \vee B \rightarrow C$
9. $(A \rightarrow \neg B) \rightarrow (A \rightarrow B) \rightarrow \neg A$
10. $\neg A \rightarrow A \rightarrow B$
11. $\neg\neg A \rightarrow A$

Reference Rule

$$\frac{A \quad A \rightarrow B}{B} [\text{MP}]$$

- ▶ 1–8+MP=Positive Calculus
- ▶ P+9=Minimal Calculus
- ▶ M+10=Intuitionistic Calculus
- ▶ I+11=Classical Calculus

Gödel's $\neg\neg$ Translation

$$p' := \neg\neg p$$

$$(A \wedge B)' := A' \wedge B'$$

$$(A \vee B)' := \neg(\neg A' \wedge \neg B')$$

$$(A \rightarrow B)' := A' \rightarrow B'$$

$$(\forall x A)' := \forall x A'$$

$$(\exists x A)' := \neg\forall x \neg A'$$

► $\Gamma \vdash_C A \iff \Gamma' \vdash_I A'$ where $\Gamma' := \{A' : A \in \Gamma\}$.

► $\vdash_C A \iff \vdash_I \neg\neg A$

Remark:

- Each classical theory can be translated into intuitionistic logic, yielding a classically equivalent result.
- Intuitionistic logic is more expressive than classical logic since it allows to distinguish formulas which are classically equivalent.

Intuitionistic Logic vs Classical Logic

- ▶ The difference between intuitionistic and classical logic is in the criteria for truth, i.e. what evidence must be provided before a statement is accepted as true. Speaking vaguely, intuitionistic logic demands positive evidence, while classical logic is happy with lack of negative evidence.
- ▶ $\neg\neg A$ holds if it is contradictory to assume that it is contradictory to assume A . In essence, it says that $\neg\neg A$ is accepted when there is no evidence against it. In other words, $\neg\neg A$ means something like “ A cannot be falsified” or “ A is potentially true”.

Theorem

The axiom of choice implies excluded middle.

Proof.

Consider an arbitrary proposition P . To decide P , define

$$\begin{aligned}A &:= \{x \in \{0, 1\} : P \vee x = 0\} \\B &:= \{x \in \{0, 1\} : P \vee x = 1\}\end{aligned}$$

Every member of $\{A, B\}$ is inhabited because $0 \in A$ and $1 \in B$. By the axiom of choice there is a function $f : \{A, B\} \rightarrow A \cup B$ s.t. $f(A) \in A$ and $f(B) \in B$. Then

1. $f(A) = 1 \implies P$
2. $f(B) = 0 \implies P$
3. $f(A) = 0 \& f(B) = 1 \implies \neg P$, otherwise
 $P \implies A = B = \{0, 1\} \implies 0 = f(A) = f(B) = 1.$

In each case we decided whether P or $\neg P$ holds.

Categoricity

Definition (categoricity / κ -categoricity)

- ▶ A theory is *categorical* iff it has exactly one model.
- ▶ A theory is κ -*categorical* iff it has exactly one model of cardinality κ .

Theorem

A theory T is complete iff for all $M \models T$ and $N \models T$: $M \equiv N$.

Theorem

If a theory is categorical, then it is complete.

Theorem

For a theory with finite models, it is complete iff it is categorical.

Dense Linear Ordering without Endpoints

1. $x \not< x$
2. $x < y \rightarrow y < z \rightarrow x < z$
3. $x < y \vee x = y \vee y < x$
4. $x < y \rightarrow \exists z(x < z < y)$
5. $\exists yz(y < x < z)$

Definition (κ -categoricity)

A theory is κ -categorical iff it has a unique model of cardinality κ .

Theorem (Cantor)

- *The theory of dense linear orderings without endpoints is \aleph_0 -categorical.*
- *$(\mathbb{R}, <)$ is the unique complete linear ordering that has a countable dense subset isomorphic to $(\mathbb{Q}, <)$.*

Theorem ($\mathsf{\acute{L}o\acute{s}-Vaught\ Test}$)

If a theory with no finite model is κ -categorical, then it is complete.

Theorem

The theory ACF_p of algebraically closed fields of characteristic p (for p prime or 0) is κ -categorical for all uncountable cardinals κ .

Corollary

For $p \in \mathbb{P}$ or $p = 0$, ACF_p is complete and decidable.

Theorem (Morley's Categoricity Theorem)

If a theory is κ -categorical for some $\kappa \geq |\mathcal{L}|$, then it is categorical in all cardinalities $\geq |\mathcal{L}|$.

Problem

1. *Which view is the more plausible — that theories are the better the more nearly they are categorical, or that theories are the better the more they give rise to significant non-isomorphic interpretations?*
 2. *Or is it rather the case that categoricity is a virtue in some theories but not in others?*
- ▶ The field of real numbers is not κ -categorical for any uncountable κ .
 - ▶ The field of complex numbers is κ -categorical for any uncountable κ .
 - ▶ Euclidean geometry studies spaces with real co-ordinates, smooth trajectories in these spaces and fits best with Newtonian physics.
 - ▶ Algebraic geometry studies spaces with complex co-ordinates, or more generally, co-ordinates over algebraically closed fields in which all polynomial equations have solutions.

Remark: Categoricity versus Algorithmic Compressibility. If physical universe is co-ordinatizable in terms of complex numbers, then this explains that the comprehensive physical science is possible.

Lefschetz's Transfer Principle

Theorem (Lefschetz's Transfer Principle)

For a sentence A in the language of fields, the following are equivalent:

1. $\mathbb{C} \models A$
2. $\text{ACF}_0 \models A$
3. $\text{ACF}_p \models A$ for all sufficiently large primes p .
4. $\text{ACF}_p \models A$ for infinitely many primes p .

Proof.

(1 \leftrightarrow 2) follows from the completeness of ACF_0 .

(2 \rightarrow 3) assume $\text{ACF}_0 \models A$, since the deduction $\text{ACF}_0 \vdash A$ only use finitely

n times

many instances of $\overbrace{1+1+\cdots+1}^n \neq 0$, then for some finite

$\Delta \subset \text{ACF}_0 : \Delta \vdash A$, and $\text{ACF}_p \models \Delta$ for all sufficiently large primes p .

(3 \rightarrow 4) is trivial.

(4 \rightarrow 2) $\text{ACF}_0 \not\models A \implies \text{ACF}_0 \vdash \neg A \implies \text{ACF}_p \vdash \neg A$ for all sufficiently large primes p .

Ax-Grothendieck Theorem

- ▶ An *affine variety* is a set $V \subset \mathbb{C}^n$ s.t.
$$V = \{(x_1, \dots, x_n) : f_i(x_1, \dots, x_n) = 0, 1 \leq i \leq k\}$$
 with
 $f_i \in \mathbb{C}[x_1, \dots, x_n].$
- ▶ For any field K a map $f : K^n \rightarrow K^n$ is *polynomial* iff
$$f(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$
 with
 $f_i \in K[x_1, \dots, x_n].$

Theorem (Ax-Grothendieck Theorem)

Let $f : V \rightarrow V$ be a polynomial map of an affine variety in \mathbb{C}^n . If f is injective, then it is surjective.

Ax-Grothendieck Theorem

Every injective polynomial map $f: \mathbb{C}^n \rightarrow \mathbb{C}^n$ is surjective.

Let $A :=$ “Every injective polynomial map f of degree d is surjective”.

By Lefschetz's transfer principle, we just have to show for all primes p , $\text{ACF}_p \vdash A$.

Moreover, for each p , by completeness of ACF_p , we only need to show A is true in some model of ACF_p .

Consider the algebraic closure $F := \bar{\mathbb{F}}_p$ of the prime field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. We have $F = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

Let $\{a_1, \dots, a_k\}$ be the set of coefficients appearing in $f : F^n \rightarrow F^n$.

For $(b_1, \dots, b_n) \in F^n$, let K be the subfield of F generated by $\{a_1, \dots, a_k, b_1, \dots, b_n\}$.

Since K is finitely generated and $\exists N : K \subset \bigcup_{n=1}^N \mathbb{F}_{p^n}$, hence it is finite.

So $f|_{K^n} : K^n \rightarrow K^n$ that is injective must be surjective.

Hence $f : F^n \rightarrow F^n$ is surjective.

Contents

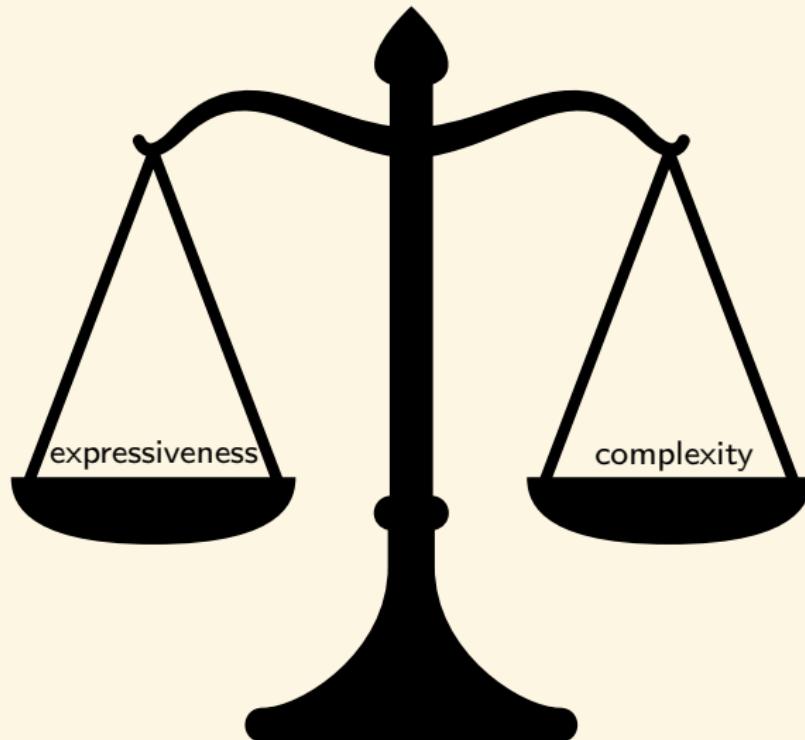
Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Paradox of Material Implication

- ▶ If God does not exist, then it's not the case that **if I believe in God, I will have eternal life**;
- ▶ and I don't believe in God;
- ▶ so God exists!

Why Study Modal Logic?

- ▶ Modal languages are simple yet expressive languages for talking about relational structures.
- ▶ Modal languages provide an internal, local perspective on relational structures.
- ▶ Modal languages are not isolated formal systems.
 - ▶ Modal vs classical (FOL,SOL), internal vs external perspective.
In FOL, structures are described from the top point of view. Each object and relation can be named. In modal logic, relational structures are described from an internal perspective, there is no way to mention objects and relations.
 - ▶ Relational structures vs Boolean algebra with operators.
(Jónsson and Tarski's representation theorem.)
- ▶ Decidability.
(seeking a balance between expressiveness and efficiency/complexity)



Contents

Introduction	Set Theory
Term Logic	Recursion Theory
Propositional Logic	Equational Logic
Predicate Logic	Homotopy Type Theory
Modal Logic	Category Theory
Syntax	Quantum Computing
Semantics	Answers to the Exercises
Formal System	References
Logic of Knowledge and Action	1436

Logics about Modalities

Mary ____ married.

- ▶ is possibly (basic modal logic)
- ▶ will be (temporal logic)
- ▶ is permitted to be (deontic logic)
- ▶ is known/believed (to A) to be (epistemic logic)
- ▶ is proved to be (provability logic)
- ▶ will be (after certain procedure) (dynamic logic)
- ▶ can be ensured (by her parents) to be (coalition logic)



Figure: Kripke

Syntax

Language

$$\mathcal{L} := \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \Box, \Diamond, (,), \} \cup \text{Var}$$

where $\text{Var} := \{p_1, p_2, p_3, \dots\}$.

Definition (Well-Formed Formula Wff)

$$A ::= p \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid A \leftrightarrow A \mid \Box A \mid \Diamond A$$

- ▶ It will always be A . GA
- ▶ You ought to do A . OA
- ▶ I know A . $K_i A$
- ▶ I believe A . $B_i A$
- ▶ A is provable in T . $\Box_T A$
- ▶ After the execution of the program α , A holds. $[\alpha] A$

Examples

1. “Ought” implies “can”, but it does not imply “is”.

$$(\Box p \rightarrow \Diamond p) \wedge \neg(\Box p \rightarrow p)$$

2. What must be is, and what is, is possible.

$$(\Box p \rightarrow p) \wedge (p \rightarrow \Diamond p)$$

3. Just because it happened that doesn’t make it acceptable.

$$\neg(p \rightarrow \Diamond p)$$

4. Just because it happened that doesn’t mean it ought to be permitted.

$$\neg(p \rightarrow \Box \Diamond p)$$

5. If it is raining, it is necessarily possible that it is raining.

$$p \rightarrow \Box \Diamond p$$

6. If it is possible that it is raining then it is necessarily possible that the corners are slippery.

$$\Diamond p \rightarrow \Box \Diamond q$$

7. Necessarily, if it is raining then it is possible that the corners are slippery.

$$\Box(p \rightarrow \Diamond q)$$

Contents

Introduction	Set Theory
Term Logic	Recursion Theory
Propositional Logic	Equational Logic
Predicate Logic	Homotopy Type Theory
Modal Logic	Category Theory
Syntax	Quantum Computing
Semantics	
Formal System	Answers to the Exercises
Logic of Knowledge and Action	References 1436

Possible World Semantics

A Kripke frame is a pair $\mathcal{F} := (W, R)$, where

- ▶ $W \neq \emptyset$
- ▶ $R \subset W \times W$

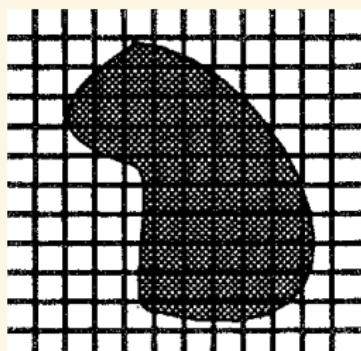
A Kripke model is $\mathcal{M} := (\mathcal{F}, V) = (W, R, V)$, where $V : \text{Var} \rightarrow \text{P}(W)$.

- ▶ $\mathcal{M}, w \Vdash p$ iff $w \in V(p)$
- ▶ $\mathcal{M}, w \Vdash \neg A$ iff $\mathcal{M} \not\Vdash A$
- ▶ $\mathcal{M}, w \Vdash A \wedge B$ iff $\mathcal{M}, w \Vdash A$ and $\mathcal{M}, w \Vdash B$
- ▶ $\mathcal{M}, w \Vdash \Box A$ iff $\forall v \in W : R w v \implies \mathcal{M}, v \Vdash A$
- ▶ $\mathcal{M}, w \Vdash \Diamond A$ iff $\exists v \in W : R w v \ \& \ \mathcal{M}, v \Vdash A$

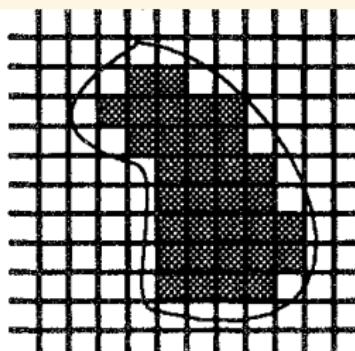
Possible World Semantics*

We extend V to $\llbracket \cdot \rrbracket : \text{Wff} \rightarrow \text{P}(W)$ by recursion as follows:

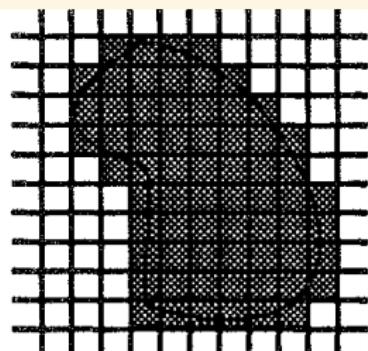
- $\llbracket p \rrbracket := V(p)$
- $\llbracket \neg A \rrbracket := W \setminus \llbracket A \rrbracket$
- $\llbracket A \wedge B \rrbracket := \llbracket A \rrbracket \cap \llbracket B \rrbracket$
- $\llbracket A \vee B \rrbracket := \llbracket A \rrbracket \cup \llbracket B \rrbracket$
- $\llbracket A \rightarrow B \rrbracket := (W \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket$
- $\llbracket \Box A \rrbracket := \Box_R \llbracket A \rrbracket$ where $\Box_R X := \{w \in W : R(w) \subset X\}$
- $\llbracket \Diamond A \rrbracket := \Diamond_R \llbracket A \rrbracket$ where $\Diamond_R X := \{w \in W : R(w) \cap X \neq \emptyset\}$



A



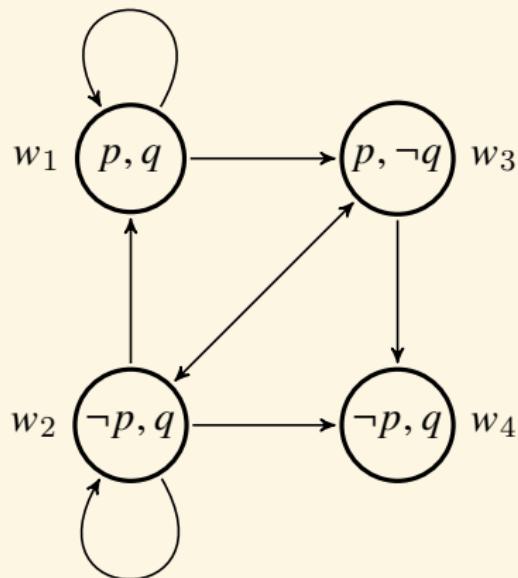
$\Box A$



$\Diamond A$

$$\mathcal{M}, w \Vdash A \iff w \in \llbracket A \rrbracket$$

Example



$$\mathcal{M}, w_1 \Vdash p \wedge \Box p$$

$$\mathcal{M}, w_1 \Vdash q \wedge \Diamond q$$

$$\mathcal{M}, w_1 \Vdash \neg \Box q$$

$$\mathcal{M}, w_2 \Vdash q \wedge \Diamond \neg q$$

$$\mathcal{M}, w_3 \Vdash p$$

$$\mathcal{M}, w_3 \Vdash \Box \neg p$$

$$\mathcal{M}, w_4 \Vdash \Box p \wedge \neg \Diamond p$$

Satisfiability & Validity

- ▶ A is satisfiable at \mathcal{M}, w iff $\mathcal{M}, w \Vdash A$.
- ▶ A is true in \mathcal{M} ($\mathcal{M} \Vdash A$) iff $\forall w \in W : \mathcal{M}, w \Vdash A$
- ▶ A is valid in a pointed frame \mathcal{F}, w ($\mathcal{F}, w \Vdash A$) iff $\mathcal{M}, w \Vdash A$ for every model \mathcal{M} based on \mathcal{F} .
- ▶ A is valid in \mathcal{F} ($\mathcal{F} \Vdash A$) iff $\mathcal{M} \Vdash A$ for every model \mathcal{M} based on \mathcal{F} .
- ▶ $\Vdash A$ iff $\mathcal{F} \Vdash A$ for every \mathcal{F} .

Truth is in the eye of the beholder.

Example

$$\Vdash \Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B$$

Semantic Entailment

- ▶ local semantic entailment

$$\Gamma \Vdash_C A := \forall M \in C \forall w \in W : M, w \Vdash \Gamma \implies M, w \Vdash A$$

- ▶ global semantic entailment

$$\Gamma \Vdash_C^g A := \forall M \in C : M \Vdash \Gamma \implies M \Vdash A$$

Example

- ▶ $p \Vdash_C \Box p$
- ▶ $p \Vdash_C^g \Box p$

Material Implication vs Strict Implication

$$p \rightarrow q := \square(p \rightarrow q)$$

- $p \rightarrow q \rightarrow p$?
- $(p \rightarrow q) \vee (q \rightarrow r)$?
- $\neg(p \rightarrow q) \rightarrow (p \wedge \neg q)$?
- $(p \wedge \neg p) \rightarrow q$
- $p \rightarrow (q \vee \neg q)$
- $\square p \rightarrow q \rightarrow p$

Accessibility

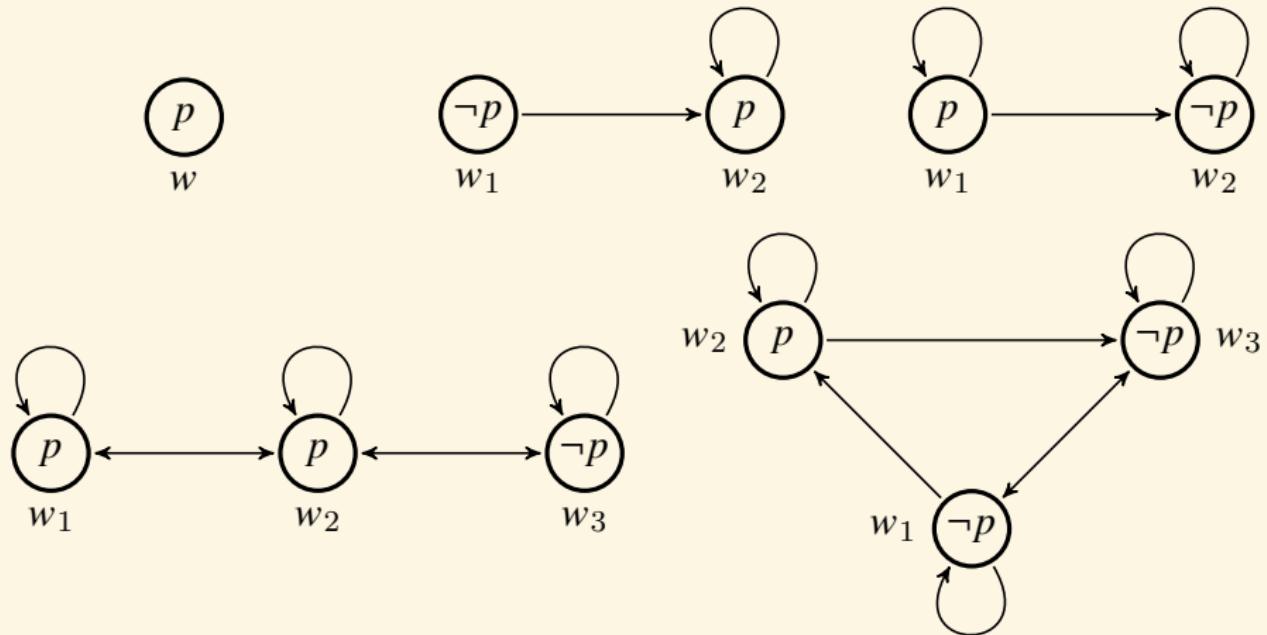
serial	$\forall x \exists y : Rxy$
reflexive	$\forall x : Rx x$
symmetric	$\forall xy : Rxy \rightarrow Ryx$
transitive	$\forall xyz : Rxy \wedge Ry z \rightarrow Rxz$
euclidean	$\forall xyz : Rxy \wedge Rxz \rightarrow Ry z$
total	$\forall xy : Rxy \vee Ryx$
isolation	$\exists x \forall y : \neg Rxy \wedge \neg Ryx$
successor reflexive	$\forall x \exists y : Rxy \wedge Ryy$
asymmetric	$\forall xy : Rxy \rightarrow \neg Ryx$
antisymmetric	$\forall xy : Rxy \wedge Ryx \rightarrow x = y$

Accessibility

Theorem

- | | | | |
|----------|--|--------|------------------------|
| <i>D</i> | $W, R \Vdash \Box p \rightarrow \Diamond p$ | \iff | <i>R is serial</i> |
| <i>T</i> | $W, R \Vdash \Box p \rightarrow p$ | \iff | <i>R is reflexive</i> |
| <i>B</i> | $W, R \Vdash p \rightarrow \Box \Diamond p$ | \iff | <i>R is symmetric</i> |
| <i>4</i> | $W, R \Vdash \Box p \rightarrow \Box \Box p$ | \iff | <i>R is transitive</i> |
| <i>5</i> | $W, R \Vdash \Diamond p \rightarrow \Box \Diamond p$ | \iff | <i>R is euclidean</i> |

Counter-model for D,T,B,4,5



Standard Translation

Definition (Standard Translation)

$$T_x(p) = P(x)$$

$$T_y(p) = P(y)$$

$$T_x(\neg A) = \neg T_x(A)$$

$$T_y(\neg A) = \neg T_y(A)$$

$$T_x(A \wedge B) = T_x(A) \wedge T_x(B)$$

$$T_y(A \wedge B) = T_y(A) \wedge T_y(B)$$

$$T_x(\Box A) = \forall y(Rxy \rightarrow T_y(A))$$

$$T_y(\Box A) = \forall x(Ryx \rightarrow T_x(A))$$

Theorem (Correspondence on Models)

$$\mathcal{M}, w \Vdash A \iff \mathcal{M} \models T_x(A)[w]$$

$$\mathcal{M} \Vdash A \iff \mathcal{M} \models \forall x T_x(A)$$

$$\mathcal{F}, w \Vdash A \iff \mathcal{F} \models \forall P_1, \dots, P_n T_x(A)[w]$$

$$\mathcal{F} \Vdash A \iff \mathcal{F} \models \forall P_1, \dots, P_n \forall x T_x(A)$$

Contents

Introduction	Set Theory
Term Logic	Recursion Theory
Propositional Logic	Equational Logic
Predicate Logic	Homotopy Type Theory
Modal Logic	Category Theory
Syntax	Quantum Computing
Semantics	
Formal System	Answers to the Exercises
Logic of Knowledge and Action	References 1436

Tree Method for Modal Logic

$w \models \Box A$



$v \models A$

$w \not\models \Box A$



Rwv

$v \not\models A$

if Rwv is already in the branch.

where v is new in the branch.

$w \models \Diamond A$



Rwv

$v \models A$

where v is new in the branch.

$w \not\models \Diamond A$

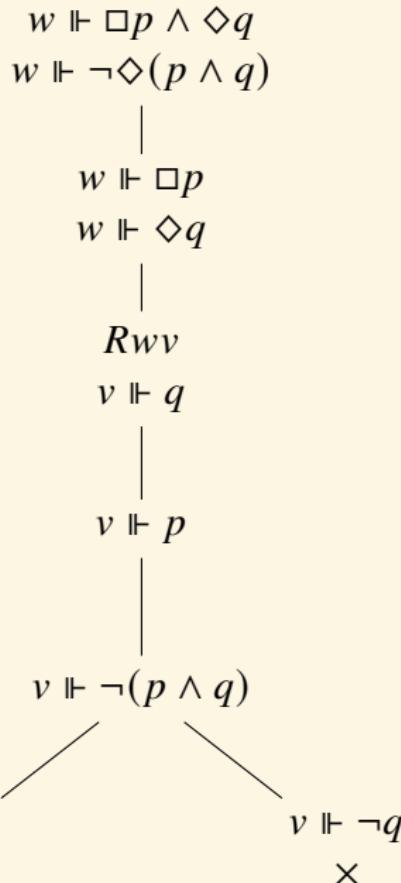


$v \not\models A$

if Rwv is already in the branch.

Example — Tree Method for Modal Logic

$$\Vdash \Box p \wedge \Diamond q \rightarrow \Diamond(p \wedge q)$$



Formal System = Axiom + Inference Rule

Axiom Schema

tautologies

Dual $\diamond A \leftrightarrow \neg \Box \neg A$

K $\Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B$

D $\Box A \rightarrow \diamond A$

T $\Box A \rightarrow A$

B $A \rightarrow \Box \diamond A$

4 $\Box A \rightarrow \Box \Box A$

5 $\diamond A \rightarrow \Box \diamond A$

L $\Box(\Box A \rightarrow A) \rightarrow \Box A$

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} \text{ [MP]}$$

$$\frac{A}{\Box A} \text{ [N]}$$

Intuitionistic Logic vs Modal Logic

$$\text{S4} := K + T + 4$$

$$\text{Grz} := \text{S4} + \square(\square(A \rightarrow \square A) \rightarrow A) \rightarrow A$$

$$p^* := \square p$$

$$(\neg A)^* := \square \neg A^*$$

$$(A \wedge B)^* := A^* \wedge B^*$$

$$(A \vee B)^* := A^* \vee B^*$$

$$(A \rightarrow B)^* := \square(A^* \rightarrow B^*)$$

$$\text{GL} := K + L$$

$$p' := p$$

$$(\neg A)' := \neg A'$$

$$(A \wedge B)' := A' \wedge B'$$

$$(A \vee B)' := A' \vee B'$$

$$(A \rightarrow B)' := A' \rightarrow B'$$

$$(\square A)' := A' \wedge \square A'$$

$$\vdash_{\text{I}} A \iff \vdash_{\text{S4}} A^* \iff \vdash_{\text{Grz}} A^*$$

$$\vdash_{\text{Grz}} A \iff \vdash_{\text{GL}} A'$$

$$\vdash_{\text{I}} A \iff \vdash_{\text{GL}} (A^*)'$$

$$\Box(\Box A \rightarrow A) \rightarrow \Box A \vdash_{\text{GL}} \Box A \rightarrow \Box\Box A$$

- $A \wedge \Box A \wedge \Box\Box A \rightarrow A \wedge \Box A$
- $A \rightarrow \Box(A \wedge \Box A) \rightarrow A \wedge \Box A$ $\Box(p \wedge q) \leftrightarrow \Box p \wedge \Box q$
- $\Box(\Box(A \wedge \Box A) \rightarrow A \wedge \Box A) \rightarrow \Box(A \wedge \Box A)$ L
- $\Box A \rightarrow \Box(A \wedge \Box A)$
- $\Box A \rightarrow \Box\Box A$

Theorem

$W, R \Vdash \Box(\Box A \rightarrow A) \rightarrow \Box A \iff R \text{ is transitive \& } R \text{ is reverse well-founded: there are no chains } w_0 R w_1 R w_2 \dots$

Proof.

Assume Rw_0w_1 and Rw_1w_2 , but not Rw_0w_2 . Setting $V(p) := W \setminus \{w_1, w_2\}$ makes L false at w_0 .

Assume R is transitive, and there is an ascending sequence $w_0 R w_1 R w_2 \dots$. Then $V(p) := W \setminus \{w_0, w_1, w_2, \dots\}$ refutes L at w_0 .

Conversely, if L fails at w_0 , there must be an infinite upward sequence of $\neg p$ -worlds. This arises by taking any successor of w_0 where p fails, and repeatedly applying the truth of $\Box(\Box p \rightarrow p)$ — using the transitivity of the frame.

Remark: transitivity is definable in first order logic, but well-foundedness can't be defined in first order logic. Frame truth is a second order notion.

Provability Logic

Theorem (Craig Interpolation)

If $\text{GL} \vdash A \rightarrow B$, then there is a C with $\text{Var}(C) \subset \text{Var}(A) \cap \text{Var}(B)$ s.t.
 $\text{GL} \vdash A \rightarrow C$ and $\text{GL} \vdash C \rightarrow B$

Corollary (Beth Definability)

Assume $\text{GL} \vdash A(p) \wedge A(q) \rightarrow (p \leftrightarrow q)$ where $q \notin \text{Var}(A)$ and $A(q)$ is obtained from $A(p)$ by replacing all occurrences of p by q . Then there exists a formula B with $\text{Var}(B) \subset \text{Var}(A) \setminus \{p\}$ s.t.

$$\text{GL} \vdash A(p) \rightarrow (p \leftrightarrow B)$$

Proof.

Let B be an interpolant for $\text{GL} \vdash A(p) \wedge p \rightarrow (A(q) \rightarrow q)$.

Theorem (Uniqueness of Fixpoint)

If p occurs only boxed in $A(p)$ and $q \notin \text{Var}(A)$, then

$$\text{GL} \vdash \square((p \leftrightarrow A(p)) \wedge (q \leftrightarrow A(q))) \rightarrow (p \leftrightarrow q)$$

where $\square A := A \wedge \square A$.

Corollary

In GL, if p occurs only boxed in $A(p)$, then

$$\frac{\begin{array}{c} B \leftrightarrow A(B) \\ C \leftrightarrow A(C) \end{array}}{B \leftrightarrow C}$$

Theorem (Existence of Fixpoint)

If p occurs only boxed in $A(p)$, then there exists a formula B with $\text{Var}(B) \subset \text{Var}(A) \setminus \{p\}$ s.t.

$$\text{GL} \vdash B \leftrightarrow A(B)$$

Uniqueness of Fixpoint + Beth Definability \implies Existence of Fixpoint

$$\text{GL} \vdash \neg \square \perp \leftrightarrow \neg \square(\neg \square \perp)$$

$$\text{GL} \vdash T \leftrightarrow \square T$$

Soundness & Completeness

Definition (Theorem & Local Syntactic Deduction)

- $\vdash_S A$
- $\Gamma \vdash_S A$ iff $\vdash_S \bigwedge_{i=1}^n B_i \rightarrow A$ for some finite subset $\{B_1, \dots, B_n\} \subset \Gamma$.

Theorem (Soundness & Completeness)

Let S be the normal system $KX_1 \dots X_n$ and $C = \bigcap_{i=1}^n C_i$ where each C_i is the corresponding class of frames for axiom schema X_i .

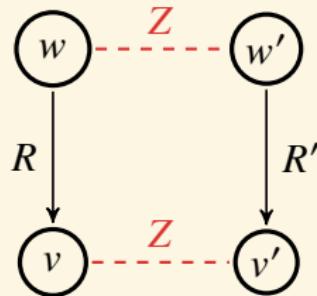
$$\Gamma \vdash_S A \iff \Gamma \Vdash_C A$$

Bisimulation

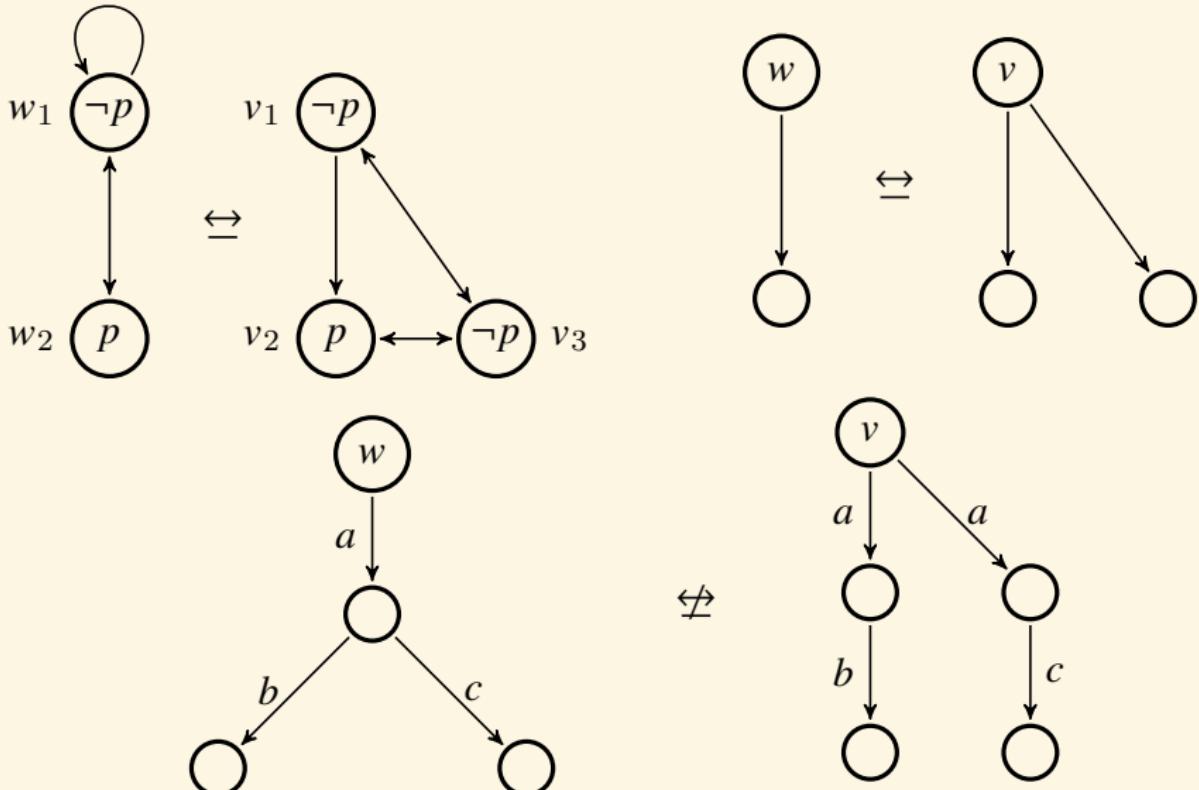
Definition (Bisimulation)

A bisimulation $Z : \mathcal{M} \leftrightarrow \mathcal{M}'$ between Kripke models $\mathcal{M} = (W, R, V)$ and $\mathcal{M}' = (W', R', V')$ is a binary relation $Z \subset W \times W'$ s.t.

1. If Zww' then w and w' satisfy the same proposition letters.
2. If Zww' and Rwv , then there exists $v' \in W'$ s.t. Zvv' and $R'w'v'$.
3. If Zww' and $R'w'v'$, then there exists $v \in W$ s.t. Zvv' and Rwv .

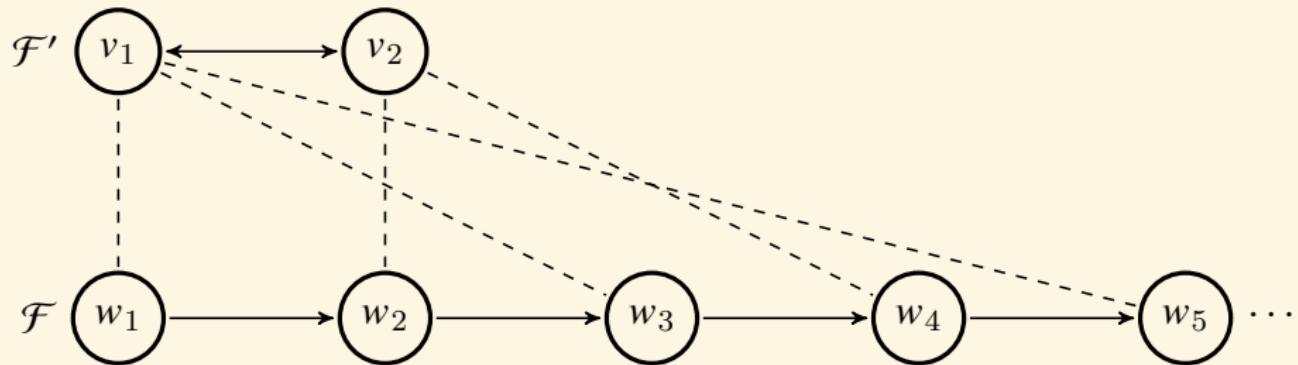


Bisimulation — Example



$$\square_a (\diamond_b \top \wedge \diamond_c \top)$$

反对称性不可模态定义



假设公式 A 定义反对称性，则对任意框架 $\mathcal{F} : \mathcal{F} \models A \iff \mathcal{F}$ 是反对称的。考虑如上两个框架： $\mathcal{F} \models A, \mathcal{F}' \not\models A$ ，这意味着 \mathcal{F}' 有赋值 V' 和点 v 使得 $\mathcal{F}', V', v \models A$ ，但是按照虚线我们可以把这个赋值迁移到 \mathcal{F} 上（记为 V ），并使虚线是互模拟，所以 $\mathcal{F}', V', v \Leftarrow \mathcal{F}, V, w$ ，因而 $\mathcal{F}, V, w \models A$ ，这与 $\mathcal{F} \models A$ 矛盾。

Bisimulation

Theorem (van Benthem Characterization Theorem 1976)

Let $A(x)$ be a first order formula. Then $A(x)$ is bisimulation invariant iff it is (equivalent to) the standard translation of a modal formula.

Remark: Modal logic is the bisimulation-invariant fragment of first-order logic!

Theorem (van Benthem 2007)

An abstract modal logic extending basic modal logic and satisfying compactness and bisimulation invariance is equally expressive as the basic modal logic K .

Topological Semantics for Modal Logic S4

$$\llbracket \neg A \rrbracket := W \setminus \llbracket A \rrbracket$$

$$\llbracket A \wedge B \rrbracket := \llbracket A \rrbracket \cap \llbracket B \rrbracket$$

$$\llbracket A \vee B \rrbracket := \llbracket A \rrbracket \cup \llbracket B \rrbracket$$

$$\llbracket A \rightarrow B \rrbracket := (W \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket$$

$$\llbracket \perp \rrbracket := \emptyset$$

$$\llbracket \top \rrbracket := W$$

$$\llbracket \Box A \rrbracket := (\llbracket A \rrbracket)^\circ$$

$$\llbracket \Diamond A \rrbracket := \overline{\llbracket A \rrbracket}$$

where \circ is the interior operator $A^\circ := \bigcup\{U \in O(W) : U \subset A\}$, and $\overline{-}$ is the closure operator $\overline{A} := W \setminus (W \setminus A)^\circ$.

$$O(W) \Vdash A := \llbracket A \rrbracket = W$$

Theorem

$A \vdash_{S4} B \iff \llbracket A \rrbracket \subset \llbracket B \rrbracket$ for every topological interpretation $(W, O(W), \llbracket \rrbracket)$

Neighborhood Semantics for Modal Logic

Definition (Neighborhood Model)

A neighborhood model is $\mathcal{M} = (W, N, V)$, where $W \neq \emptyset$, $N : W \rightarrow P(P(W))$ is a neighborhood function, and $V : \text{Var} \rightarrow P(W)$ is a assignment function.

Definition (Truth)

$$\mathcal{M}, w \models p \iff w \in V(p)$$

$$\mathcal{M}, w \models \neg A \iff \mathcal{M}, w \not\models A$$

$$\mathcal{M}, w \models A \wedge B \iff \mathcal{M}, w \models A \ \& \ \mathcal{M}, w \models B$$

$$\mathcal{M}, w \models \Box A \iff \llbracket A \rrbracket \in N(w)$$

$$\mathcal{M}, w \models \Diamond A \iff W \setminus \llbracket A \rrbracket \notin N(w)$$

where $\llbracket A \rrbracket := \{w : \mathcal{M}, w \models A\}$.

Remark:

$$\llbracket \Box A \rrbracket = \Box_N \llbracket A \rrbracket \quad \text{where} \quad \Box_N X := \{w \in W : X \in N(w)\}$$

$$\llbracket \Diamond A \rrbracket = \Diamond_N \llbracket A \rrbracket \quad \text{where} \quad \Diamond_N X := \{w \in W : W \setminus X \notin N(w)\}$$

Topological Semantics vs Neighborhood Semantics

Definition (Topological Space Definition via Neighborhoods)

(W, N) is a topological space iff $N : W \rightarrow P(P(W))$ satisfies

1. $U \in N(w) \implies w \in U$
2. $U, V \in N(w) \implies U \cap V \in N(w)$
3. $U \in N(w) \ \& \ U \subset V \implies V \in N(w)$
4. $U \in N(w) \implies \exists V \in N(w) : V \subset U \ \& \ \forall v \in V : U \in N(v)$

Topological space via open sets $(W, O(W))$ and topological space via neighborhoods (W, N) .

We know that $U \subset W$ is open iff $\forall w \in U : U \in N(w)$.

Conversely, $V \in N(w)$ is a neighborhood of w iff $\exists U \in O(W) : w \in U \subset V$.

Remark: Topological semantics is subsumed by neighborhood semantics, being just neighborhood semantics with the above conditions in definition 189.

$$[\![A]\!] \in N(w) \iff \exists U \in O(W) : w \in U \subset [\![A]\!] \iff w \in ([\![A]\!])^\circ$$

Intension vs Extension

$$\llbracket P \rrbracket = \lambda w. \llbracket P \rrbracket^w$$

Intension as a function from possible worlds to extensions

- The intension of a name is a function from possible worlds to objects.

$$\llbracket \text{alice} \rrbracket^w = \text{Alice}$$

- The intension of a predicate is a function from possible worlds to functions from objects to truth-values.

$$\llbracket \text{smoke} \rrbracket^w = \lambda x. \llbracket x \text{ smokes in } w \rrbracket$$

- The intension of a sentence is a function from possible worlds to truth-values.

	w_1	w_2
$\llbracket a = a \rrbracket$	1	1
$\llbracket a = b \rrbracket$	1	0

Contents

Introduction	Set Theory
Term Logic	Recursion Theory
Propositional Logic	Equational Logic
Predicate Logic	Homotopy Type Theory
Modal Logic	Category Theory
Syntax	Quantum Computing
Semantics	
Formal System	Answers to the Exercises
Logic of Knowledge and Action	References 1436

Jaakko Hintikka



Figure: Jaakko Hintikka: 1929–2015. Epistemic Logic / Game Semantics / Independence-Friendly Logic

Logic of Knowledge

- ▶ 什么是密码？你知我知。
- ▶ 微信群是干嘛的？制造公共知识。
- ▶ 邮件密送是干嘛的？你知他知，他不知你知，且这是你我的公共知识。
- ▶ “代我问他好”是干嘛的？让你知道我尊重他。
- ▶ 送什么礼物给太太？我知道她也知道对她有用的。
- ▶ 广告语的意义？制造带意义的动作传递知识。
- ▶ 《三体》中的黑暗森林法则：爱好和平的公共知识难以达成。
- ▶ 如何建设健康学术环境：让他知道你知道学术规范。
- ▶ 狼人杀？理性利用别人的不理性。
- ▶ 付费知识分享平台：让你相信你知道很多。
- ▶ Would you like to come up to my apartment to see my etchings?
阿 Q：我想和你困觉！
- Nash: Could we just go straight to the sex? ✅

Reasoning about Knowledge

- ▶ Knowledge is power: act properly to achieve goals;
- ▶ Knowledge is time: to make decisions more efficiently;
- ▶ Knowledge is money: can be traded;
- ▶ Knowledge is responsibility: to prove someone is guilty;
- ▶ Knowledge is you: to identify oneself;
- ▶ Knowledge is an immune system: to protect you;
- ▶ Knowledge satisfies our curiosity.

“The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge.”

— Stephen Hawking

“The only good is knowledge and the only evil is ignorance.”

— Socrates

know the unknown from the known

- There are things we know we know. There are things we know we don't know. There are things we don't know we don't know.

$$\exists x KKx \wedge \exists x K\neg Kx \wedge \exists x \neg K\neg Kx$$

- 知之为知之，不知为不知，是知也。

$$Kp \rightarrow KKp \quad \& \quad \neg Kp \rightarrow K\neg Kp$$

“Real knowledge is to know the extent of one's ignorance.”

— Confucius

- ▶ Mutual Knowledge:
 - everybody in G knows p .
- ▶ Distributed Knowledge:
 - everybody in G would know p
if agents in G shared all their information.
- ▶ Common Knowledge:
 - everybody in G knows p ,
 - everybody knows that everybody knows,
 - and so on.

Mutual Knowledge

Suppose a group $G \subset \{1 \dots n\}$ of agents, everyone in G knows A :

$$E_G A := \bigwedge_{i \in G} K_i A$$

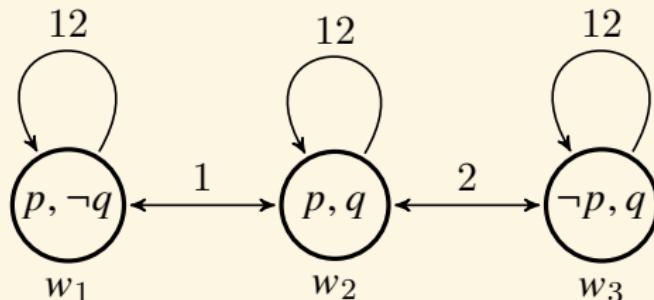
$$R_E := \bigcup_{i \in G} R_i$$

$$\mathcal{M}, w \models E_G A \quad \text{iff} \quad \forall v \in W : R_E w v \implies \mathcal{M}, v \models A$$

Distributed Knowledge

$$R_D := \bigcap_{i \in G} R_i$$

$\mathcal{M}, w \Vdash D_G A$ iff $\forall v \in W : R_D w v \implies \mathcal{M}, v \Vdash A$



$w_2 \models K_1 p \wedge \neg K_1 q \wedge K_2 q \wedge \neg K_2 p \wedge D_{\{1,2\}}(p \wedge q)$

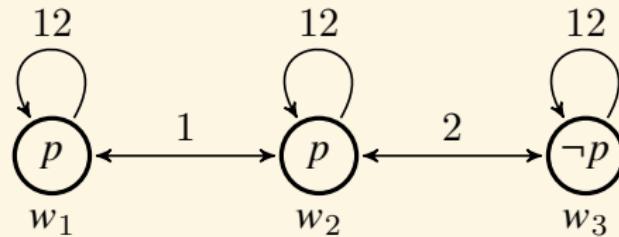
Common Knowledge

$$\begin{array}{ll} E_G^1 A := E_G A & R^1 := R \\ E_G^{k+1} A := E_G E_G^k A & R^{k+1} := R \circ R^k \\ C_G A := \bigwedge_{k=1}^{\infty} E_G^k A & R \circ S := \{(x, y) : \exists z (Rxz \wedge Szy)\} \\ & R^* := \bigcup_{k=1}^{\infty} R^k \\ R_C := \left(\bigcup_{i \in G} R_i \right)^* & \\ \mathcal{M}, w \Vdash C_G A \text{ iff } \forall v \in W : R_C wv \implies \mathcal{M}, v \Vdash A & \end{array}$$

A Hierarchy of States of Knowledge

$$C_G A \implies \cdots E_G^k A \implies \cdots E_G A \implies \bigvee_{i \in G} K_i A \implies D_G A \implies A$$

Can we easily have full common knowledge?



$$w_1 \models E_{\{1,2\}} p \wedge \neg C_{\{1,2\}} p$$

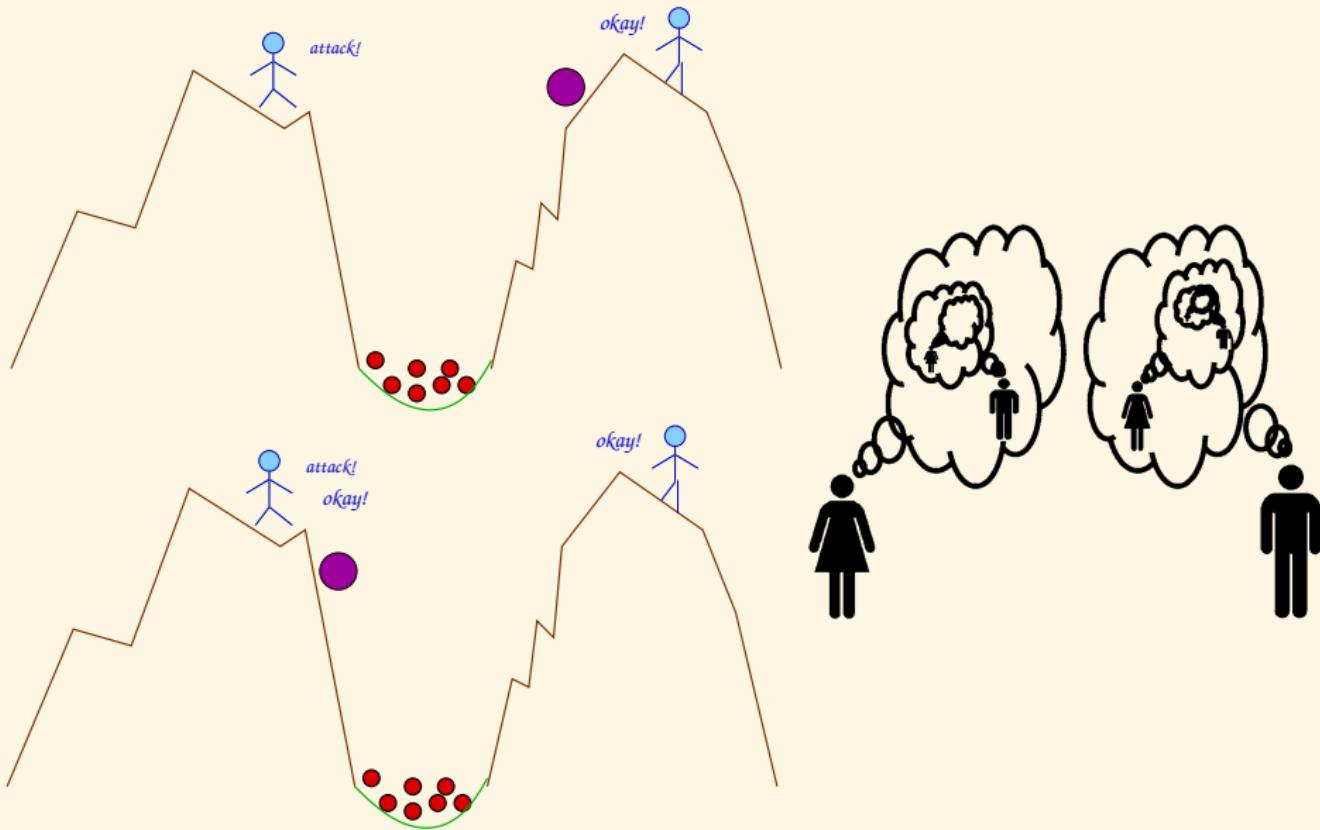
假设 C 秘密的分别给了 A 和 B 两个数字 2 和 3，他只告诉他们俩这两个数字是相邻的自然数。令 p 为“两数字之和小于一千万”，请问 p 是 A 和 B 的公共知识么？

$$(0, 1) \xleftrightarrow{B} (2, 1) \xleftrightarrow{A} \underline{(2, 3)} \xleftrightarrow{B} (4, 3) \xleftrightarrow{A} (4, 5) \xleftrightarrow{B} (6, 5) \cdots$$

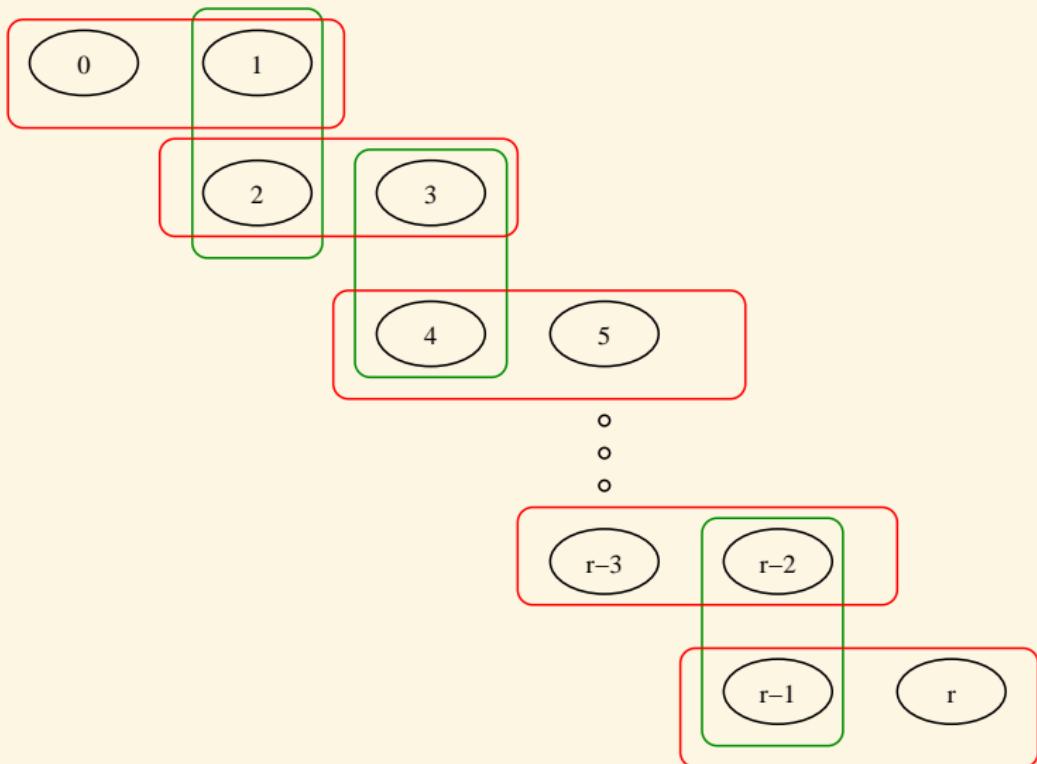
$$(2, 3) \Vdash \neg K_B K_A K_B (x + y \leq 10)$$

A and B commonly know that B 's number is odd.

Coordinated Attack



Coordinated Attack



《三体》— 黑暗森林

黑暗森林-猜疑链

如果你认为我是善意的，这并不是你感到安全的理由，因为按照第一条公理，善意文明并不能预先把别的文明也想成善意的，所以，你现在还不知道我是怎么认为你的，你不知道我认为你是善意还是恶意；进一步，即使你知道我也把你想象成善意的，我也知道你把我想象成善意的，但是我不知道你是怎么想我怎么想你怎么想我的……

“Every driver must drive on the right.”

What kind of knowledge is enough to let people feel safe in driving on the right?

Aumann's Agreement Theorem

Theorem (Aumann's Agreement Theorem)

If two people are genuine Bayesian rationalists with common priors, and their posteriors are common knowledge, then these posteriors are equal.

如果两个人有相同的先验知识，则他们不可能对有分歧的后验知识（经过各自的实验获取私人信息）形成公共知识。不管怎么根据进一步的私人证据进行充分的更新和交流，大家都不可能最后 agree to disagree!

Aumann's Agreement Theorem

$(W, \{\mathcal{I}_i\}_{i \in G}, \{K_i\}_{i \in G})$.

- ▶ W is a non-empty set of worlds.
 - ▶ \mathcal{I}_i is agent i 's partition of W . $\mathcal{I}_i(w)$ is the element of the partition that contains w .
 - ▶ $K_i : P(W) \rightarrow P(W)$ is agent i 's knowledge operator.
 $K_i(A) = \{w : \mathcal{I}_i(w) \subset A\}$.
 - ▶ Mutual Knowledge $E_G(A) := \bigcap_{i \in G} K_i(A)$.
 - ▶ Common knowledge $C_G(A) := \bigcap_{n=1}^{\infty} E_G^n(A)$.
1. $K(W) = W$
 2. $A \subset B \implies K(A) \subset K(B)$
 3. $K(A) \cap K(B) = K(A \cap B)$
 4. $K(A) \subset A$
 5. $K(A) \subset K(K(A))$
 6. $W \setminus K(A) \subset K(W \setminus K(A))$

Aumann's Agreement Theorem

Lemma

If $C_G(A) \neq \emptyset$, then $\forall i \in G \exists \mathcal{D}_i \subset \mathcal{I}_i : C_G(A) = \bigcup \mathcal{D}_i$.

Proof.

$w \in C_G(A) \implies \forall i \forall n : w \in K_i E_G^n(A) \implies \forall i \forall n : \mathcal{I}_i(w) \subset E_G^n(A) \implies \forall i : \mathcal{I}_i(w) \subset C_G(A)$

Theorem (Aumann's Agreement Theorem)

Let P be the common prior belief, and $B := \bigcap_{i \in G} \{w : P(A | \mathcal{I}_i(w)) = q_i\}$. If $P(C_G(B)) > 0$, then $\forall i \in G : q_i = P(A | C_G(B))$.

Proof.

$$P(A | C_G(B)) = \frac{P(A \cap \bigcup \mathcal{D}_i)}{\sum_{D \in \mathcal{D}_i} P(D)} = \frac{\sum_{D \in \mathcal{D}_i} P(A | D)P(D)}{\sum_{D \in \mathcal{D}_i} P(D)} = \frac{\sum_{D \in \mathcal{D}_i} q_i P(D)}{\sum_{D \in \mathcal{D}_i} P(D)} = q_i$$

Epistemic Logic

- Knowledge $S5 := K + T + 4 + 5$

知之为知之(4), 不知为不知(5), 是知也

- Belief $K + D + 4 + 5$

- Common Knowledge

S5

+

$$C_G A \leftrightarrow A \wedge E_G C_G A$$

+

$$A \wedge C_G(A \rightarrow E_G A) \rightarrow C_G A$$

- Distributed Knowledge

S5

+

$$D_{\{i\}} A \leftrightarrow K_i A$$

+

$$D_G A \rightarrow D_{G'} A \text{ if } G \subset G'$$

Knowledge vs Belief

$$1. \ K(p \rightarrow q) \rightarrow Kp \rightarrow Kq$$

$$2. \ Kp \rightarrow p$$

$$3. \ Kp \rightarrow KKp$$

$$4. \ \neg Kp \rightarrow K\neg Kp$$

$$1. \ Kp \rightarrow Bp$$

$$2. \ Bp \rightarrow BKp$$

$$3. \ Bp \rightarrow KBp$$

$$4. \ \neg Kp \rightarrow K\neg Bp$$

$$1. \ B(p \rightarrow q) \rightarrow Bp \rightarrow Bq$$

$$2. \ Bp \rightarrow \neg B\neg p$$

$$3. \ Bp \rightarrow Bp$$

$$4. \ \neg Bp \rightarrow B\neg Bp$$

$$Bp \leftrightarrow \neg K\neg Kp$$

Moore's Paradox

It's raining but I don't believe it's raining.

$$\vdash \neg B(p \wedge \neg Bp)$$

1. $B(p \wedge \neg Bp)$ Assumption
2. $Bp \wedge B\neg Bp$ $B(p \wedge q) \rightarrow Bp \wedge Bq$
3. Bp
4. BBp $Bp \rightarrow BBp$
5. $B\neg Bp$
6. $BBp \wedge B\neg Bp$
7. $\neg(BBp \wedge B\neg Bp)$ $(Bp \rightarrow \neg B\neg p) \leftrightarrow \neg(Bp \wedge B\neg p)$
8. $\neg B(p \wedge \neg Bp)$

Moore's Paradox

It's raining but I don't know it's raining.

$$\vdash \neg K(p \wedge \neg Kp)$$

1. $K(p \wedge \neg Kp)$ Assumption
2. Kp
3. $K\neg Kp$
4. $\neg Kp$ $Kp \rightarrow p$
5. $Kp \wedge \neg Kp$
6. $\neg K(p \wedge \neg Kp)$

Fitch's Paradox of Knowability

Are all truths knowable?

If all truths are knowable, then all truths are known.

$$\forall p(p \rightarrow \diamond Kp) \vdash \forall p(p \rightarrow Kp)$$

1. $\neg K(p \wedge \neg Kp)$
2. $\neg \diamond K(p \wedge \neg Kp)$ $\vdash \neg p \implies \vdash \neg \diamond p$
3. $p \wedge \neg Kp$ Assumption
4. $\diamond K(p \wedge \neg Kp)$ $p \rightarrow \diamond Kp$
5. $\neg(p \wedge \neg Kp)$
6. $p \rightarrow Kp$

Against Negative Introspection?

1. $\neg p \wedge BKp$ suppose you falsely believes that you know p
2. $\neg Kp$ knowledge implies truth
3. $K\neg Kp$ negative introspection
4. $B\neg Kp$ knowledge implies belief
5. $B\perp$

Margin for Error and Against Positive Introspection?

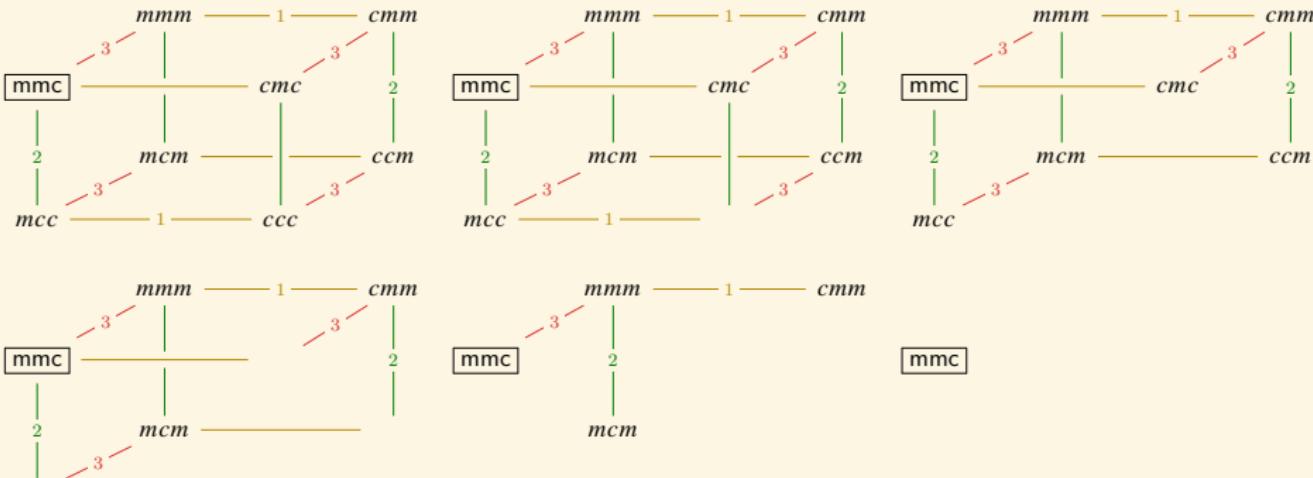
- | | |
|--|------------------------|
| 1. $K\neg p_n$ | Assumption |
| 2. $K(p_{n+1} \rightarrow \neg K\neg p_n)$ | Margin for Error |
| 3. $K(K\neg p_n \rightarrow \neg p_{n+1})$ | |
| 4. $K\neg p_n \rightarrow KK\neg p_n$ | Positive Introspection |
| 5. $K\neg p_{n+1}$ | ? |

Information Update — Muddy Children Problem



Problem (Muddy Children Problem)

Consider k of n children get mud on their heads. Each child can see the mud on others but can't see his or her own head. Their father says "at least one is muddy." He then asks the following question repeatedly: "does anyone know whether you have mud on your own head?" Assuming that the children are intelligent, honest, and answer simultaneously, what will happen?



1. "At least one is muddy. Does anyone...?" $\neg K_1 m_1 \wedge \neg K_2 m_2 \wedge \neg K_3 m_3$
2. "Does anyone...?" $K_1 m_1 \wedge K_2 m_2 \wedge \neg K_3 m_3$
3. $K_3 \neg m_3$

Public Announcement Logic

$$A ::= p \mid \neg A \mid A \wedge A \mid K_i A \mid [A]A$$

$$\mathcal{M}, w \models [B]A \text{ iff } \mathcal{M}, w \models B \implies \mathcal{M}|_B, w \models A$$

$$\mathcal{M}, w \models \langle B \rangle A \text{ iff } \mathcal{M}, w \models B \text{ \& } \mathcal{M}|_B, w \models A$$

where

$$\mathcal{M}|_B := (W', \{R'_i\}_{i \in G}, V')$$

and

$$W' := \{w \in W : \mathcal{M}, w \models B\} \quad R'_i := R_i|_{W' \times W'} \quad V'(p) := V(p) \cap W'$$

Muddy Children Problem

$$\mathcal{M}, mmc \Vdash m_1 \wedge m_2 \wedge \neg m_3$$

$$\mathcal{M}, mmc \Vdash E_{\{1,2,3\}} P$$

$$\mathcal{M}, mmc \Vdash \neg C_{\{1,2,3\}} P$$

$$\mathcal{M}, mmc \Vdash \neg K_1 m_1 \wedge K_1 m_2$$

$$\mathcal{M}, mmc \Vdash K_1 K_3 m_2 \wedge K_1 \neg K_2 m_2$$

$$\mathcal{M} \upharpoonright_P, mcc \Vdash K_1 m_1$$

$$\mathcal{M} \upharpoonright_P, mmc \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$$

$$\mathcal{M} \upharpoonright_P, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$$

$$\mathcal{M} \upharpoonright_P \upharpoonright_{\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3}, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$$

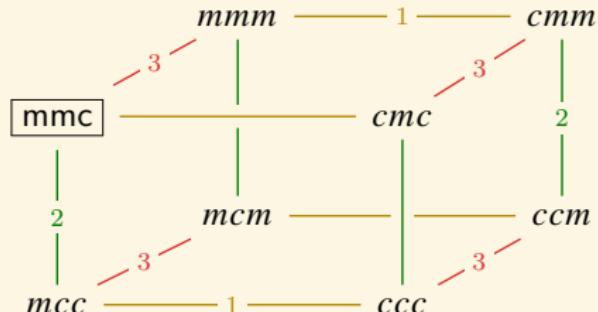
1. “At least one is muddy.” $P := m_1 \vee m_2 \vee m_3$

2. “Does anyone...?” $\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$ where $Q_i := K_i m_i \vee K_i \neg m_i$

3. “Does anyone...?” $Q_1 \wedge Q_2 \wedge \neg Q_3$

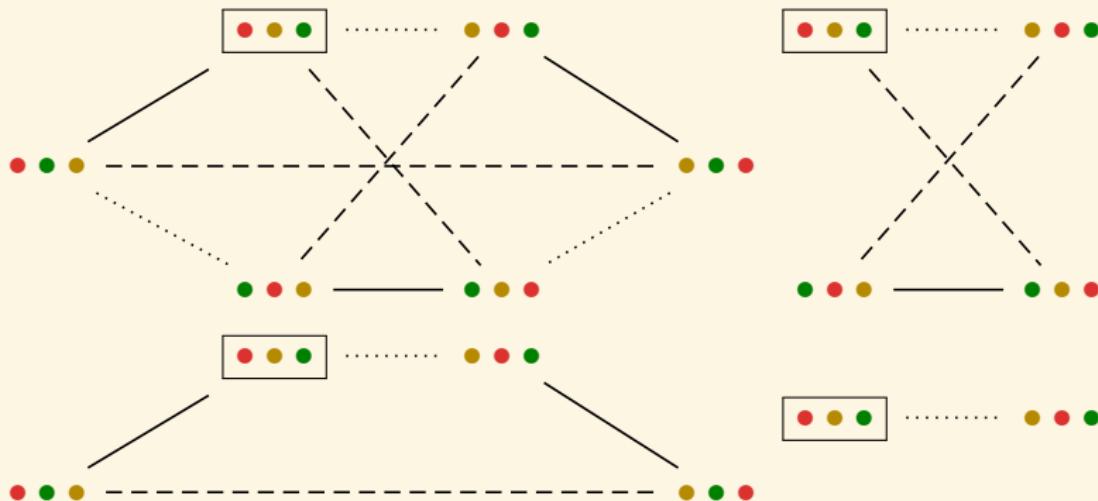
$$\mathcal{M}, mmc \Vdash [P][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3][Q_1 \wedge Q_2 \wedge \neg Q_3](K_1 m_1 \wedge K_2 m_2 \wedge K_3 \neg m_3)$$

$$\mathcal{M}, mmm \Vdash [P][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3](K_1 m_1 \wedge K_2 m_2 \wedge K_3 m_3)$$



Three Cards Puzzle

- ▶ Three cards 'red', 'yellow', 'green' are given to three children: 1, 2, 3.
- ▶ The children can only see their own cards.
- ▶ 2 asks 1: "Do you have the green card?"
- ▶ 1 answers: "No".



Ages of Three Children

- ▶ A census-taker approaches a woman and asks about her children.
- ▶ She says “I have three children and the product of their ages is 36. The sum of their ages is today’s date.”
- ▶ The census-taker complains “I still can’t tell.”
- ▶ The woman replies “I have to go, my eldest child is sleeping upstairs.”

Birthday Puzzle

A and **B** want to know when **C**'s birthday is.

C provides a list of 10 possible dates:

5.15	5.16	5.19
6.17	6.18	
7.14	7.16	
8.14	8.15	8.17

C then tells **A** and **B** separately the month and the day of her birthday.

- ▶ **A:** I don't know when **C**'s birthday is, but I know that **B** also does not know.
- ▶ **B:** At first I didn't know, but now I know.
- ▶ **A:** Then I also know it.

Russian Cards

Russian Cards

- ▶ From a pack of seven known cards “0123456” A and B each draw three cards and C gets the remaining card.
- ▶ How can A and B openly inform each other about their cards, without C learning of any of their cards who holds it?
- ▶ Assume A ' hand is ijk and the remaining cards is $lmno$. Choose one from ijk , say i , and choose two from $lmno$, say lm . Three of the hands are ijk, ilm, ino . From lm choose one, say l , and from no choose one, say n . Two hands are jln, kmo . A announces these five hands.
- ▶ B announces C 's card.

Unsuccessful Update

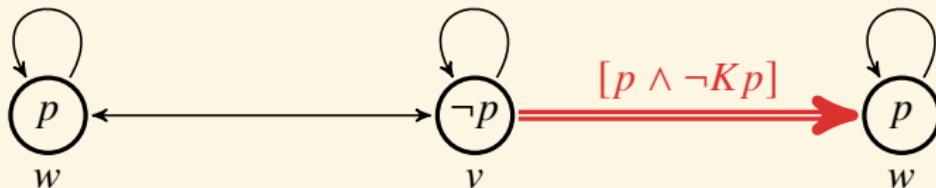
$$\Vdash [p]C_G p$$

$$\Vdash [C_G A]C_G A$$

$$\stackrel{?}{\Vdash} [A]C_G A$$

$$\stackrel{?}{\Vdash} [A]KA$$

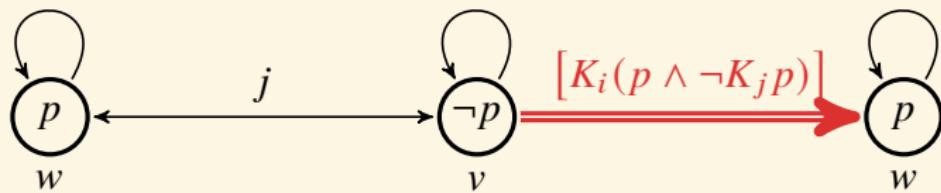
$$\stackrel{?}{\Vdash} [A]A$$



$$\mathcal{M}, w \Vdash (p \wedge \neg Kp) \wedge [p \wedge \neg Kp] Kp$$

Remark: If the goal of the announcing person was to “spread the truth of this formula,” then this attempt was clearly unsuccessful.

Unsuccessful Update



$$\mathcal{M}, w \Vdash (p \wedge \neg K_j p) \wedge K_i(p \wedge \neg K_j p) \wedge [K_i(p \wedge \neg K_j p)] K_i K_j p$$

- $\langle B \rangle A \leftrightarrow B \wedge [B]A$
- $[B](A \rightarrow C) \leftrightarrow ([B]A \rightarrow [B]C)$
- $[B]p \leftrightarrow (B \rightarrow p)$
- $[B]\neg A \leftrightarrow (B \rightarrow \neg A)$?
- $[B]\neg A \leftrightarrow \neg[B]A$?
- $[B]\neg A \leftrightarrow (B \rightarrow \neg[B]A)$
- $[B]K_i A \leftrightarrow (B \rightarrow K_i(B \rightarrow [B]A))$
- $[B]K_i A \leftrightarrow (B \rightarrow K_i[B]A)$
- $[B][C]A \leftrightarrow [B \wedge C]A$?
- $[B][C]A \leftrightarrow [B \wedge [B]C]A$
- $$\frac{A}{[B]A} \quad \frac{A(p)}{A(B)} \text{ ?} \quad \frac{A \leftrightarrow B}{[A]C \leftrightarrow [B]C} \quad \frac{A \leftrightarrow B}{[C]A \leftrightarrow [C]B}$$

Public Announcement Logic (PAL)

Axiom Schema

1. tautologies
2. $K_i(A \rightarrow B) \rightarrow K_iA \rightarrow K_iB$
3. $[B]p \leftrightarrow (B \rightarrow p)$
4. $[B]\neg A \leftrightarrow (B \rightarrow \neg[B]A)$
5. $[B](A \wedge C) \leftrightarrow [B]A \wedge [B]C$
6. $[B]K_iA \leftrightarrow (B \rightarrow K_i[B]A)$
7. $[B][C]A \leftrightarrow [B \wedge [B]C]A$

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} \text{ [MP]}$$

$$\frac{A}{K_iA} \text{ [N]}$$

Expressive Power

Theorem

PAL is equally expressive as basic modal logic.

Proof.

$$\begin{array}{ll} t(\top) = \top & t([B]\top) = t(B \rightarrow \top) \\ t(p) = p & t([B]p) = t(B \rightarrow p) \\ t(\neg A) = \neg t(A) & t([B]\neg A) = t(B \rightarrow \neg[B]A) \\ t(A \wedge B) = t(A) \wedge t(B) & t([B](A \wedge C)) = t([B]A \wedge [B]C) \\ t(K_i A) = K_i t(A) & t([B]K_i A) = t(B \rightarrow K_i[B]A) \\ & t([B][C]A) = t([B \wedge [B]C]A) \\ & \Vdash A \leftrightarrow t(A) \end{array}$$

Succinctness

Theorem

PAL is complete w.r.t. the standard semantics of Public Announcement Logic.

Proof.

$$\Vdash A \implies \Vdash t(A) \implies \vdash_K t(A) \implies \vdash_{\text{PAL}} t(A) \implies \vdash_{\text{PAL}} A$$

Theorem

PAL is exponentially more succinct than modal logic on arbitrary models.

$$A_0 := \top$$

$$A_{n+1} := \langle \langle A_n \rangle \diamond_1 \top \rangle \diamond_2 \top$$

where $\diamond_i A := \neg K_i \neg A$ and $\langle B \rangle A := \neg [B] \neg A$.

Announcement and Common Knowledge

$$\frac{P \rightarrow [Q]A \quad P \wedge Q \rightarrow E_G P}{P \rightarrow [Q]C_G A}$$

'Common knowledge induction' is a special case.

Take $P := A$ and $Q := \top$.

$$C_G(A \rightarrow E_G A) \rightarrow A \rightarrow C_G A$$

Propositional Dynamic Logic

$$A ::= \top \mid p \mid \neg A \mid A \wedge A \mid [\alpha]A$$

$$\alpha ::= a \mid A? \mid \alpha; \alpha \mid \alpha \cup \alpha \mid \alpha^*$$

$$\mathcal{M}, w \Vdash [\alpha]A \text{ iff } \forall v \in W : R_\alpha wv \implies \mathcal{M}, v \Vdash A$$

$$\mathcal{M}, w \Vdash \langle \alpha \rangle A \text{ iff } \exists v \in W : R_\alpha wv \text{ \& } \mathcal{M}, v \Vdash A$$

where

$$R_{A?} := \{(w, w) : \mathcal{M}, w \Vdash A\}$$

$$R_{\alpha; \beta} := \{(w, v) : \exists u (R_\alpha wu \wedge R_\beta uv)\}$$

$$R_{\alpha \cup \beta} := R_\alpha \cup R_\beta$$

$$R_{\alpha^*} := \bigcup_{n=0}^{\infty} R_{\alpha^n}$$

Propositional Dynamic Logic (PDL)

Axiom Schema

1. tautologies
2. $[\alpha](A \rightarrow B) \rightarrow [\alpha]A \rightarrow [\alpha]B$
3. $[B?]A \leftrightarrow (B \rightarrow A)$
4. $[\alpha; \beta]A \leftrightarrow [\alpha][\beta]A$
5. $[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
6. $[\alpha^*]A \leftrightarrow A \wedge [\alpha][\alpha^*]A$
7. $A \wedge [\alpha^*](A \rightarrow [\alpha]A) \rightarrow [\alpha^*]A$

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} \text{ [MP]}$$

$$\frac{A}{[\alpha]A} \text{ [N]}$$

PDL is sound and weak complete.

PDL is not compact. $\{\langle a^* \rangle p, \neg p, \neg \langle a \rangle p, \neg \langle a; a \rangle p, \neg \langle a; a; a \rangle p, \dots\}$
Its satisfiability is decidable (in EXPTIME).

First Order Dynamic Logic

Axiom Schema

1. FOL
2. PDL
3. $\langle x := t \rangle A \leftrightarrow A[t/x]$

Inference Rule

$$\frac{A \quad A \rightarrow B}{B} \text{ [MP]}$$

$$\frac{A \rightarrow [\alpha^n]B, \quad n \in \omega}{A \rightarrow [\alpha^*]B} \text{ [IC]}$$

$$\frac{A}{[\alpha]A} \text{ [N]}$$

$$\frac{A}{\forall x A} \text{ [G]}$$

Application — Program Analysis

skip := $\top?$

fail := $\perp?$

if B **then** α **else** β := $B?; \alpha \cup \neg B?; \beta$

while B **do** α := $(B?; \alpha)^*; \neg B?$

repeat α **until** B := $\alpha; (\neg B?; \alpha)^*; B?$

$\{A\} \alpha \{B\}$:= $A \rightarrow [\alpha]B$

Algorithm 1 GCD

while $x \neq y$ **do**
 if $x > y$ **then**
 $x \leftarrow x - y$
 else
 $y \leftarrow y - x$
 end if
end while

$$[(x = m \wedge y = n)?] \langle (x \neq y?; (x > y?; x \leftarrow x - y) \cup (x < y?; y \leftarrow y - x))^*; x = y? \rangle x = \gcd(m, n)$$

Hoare Logic

$$\overline{\{P\} \text{ skip } \{P\}}$$

$$\overline{\{P[t/x]\} x := t \{P\}}$$

$$\frac{\{P\} \alpha \{Q\} \quad \{Q\} \beta \{R\}}{\{P\} \alpha; \beta \{R\}}$$

$$\frac{\{B \wedge P\} \alpha \{Q\} \quad \{\neg B \wedge P\} \beta \{Q\}}{\{P\} \text{ if } B \text{ then } \alpha \text{ else } \beta \{Q\}}$$

$$\frac{P_1 \rightarrow P_2 \quad \{P_2\} \alpha \{Q_2\} \quad Q_2 \rightarrow Q_1}{\{P_1\} \alpha \{Q_1\}}$$

$$\frac{\{P \wedge B\} \alpha \{P\}}{\{P\} \text{ while } B \text{ do } \alpha \{\neg B \wedge P\}}$$

$\{x = 4 \wedge y = 3\}$ if $x < y$ then $z := x; y := y + 1$ else $z := y; z := z + 1$ $\{x = 4 \wedge y = 3 \wedge z = 4\}$

宿命论论证

1. 如果明天有海战为真，那么明天有海战就不可能为假，即明天必然有海战。
2. 如果明天有海战为假，那么明天有海战就不可能为真，即明天必然没有海战。
3. 因此，要么明天必然有海战，要么明天必然没有海战。

$$\frac{\begin{array}{c} p \rightarrow \Box p \\ \neg p \rightarrow \Box \neg p \\ \hline \Box p \vee \Box \neg p \end{array}}{\begin{array}{c} \Box(p \rightarrow p) \\ \Box(\neg p \rightarrow \neg p) \\ \hline \Box p \vee \Box \neg p \end{array}} \times$$

knowing-whether	$KA \vee K\neg A$
knowing-what	$\exists xK(A \rightarrow x = c)$
knowing-how	$\exists \alpha [\alpha]A$
knowing-why	$\exists tK(t : A)$

Table: Yanjing Wang: Beyond Knowing That

庄子《秋水》

庄子与惠子游于濠梁之上。

1. 庄子：鲦鱼出游从容，是鱼之乐也。
2. 惠子：子非鱼，安知鱼之乐？

$$\forall xy(K_x Hy \vee K_x \neg Hy \rightarrow Fy \rightarrow Fx)$$

$$\forall x(K_x Hf \vee K_x \neg Hf \rightarrow x = f)$$

3. 庄子：子非我，安知我不知鱼之乐？

$$\forall xy(K_x K_y Hf \vee K_x \neg K_y Hf \rightarrow x = y)$$

4. 惠子：我非子，固不知子矣；子固非鱼也，子之不知鱼之乐，全矣。

For any '**subjective**' formula A ,

$$\frac{\forall xy(K_x A(y) \vee K_x \neg A(y) \rightarrow x = y) \quad h \neq z \quad z \neq f}{\neg K_z Hf \wedge \neg K_h \neg K_z Hf} \text{ Moore's Paradox?}$$

5. 庄子：请循其本。子曰‘汝安知鱼乐’云者，既已知吾知之而问我。我知之濠上也。

Proof of God's Existence?

1. God is a being which has every perfection.
2. Existence is a perfection.
3. Hence God exists.

$$E(\iota_x(Px \wedge Ex))$$

Ontological Argument

- ▶ R : reality
 - ▶ M : mind
 - ▶ P : the positive qualities
 - ▶ $x \in y$: x belongs to y
1. There exists a thing belonging to mind that has all the positive qualities and no negative quality.
$$\exists x [x \in M \wedge \forall y (y \in P \leftrightarrow x \in y)]$$
 2. “Being real” is a positive quality.
$$R \in P$$
3. Two things belonging to mind that have exactly the same qualities are identical.
$$\forall xy [x \in M \wedge y \in M \rightarrow \forall z (x \in z \leftrightarrow y \in z) \rightarrow x = y]$$
4. God belongs to reality.
$$\iota_x [x \in M \wedge \forall y (y \in P \leftrightarrow x \in y)] \in R$$

Gödel's Proof of God's Existence

Ax.1 Either a property or its negation is positive, but not both. $\forall X[P(\neg X) \leftrightarrow \neg P(X)]$

Ax.2 A property necessarily implied by a positive property is positive.

$$\forall X \forall Y [P(X) \wedge \Box \forall x[X(x) \rightarrow Y(x)] \rightarrow P(Y)]$$

Th.1 Positive properties are possibly exemplified.

$$\forall X[P(X) \rightarrow \Diamond \exists x X(x)]$$

Df.1 A *God-like* being possesses all positive properties.

$$G(x) := \forall X[P(X) \rightarrow X(x)]$$

Ax.3 The property of being God-like is positive.

$$P(G)$$

Th.2 Possibly, God exists.

$$\Diamond \exists x G(x)$$

Ax.4 Positive properties are necessarily positive.

$$\forall X[P(X) \rightarrow \Box P(X)]$$

Df.2 An essence of an individual is a property necessarily implying any of its properties.

$$E(X, x) := X(x) \wedge \forall Y(Y(x) \rightarrow \Box \forall y(X(y) \rightarrow Y(y)))$$

Th.3 Being God-like is an essence of any God-like being. $\forall x[G(x) \rightarrow E(G, x)]$

Df.3 Necessary existence of an individual is the necessary exemplification of all its essences.

$$N(x) := \forall X[E(X, x) \rightarrow \Box \exists y X(y)]$$

Ax.5 Necessary existence is a positive property.

$$P(N)$$

Th.4 Necessarily, God exists.

$$\Box \exists x G(x)$$

Pride and Prejudice

$C_{\text{Human}} \left(\forall x \left(\text{Man}(x) \wedge \text{Single}(x) \wedge \text{Fortune}(x) \rightarrow \text{Desire}_x \left(\exists y \left(\text{Woman}(y) \wedge \text{Marry}(x, y) \right) \right) \right) \right)$

— Jane Austen

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Georg Cantor 1845-1918

- ▶ Mathematics \leadsto Set Theory.
- ▶ Diagonalization.
- ▶ There are many different levels of infinity.
- ▶ Cantor set.
- ▶ Continuum Hypothesis (CH).
How many points on the line?



Welcome to Cantor's Paradise



Contents

Introduction

Cardinal Numbers
Axiom of Choice

Term Logic

Recursion Theory

Propositional Logic

Equational Logic

Predicate Logic

Homotopy Type Theory

Modal Logic

Category Theory

Set Theory

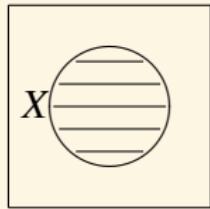
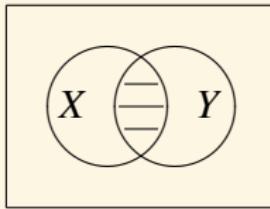
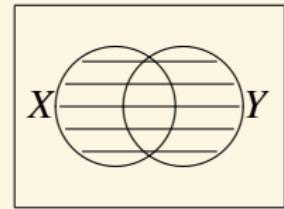
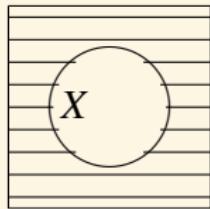
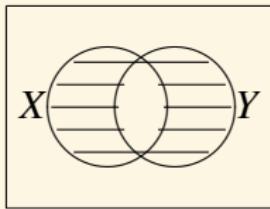
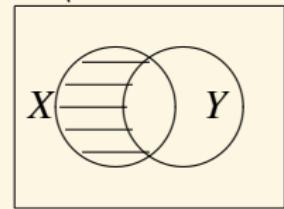
Quantum Computing

Axioms of ZFC

Ordinal Numbers

Answers to the Exercises

References 1436

X  $X \cap Y$  $X \cup Y$  \overline{X}  $X \Delta Y$  $X \setminus Y$ 

ZFC — Axioms

- ▶ $a \in A$ reads: a is an element of A . (Definition? No!)
- ▶ **Extensionality.**

$$X = Y \leftrightarrow \forall u(u \in X \leftrightarrow u \in Y)$$

- ▶ **Axiom Schema of Comprehension.** (✗)

For any formula A , there exists a set $Y = \{x : A(x)\}$.

$$R := \{x : x \notin x\} \quad R \in R? \quad (\text{Russell Paradox})$$

- ▶ **Separation Schema.**

For any formula A , for any X , there exists a set $Y = \{u \in X : A(x)\}$.

$$\forall X \exists Y \forall u(u \in Y \leftrightarrow u \in X \wedge A(x))$$

Curry's Paradox

- ▶ $X := \{x : x \in x \rightarrow A\}$
- ▶ $X \in X \iff X \in X \rightarrow A$
- ▶ A

ZFC — Axioms

- **Pairing.** For any a and b there exists a set $c = \{a, b\}$.

$$\forall ab \exists c \forall x (x \in c \leftrightarrow x = a \vee x = b)$$

- **Power.** For any X there exists a set $Y = P(X) := \{u : u \subset X\}$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \forall z (z \in u \rightarrow z \in X))$$

- **Union.** For any X there exists a set $Y = \bigcup X$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \exists z (z \in X \wedge u \in z))$$

$$\bigcup_{i \in I} X_i := \bigcup \{X_i : i \in I\}$$

$$\bigcap X := \{u : \forall z (z \in X \rightarrow u \in z)\}$$

Relation

- ordered pair.

$$(a, b) := \{\{a\}, \{a, b\}\}$$

$$(a_1, \dots, a_{n+1}) := ((a_1, \dots, a_n), a_{n+1})$$

$$(a_1, \dots, a_n) = (b_1, \dots, b_n) \rightarrow a_i = b_i \quad \text{for } 1 \leq i \leq n$$

$$X \subsetneq Y \quad X \cup Y \quad X \cap Y \quad X \setminus Y \quad X \Delta Y \quad X \times Y \quad \prod_{i=1}^n X_i \quad X^n$$

- n -ary relation R on X_1, \dots, X_n .

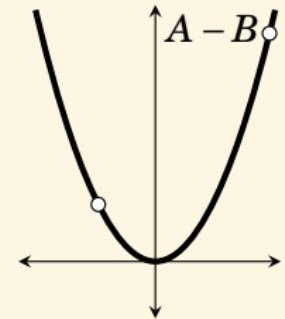
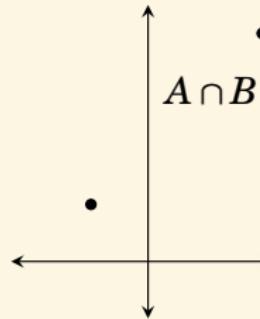
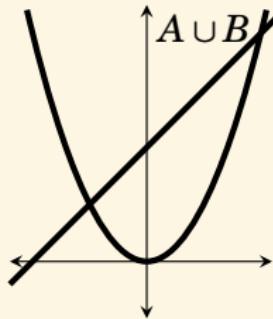
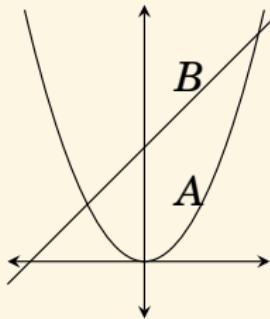
$$R \subset \prod_{i=1}^n X_i$$

$$R(x_1, \dots, x_n) := (x_1, \dots, x_n) \in R$$

Union & Intersection & Difference

$$A := \{(x, x^2) : x \in \mathbb{R}\} \quad y = x^2$$

$$B := \{(x, x + 2) : x \in \mathbb{R}\} \quad y = x + 2$$



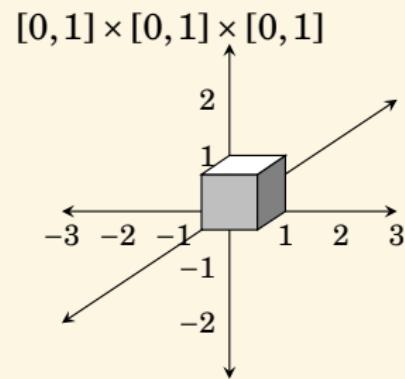
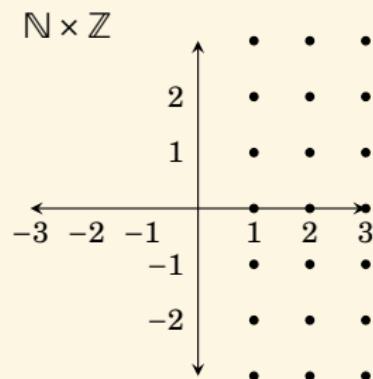
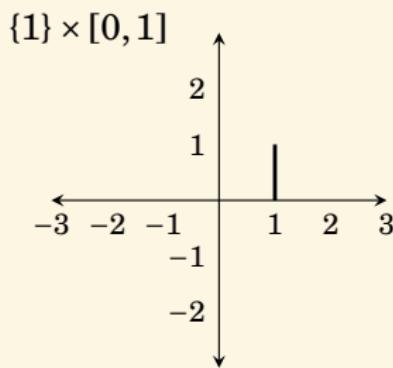
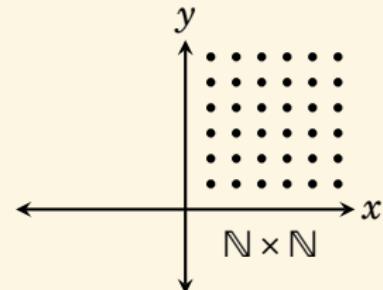
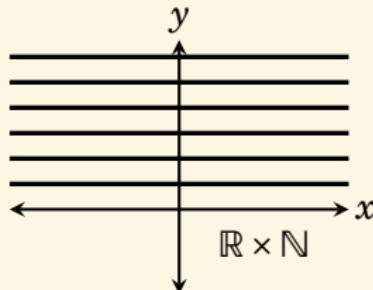
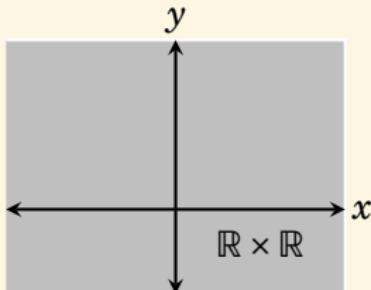
$$A \cup B = \{(x, y) : x \in \mathbb{R}, y = x^2 \vee y = x + 2\}$$

$$A \cap B = \{(-1, 1), (2, 4)\}$$

$$A \setminus B = \{(x, x^2) : x \in \mathbb{R} \setminus \{-1, 2\}\}$$

Cartesian Product

$$X \times Y := \{(x, y) : x \in X \wedge y \in Y\}$$



Equivalence Relation, Quotient, Partition

- ▶ $x \sim x$ (Reflexivity)
- ▶ $x \sim y \rightarrow y \sim x$ (Symmetry)
- ▶ $x \sim y \wedge y \sim z \rightarrow x \sim z$ (Transitivity)
- ▶ equivalence class: $[x] := \{y \in X : x \sim y\}$
- ▶ quotient set: $X/\sim := \{[x] : x \in X\}$
- ▶ we say $\mathcal{P} \subset P(X)$ is a **partition** of X iff
 1. $\forall xy \in \mathcal{P} : x \neq y \rightarrow x \cap y = \emptyset$
 2. $\bigcup \mathcal{P} = X$
- ▶ X/\sim is a partition of X .
- ▶ $R \subset X^2$ is an equivalence relation iff there is a partition \mathcal{P} of X s.t
 $R(x, y) \iff \exists A \in \mathcal{P} : x, y \in A.$

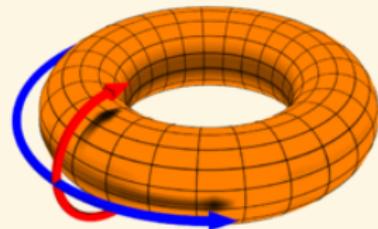
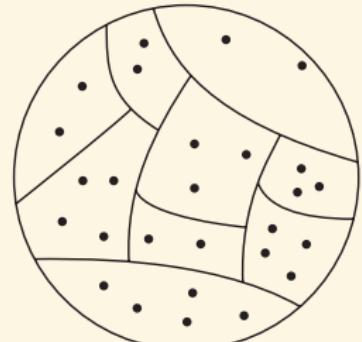


Figure: torus \mathbb{R}^2/\sim

$$(x, y) \sim (x', y') := (x - x', y - y') \in \mathbb{Z}^2$$



Function

- A n -ary operation $f : \prod_{i=1}^n X_i \rightarrow Y$ is a function iff

$$(\mathbf{x}, y) \in f \wedge (\mathbf{x}, z) \in f \rightarrow y = z$$

- injection (one-to-one). $f : X \rightarrowtail Y$

$$f(x) = f(y) \rightarrow x = y$$

- surjection (onto). $f : X \twoheadrightarrow Y$.

$$\forall y \in Y \exists x \in X (f(x) = y)$$

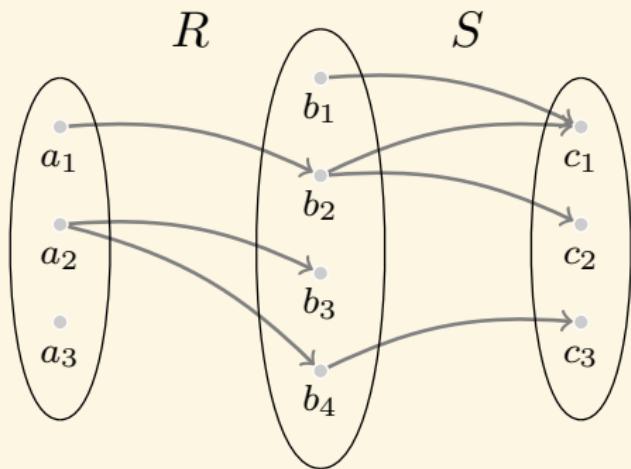
- bijection. $f : X \rightleftarrows Y$

- restriction. composition. image. inverse image. inverse function.

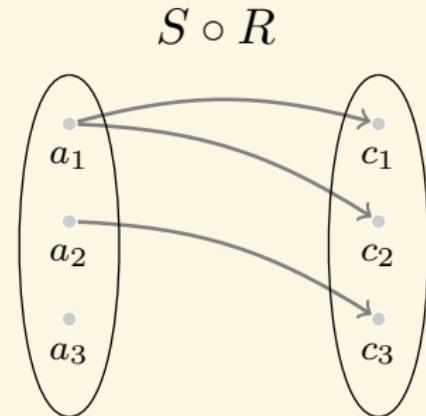
$$f \upharpoonright_A := \{(x, y) \in f : x \in A\} \quad (f \circ g)(x) := f(g(x))$$

$$f(A) := \{f(x) : x \in A\} \quad f^{-1}(A) := \{x : f(x) \in A\}$$

Relation Composition



~



$$S \circ R := \{(a, c) : \exists b (Rab \wedge Sbc)\}$$

Exercises

In Set,

$$\begin{aligned} f : X \rightarrowtail Y &\text{ iff } \exists g : Y \rightarrow X : gf = 1_X \\ &\text{ iff } \forall Z \forall g_1 g_2 : Z \rightarrow X : fg_1 = fg_2 \implies g_1 = g_2 \\ f : X \twoheadrightarrow Y &\text{ iff } \exists g : Y \rightarrow X : fg = 1_Y \\ &\text{ iff } \forall Z \forall g_1 g_2 : Y \rightarrow Z : g_1 f = g_2 f \implies g_1 = g_2 \end{aligned}$$

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow 1_X & \downarrow g \\ & & X \end{array}$$

$$\begin{array}{ccc} Y & \xrightarrow{g} & X \\ & \searrow 1_Y & \downarrow f \\ & & Y \end{array}$$

$$\begin{array}{ccccc} Z & \xrightarrow{\quad g_1 \quad} & X & \xrightarrow{f} & Y \\ & \xrightarrow{\quad g_2 \quad} & & & \end{array} \qquad \begin{array}{ccccc} X & \xrightarrow{f} & Y & \xrightarrow{\quad g_1 \quad} & Z \\ & & \downarrow g & \xrightarrow{\quad g_2 \quad} & \\ & & X & \xrightarrow{f} & Y \end{array}$$

$f : X \twoheadrightarrow Y$ iff the diagram commutes:

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & & \\ & \searrow 1_X & \downarrow g & \searrow 1_Y & \\ & & X & \xrightarrow{f} & Y \end{array}$$

Equivalence Relation / Partition / Transformation Group

Definition (Transformation Group)

A *transformation group* G on some set X is a set of invertible functions $f : X \rightarrow X$ which is closed under inversion and composition.

1. if $f \in G$, then its inverse $f^{-1} \in G$.
2. if $f, g \in G$, then their composition $g \circ f \in G$.

Obviously, the identity transformation $1_X \in G$.

- i. The effect of composition $g \circ f$ is
first do f , then do g
- ii. To undo the effect of $g \circ f$,
first do g^{-1} , then do f^{-1}
- iii. In symbols, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

- Let $R(x, y) := \exists f \in G : y = f(x)$. Then R is an equivalence relation.
- Conversely, suppose R is an equivalence relation, then there is a group G s.t. $R(x, y) \iff \exists f \in G : y = f(x)$.

Order

- ▶ pre-order: $x \leq x, x \leq y \wedge y \leq z \rightarrow x \leq z$.
- ▶ partial order: pre-order with $x \leq y \wedge y \leq x \rightarrow x = y$.
- ▶ strict partial order: $x \not\leq x, x < y \wedge y < z \rightarrow x < z$.
- ▶ total order: partial order with $x \leq y \vee y \leq x$.
- ▶ A total order of P is a *well order* iff every non-empty subset of P has a **least** element.

Definition

If (P, \leq) is a partially ordered set, $X \subset P$, and $a \in P$, then:

- ▶ a is a *maximal* element of X iff $a \in X \wedge \forall x \in X(a \leq x \rightarrow a = x)$;
- ▶ a is a *greatest* element of X iff $a \in X \wedge \forall x \in X(x \leq a)$;
- ▶ a is an *upper bound* of X iff $\forall x \in X(x \leq a)$;
- ▶ a is the *supremum* of X iff a is the least upper bound of X .

ZFC — Axioms

- ▶ **Replacement Schema.**

If a class F is a function, then for every set X , $F(X)$ is a set.

$$\forall xyz(A(x, y) \wedge A(x, z) \rightarrow y = z) \rightarrow \forall X \exists Y \forall y(y \in Y \leftrightarrow \exists x \in X A(x, y))$$

- ▶ **Axiom of Regularity.** Every non-empty set has an \in -minimal element.

$$\forall X(X \neq \emptyset \rightarrow \exists x(x \in X \wedge X \cap x = \emptyset))$$

- ▶ **Axiom of Infinity.**

$$\exists X(\emptyset \in X \wedge \forall x(x \in X \rightarrow x \cup \{x\} \in X))$$

- ▶ **Axiom of Choice (AC).** For any set X of non-empty sets, there exists a choice function f defined on X .

$$\forall X \left[\emptyset \notin X \rightarrow \exists f : X \rightarrow \bigcup X \ \forall A \in X (f(A) \in A) \right]$$

Contents

Introduction

Cardinal Numbers
Axiom of Choice

Term Logic

Recursion Theory

Propositional Logic

Equational Logic

Predicate Logic

Homotopy Type Theory

Modal Logic

Category Theory

Set Theory

Quantum Computing

Axioms of ZFC

Ordinal Numbers

Answers to the Exercises

References 1436

Ordinal vs Cardinal

- ▶ ordinal. (“length”) A set is an ordinal iff it is transitive and well-ordered by \in . or equivalently,

$$\text{Ord}(x) := \bigcup x \subset x \wedge \forall yz(y \in x \wedge z \in x \rightarrow y \in z \vee y = z \vee z \in y)$$

- ▶ cardinal. (“size”) $\text{Card}(x) := \text{Ord}(x) \wedge \forall y \in x(|y| \neq |x|)$

$$|M| = |N| := \exists f : M \rightarrowtail N \quad |M| \leq |N| := \exists f : M \rightarrowtail N$$

$$|M| := \min\{\alpha \in \text{Ord} : |\alpha| = |M|\}$$

The infinite ordinal numbers that are cardinals are called alephs.

Ordinal

$$\alpha < \beta := \alpha \in \beta$$

- ▶ \emptyset is an ordinal.
- ▶ If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.
- ▶ If $\alpha \neq \beta$ are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.
- ▶ If α, β are ordinals, then either $\alpha \subset \beta$ or $\beta \subset \alpha$.
- ▶ $<$ is a linear ordering of the class Ord .
- ▶ For each α , $\alpha = \{\beta : \beta < \alpha\}$.
- ▶ If C is a non-empty class of ordinals, then $\bigcap C$ is an ordinal, $\bigcap C \in C$ and $\bigcap C = \inf C$.
- ▶ If X is a non-empty set of ordinals, then $\bigcup X$ is an ordinal, $\bigcup X = \sup X$.
- ▶ For every α , $\alpha \cup \{\alpha\}$ is an ordinal and $\alpha \cup \{\alpha\} = \inf\{\beta : \beta > \alpha\}$.

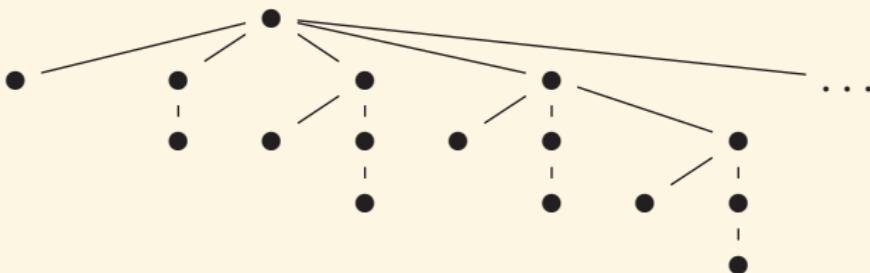
Natural Number \mathbb{N}

What is “number”? What is “infinity”? What is beyond “infinity”?

$$\alpha + 1 := \alpha \cup \{\alpha\}$$

$$0 := \emptyset, \quad 1 := 0 + 1, \quad 2 := 1 + 1, \quad 3 := 2 + 1, \dots$$

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots\}$$



- A set A is **inductive** iff $\emptyset \in A$ and $\forall x \in A : x + 1 \in A$.
- A **natural number** is a set that belongs to every inductive set.

$$\mathbb{N} := \{n : \forall A (\emptyset \in A \wedge \forall x \in A (x + 1 \in A) \rightarrow n \in A)\}$$

- A set A is **finite** iff $\exists n \in \mathbb{N} : |A| = n$.
- A set A is **countable** iff $|A| \leq |\mathbb{N}|$.

Integer \mathbb{Z}

$$(m, n) \sim (p, q) := m +_{\mathbb{N}} q = p +_{\mathbb{N}} n$$

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim$$

$$0_{\mathbb{Z}} := [(0, 0)]$$

$$[(m, n)] \leq_{\mathbb{Z}} [(p, q)] := m +_{\mathbb{N}} q \leq_{\mathbb{N}} p +_{\mathbb{N}} n$$

$$[(m, n)] +_{\mathbb{Z}} [(p, q)] := [(m +_{\mathbb{N}} p, n +_{\mathbb{N}} q)]$$

$$[(m, n)] \cdot_{\mathbb{Z}} [(p, q)] := [(m \cdot_{\mathbb{N}} p + n \cdot_{\mathbb{N}} q, m \cdot_{\mathbb{N}} q + n \cdot_{\mathbb{N}} p)]$$

$$- [(m, n)] := [(n, m)]$$

$$\mathbb{Z}^+ := \{x \in \mathbb{Z} : x >_{\mathbb{Z}} 0_{\mathbb{Z}}\}$$

$$\exists f : \mathbb{N} \rightarrow \mathbb{Z} \quad n \mapsto [(n, 0)]$$

Rational Number \mathbb{Q}

$$(m, n) \sim (p, q) := m \cdot_{\mathbb{Z}} q = p \cdot_{\mathbb{Z}} n$$

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^+ / \sim$$

$$0_{\mathbb{Q}} := [(0_{\mathbb{Z}}, x)]$$

$$1_{\mathbb{Q}} := [(x, x)]$$

$$[(m, n)] \leq_{\mathbb{Q}} [(p, q)] := m \cdot_{\mathbb{Z}} q \leq_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n$$

$$[(m, n)] +_{\mathbb{Q}} [(p, q)] := [(m \cdot_{\mathbb{Z}} q +_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n, n \cdot_{\mathbb{Z}} q)]$$

$$[(m, n)] \cdot_{\mathbb{Q}} [(p, q)] := [(m \cdot_{\mathbb{Z}} p, n \cdot_{\mathbb{Z}} q)]$$

$$- [(m, n)] := [(-m, n)]$$

$$\exists f : \mathbb{Z} \rightarrow \mathbb{Q} \quad x \mapsto [(x, 1)]$$

Dedekind Cut and Real Number \mathbb{R}

Definition (Real Number)

\mathbb{R} is the set of all $x \in P(\mathbb{Q})$ s.t.

- ▶ $x \neq \emptyset, x \neq \mathbb{Q}$
- ▶ $\forall p \in x \exists q \in x : p < q$
- ▶ $\forall pq \in x : p \in x \wedge q < p \rightarrow q \in x \quad \exists f : \mathbb{Q} \rightarrow \mathbb{R} \quad x \mapsto \{q \in \mathbb{Q} : q < x\}$

$$x \leq_{\mathbb{R}} y := x \subset y$$

$$x +_{\mathbb{R}} y := \{p +_{\mathbb{Q}} q : p \in x \wedge q \in y\}$$

$$-x := \{q \in \mathbb{Q} : \exists p > q (-p \notin x)\}$$

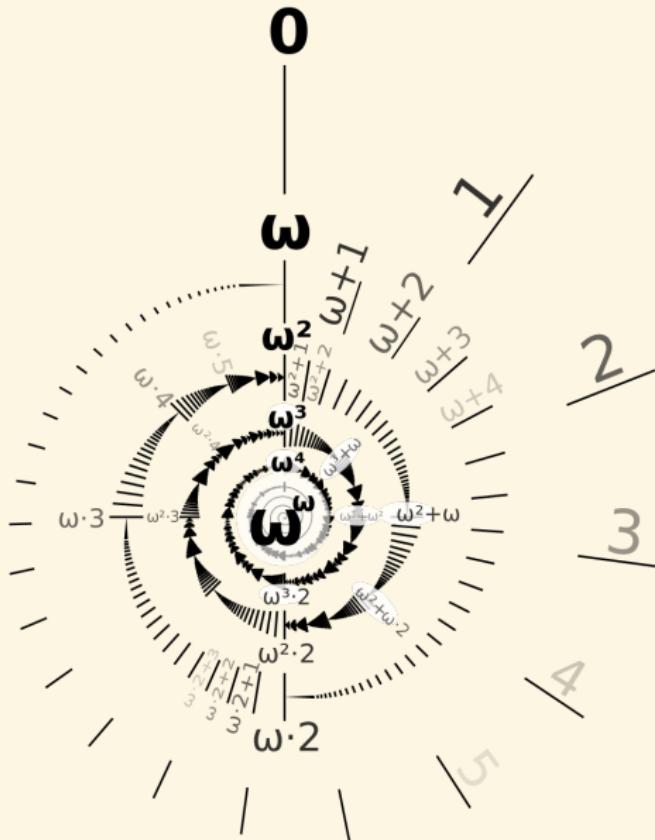
$$|x| := x \cup -x$$

$$x \cdot_{\mathbb{R}} y := \begin{cases} \{r : r \leq p \cdot_{\mathbb{Q}} q \wedge p \in x \wedge q \in y\} & \text{if } x > 0, y > 0 \\ 0 & \text{if } x = 0 \text{ or } y = 0 \\ |x| \cdot_{\mathbb{R}} |y| & \text{if } x < 0, y < 0 \\ -(|x| \cdot_{\mathbb{R}} |y|) & \text{if } x < 0, y > 0 \text{ or } x > 0, y < 0 \end{cases}$$

Theorem (Least-upper-bound)

Any bounded non-empty subset of \mathbb{R} has a least upper bound.

Ordinal



0, 1, 2, 3, ...

$\omega, \omega + 1, \omega + 2, \dots$

$\omega \cdot 2, (\omega \cdot 2) + 1, (\omega \cdot 2) + 2, \dots$

:

$\omega^2, \omega^2 + 1, \omega^2 + 2, \dots$

:

$\omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \dots$

:

$\omega^{\omega^\omega}, \dots$

:

$\omega^{\omega^{\omega^\omega}}, \dots$

:

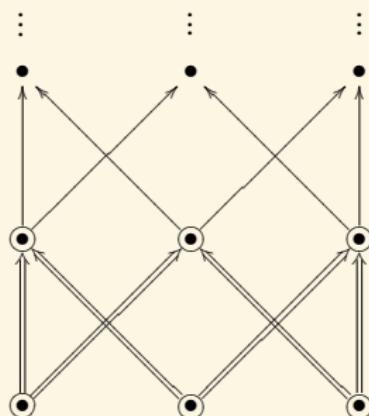
Ordinal and Induction

Theorem (Transfinite Induction Theorem)

Given a well ordered set A , let P be a property. Then

$$P(\min(A)) \wedge \forall x \in A [\forall y < x P(y) \rightarrow P(x)] \rightarrow \forall x \in A P(x)$$

$$\forall P [P(0) \wedge \forall k \in \mathbb{N} (P(k) \rightarrow P(k+1)) \rightarrow \forall n \in \mathbb{N} P(n)]$$

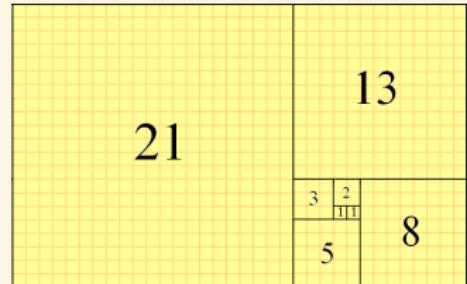


Induction — Example

Theorem

$$\sum_{i=0}^n F_i^2 = F_n F_{n+1}$$

where $F_0 = 1, F_1 = 1, F_n = F_{n-1} + F_{n-2}$.



Proof.

Base step:

$$F_0^2 = 1^2 = 1 = 1 \times 1 = F_0 F_1$$

Inductive step:

$$\sum_{i=0}^{n+1} F_i^2 = \sum_{i=0}^n F_i^2 + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}$$

Induction — Example

Theorem

$$F_n^2 + F_{n+1}^2 = F_{2n+2}$$

Proof.

Strengthen the original statement to

$$F_n^2 + F_{n+1}^2 = F_{2n+2} \text{ and } F_{n+1}^2 + 2F_n F_{n+1} = F_{2n+3}$$

Problem

For all natural numbers n , $n \neq n$.

Induction — Example ☹

All horses are the same color ☹

Let us assume the proposition $P(k)$ that k horses are the same color.
Obviously, $P(1)$ is true.

Given the set of $k + 1$ horses, we remove one horse; then the remaining k horses are the same color, by hypothesis. We remove another horse and replace the first; the k horses, by hypothesis, are again the same color. We repeat this until by exhaustion the $k + 1$ sets of k horses have been shown to be the same color. Therefore $P(k + 1)$.

All positive integers are interesting ☹

Assume the contrary. Then there is a lowest non-interesting positive integer. But that's pretty interesting!

Induction — Example ☹

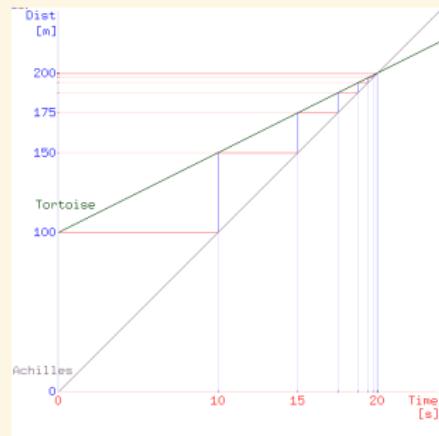
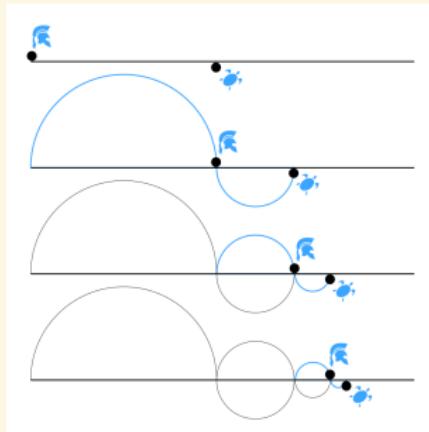
Surprise Exam Paradox ☹

A teacher announces in class: “next week you are going to have an exam, but you will not be able to know on which day of the week the exam is held until that day”.

The students argue that a surprise exam can't occur:

- ▶ The exam can't be held on the last day, because otherwise, the night before the students will know that the exam is going to be held the next day.
- ▶ Since the last day has already been eliminated, the same logic applies to the day before the last day.
- ▶ Similarly, all the days can be removed from the list.
- ▶ So the teacher can't give a surprise exam at all.

Zeno's Paradox



Ross-Littlewood Paradox — Hilbert's Train

- ▶ Suppose a train is empty at 1 minute before noon.
- ▶ At 2^{-n} minutes before noon, 10 passenger get on, and 1 gets off.
 1. the first gets off?
 2. the last gets off?
 3. randomly gets off?
- ▶ How many passengers are on the train at noon?

Proof.

Define E_n to be the event that passenger 1 is still on the train after the first n station, and F_i the event that passenger i is on the train at noon.

$$P(F_1) = P\left(\bigcap_{n=1}^{\infty} E_n\right) = \lim_{n \rightarrow \infty} P(E_n) = \prod_{i=1}^{\infty} \frac{9n}{9n+1} = 0$$

$$\forall i : P(F_i) = 0 \implies P\left(\bigcup_{i=1}^{\infty} F_i\right) \leq \sum_{i=1}^{\infty} P(F_i) = 0$$

The Delayed Heaven Paradox

Problem (The Delayed Heaven Paradox)

- ▶ *Heaven: 1 every day for eternity.*
- ▶ *Hell: -1 every day for eternity.*
- ▶ *Limbo: 0 every day for eternity.*

God offers you the chance

1. *to go straight to Limbo, or*
2. *to take one day in Hell, followed by two days in Heaven, followed by the rest of eternity in Limbo.*

Suppose you die and the devil offers to play a game of chance. If you win, you can go to heaven. If you lose, you'll stay in hell forever. If you play today, you have $1/2$ chance of winning. Tomorrow $2/3$. Then $3/4, 4/5, 5/6, 6/7 \dots$ Will you stay forever in hell in order to increase the chance of leaving it?

Transfinite Recursion Theorem

Theorem (Transfinite Recursion Theorem)

Given a class function $G : V \rightarrow V$, there exists a unique function $F : \text{Ord} \rightarrow V$ s.t.

$$F(\alpha) = G(F \upharpoonright \alpha)$$

for each α .

Ordinal Arithmetic

Definition (Addition)

1. $\alpha + 0 = \alpha$
2. $\alpha + (\beta + 1) = \alpha + \beta + 1$
3. $\alpha + \beta = \lim_{\xi \rightarrow \beta} (\alpha + \xi)$ for limit $\beta > 0$

Definition (Multiplication)

1. $\alpha \cdot 0 = 0$
2. $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$
3. $\alpha \cdot \beta = \lim_{\xi \rightarrow \beta} \alpha \cdot \xi$ for limit $\beta > 0$

Definition (Exponentiation)

1. $\alpha^0 = 1$
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$
3. $\alpha^\beta = \lim_{\xi \rightarrow \beta} \alpha^\xi$ for limit $\beta > 0$

- $\omega = 0 < 1 < 2 < 3 < \dots$
- $\omega + 1 = 0 < 1 < 2 < 3 < \dots < \omega$
- $1 + \omega = \bullet < 0 < 1 < 2 < 3 < \dots$
- $1 + \omega = \omega \neq \omega + 1$
- $2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$
- $(\omega + 1) \cdot 2 \neq \omega \cdot 2 + 1 \cdot 2$
- $(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2$
- $\beta < \gamma \rightarrow \alpha + \beta < \alpha + \gamma$
- $\alpha < \beta \rightarrow \exists \delta (\alpha + \delta = \beta)$
- $\beta < \gamma \wedge \alpha > 0 \rightarrow \alpha \cdot \beta < \alpha \cdot \gamma$
- $\beta < \gamma \wedge \alpha > 1 \rightarrow \alpha^\beta < \alpha^\gamma$
- $\alpha > 0 \rightarrow \forall \gamma \exists! \beta \exists! \rho < \alpha (\gamma = \alpha \cdot \beta + \rho)$
- $\alpha < \beta \rightarrow \alpha + \gamma \leq \beta + \gamma$
- $\alpha < \beta \rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$
- $\alpha < \beta \rightarrow \alpha^\gamma \leq \beta^\gamma$
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
- $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
- $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$

Cantor's Normal Form Theorem

Theorem (Cantor's Normal Form Theorem)

Every ordinal $\alpha > 0$ can be represented uniquely in the form

$$\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n$$

where $n \geq 1, \alpha \geq \beta_1 > \cdots > \beta_n$, and $k_1, \dots, k_n \in \mathbb{N}^+$.

Now I Know!

1. **C:** Hello **A** and **B**! I have given you each a different natural number.
Who of you has the larger number?
2. **A:** I don't know.
3. **B:** Neither do I.
4. **A:** Even though you say that, I still don't know.
5. **B:** Still neither do I.
6. **A:** Alas, even now I do not know.
7. **B:** I regret that I also do not know.
8. **A:** Yet, I still do not know.
9. **B:** Aha! Now I know which has the larger number.
10. **A:** Then I know both our numbers.
11. **B:** Well, now I also know them.

Now I Know! — transfinite

1. **C:** I have given you each a different ordinal. Who has the larger one?
2. **A:** I don't know.
3. **B:** Neither do I.
4. **A:** I still don't know.
5. **B:** Still neither do I.
6. **C:** Well, I can tell you that no matter how long you continue that back-and-forth, you shall not come to know who has the larger number.
7. **A:** What interesting new information! But I still do not know.
8. **B:** And still neither do I.
9. **A:** Alas, even now I do not know!
10. **B:** I regret that I also do not know.
11. **C:** Let me say once again that no matter how long you continue that back-and-forth, you will not know who has the larger number.
12. **A:** Yet, I still do not know.
13. **B:** Aha! Now I know who has the larger ordinal.
14. **A:** Then I know both our ordinals.
15. **B:** Well, now I also know them.

Now I Know! — transfinite

1. **C:** I have given you each a different rational number of the form

$$n - \frac{1}{2^k} - \frac{1}{2^{k+r}}$$

where $n, k \in \mathbb{N}^+$ and $r \in \mathbb{N}$. Who of you has the larger number?

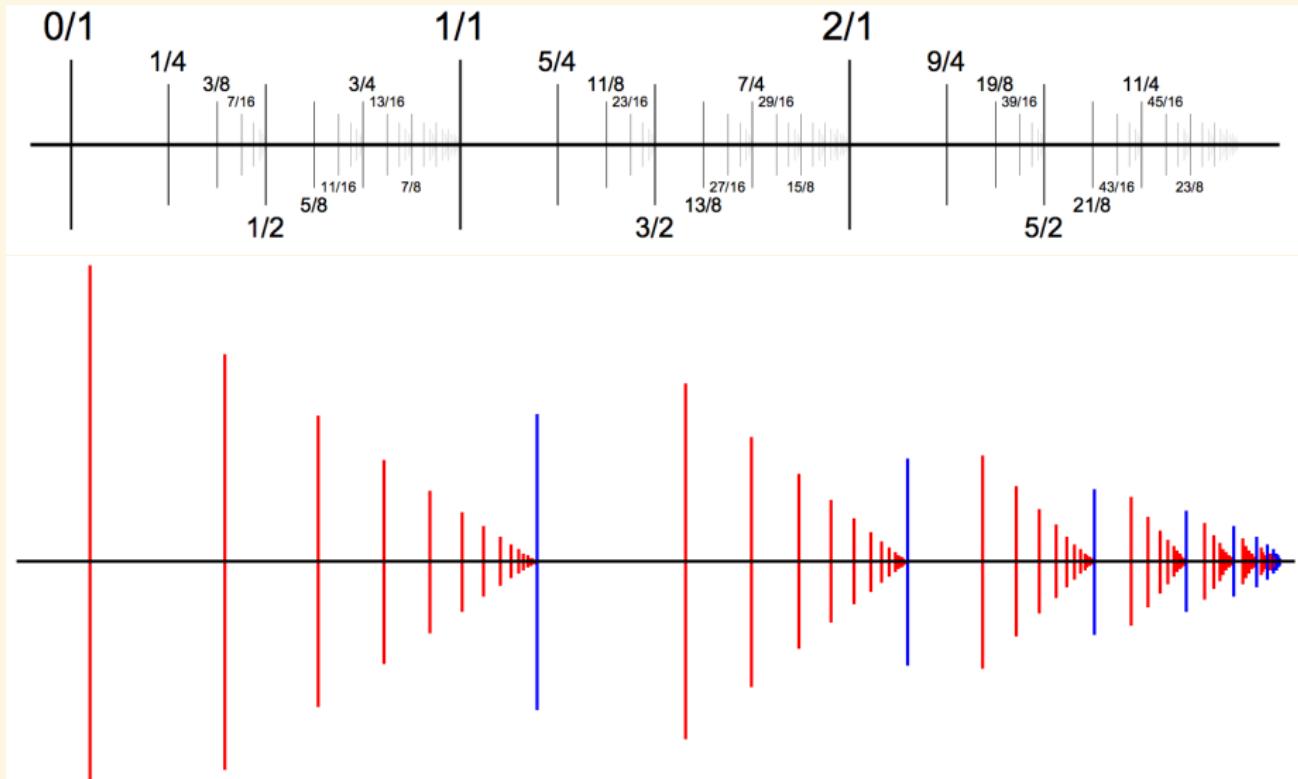
2. **A:** I don't know.
3. **B:** Neither do I.
4. **A:** I still don't know.
5. **B:** Still neither do I.
6. **C:** Well, I can tell you that no matter how long you continue that back-and-forth, you shall not come to know who has the larger number.
7. **A:** What interesting new information! But I still do not know.
8. **B:** And still neither do I.
9. **A:** Alas, even now I do not know!
10. **B:** I regret that I also do not know.
11. **C:** Let me say once again that no matter how long you continue that back-and-forth, you will not know who has the larger number.

Now I Know! — transfinite — continued

12. **A:** Yet, I still do not know.
13. **B:** And also I remain in ignorance. However shall we come to know?
14. **C:** Well, in fact, no matter how long we three continue from now in the pattern we have followed so far — namely, the pattern in which you two state back-and-forth that still you do not yet know whose number is larger and then I tell you yet again that no further amount of that back-and-forth will enable you to know — then still after as much repetition of that pattern as we can stand, you will not know whose number is larger! Furthermore, I could make that same statement a second time, even after now that I have said it to you once, and it would still be true!
15. **A:** Such powerful new information! But I still do not know.
16. **B:** And also I do not know.
17. **A:** Aha! Now I know who has the larger number!
18. **B:** Then I know both our numbers!
19. **A:** Well, now I also know them!

Now I Know! — Solution

$$(7, 6) \quad (\omega \cdot 2 + 1, \omega \cdot 2) \quad \left(\frac{19}{8}, \frac{39}{16}\right)$$



Well-Founded Relation

- ▶ $R \subset A^2$ is *set-like* iff $\text{ext}_R(x) := \{y \in A : Ryx\}$ is a set for every $x \in A$.
- ▶ $y \in A$ is *R -minimal* in A iff $\neg \exists z(z \in A \wedge Rzy)$.
- ▶ A set-like relation R is *well-founded* on A iff every non-empty set $X \subset A$ has a R -minimal element.
- ▶ R *well-orders* A iff R totally orders A strictly and R is well-founded on A .



Figure: Noether

Well-Founded Induction/Recursion

Theorem (Well-Founded/Noetherian Induction)

Let R be a well-founded relation on A . Let P be a property.

$$\forall x \in \min(A) P(x) \wedge \forall x \in A [\forall y \in A (Ryx \rightarrow P(y)) \rightarrow P(x)] \rightarrow \forall x \in A P(x)$$

Theorem (Well-Founded Recursion)

Let R be a well-founded relation on A . Let G be a function. Then there is a unique function F on A s.t. for every $x \in A$,

$$F(x) = G(x, F \upharpoonright_{\text{ext}_R(x)})$$

Perfect Set

- x is a *limit point* of A iff every neighborhood of x intersects A in some point other than x itself.
- $A' := \{x : x \text{ is a limit point of } A\}$
- A is *closed* if $A' \subset A$.
- A is *perfect* if $A' = A$.

Every perfect set has cardinality 2^{\aleph_0} .

- $\text{rank}(A) := \mu\alpha [A_\alpha = A_{\alpha+1}]$ where

$$A_0 := A$$

$$A_{\alpha+1} := A'_\alpha$$

$$A_\alpha := \bigcap_{\gamma < \alpha} A_\gamma \text{ if } \alpha \text{ is a limit ordinal.}$$

Cantor-Bendixson Theorem

Theorem (Cantor-Bendixson Theorem)

If A is an uncountable closed set, then $A = P \cup S$, where P is perfect and S is countable.

Proof.

Let $P := A_{\text{rank}(A)}$. Then

$$A \setminus P = \bigcup_{\alpha < \text{rank}(A)} (A_\alpha \setminus A'_\alpha)$$

Let $\langle J_k : k \in \mathbb{N} \rangle$ be an enumeration of rational intervals.

Hence for $a \in A \setminus P$, there is a unique α s.t. a is an isolated point of A_α .

Let $f(a) := \mu k [A_\alpha \cap J_k = \{a\}]$. Then $f : A \setminus P \rightarrow \mathbb{N}$ is injective.

Trigonometric Expansion

Definition (Trigonometric Expansion)

A function $f : \mathbb{R} \rightarrow \mathbb{C}$ admits a trigonometric expansion iff

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx)$$

For example, a continuously differentiable function admits a trigonometric expansion, where a_n, b_n can be computed by Fourier formulas

$$a_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \cos nt \, dt$$

$$b_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \sin nt \, dt$$

Cantor-Lebesgue Theorem

- ▶ Characterization: which functions admit a trigonometric expansion?
- ▶ Coefficient: How to “compute” the coefficients of the expansion?
- ▶ **Uniqueness:** Is such an expansion unique?

Theorem (Cantor-Lebesgue Theorem)

For any $A \subset \mathbb{R}$, if $A_{\text{rank}(A)} = \emptyset$, then

$$\forall x \in \mathbb{R} \setminus A \left(\frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx) = 0 \right) \implies \forall n \in \mathbb{N} (a_n = b_n = 0)$$

If f is continuous at all but countable points, then it admits an unique trigonometric expansion.

Contents

Introduction

Cardinal Numbers
Axiom of Choice

Term Logic

Recursion Theory

Propositional Logic

Equational Logic

Predicate Logic

Homotopy Type Theory

Modal Logic

Category Theory

Set Theory

Quantum Computing

Axioms of ZFC

Ordinal Numbers

Answers to the Exercises

References 1436

How do we count a finite set?

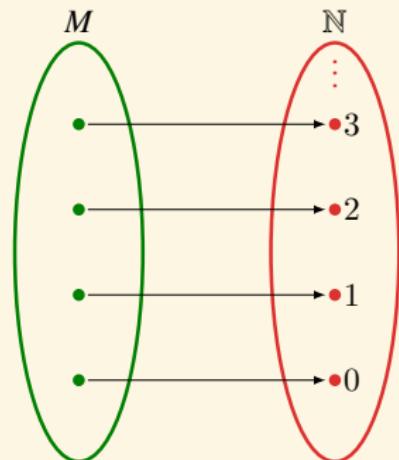
$$M := \{\text{apple, orange, banana, grape}\}$$

What does $|M| = 4$ mean?

There is a bijection between M and $N := \{1, 2, 3, 4\}$.

apple	\longleftrightarrow	1
orange	\longleftrightarrow	2
banana	\longleftrightarrow	3
grape	\longleftrightarrow	4

$$|M| = |N| := \exists f : M \rightarrow N$$



A set A is **finite** iff $\exists n \in \mathbb{N} : |A| = n$.

Does renaming the elements of a set change its size? No!
Bijection is nothing more than renaming.

How do we compare the sizes of finite sets?

$$M := \{\text{apple, orange, banana, grape}\}$$

$$N := \{\text{John, Peter, Bell, Emma, Sam}\}$$

$$\begin{array}{lll} \text{apple} & \longrightarrow & \text{John} \\ \text{orange} & \longrightarrow & \text{Peter} \\ \text{banana} & \longrightarrow & \text{Bell} \\ \text{grape} & \longrightarrow & \text{Emma} \\ & & \text{Sam} \end{array}$$

What does $|M| \leq |N|$ mean?

$$\begin{array}{llll} \text{apple} & \longleftrightarrow & 1 & \longleftrightarrow \\ & & & \text{John} \\ \text{orange} & \longleftrightarrow & 2 & \longleftrightarrow \\ & & & \text{Peter} \\ \text{banana} & \longleftrightarrow & 3 & \longleftrightarrow \\ & & & \text{Bell} \\ \text{grape} & \longleftrightarrow & 4 & \longleftrightarrow \\ & & & \text{Emma} \\ & & 5 & \longleftrightarrow \\ & & & \text{Sam} \end{array}$$

$$|M| \leq |N| := \exists f : M \rightarrowtail N$$

$$|M| \leq |N| := \exists f : N \twoheadrightarrow M$$

$$\begin{array}{lll} \text{apple} & \leftarrow & \text{John} \\ \text{orange} & \leftarrow & \text{Peter} \\ \text{banana} & \leftarrow & \text{Bell} \\ \text{grape} & \leftarrow & \text{Emma} \\ & \swarrow & \text{Sam} \end{array}$$

The way of comparing the size of finite sets generalizes to infinite sets!

$$|\mathbb{N}| = |\mathbb{Z}|$$

0	\longleftrightarrow	0
1	\longleftrightarrow	1
2	\longleftrightarrow	-1
3	\longleftrightarrow	2
4	\longleftrightarrow	-2
5	\longleftrightarrow	3
6	\longleftrightarrow	-3
7	\longleftrightarrow	4
8	\longleftrightarrow	-4
:		:

Dedekind-Infinite

A set A is Dedekind-infinite iff some proper subset $B \subsetneq A$ is equinumerous to A .

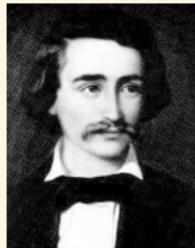


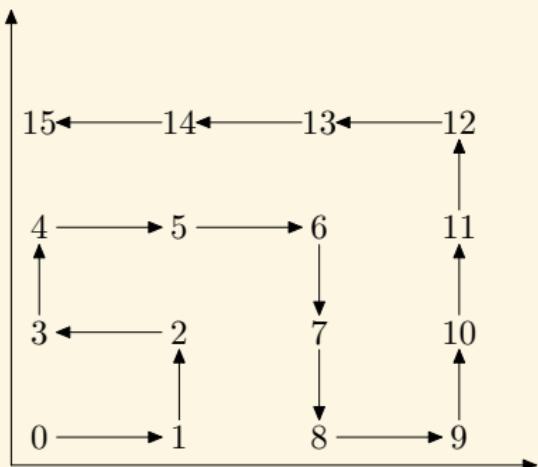
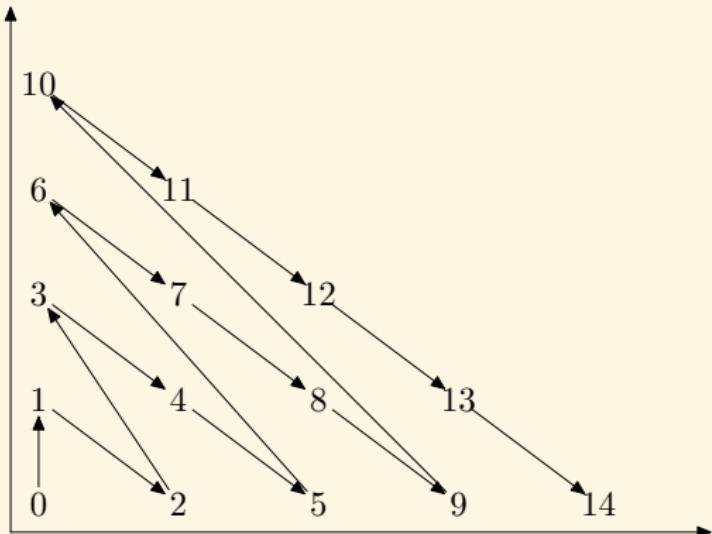
Figure: Dedekind

Countable?

$\{0, 1, 2, 3, 4, \dots\}$	$ \mathbb{N} = 2^{<\omega} $
$\{1, 3, 5, 7, 9, \dots\}$	$0 \longleftrightarrow \epsilon$
$\{0, 2, 4, 6, 8, \dots\}$	$1 \longleftrightarrow 0$
$\{0, 1, 4, 9, 16, \dots\}$	$2 \longleftrightarrow 1$
$\{2, 3, 5, 7, 11, \dots\}$	$3 \longleftrightarrow 00$
	$4 \longleftrightarrow 01$
	$5 \longleftrightarrow 10$
	$6 \longleftrightarrow 11$
► A set A is countable iff $ A \leq \mathbb{N} $.	$7 \longleftrightarrow 000$
► Is it possible that A is infinite, but $ A < \mathbb{N} $?	$8 \longleftrightarrow 001$
► A set A is countably infinite iff $ A = \mathbb{N} $.	$\vdots \qquad \vdots$

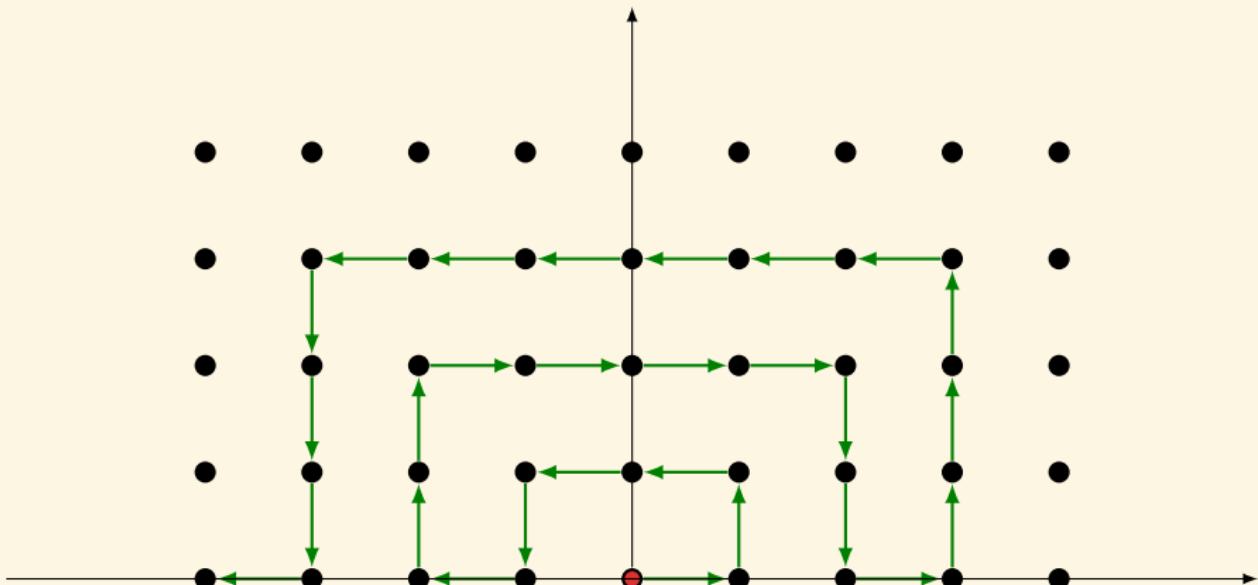
Countable?

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$$



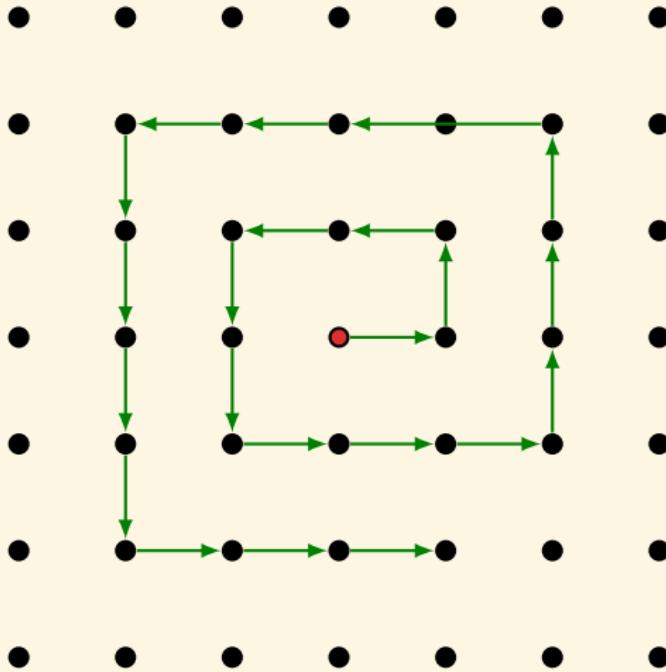
Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{N}|$$

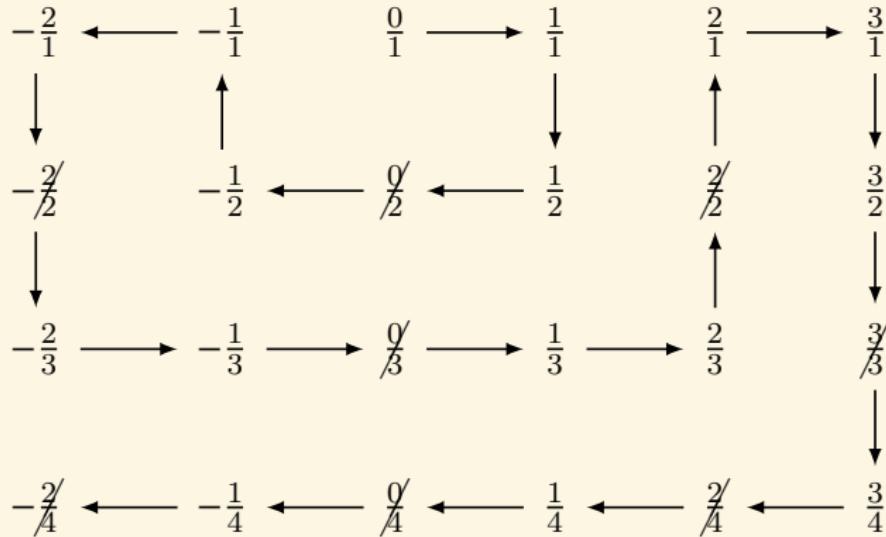


Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$$

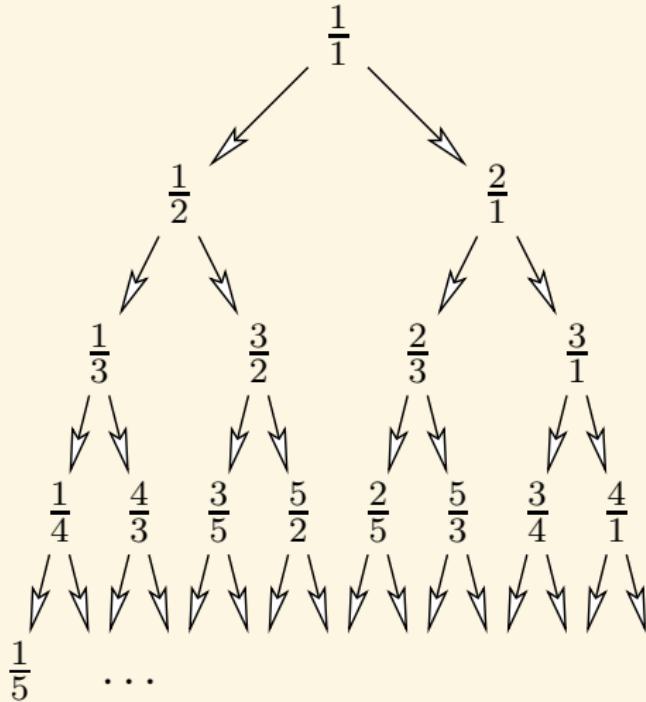
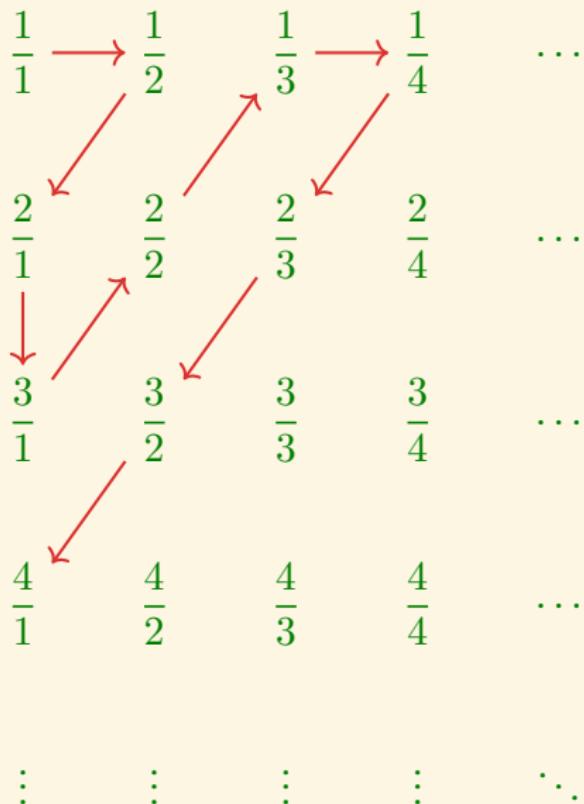


$$|\mathbb{N}| = |\mathbb{Q}|$$



$$|\mathbb{N}| = |\mathbb{Z}| = |2^{<\omega}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Q}|$$

$$|N| = |Q^+|$$



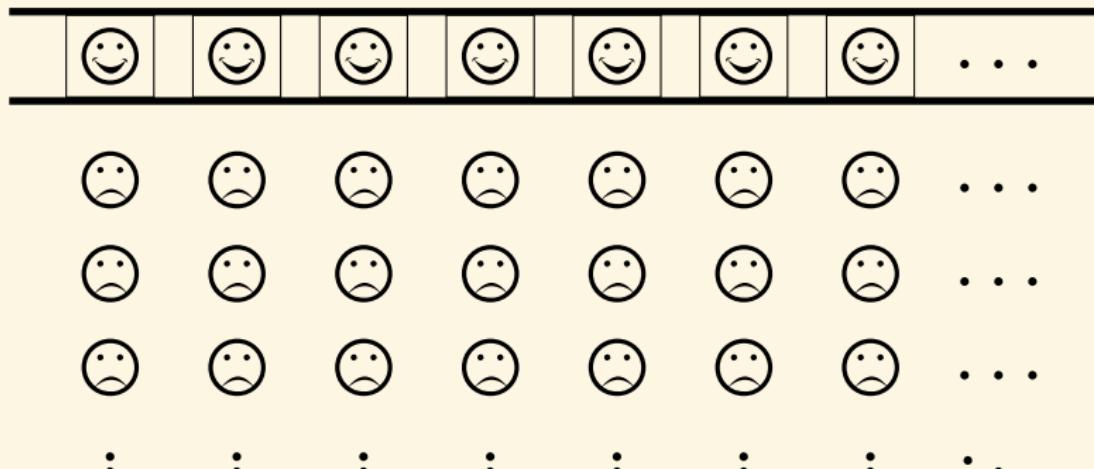
$$x \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

Hilbert's Hotel

Problem (Hilbert's Hotel)

Consider a hypothetical hotel with a countably infinite number of rooms, all of which are occupied.

1. Finitely many new guests.
2. Infinitely many new guests.
3. Infinitely many buses with infinitely many guests each.



Hilbert's Hotel

$$\aleph_0 + n = \aleph_0$$

$$\aleph_0 \cdot n = \aleph_0$$

$$\aleph_0 \cdot \aleph_0 = \aleph_0$$

Theorem

Let A be a countable set. Then the set of all finite sequences of members of A is also countable.

Proof.

$$f : A \rightarrow \mathbb{N} \implies \exists g : \bigcup_{n \in \mathbb{N}} A^{n+1} \rightarrow \mathbb{N} \quad (a_1, \dots, a_n) \mapsto \prod_{i=1}^n p_i^{f(a_i)+1}$$

The set of real numbers is uncountable

Is every set countable?

Theorem (Cantor)

$$|\mathbb{R}| > |\mathbb{N}|$$

Proof.

0 .	r_{11}	r_{12}	r_{13}	r_{14}	...
0 .	r_{21}	r_{22}	r_{23}	r_{24}	...
0 .	r_{31}	r_{32}	r_{33}	r_{34}	...
0 .	r_{41}	r_{42}	r_{43}	r_{44}	...
:	:	:	:	:	..

Let $d = 0.d_1d_2\dots$ where

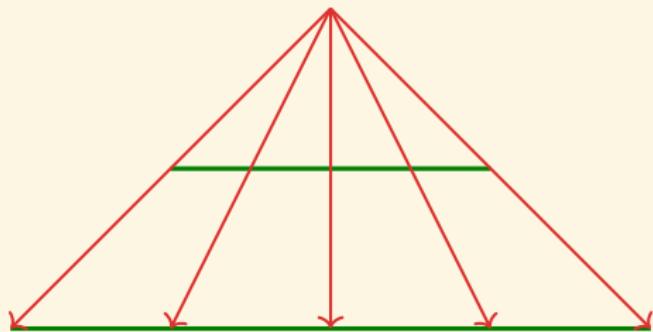
$$d_n = 9 - r_{nn}$$

The set of real numbers is uncountable — another proof

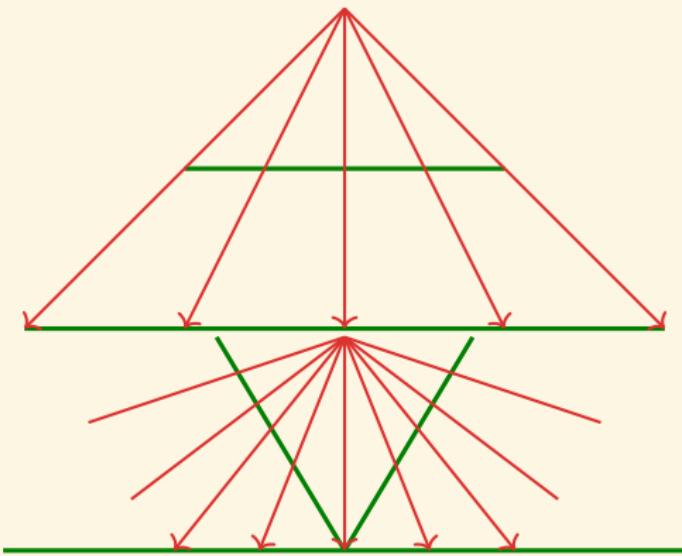
Proof.

- ▶ **Game.** Fix $S \subset [0, 1]$. Let $a_0 = 0, b_0 = 1$. In round $n \geq 1$, Alice chooses a_n s.t. $a_{n-1} < a_n < b_n$, then Bob chooses b_n s.t. $a_n < b_n < b_{n-1}$. Since a monotonically increasing sequence of real numbers bounded above has a limit, $\alpha = \lim_{n \rightarrow \infty} a_n$ is well-defined. Alice wins if $\alpha \in S$, otherwise Bob wins.
- ▶ Assume S is countable, $S = \{s_1, s_2, \dots\}$. On move $n \geq 1$, Bob chooses $b_n = s_n$ if this is a legal move, otherwise he randomly chooses any allowable number for b_n . Bob always wins with this strategy!
- ▶ But when $S = [0, 1]$, Alice can't lose!

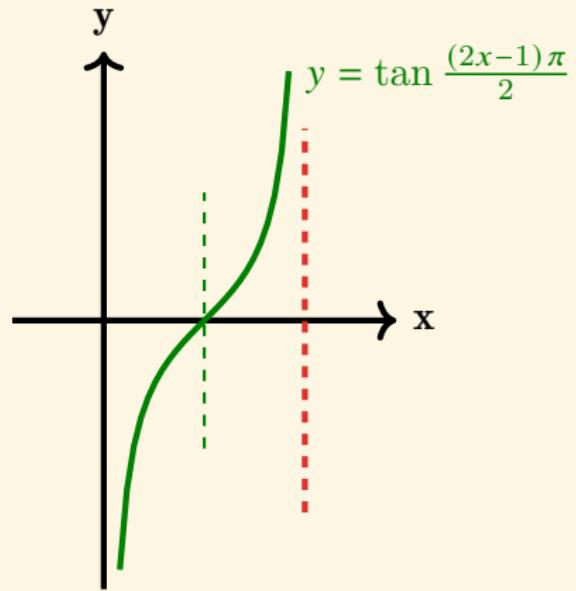
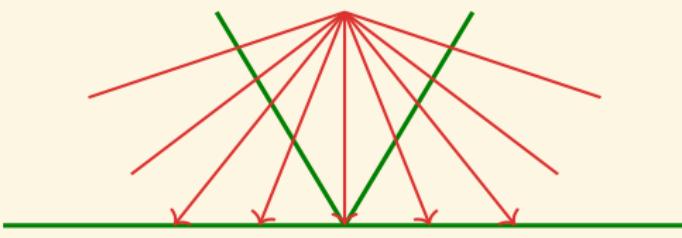
Continuum



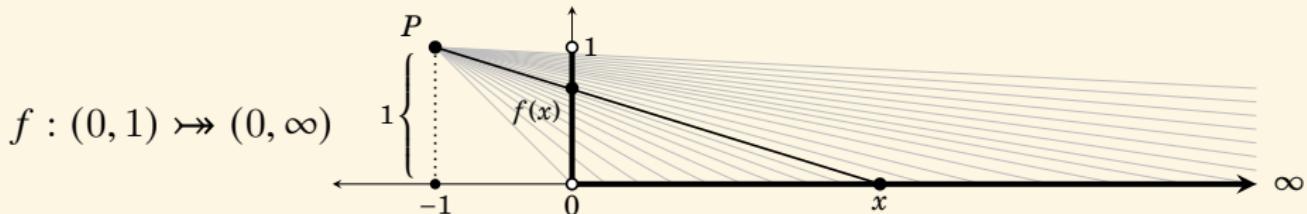
Continuum



Continuum



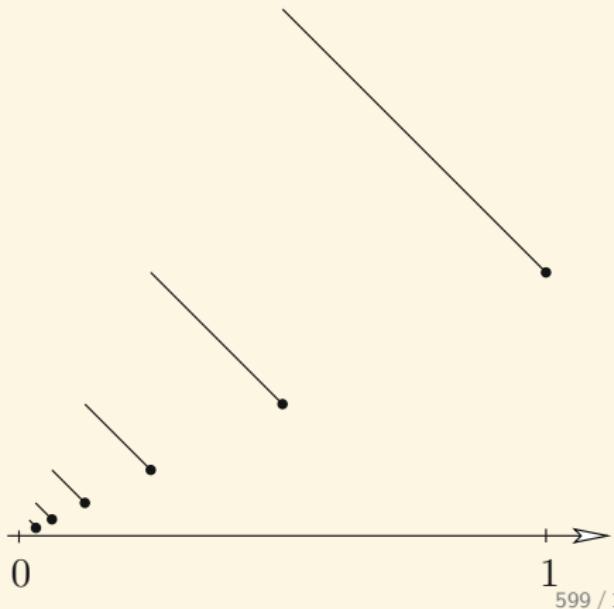
Continuum



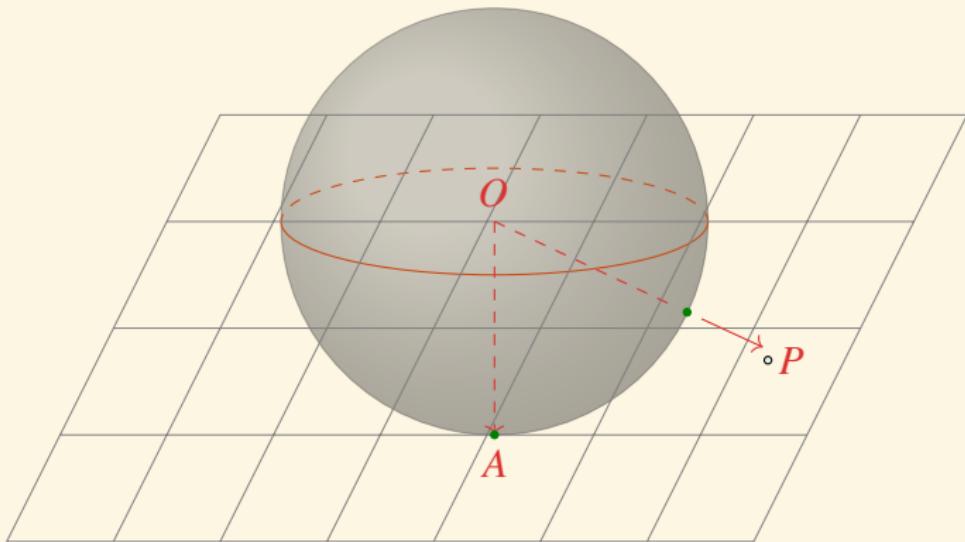
$$f : (0, 1] \rightarrow (0, 1)$$

$$f(x) := \begin{cases} \frac{3}{2} - x & \text{for } \frac{1}{2} < x \leq 1 \\ \frac{3}{4} - x & \text{for } \frac{1}{4} < x \leq \frac{1}{2} \\ \frac{3}{8} - x & \text{for } \frac{1}{8} < x \leq \frac{1}{4} \\ \vdots \end{cases}$$

$$f(x) := \begin{cases} \frac{x}{x+1} & \text{if } \exists n \in \mathbb{N} : x = \frac{1}{n} \\ x & \text{otherwise} \end{cases}$$



Continuum



Continuum

Theorem

$$|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$$

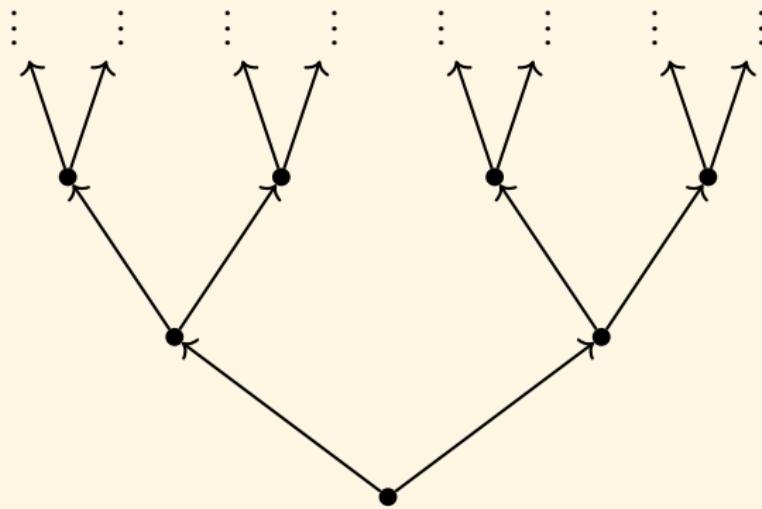
Proof.

$$x = 0.3 \quad 01 \quad 2 \quad 007 \quad 08\dots$$

$$y = 0.009 \quad 2 \quad 05 \quad 1 \quad 0003\dots$$

$$z = 0.3 \ 009 \ 01 \ 2 \ 2 \ 05 \ 007 \ 1 \ 08 \ 0003 \dots$$

Continuum



$$[0, 1] = \left\{ \sum_{n=1}^{\infty} \frac{x_n}{2^n} : x_n = 0 \vee x_n = 1 \right\}$$

Cantor's Theorem

Theorem (Cantor's Theorem)

$$|X| < |\mathcal{P}(X)|$$

Proof.

If $f : X \rightarrow \mathcal{P}(X)$, then

$$Y := \{x \in X : x \notin f(x)\}$$

is not in the range of f .

Cantor's Paradox

the 'set' of all sets?

Cantor's Theorem

$1, 2, \dots, \aleph_0, \aleph_1, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots, \aleph_{\omega \cdot 2}, \dots, \aleph_{\omega^2}, \dots, \aleph_{\omega^\omega}, \dots, \aleph_{\varepsilon_0}, \dots, \aleph_{\aleph_0}, \dots, \aleph_{\aleph_{\aleph_0}}, \dots$
the first cardinal to succeed all of these is labeled by the ordinal $\kappa = \aleph_\kappa$.
(So big that it needs itself to say how big it is!)

The 'set' I of all distinct levels of infinity is so large that it can't be a set!

$$\forall d \in I : |S_d| \leq \left| \bigcup_{c \in I} S_c \right| < \left| P \left(\bigcup_{c \in I} S_c \right) \right|$$

where S_c is a representative set that has cardinality c .

Cantor's Continuum Hypothesis

Cantor's Continuum Hypothesis (CH)

$$2^{\aleph_0} \stackrel{?}{=} \aleph_1$$



Cantor-Schröder-Bernstein Theorem

Theorem (Cantor-Schröder-Bernstein Theorem)

$$\left. \begin{array}{l} |M| \leq |N| \\ |N| \leq |M| \end{array} \right\} \implies |M| = |N|$$

1. Finite cycles on $2k + 2$ distinct elements ($k \geq 0$)

$$m_0 \xrightarrow{\text{green}} n_0 \xrightarrow{\text{red}} m_1 \xrightarrow{\text{green}} \cdots \xrightarrow{\text{red}} m_k \xrightarrow{\text{green}} n_k$$

2. Two-way infinite chains of distinct elements

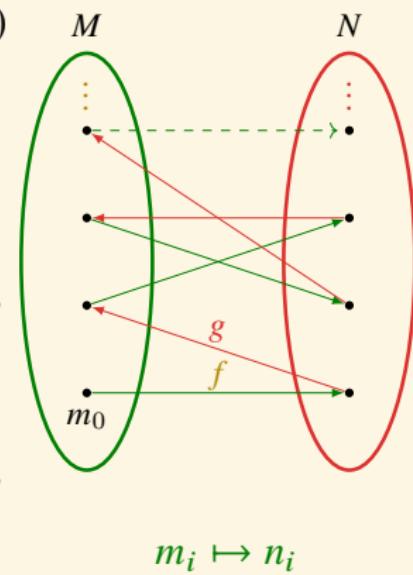
$$\cdots \xrightarrow{\text{red}} m_0 \xrightarrow{\text{green}} n_0 \xrightarrow{\text{red}} m_1 \xrightarrow{\text{green}} n_1 \xrightarrow{\text{red}} \cdots$$

3. The one-way infinite chains of distinct elements that start at the elements $m_0 \in M \setminus g(N)$

$$m_0 \xrightarrow{\text{green}} n_0 \xrightarrow{\text{red}} m_1 \xrightarrow{\text{green}} n_1 \xrightarrow{\text{red}} m_2 \xrightarrow{\text{green}} \cdots$$

4. The one-way infinite chains of distinct elements that start at the elements $n_0 \in N \setminus f(M)$

$$n_0 \xrightarrow{\text{red}} m_0 \xrightarrow{\text{green}} n_1 \xrightarrow{\text{red}} m_1 \xrightarrow{\text{green}} n_2 \xrightarrow{\text{red}} \cdots$$



Tarski's Fixpoint Theorem

- ▶ A complete lattice is a partially ordered set in which every non-empty subset has both a supremum and an infimum.

Theorem (Tarski's Fixpoint Theorem)

For a complete lattice (L, \sqsubseteq) and an order-preserving function $f : L \rightarrow L$, the set of fixpoints of f is also a complete lattice, with greatest fixpoint $\bigcup\{x : x \sqsubseteq f(x)\}$ and least fixpoint $\bigcap\{x : f(x) \sqsubseteq x\}$.

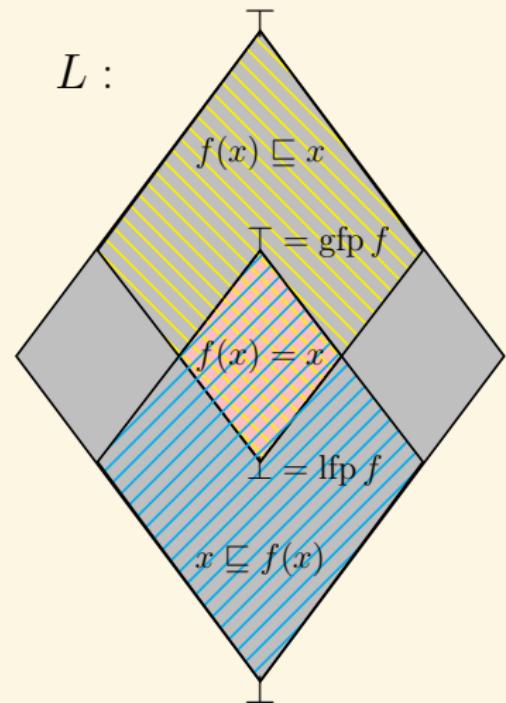
Proof.

Let $D := \{x \in L : x \sqsubseteq f(x)\}$, and $u := \bigcup D$.

Then for $x \in D$, $x \sqsubseteq u$ and $x \sqsubseteq f(x) \sqsubseteq f(u)$, hence $u \sqsubseteq f(u)$.

Then $f(u) \sqsubseteq f(f(u))$.

So we have $f(u) \in D$ and $f(u) \sqsubseteq u$, from which follows $f(u) = u$.



Cantor-Schröder-Bernstein Theorem — another proof

Proof.

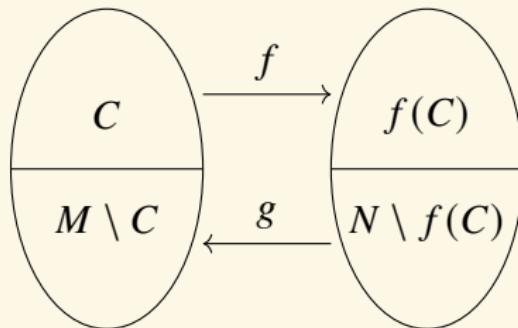
$(P(M), \subset)$ is a complete lattice.

Since the map

$$h : S \mapsto M \setminus g(N \setminus f(S))$$

is nondecreasing, it has a fixpoint C and $M \setminus C = g(N \setminus f(C))$.

$$f|_C \cup g^{-1}|_{M \setminus C}$$



Cantor-Schröder-Bernstein Theorem — another proof

Proof.

$$C_0 := M \setminus g(N)$$

$$D_0 := f(C_0)$$

$$C_{n+1} := g(D_n)$$

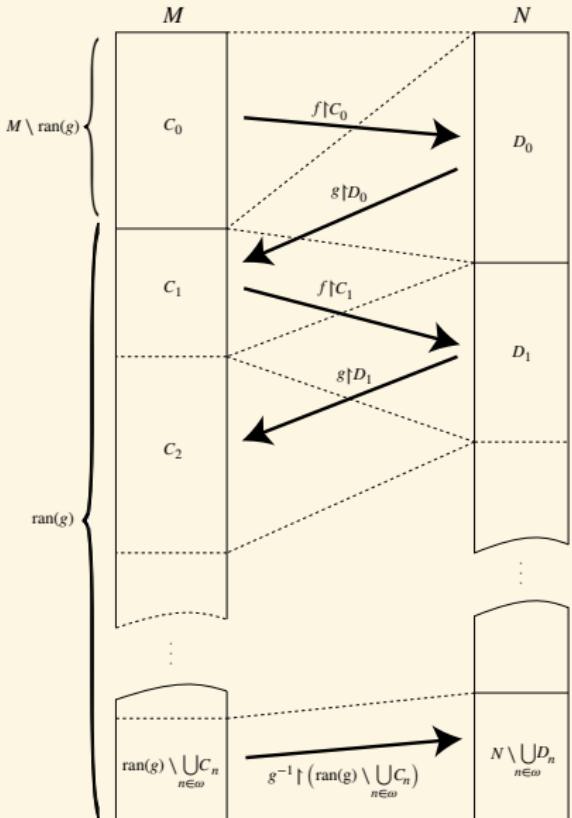
$$D_{n+1} := f(C_n)$$

$$C := \bigcup_{n \in \mathbb{N}} C_n$$

$$f \upharpoonright C \cup g^{-1} \upharpoonright_{g(N) \setminus C}$$

$$C = \bigcup_{n \rightarrow \infty} h^n(\emptyset)$$

$$= \bigcap \left\{ S : (M \setminus g(N)) \cup g(f(S)) \subset S \right\}$$



Cantor-Schröder-Bernstein Theorem — another proof

Proof.

$$M_0 := M, \quad M_1 := g(N), \quad M_{k+2} := g \circ f(M_k)$$

$$M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_k \supset M_{k+1} \supset \cdots$$

$$A := \bigcup_{k=0}^{\infty} (M_{2k+1} \setminus M_{2k+2}) \quad B := \bigcup_{k=0}^{\infty} (M_{2k} \setminus M_{2k+1}) \quad C := \bigcup_{k=1}^{\infty} (M_{2k} \setminus M_{2k+1})$$

$$D := \bigcap_{k=0}^{\infty} M_k$$

$$M = A \cup B \cup D$$

$$M_1 = A \cup C \cup D$$

$$|M_{2k} \setminus M_{2k+1}| = |g \circ f(M_{2k}) \setminus g \circ f(M_{2k+1})| = |M_{2k+2} - M_{2k+3}| \implies |B| = |C|$$

$$|M| = |M_1| = |N|$$

Cardinal Arithmetic

Definition (Cardinal Arithmetic)

$$\kappa + \lambda = |(A \times \{0\}) \cup (B \times \{1\})|$$

$$\kappa \cdot \lambda = |A \times B|$$

$$\kappa^\lambda = |A^B|$$

where $|A| = \kappa, |B| = \lambda$.

Theorem

- ▶ *+ and \cdot are associative, commutative and distributive.*
- ▶ $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$
- ▶ $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$
- ▶ $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$
- ▶ $\kappa \leq \lambda \implies \kappa^\mu \leq \lambda^\mu$
- ▶ $0 < \lambda \leq \mu \implies \kappa^\lambda \leq \kappa^\mu$
- ▶ $\kappa^0 = 1; 1^\kappa = 1; 0^\kappa = 0$ if $\kappa > 0$.

Theorem

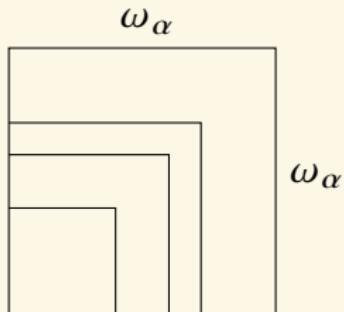
$$\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$$

Proof.

We define $(\alpha, \beta) < (\gamma, \delta)$ iff either

- ▶ $\max\{\alpha, \beta\} < \max\{\gamma, \delta\}$, or
- ▶ $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$ and $\alpha < \gamma$, or
- ▶ $\max\{\alpha, \beta\} = \max\{\gamma, \delta\}$, $\alpha = \gamma$ and $\beta < \delta$.

Obviously, $<$ is a well-order on $\text{Ord} \times \text{Ord}$ and $\alpha \times \alpha = \{(\xi, \eta) : (\xi, \eta) < (0, \alpha)\}$.



Let $\Gamma(\alpha, \beta) := \text{otp} \{(\xi, \eta) : (\xi, \eta) < (\alpha, \beta)\}$. Then

$(\alpha, \beta) < (\gamma, \delta) \iff \Gamma(\alpha, \beta) < \Gamma(\gamma, \delta)$, and $\Gamma(\omega, \omega) = \omega$, $\Gamma(\alpha, \alpha) \geq \alpha$.

Assume α is the least ordinal s.t. $\Gamma(\omega_\alpha, \omega_\alpha) \neq \omega_\alpha$. Let $\beta, \gamma < \omega_\alpha$ s.t. $\Gamma(\beta, \gamma) = \omega_\alpha$. Pick $\delta < \omega_\alpha$ s.t. $\delta > \beta, \gamma$. We have $\Gamma(\delta, \delta) \supset \omega_\alpha$ and so $|\delta \times \delta| \geq \aleph_\alpha$. However, $|\delta \times \delta| = |\delta| \cdot |\delta| = |\delta| < \aleph_\alpha$. Contradiction.

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$$

Cantor Set



$$C_0 := [0, 1]$$

$$C_{k+1} := \frac{C_k}{3} \cup \left(\frac{2}{3} + \frac{C_k}{3} \right)$$

$$C := \bigcap_{k=0}^{\infty} C_k = \bigcap_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\left[\frac{3k+0}{3^n}, \frac{3k+1}{3^n} \right] \cup \left[\frac{3k+2}{3^n}, \frac{3k+3}{3^n} \right] \right)$$

$$= [0, 1] \setminus \bigcup_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\frac{3k+1}{3^n}, \frac{3k+2}{3^n} \right)$$

$$C = \left\{ \sum_{n=1}^{\infty} \frac{x_n}{3^n} : x_n = 0 \vee x_n = 2 \right\} \implies |C| = 2^{\aleph_0}$$

Banach's Fixpoint Theorem

Theorem (Banach's Fixpoint Theorem)

Let (M, d) be a complete metric space and $T : M \rightarrow M$ be a contraction mapping, with Lipschitz constant $\gamma < 1$. Then T has a unique fixpoint $x \in M$. Further, for each $x_0 \in M$, $\lim_{n \rightarrow \infty} T^n(x_0) = x$, and the convergence is geometric:

$$d(T^n(x_0), x) \leq \gamma^n d(x_0, x)$$

Banach's Fixpoint Theorem and Cantor Set

- Let (M, d) be a complete metric space and let \mathcal{M} be the set of all non-empty bounded closed subsets of M .

For $A \in \mathcal{M}$ and $\varepsilon > 0$, let $N_\varepsilon(A) := \{x \in M : d(x, A) < \varepsilon\}$ where $d(x, A) := \inf_{y \in A} d(x, y)$. Let

$$d_H(A, B) := \inf \{\varepsilon : A \subset N_\varepsilon(B) \text{ & } B \subset N_\varepsilon(A)\}$$

Then (\mathcal{M}, d_H) is a complete metric space.

- Let $T_i : M \rightarrow M, i = 1, \dots, n$ be a set of contractions. Let \mathcal{M}' be the set of all compact sets of \mathcal{M} . Define the map $S : \mathcal{M}' \rightarrow \mathcal{M}'$ by

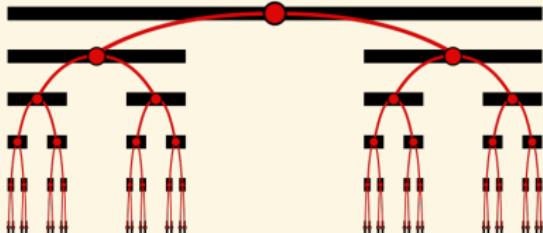
$$S(X) = \bigcup_{i=1}^n T_i(X). \text{ Then } S \text{ is a contraction.}$$

- According to Banach's fixpoint theorem, $\exists X \in \mathcal{M}' : S(X) = X$.

Furthermore, $\forall Y \in \mathcal{M}' : S(Y) \subset Y \implies X = \bigcap_{k=0}^{\infty} S^k(Y)$.

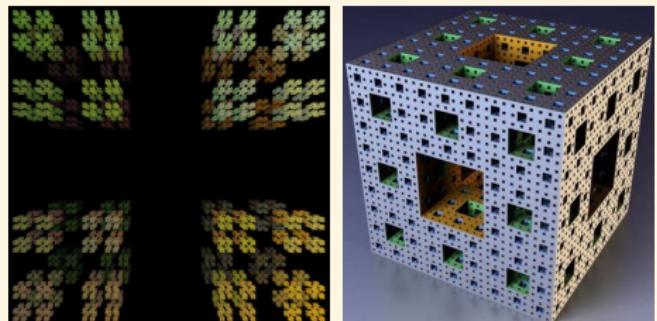
- Cantor set C is the fixpoint of $x \mapsto \frac{x}{3} \cup \left(\frac{x}{3} + \frac{2}{3}\right)$.

Cantor Set



- ▶ $|C| = 2^{\aleph_0}$
- ▶ C is perfect.
- ▶ C is *nowhere dense* in $[0, 1]$.
- ▶ Lebesgue measure: 0
- ▶ Hausdorff dimension: $\log_3 2$
- ▶ compact metric space

Figure: Torricelli trumpet



(a) Cantor dust(3D) (b) Menger sponge:
infinite surface area
but 0 volume

Fractal, Hausdorff Dimension, Topological Dimension

A set A is a *fractal* iff $\dim_H(A) > \dim_T(A)$.

$$H_\varepsilon^d(A) := \inf \left\{ \sum_{k=1}^{\infty} \text{diam}(B_k)^d : A \subset \bigcup_{k=1}^{\infty} B_k \text{ } \& \text{ diam}(B_k) \leq \varepsilon \right\}$$

$$\dim_H(A) := \inf \left\{ d \geq 0 : \lim_{\varepsilon \rightarrow 0} H_\varepsilon^d(A) = 0 \right\}$$

Definition (Topological Dimension)

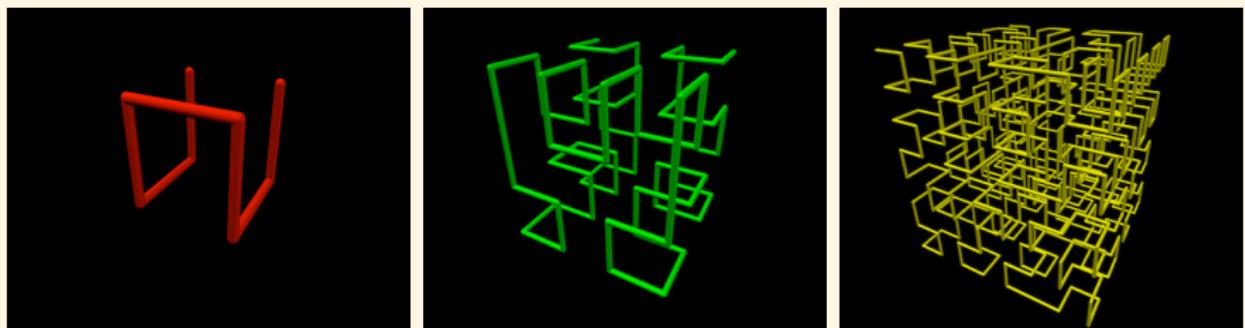
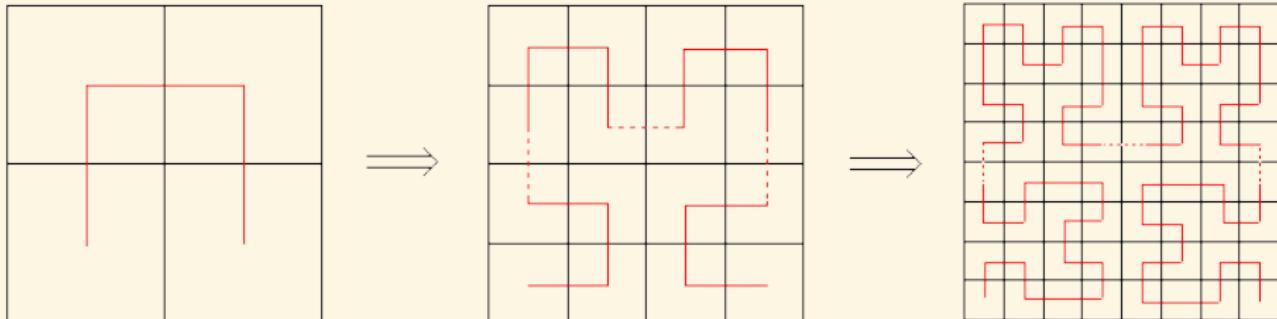
The *topological dimension* of a space X is defined by induction as

$$\dim_T(\emptyset) := -1$$

$$\dim_T(X) := \inf \{d : X \text{ has a basis } \mathcal{U} \text{ s.t. } \forall U \in \mathcal{U} : \dim_T(\partial U) \leq d - 1\}.$$

The topological dimension of a space X is the smallest integer d such that every open cover \mathcal{U} of X has a refinement \mathcal{V} in which no point of X lies in more than $d + 1$ elements of \mathcal{V} .

Hilbert's Space-filling Curve



Hilbert's Space-filling Curve

- ▶ When we draw h_n , we impose a $2^n \times 2^n$ grids onto the square S . The diagonal of each grid is of length $\sqrt{(2^{-n})^2 + (2^{-n})^2} = 2^{\frac{1}{2}-n}$.
- ▶ We define the curve h as the limit of these successive functions $h_1, h_2 \dots$ s.t. $h(x) = \lim_{n \rightarrow \infty} h_n(x)$.
- ▶ Each point in S is at most $2^{\frac{1}{2}-n}$ distance away from some point on h_n . So the maximum distance of any point from h is $\lim_{n \rightarrow \infty} 2^{\frac{1}{2}-n} = 0$. **So h fills space!**
- ▶ Definition. A curve is a continuous map from unit interval L to unit square S .
- ▶ For a point $p \in S$ and $\varepsilon > 0$, there is some n s.t. some grid of the $2^n \times 2^n$ grids on S lies within the circle with centre p and radius ε . let I be the largest open part of L which h_n maps into the relevant grid. Whenever $x \in I$, $h_m(x)$ lies in that same grid, for any $m > n$. **So h is continuous.**
- ▶ Hilbert's curve is continuous everywhere but differentiable nowhere.
- ▶ Hausdorff dimension: 2

Cardinality of the Permutations of \mathbb{N} — $|\text{Aut}(\mathbb{N})|$

Proof1. Diagonal method: For any countable sequence $(\sigma_n)_{n \in \mathbb{N}}$ of permutations, let $f : 2n \mapsto \min(2\mathbb{N} \setminus \{\sigma_0(0), \sigma_1(2), \dots, \sigma_n(2n)\})$, and $f : 2n + 1 \mapsto$ the n^{th} element of $\mathbb{N} \setminus f(2\mathbb{N})$. Then $\forall n : f \neq \sigma_n$.

Proof1'. Let f be the bijection s.t. for each n , f swaps $2n$ and $2n + 1$ if $\sigma_n(2n) = 2n$, leaving the rest fixed. $|\text{Aut}(\mathbb{N})| > \aleph_0$.

Proof2. For any n , either swap $(2n, 2n + 1)$ or keep them fixed.

Proof2'. The set of fixpoints of any permutation can be any subset of \mathbb{N} except ones of the form $\mathbb{N} \setminus \{n\}$ for some n . $|\text{Aut}(\mathbb{N})| \geq 2^{\aleph_0}$.

Proof3. Riemann rearrangement $\left(\text{e.g. } \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \right) \implies \mathbb{R} \rightarrowtail \text{Aut}(\mathbb{N})$.

Theorem (Riemann Rearrangement Theorem)

Any conditionally convergent series can be rearranged in a permutation to

1. converge to any real number;
2. diverge to ∞ or $-\infty$;
3. oscillate finitely or infinitely.



The Pasadena Paradox

The Pasadena Game

Toss a fair coin until the first head appears. If the first head appears on toss n , the payoff is $\frac{(-1)^{n+1}2^n}{n}$.

How to calculate the expected utility?

$$\sum_{n=1}^{\infty} \frac{1}{2^n} \frac{(-1)^{n+1}2^n}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} = \ln 2 \quad \sum_{n=1}^{\infty} \left| \frac{(-1)^{n+1}}{n} \right| = \infty$$

Cofinality and Inaccessible Cardinal

- ▶ $\text{cf}(\alpha) :=$ the least limit ordinal β s.t. there is an increasing β -sequence $\langle \alpha_\xi : \xi < \beta \rangle$ with $\lim_{\xi \rightarrow \beta} \alpha_\xi = \alpha$.
- ▶ An infinite cardinal κ is *regular* iff $\text{cf}(\kappa) = \kappa$. It is *singular* iff $\text{cf}(\kappa) < \kappa$.
- ▶ A cardinal κ is a *strong limit* cardinal iff $\forall \lambda < \kappa (2^\lambda < \kappa)$.
- ▶ A cardinal κ is *inaccessible* iff it is a regular strong limit uncountable cardinal.

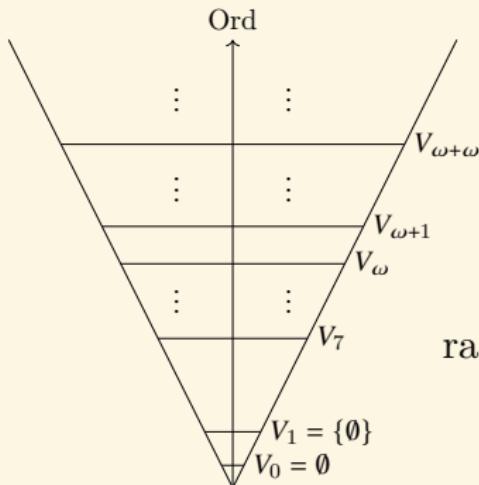
von Neumann Universe

Definition (von Neumann Universe)

$$V_0 := \emptyset$$

$$V_{\alpha+1} := P(V_\alpha)$$

$$V_\alpha := \bigcup_{\beta < \alpha} V_\beta \quad \text{for limit } \alpha.$$



$$V := \{x : x = x\}$$

$$V = \bigcup_{\alpha \in \text{Ord}} V_\alpha$$

$\text{rank}(x) := \text{the least } \alpha \text{ s.t. } x \subset V_\alpha$

Constructable Universe

$$\text{Def}(M) := \{X \subset M : X \text{ is } M\text{-definable over } (M, \in)\}$$

Definition (Constructable Universe)

Axiom of Constructibility

$$L_0 := \emptyset$$

$$V = L$$

$$L_{\alpha+1} := \text{Def}(L_\alpha)$$

$$L_\alpha := \bigcup_{\beta < \alpha} L_\beta \quad \text{for limit } \alpha.$$

$$L \models \text{ZF}$$

$$L := \bigcup_{\alpha \in \text{Ord}} L_\alpha$$

$$L \models V = L$$

$$\text{ZF} + V = L \vdash \text{AC} + \text{GCH}$$

An inner model is a transitive class model of ZF that contains all ordinals.
 L is the smallest inner model of ZF.

Grothendieck Universe

Definition (Grothendieck Universe)

1. $x \in y \in U \implies x \in U$
2. $x \in U \ \& \ y \in U \implies \{x, y\} \in U$
3. $x \in U \implies P(x) \in U$
4. $I \in U \ \& \ x : I \rightarrow U \implies \bigcup_{i \in I} x_i \in U$
5. $\omega \in U$



Universe Axiom

For every set x , there exists a Grothendieck universe U s.t. $x \in U$.

U is a Grothendieck universe iff $U = V_\kappa$ for some inaccessible κ .

The Universe Axiom is equivalent to the “inaccessible cardinal axiom” that “there exist arbitrarily large inaccessible cardinals.”

$$U \models \text{ZFC}$$

$$\frac{\text{super-infinite}}{\text{infinite}} \approx \frac{\text{infinite}}{\text{finite}}$$

- | | | |
|----------------|--------|--|
| finite | \iff | every self-embedding is bijective. |
| infinite | \iff | admits a non-surjective self-embedding. |
| super-infinite | \iff | admits a non-surjective elementary self-embedding. |

Example: \mathbb{N} is infinite but not super-infinite.

Axiom (Axiom I3)

For some λ , V_λ is super-infinite.

Shelf

Definition (Shelf)

A left (right) *shelf* is a set S with an operation $*$ satisfying

$$x * (y * z) = (x * y) * (x * z) \quad (\text{left self-distributive})$$

$$(x * y) * z = (x * z) * (y * z) \quad (\text{right self-distributive})$$

Example:

- ▶ S set, $f : S \rightarrow S$, and $x * y := f(y)$
- ▶ E module and $x * y := (1 - \lambda)x + \lambda y$
- ▶ G group and $x * y := xyx^{-1}$
- ▶ B boolean algebra and $x * y := \bar{x} + y$

Under the logical interpretation, $*$ corresponds to implication \rightarrow .

Laver Tables

Theorem (Laver)

1. For every N , there exists a unique binary operation $*$ on $\{1, \dots, N\}$ s.t.

$$x * 1 = x + 1 \bmod N$$

$$x * (y * 1) = (x * y) * (x * 1)$$

2. The operation thus obtained obeys

$$x * (y * z) = (x * y) * (x * z)$$

iff N is a power of 2.

Laver Tables

Definition (Laver Table)

Laver table A_n is the unique left shelf $(\{1, \dots, 2^n\}, *)$ satisfying

$$x * 1 = x + 1 \bmod 2^n$$

		A_2			
		1	2	3	4
		1	2	3	4
A_0	1				
1	1	2	4	2	4
		3	4	3	4
		4	4	4	4
		1	2	3	4

$x \mapsto x \bmod 2^{n-1}$ is a surjective homomorphism from A_n to A_{n-1} .

Period

Theorem (Laver)

For every $p \leq 2^n$, there exists a number $\pi_n(p)$, a power of 2, such that the p^{th} row in the table of A_n is the repetition of $\pi_n(p)$ values increasing from $p + 1 \bmod 2^n$ to 2^n .

$$\pi_n(p) := \mu x [p * x = 2^n]$$

A_3	1	2	3	4	5	6	7	8	period
1	2	4	6	8	2	4	6	8	$\pi_3(1) = 4$
2	3	4	7	8	3	4	7	8	$\pi_3(2) = 4$
3	4	8	4	8	4	8	4	8	$\pi_3(3) = 2$
4	5	6	7	8	5	6	7	8	$\pi_3(4) = 4$
5	6	8	6	8	6	8	6	8	$\pi_3(5) = 2$
6	7	8	7	8	7	8	7	8	$\pi_3(6) = 2$
7	8	8	8	8	8	8	8	8	$\pi_3(7) = 1$
8	1	2	3	4	5	6	7	8	$\pi_3(8) = 8$

n	0	1	2	3	4	5	6	7	8	9	10	11	...
$\pi_n(1)$	1	1	2	4	4	8	8	8	8	16	16	16	...
$\pi_n(2)$	-	2	2	4	4	8	8	16	16	16	16	16	...

$\mu n[\pi_n(1) = 32] \geq A(9, A(8, A(8, 254)))$ where A is the Ackermann Function

Theorem (Laver)

1. ZFC + I3 $\vdash \forall n(\pi_n(2) \geq \pi_n(1))$
2. ZFC + I3 $\vdash \lim_{n \rightarrow \infty} \pi_n(1) = \infty$

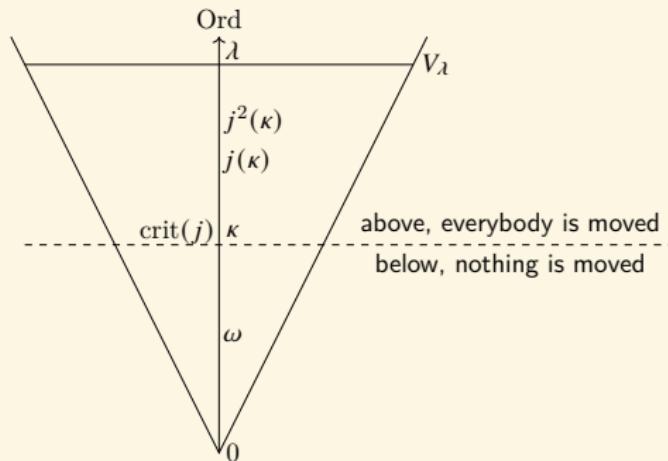
Can one find alternative proofs using no large cardinal?

Analogy:

- In physics: using a physical intuition, guess statements, then pass them to the mathematician for a formal proof;
- In logic: using a logical intuition (existence of a super-infinite set), guess statements (periods in Laver tables tend to ∞), then pass them to the mathematician for a formal proof.

$$\text{crit}(j) := \mu\alpha [j(\alpha) > \alpha]$$

The critical ordinal $\text{crit}(j)$ of the elementary embedding j is the least ordinal that is not invariant under j .



$$\mathcal{E}_\lambda := \{j : V_\lambda \prec V_\lambda \text{ } \& \text{ } j \text{ is non-surjective}\}$$

$$i[j] := \bigcup_{\alpha < \lambda} i(j \cap V_\alpha^2)$$

$$(\mathcal{E}_\lambda, []) \text{ is a left-shelf: } i[j[k]] = i[j][i[k]]$$

$$\text{crit}(j \circ j) = \text{crit}(j) \quad \text{but} \quad \text{crit}(j[j]) = j(\text{crit}(j)) > \text{crit}(j)$$

$$j_{[n]} := \underbrace{j[j][j] \cdots [j]}_{n \text{ times}}$$

$$\text{Iter}(j) := \{j_{[n]} : n \in \mathbb{N}^+\}$$

($\text{Iter}(j), []$) is a left-shelf.

For $k, k' \in \text{Iter}(j)$, declare $k \equiv_n k' := \forall x \in V_\gamma (k(x) \cap V_\gamma = k'(x) \cap V_\gamma)$ with $\gamma := \text{crit}(j_{[2^n]})$. Then

$\text{Iter}(j)/\equiv_n$ is (isomorphic to) the Laver table A_n .

Ordinal

$0, 1, 2, 3, \dots$

$\omega, \omega + 1, \omega + 2, \dots$

$\omega \cdot 2, (\omega \cdot 2) + 1, (\omega \cdot 2) + 2, \dots$

$\omega^2, \omega^2 + 1, \omega^2 + 2, \dots$

$\omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \dots$

$\omega^{\omega^\omega}, \dots$

$\varepsilon_0 = \omega^{\omega^{\omega^\dots}} = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\}$

$\varepsilon_1 = \sup\{\varepsilon_0 + 1, \omega^{\varepsilon_0+1}, \omega^{\omega^{\varepsilon_0+1}}, \omega^{\omega^{\omega^{\varepsilon_0+1}}}, \dots\} = \sup\{0, 1, \varepsilon_0, \varepsilon_0^{\varepsilon_0}, \varepsilon_0^{\varepsilon_0^{\varepsilon_0}}, \dots\}$

$\varepsilon_{\alpha+1} = \sup\{\varepsilon_\alpha + 1, \omega^{\varepsilon_\alpha+1}, \omega^{\omega^{\varepsilon_\alpha+1}}, \dots\} = \sup\{0, 1, \varepsilon_\alpha, \varepsilon_\alpha^{\varepsilon_\alpha}, \varepsilon_\alpha^{\varepsilon_\alpha^{\varepsilon_\alpha}}, \dots\}$

$\varepsilon_\alpha = \sup\{\varepsilon_\beta : \beta < \alpha\}$ if α is a limit ordinal.

$\boxed{\varepsilon_\alpha \text{ is countable iff } \alpha \text{ is countable.}}$

$\boxed{\forall \alpha \geq 1 : \varepsilon_{\omega_\alpha} = \omega_\alpha}$

Veblen Hierarchy

$$\varphi_0(\alpha) := \omega^\alpha$$

$\varphi_{\gamma+1}(\alpha) := \alpha^{\text{th}}$ ordinal s.t. $\varphi_\gamma(\beta) = \beta$

$\varphi_\delta(\alpha) := \alpha^{\text{th}}$ common fixpoint of φ_γ for all $\gamma < \delta$

$\Gamma_\alpha := \alpha^{\text{th}}$ ordinal s.t. $\varphi_\alpha(0) = \alpha$

$$\varepsilon_\alpha = \varphi_1(\alpha)$$

All sets here and above are **uncountable**

All sets here are **countable** (same size as \mathbb{N})

All sets here are finite

empty set \emptyset

$\kappa = \aleph_\kappa$

\aleph_ω

\aleph_1

ε_0

$\omega = \aleph_0$

6

5

65,536 sets
below Stage 5!

“inaccessible” cardinals
(ZF axioms cannot be used to prove the existence of these sets)

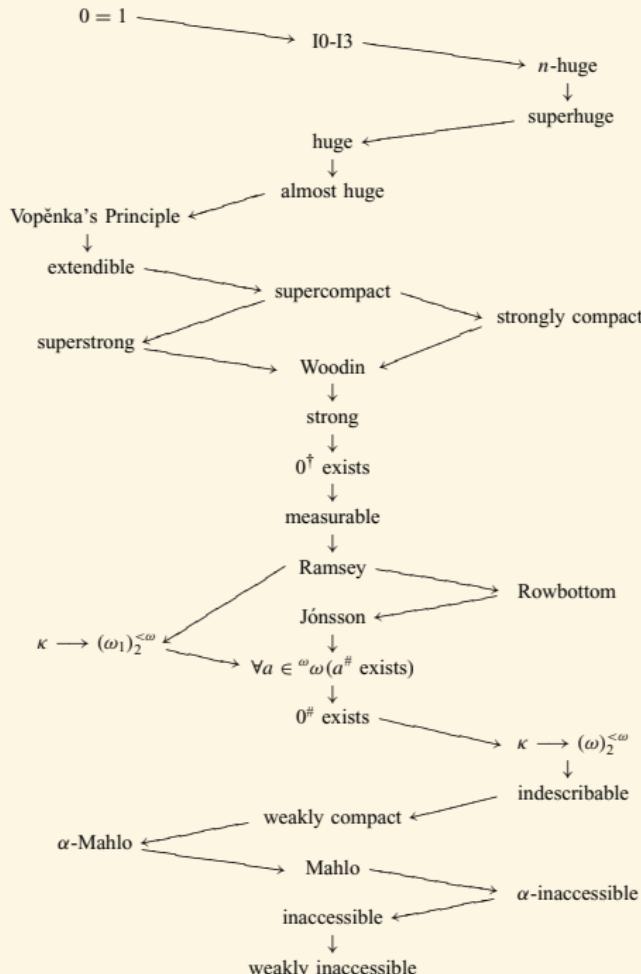
First cardinal that can only be named by the ordinal that is as big as itself

First cardinal to be preceded by infinitely many cardinals

Second infinite cardinal
(first uncountable ordinal)

First infinite cardinal/ordinal (\mathbb{N})

The number of sets here has 20,000 digits!



Contents

Introduction

Cardinal Numbers
Axiom of Choice

Term Logic

Recursion Theory

Propositional Logic

Equational Logic

Predicate Logic

Homotopy Type Theory

Modal Logic

Category Theory

Set Theory

Quantum Computing

Axioms of ZFC

Ordinal Numbers

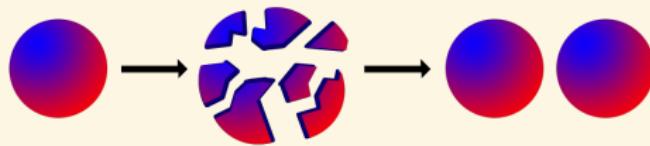
Answers to the Exercises

References 1436

AC and Banach-Tarski Paradox

The Axiom of Choice is necessary to select a set from an infinite number of pairs of socks, but not an infinite number of pairs of shoes.

— Russell



Theorem (Banach-Tarski Theorem)

If A and B are bounded subsets of \mathbb{R}^n , $n \geq 3$, with non-empty interior, then there are finite partitions $A = \coprod_{i=1}^n A_i$, $B = \coprod_{i=1}^n B_i$ s.t. each A_i is congruent to B_i for $1 \leq i \leq n$.

AC vs AD

Axiom of Determinacy (AD)

Consider $A \subset \omega^\omega$. Two players alternately pick natural numbers

$$n_0, n_1, n_2, \dots$$

Player 1 wins the game iff $(n_i)_{i \in \omega} \in A$.

The axiom of determinacy states that for every $A \subset \omega^\omega$, the game is determined, i.e. one of the two players has a winning strategy.

$$\forall A \subset \omega^\omega : \left(\forall n_0 \exists n_1 \forall n_2 \exists n_3 \dots [(n_i)_{i \in \omega} \in A] \right) \vee \left(\exists n_0 \forall n_1 \exists n_2 \forall n_3 \dots [(n_i)_{i \in \omega} \notin A] \right)$$

- ▶ AD is inconsistent with AC.
- ▶ AD implies countable axiom of choice.
- ▶ AD implies that every subset of reals is Lebesgue measurable.
- ▶ $\text{AD} \implies \text{CH}$. Since $\text{GCH} \implies \text{AC}$, AD is inconsistent with GCH.

Equivalents of AC

- ▶ Well-ordering theorem: Every set can be well-ordered.
- ▶ Trichotomy: For any two cardinals κ and λ : $\kappa < \lambda \vee \kappa = \lambda \vee \kappa > \lambda$.
- ▶ For any infinite cardinal κ : $\kappa^2 = \kappa$.
- ▶ The Cartesian product of any family of non-empty sets is non-empty.
- ▶ Every surjective function has a right inverse.
- ▶ Hausdorff's Maximal Chain Condition: Each partially ordered set contains a maximal chain.
- ▶ Zorn's lemma: If in a partially ordered set X each chain has an upper bound, then X has a maximal element.
- ▶ Every vector space has a basis.
- ▶ The closed unit ball of the dual of a normed vector space over the reals has an extreme point.
- ▶ Tychonoff's theorem: The product of compact topological spaces is compact.
- ▶ If a set Γ of formulas with $|\mathcal{L}| = \kappa$ is finitely satisfiable, then it has a model with cardinality $\leq \kappa + \aleph_0$.

Theorem (Well-Ordering Theorem)

Every set can be well-ordered.

Proof.

Assume f is a choice function for $P(A) \setminus \{\emptyset\}$. Let

$$a_\alpha = f(A \setminus \{a_\xi : \xi < \alpha\})$$

$$\theta := \mu\alpha [A = \{a_\xi : \xi < \alpha\}]$$

Then $\langle a_\alpha : \alpha < \theta \rangle$ enumerates A .

Lemma (König's Lemma)

Every finitely branching tree with infinitely many nodes contains an infinite path.

Consistence & Independence

Theorem (Gödel 1938)

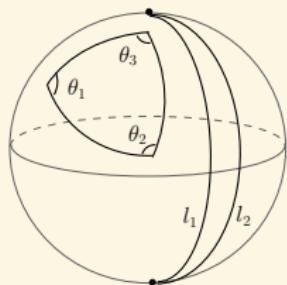
$$\text{Con}(\text{ZF}) \rightarrow \text{Con}(\text{ZFC} + \text{GCH})$$



Theorem (Cohen 1963)

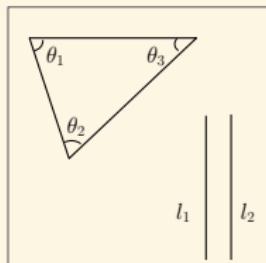
- ▶ $\text{Con}(\text{ZF}) \rightarrow \text{Con}(\text{ZF} + \neg\text{AC})$
- ▶ $\text{Con}(\text{ZF}) \rightarrow \text{Con}(\text{ZFC} + \neg\text{GCH})$

Figure: Cohen



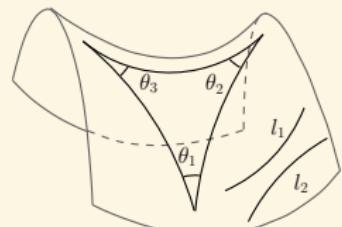
$$\theta_1 + \theta_2 + \theta_3 > 180^\circ$$

Spherical (positive curvature)



$$\theta_1 + \theta_2 + \theta_3 = 180^\circ$$

Euclidean (zero curvature)



$$\theta_1 + \theta_2 + \theta_3 < 180^\circ$$

Hyperbolic (negative curvature)

GCH vs Weak GCH

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \quad (\text{GCH})$$



$$2^\kappa < 2^{\kappa^+} \quad (\text{WGCH})$$



$$\kappa < \lambda \implies 2^\kappa < 2^\lambda$$

“ $|X| < |Y| \implies |\mathcal{P}(X)| < |\mathcal{P}(Y)|$ ” is independent of ZFC.

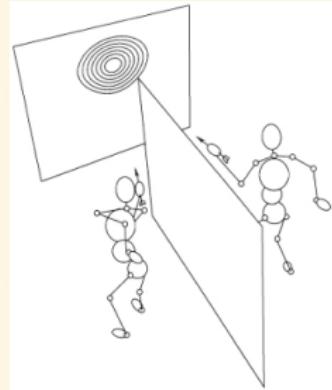
Freiling's Axiom of Symmetry

Freiling's Axiom of Symmetry (AX)

$$\forall f : \mathbb{R} \rightarrow \mathbb{R}_{\aleph_0} \exists xy [x \notin f(y) \wedge y \notin f(x)]$$

Theorem

$$\text{ZFC} \vdash \text{AX} \leftrightarrow \neg \text{CH}$$



Proof.

(\rightarrow): Let $<$ be a well ordering of \mathbb{R} of length \aleph_1 . Let $f(x) := \{y : y < x\}$. Then $f : \mathbb{R} \rightarrow \mathbb{R}_{\aleph_0}$. So $\exists xy (x < y \wedge y < x)$. Contradiction.

(\leftarrow): Assume $2^{\aleph_0} > \aleph_1$. Let x_1, x_2, \dots be an \aleph_1 -sequence of distinct reals.

Let $f : \mathbb{R} \rightarrow \mathbb{R}_{\aleph_0}$. Then $\left| \bigcup_{\alpha < \aleph_1} f(x_\alpha) \right| = \aleph_1$. So $\exists y \in \mathbb{R} \forall \alpha < \aleph_1 (y \notin f(x_\alpha))$.

Since $f(y)$ is countable, $\exists \alpha (x_\alpha \notin f(y))$. Therefore
 $y \notin f(x_\alpha) \wedge x_\alpha \notin f(y)$.

Contents

	Recursion Theory
Introduction	
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory
Turing Machine

Computability

Diagonal Method

Incompressibility Method

Incompleteness

Equational Logic

Homotopy Type Theory

Category Theory

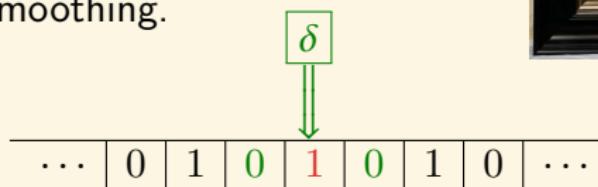
Quantum Computing

Answers to the Exercises

References 1436

Alan Turing 1912-1954

- ▶ Universal Turing Machine.
- ▶ Church-Turing Thesis.
- ▶ Halting Problem.
- ▶ Undecidability.
- ▶ Oracle Machine.
- ▶ Computable Absolutely Normal Number.
- ▶ Turing Test.
- ▶ Morphogenesis.
- ▶ Good-Turing Smoothing.
- ▶ Enigma.



What is “effective procedure”? — Recursion Theory

Turing¹³

- ▶ Computing is normally done by writing certain symbols on paper.
- ▶ We may suppose this paper is divided into squares like a child's arithmetic book.
- ▶ The number of symbols which may be printed is finite.
- ▶ The behaviour of the computer at any moment is determined by the symbols which he is observing, and his "state of mind" at that moment.
- ▶ We will also suppose that the number of states of mind which need to be taken into account is finite.

¹³Turing: On computable numbers, with an application to the Entscheidungsproblem. 1936.

(Deterministic) Turing Machine

Definition ((Deterministic) Turing Machine)

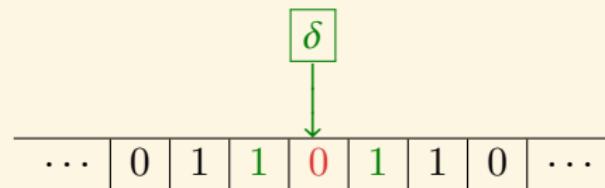
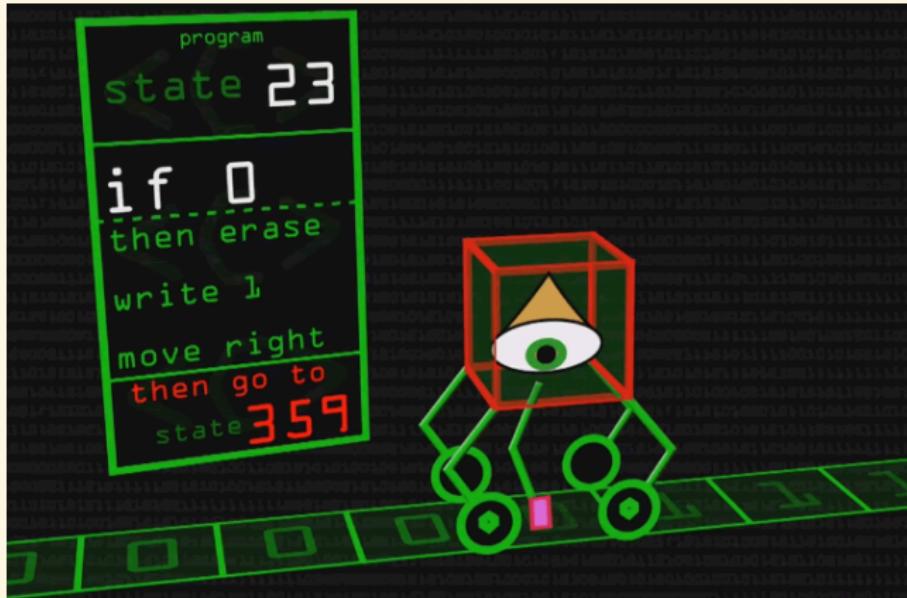
A deterministic Turing machine is a triplet (Σ, Q, δ) , where Σ is a finite alphabet with an identified blank symbol, Q is a finite set of states with identified initial state q_0 and final state $q_f \neq q_0$, and δ , a deterministic transition function

$$\delta : Q \times \Sigma \rightarrow \Sigma \times Q \times \{L, R\}$$

Here $\{L, R\}$ denote left and right, directions to move on the tape.

Definition (Configuration)

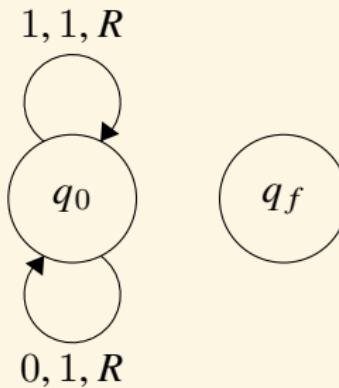
A configuration of a Turing Machine is a tuple (d, h, q) where d is a description of the contents of the tape, h is the location of the head symbol, and q represents the state the Turing machine is in.



$$\delta(q_{23}, 0) = (1, q_{359}, R)$$

Turing Machine — Example

This machine writes 1, then moves right forever. It will never halt since the function δ never maps to the state q_f .



$$\Sigma = \{0, 1\}$$

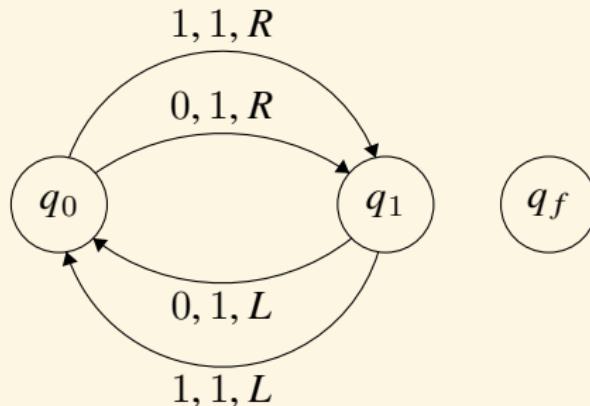
$$Q = (q_0, q_f)$$

$$\delta(q_0, 0) = (1, q_0, R)$$

$$\delta(q_0, 1) = (1, q_0, R)$$

Turing Machine — Example

This machine will move left then right and so on...



$$\Sigma = \{0, 1\}$$

$$Q = (q_0, q_1, q_f)$$

$$\delta(q_0, 0) = (1, q_1, R)$$

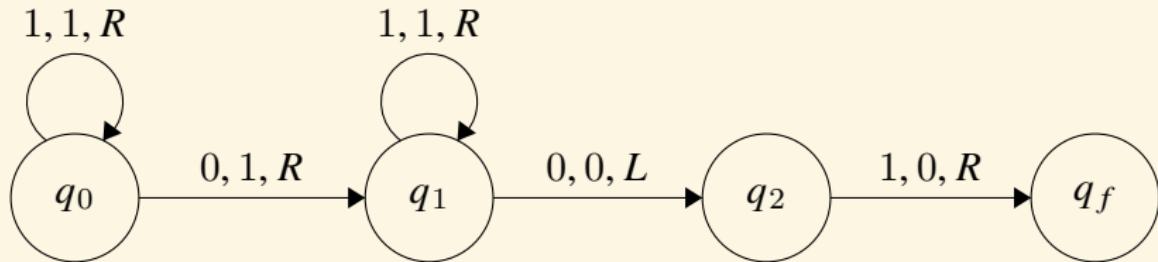
$$\delta(q_1, 0) = (1, q_0, L)$$

$$\delta(q_0, 1) = (1, q_1, R)$$

$$\delta(q_1, 1) = (1, q_0, L)$$

Turing Machine — Example

The ADD Turing machine takes an input of two unary numbers separated by a 0, $(1^l 0 1^m)$, then returns the sum of those two numbers, (1^{l+m}) .



$$\Sigma = \{0, 1\}$$

$$Q = (q_0, q_1, q_2, q_f)$$

$$\delta(q_0, 1) = (1, q_0, R)$$

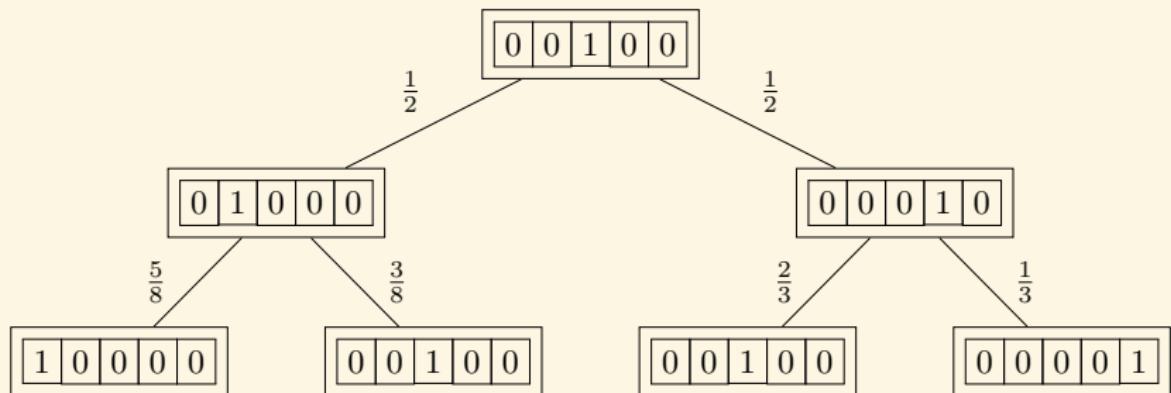
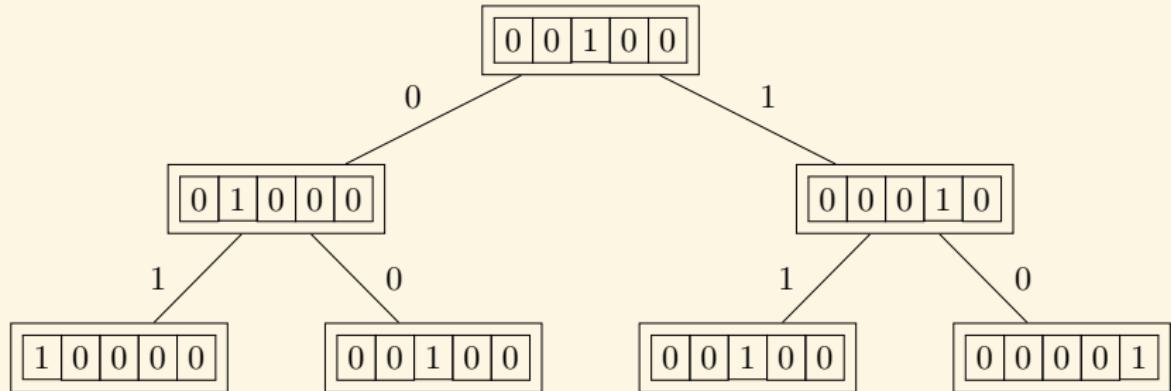
$$\delta(q_0, 0) = (1, q_1, R)$$

$$\delta(q_1, 1) = (1, q_1, R)$$

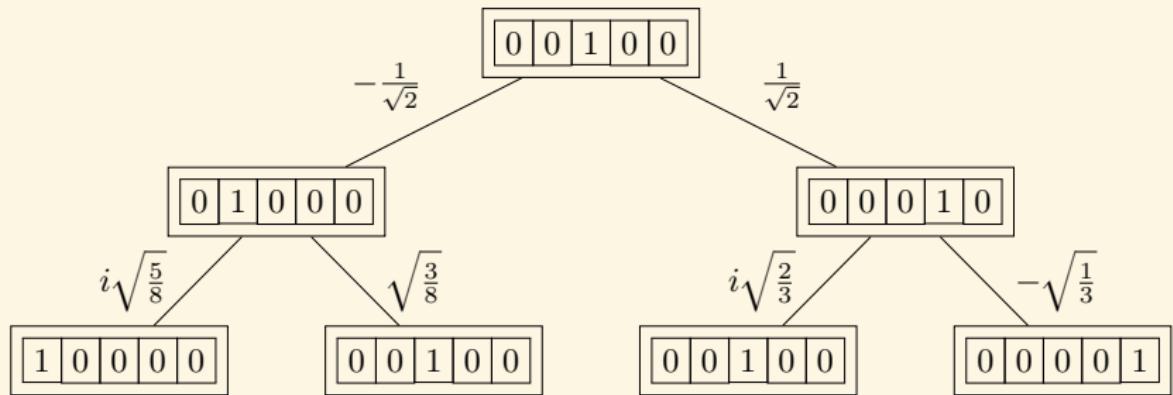
$$\delta(q_1, 0) = (0, q_2, L)$$

$$\delta(q_2, 1) = (0, q_f, R)$$

(Deterministic / Probabilistic) Turing Machine



(Quantum) Turing Machine



Thesis (Church-Turing Thesis)

effective calculable = *recursive* = *Turing Computable*

||

representable in Q = λ -definable

||

finite definable = Herbrand-Gödel computable

||

flowchart (or 'while') computable

||

neural network with unbounded tape = Conway's 'game of life'

||

Post/Markov/McCarthy/Kolmogorov-Uspensky computable . . .

- ▶ The behavior of any discrete physical system evolving according to local mechanical laws is computable?
- ▶ Any possible discrete physical process is computable?
- ▶ Any constructive function is computable?
- ▶ The mental functions can be simulated by machines?

Church-Turing Thesis

- ▶ Church-Turing Thesis

Every “function which could be regarded as computable” can be computed by a universal Turing machine.

- ▶ Church-Turing-Deutsch Thesis

Every finite physical system can be simulated to any specified degree of accuracy by a universal Turing machine.

- ▶ Feasibility Thesis — Classical / Quantum Version

A probabilistic (quantum) Turing machine can efficiently simulate any realistic model of computation.

- ▶ Wolfram’s Principle of Computational Equivalence

Almost all processes that are not obviously simple can be viewed as computations of equivalent sophistication.

- ▶ Wolfram’s Principle of Computational Irreducibility

Most of the time, the only way to see what a physical system (computer program) will do is to run it.

Computational Irreducibility vs Free Will

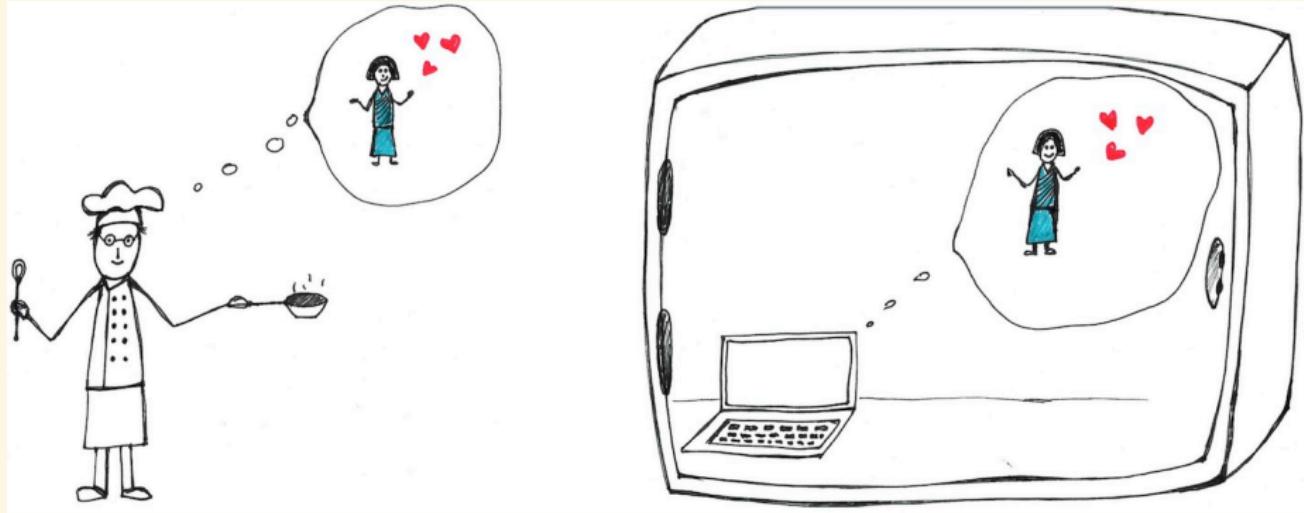


Figure: To predict John's choice of breakfast by simulation. A universal computer in the safe (on the right) reproduces the outputs of another process, i.e. its observable actions (John preparing breakfast, on the left).

Libet: We are conscious of our free choices only after 300ms our brain has made them.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory
Turing Machine

Computability

Diagonal Method

Incompressibility Method

Incompleteness

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Presburger/Robinson/Peano Arithmetic

- $x + 0 = x$
 - $x + y = y + x$
 - $(x + y) + z = x + (y + z)$
 - $x + z = y + z \rightarrow x = y$
 - $x \cdot 0 = 0$
 - $x \cdot 1 = x$
 - $x \cdot y = y \cdot x$
 - $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
 - $x \cdot (y + z) = x \cdot y + x \cdot z$
 - $P(0) \wedge \forall x(P(x) \rightarrow P(x + 1)) \rightarrow \forall xP(x)$
- 1. $s(x) \neq 0$
 - 2. $s(x) = s(y) \rightarrow x = y$
 - 3. $y = 0 \vee \exists x(s(x) = y)$
 - 4. $x + 0 = x$
 - 5. $x + s(y) = s(x + y)$
 - 6. $x \cdot 0 = 0$
 - 7. $x \cdot s(y) = (x \cdot y) + x$
 - 8. $P(0) \wedge \forall x(P(x) \rightarrow P(s(x))) \rightarrow \forall xP(x)$
- } Q

Full Second Order Arithmetic Z_2

- ▶ The basic axioms of Peano arithmetic
- ▶ The second order induction axiom

$$\forall X [0 \in X \wedge \forall n (n \in X \rightarrow s(n) \in X) \rightarrow \forall n \in \mathbb{N} (n \in X)]$$

- ▶ The comprehension axiom

$$\exists X \forall n [n \in X \leftrightarrow A(n)]$$

where A is any formula in which X does not occur freely.

Dedekind-Peano Axioms PA²

The natural numbers \mathbb{N} is a set with a chosen element $0 \in \mathbb{N}$ and an injective function $s : \mathbb{N} \rightarrow \mathbb{N}$ such that $0 \notin s(\mathbb{N})$ and such that the principle of mathematical induction holds: a set containing 0 and closed under s contains all natural numbers.

Definition (Dedekind-Peano Axioms)

1. $0 \in \mathbb{N}$
2. $\forall n \in \mathbb{N} : s(n) \in \mathbb{N}$
3. $\forall n \in \mathbb{N} : s(n) \neq 0$
4. $\forall m, n \in \mathbb{N} : s(m) = s(n) \rightarrow m = n$
5. $\forall X [0 \in X \wedge \forall n (n \in X \rightarrow s(n) \in X) \rightarrow \forall n \in \mathbb{N} (n \in X)]$

Theorem (Dedekind-Peano Categoricity Theorem)

All models of the Dedekind-Peano axioms are isomorphic.

Exponentiation is Definable in \mathcal{N} /Representable in \mathbb{Q}

$$\pi(x, y) := (x + y)^2 + x + 1$$

$$\pi_1(z) := \mu x [\exists y \leq z : \pi(x, y) = z]$$

$$\pi_2(z) := \mu y [\exists x \leq z : \pi(x, y) = z]$$

$$\beta(s, i) := \mu x < s [\pi_1(s) \equiv x \pmod{1 + (i + 1) \cdot \pi_2(s)}]$$

$$\beta^*(s, i) := \mu x < s [\exists y < s \exists z < s : s = \pi(y, z) \wedge (1 + (\pi(x, i) + 1) \cdot z) \mid y]$$

Lemma

For every sequence $a_0, \dots, a_n \in \mathbb{N}$, $\exists s \in \mathbb{N}. \forall i \leq n. \beta(s, i) = a_i$.

Proof.

$$b := \max\{n, a_0, \dots, a_n\} \quad d := b! \quad m_i := 1 + (i + 1) \cdot d$$

m_0, \dots, m_n are pairwise coprime.

$$c := \mu x [\forall i \leq n : x \equiv a_i \pmod{m_i}] \text{ by Chinese Remainder Theorem.}$$
$$s := \pi(c, d)$$

$$x^y := \beta \left(\mu s [\beta(s, 0) = 1 \wedge \forall i < y : \beta(s, i + 1) = \beta(s, i) \cdot x], y \right)$$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Suppose m_0, \dots, m_n are pairwise coprime. Let a_0, \dots, a_n be arbitrary integers. Then there is $x \in \mathbb{Z}$ s.t. for $i \leq n$:

$$x \equiv a_i \pmod{m_i} \quad (\text{Chinese Remainder Theorem})$$

Proof.

$$M := \prod_{i=1}^n m_i \quad M_i := \frac{M}{m_i}$$

$$n_i := \mu x [x \cdot M_i \equiv 1 \pmod{m_i}]$$

$$x \equiv \sum_{i=1}^n n_i \cdot M_i \cdot a_i \pmod{m}$$

Gödel Numbering

Definition (Gödel Numbering)

A Gödel numbering is a mapping from a set of expressions to \mathbb{N} s.t.,

1. Different expressions receive different Gödel numbers. (injective)
2. The Gödel number of an expression can be effectively calculated. (computable)
3. It is effectively decidable whether a given number is a Gödel number or not. (its inverse function is computable)

ζ	()	,	\neg	\rightarrow	\forall	x_k	a_k	f_k^n	P_k^n
$\#\zeta$	3	5	7	9	11	13	$7 + 8k$	$9 + 8k$	$11 + 8(2^n 3^k)$	$13 + 8(2^n 3^k)$

$$\langle a_1, \dots, a_n \rangle := \mu x [\beta(x, 0) = n \wedge \beta(x, 1) = a_1 \wedge \dots \wedge \beta(x, n) = a_n]$$

$$or \quad \langle a_1, \dots, a_n \rangle := \prod_{i=1}^n p_i^{a_i+1}$$

Arithmetization of Syntax — Gödel Numbering

$$\#(\zeta_0 \cdots \zeta_n) := \langle \#\zeta_0, \dots, \#\zeta_n \rangle$$

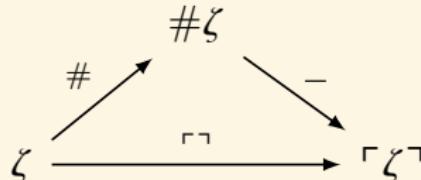
$$\ulcorner \zeta \urcorner := \underline{\#} \zeta = s^{\#\zeta} 0$$

$\text{prf}_T(y, x) :=$ "y is the code of a proof in T of the formula with code x."

$$\text{prov}_T(x) := \exists y \text{prf}_T(y, x)$$

$$\Box_T A := \text{prov}_T(\ulcorner A \urcorner)$$

Is there a wff A s.t. $T \vdash A \leftrightarrow \neg \Box_T A$?



meta-language
 $\uparrow \downarrow$
object-language

- ▶ $\text{Con}_T := \neg \Box_T \perp$
- ▶ ω -consistent: $\forall x \Box_T \neg A(\dot{x}) \rightarrow \neg \Box_T \exists x A(x)$ for any formula A
- ▶ 1-consistent: $\forall x \Box_T \neg A(\dot{x}) \rightarrow \neg \Box_T \exists x A(x)$ for $A \in \Delta_0$
- ▶ $\text{Rfn}_\Gamma(T) : \Box_T A \rightarrow A$ for any sentence $A \in \Gamma$
- ▶ $\text{RFN}_\Gamma(T) : \forall x (\Box_T A(\dot{x}) \rightarrow A(x))$ for any wff $A \in \Gamma$
- ▶ arithmetically sound: $\text{Rfn}_{\Sigma_{<\omega}}(T)$
- ▶ 1-consistent $\iff \text{Rfn}_{\Sigma_1}(T)$
- ▶ $\text{Rfn}_{\Pi_1}(T) \iff \text{RFN}_{\Pi_1}(T) \iff \text{Con}_T$

Definition (Gödelian Theory)

A theory is Gödelian iff it is

1. consistent
2. axiomatizable
3. rich enough to represent elementary arithmetic (able to represent primitive recursive functions)

Primitive Recursive Function & Recursive Function

- initial functions:

1. projection: $I_i^m(n_1, \dots, n_m) = n_i$ for $1 \leq i \leq m$
2. successor: $s(n) = n + 1$
3. zero: $z(n) = 0$

- composition: given g, h_1, \dots, h_k ,

$$f(\mathbf{x}) = g(h_1(\mathbf{x}), \dots, h_k(\mathbf{x}))$$

- primitive recursion: given g, h ,

$$f(\mathbf{x}, 0) = g(\mathbf{x})$$

$$f(\mathbf{x}, n + 1) = h(\mathbf{x}, n, f(\mathbf{x}, n))$$

- regular μ -operation: given g , and $\forall \mathbf{x} \exists y [g(\mathbf{x}, y) = 0]$,

$$f(\mathbf{x}) = \mu y [g(\mathbf{x}, y) = 0]$$

Partial Recursive Function

- μ -operation: given g ,

$$f(\mathbf{x}) = \mu y [g(\mathbf{x}, y) = 0]$$

where

$$\mu y [g(\mathbf{x}, y) = 0] = n \iff g(\mathbf{x}, n) = 0 \wedge \forall z < n (g(\mathbf{x}, z) \downarrow \neq 0)$$

bounded μ -operation: $\mu x < n [A(x)] := \mu x [A(x) \vee x = n]$

Definition (Primitive Recursive / Recursive / Partial Recursive)

The class of primitive recursive functions (**recursive functions**, **partial recursive functions**) is the smallest class of functions containing the initial functions and closed under composition, primitive recursion (**regular μ -operation**, **μ -operation**).

Ackermann Function

Definition (Ackermann Function)

$$A(m, n) := \begin{cases} n + 1 & \text{if } m = 0 \\ A(m - 1, 1) & \text{if } m > 0 \text{ and } n = 0 \\ A(m - 1, A(m, n - 1)) & \text{if } m > 0 \text{ and } n > 0 \end{cases}$$

Theorem

The Ackermann function is recursive but not primitive recursive.

$$a \uparrow^n b := \begin{cases} ab & \text{if } n = 0 \\ (a \uparrow^{n-1})^b 1 & \text{if } n \geq 1 \end{cases}$$

$$a \uparrow b = a^b \quad a \uparrow\uparrow b = \underbrace{a \uparrow (a \uparrow (\cdots \uparrow a))}_b 1 = \underbrace{\overbrace{a^a}^{\cdot \cdot \cdot \cdot \cdot}}_{b \text{ copies of } a}$$

$$A(m, n) = 2 \uparrow^{m-2} (n + 3) - 3$$

The Representability Theorem

A function/relation is representable in Robinson Q iff it is computable.

(proof sketch.) We have to show that all initial functions are representable, and the representable functions are closed under composition, regular μ -operation and primitive recursion.

Remark: To show that the set of representable functions is closed under primitive recursion, we can't use x^y and p_n , since they are defined by primitive recursion.

$$f(\mathbf{x}, 0) = g(\mathbf{x})$$

$$f(\mathbf{x}, n + 1) = h(\mathbf{x}, n, f(\mathbf{x}, n))$$

we can code the sequence of values of f from 0 to y by Gödel's β function:

$$F(\mathbf{x}, y) = \mu z [\beta(z, 0) = g(\mathbf{x}) \wedge \forall i < y : \beta(z, i + 1) = h(\mathbf{x}, i, \beta(z, i))]$$

$$f(\mathbf{x}, y) = \beta(F(\mathbf{x}, y), y)$$

Kleene Normal Form Theorem

Theorem (Kleene Normal Form Theorem)

There is a primitive recursive function U and primitive recursive predicates T , s.t. for every partial recursive function f , there is an index e s.t.

- $f(\mathbf{x}) \downarrow \iff \exists y T(e, \mathbf{x}, y)$
- $f(\mathbf{x}) = U(\mu y T(e, \mathbf{x}, y))$

$T(e, \mathbf{x}, y) :=$ “ y is the code number of some computation according to program P_e with input \mathbf{x} .”

$U(y) :=$ “the number of 1's in the final configuration of y .”

Definition

φ_e is the e^{th} partial recursive function^a:

$$\varphi_e(\mathbf{x}) := U(\mu y T(e, \mathbf{x}, y))$$

^aSometimes we write $\llbracket e \rrbracket$ for φ_e .

Incompleteness Theorem

- The function \bar{f} is a *completion* of a partial function f iff \bar{f} is total and $\forall n : f(n) \downarrow \implies f(n) = \bar{f}(n)$.
- A partial function f is *potentially recursive* iff it has a completion which is recursive.

Not every partial recursive function is potentially recursive.

$$f(n) := \varphi_n(n) + 1$$

Theorem (Incompleteness Theorem)

Any ω -consistent Gödelian T is incomplete.

Proof.

Suppose T is represented in T by γ .

$$\bar{\varphi}_e(n) := \begin{cases} U(\mu y T(e, n, y)) & \text{if } \exists y T(e, n, y) \\ 0 & \text{if } T \vdash \forall y \neg \gamma(e, n, y) \end{cases}$$

Enumeration Theorem & *smn* Theorem

Theorem (Enumeration Theorem)

The sequence $\{\varphi_e^n\}_{e \in \omega}$ is a partial recursive enumeration of the n -ary partial recursive functions, in the sense that:

- ▶ for each e , φ_e^n is a partial recursive function of n variables.
- ▶ if ψ is a partial recursive function of n variables, then there is e s.t. $\psi = \varphi_e^n$.
- ▶ there is a partial recursive function φ of $n + 1$ variables s.t. $\varphi(e, \mathbf{x}) = \varphi_e(\mathbf{x})$.

Theorem (*smn* Theorem / Parameter Theorem)

For any $m, n > 0$, there exists a primitive recursive function s_n^m of $m + 1$ arguments s.t. for every Gödel number e of a partial recursive function with $m + n$ arguments

$$\varphi_{s_n^m(e, x_1, \dots, x_m)}(y_1 \dots y_n) = \varphi_e(x_1, \dots, x_m, y_1, \dots, y_n)$$

Acceptable Numbering

Definition (Acceptable Numbering)

A numbering ψ is acceptable iff there are recursive functions f, g s.t.

$$\psi_e = \varphi_{f(e)} \quad \text{and} \quad \varphi_e = \psi_{g(e)}$$

Theorem

A numbering is acceptable iff it satisfies both enumeration and smn.

Theorem (Rogers' Equivalence Theorem)

ψ is an acceptable numbering iff there is a recursive permutation h s.t.

$$\psi_e = \varphi_{h(e)}$$

Theorem (Blum)

If ψ is an acceptable numbering, then there is a recursive permutation h s.t.

$$h(\psi_e(x)) = \varphi_{h(e)}(h(x))$$

Programming Languages

- ▶ A set Prog of programs.
- ▶ A set D of data on which programs operate.
- ▶ A pairing operation $\langle \cdot, \cdot \rangle : D^2 \rightarrow D$.
- ▶ A semantic function

$$[\![\cdot]\!] : \text{Prog} \rightarrow [D \multimap D]$$

which maps programs to partial functions on data.

Assume there is a function $\lceil \cdot \rceil : \text{Prog} \rightarrow D$ which represents program texts as data items.

Universal Turing Machine

There is a program $\text{eval} \in \text{Prog}$ such that for all $P \in \text{Prog}$ and $d \in D$

$$[\![\text{eval}]\!](\langle \lceil P \rceil, d \rangle) = [\![P]\!](d)$$

Theorem (*smn* Theorem / Parameter Theorem)

There is a primitive recursive function $[\![\text{spec}]\!]$ s.t. for every Gödel number e of a partial recursive function

$$[\![[\![\text{spec}]\!](e, x)]\!](y) = [\![e]\!](x, y)$$

Futamura Projections

- The first Futamura projection.

$$\begin{aligned} \text{target} &:= \llbracket \text{spec} \rrbracket(\text{int}, \text{source}) \\ \text{out} = \llbracket \text{source} \rrbracket(\text{in}) &= \llbracket \text{int} \rrbracket(\text{source}, \text{in}) && (\text{Definition of an interpreter}) \\ &= \llbracket \llbracket \text{spec} \rrbracket(\text{int}, \text{source}) \rrbracket(\text{in}) && (\text{Definition of a specializer}) \\ &= \llbracket \text{target} \rrbracket(\text{in}) \end{aligned}$$

- Compiler generation by the second Futamura projection.

$$\begin{aligned} \text{compiler} &:= \llbracket \text{spec} \rrbracket(\text{spec}, \text{int}) \\ \text{target} = \llbracket \text{spec} \rrbracket(\text{int}, \text{source}) &= \llbracket \llbracket \text{spec} \rrbracket(\text{spec}, \text{int}) \rrbracket(\text{source}) \\ &= \llbracket \text{compiler} \rrbracket(\text{source}) \end{aligned}$$

- Compiler generator generation by the third Futamura projection.

$$\begin{aligned} \text{cogen} &:= \llbracket \text{spec} \rrbracket(\text{spec}, \text{spec}) \\ \text{compiler} = \llbracket \text{spec} \rrbracket(\text{spec}, \text{int}) &= \llbracket \llbracket \text{spec} \rrbracket(\text{spec}, \text{spec}) \rrbracket(\text{int}) \\ &= \llbracket \text{cogen} \rrbracket(\text{int}) \end{aligned}$$

Futamura Projections

$$\begin{array}{lll} \text{out} & = & \llbracket \text{int} \rrbracket(\text{source}, \text{in}) \\ \text{target} & = & \llbracket \text{spec} \rrbracket(\text{int}, \text{source}) \\ \text{compiler} & = & \llbracket \text{spec} \rrbracket(\text{spec}, \text{int}) \\ \text{cogen} & = & \llbracket \text{spec} \rrbracket(\text{spec}, \text{spec}) \end{array} \quad \begin{array}{lll} & = & \llbracket \text{target} \rrbracket(\text{in}) \\ & = & \llbracket \text{compiler} \rrbracket(\text{source}) \\ & = & \llbracket \text{cogen} \rrbracket(\text{int}) \\ & = & \llbracket \text{cogen} \rrbracket(\text{spec}) \end{array}$$

- A program int is an interpreter iff for program p and data d :

$$\llbracket \text{int} \rrbracket(p, d) = \llbracket p \rrbracket(d)$$

- A program compiler is a compiler iff for program p and data d :

$$\llbracket \llbracket \text{compiler} \rrbracket(p) \rrbracket(d) = \llbracket p \rrbracket(d)$$

- A program spec is a specializer iff for program p and data x, y :

$$\llbracket \llbracket \text{spec} \rrbracket(p, x) \rrbracket(y) = \llbracket p \rrbracket(x, y)$$

Interpreter vs Compiler

- $\text{int} = \lambda p. \lambda d. \text{compiler}(p)(d)$
- $\text{compiler} = \text{cogen}(\text{int})$

Remark: Self-printing programs and self-generating compilers generators are two disjoint program classes.

Kleene's Fixpoint Theorem

Theorem (Kleene's Fixpoint Theorem)

Given a recursive function h , there is an index e s.t.

$$\varphi_e = \varphi_{h(e)}$$

Corollary (Second Recursion Theorem)

If $f(x, y)$ is a partial recursive function, there is an index e s.t.

$$\varphi_e(y) = f(e, y)$$

Proof.

By the smn theorem, $\varphi_{s(x)}(y) = f(x, y)$. Then

$$\exists e : \varphi_e(y) = \varphi_{s(e)}(y) = f(e, y)$$

Theorem (Kleene's Relativized Fixpoint Theorem (with Parameters))

Let $A \subset \mathbb{N}$. If $f(x, y)$ is an A -computable function, then there is a computable function $e(y)$ s.t. $\varphi_{e(y)}^A = \varphi_{f(e(y), y)}^A$ for all y . Moreover, e does not depend on A .

Proof.

Let the index e code the function

$$\varphi_e^A(x, y, z) = \begin{cases} \varphi_{\varphi_x(x, y)}^A(z) & \text{if } \varphi_x(x, y) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

By the relativized *smn* theorem there is a computable function $s(x, y)$ s.t.

$$\varphi_{s(x, y)}^A = \varphi_e^A(x, y, z)$$

We know $\exists v : \varphi_v^A(x, y) = f(s(x, y), y)$. Let $e(y) := s(v, y)$.

$$\varphi_{e(y)}^A = \varphi_{s(v, y)}^A = \varphi_{\varphi_v^A(v, y)}^A = \varphi_{f(s(v, y), y)}^A = \varphi_{f(e(y), y)}^A$$

Rice's Theorem

Theorem (Rice's Theorem)

A set of partial recursive functions \mathcal{A} is recursive iff it is trivial, i.e. either $A = \emptyset$ or $A = \omega$, where $A := \{x : \varphi_x \in \mathcal{A}\}$.

Proof.

Let $a \in A$ and $b \notin A$.

$$h(x) := \begin{cases} a & \text{if } x \notin A \\ b & \text{if } x \in A \end{cases}$$

Obviously, h is recursive, and $\forall x : x \in A \leftrightarrow h(x) \notin A$.

By Kleene's fixpoint theorem, $\exists e : \varphi_e = \varphi_{h(e)}$.

Hence $e \in A \iff h(e) \in A$. Contradiction.

Recursion Theorem

Theorem (Second Recursion Theorem)

If $f(x, y)$ is a partial recursive function, there is an index e s.t.

$$\varphi_e(y) = f(e, y)$$

Kleene's Fixpoint Theorem \iff Second Recursion Theorem

Theorem (First Recursion Theorem)

Every partial recursive functional $F(\alpha, x)$ admits a least fixpoint. In other words, there is a partial recursive function α s.t.

1. $\forall x (\alpha(x) = F(\alpha, x))$
2. $\forall x (\beta(x) = F(\beta, x)) \implies \alpha \subset \beta$

Gödel's Speed-up Theorem

Theorem (Gödel's Speed-up Theorem)

Let $T' \supset T$ be formal systems (with recursive sets of axioms and of recursive rules) such that $T' \setminus T$ is not r.e. Given a recursive function h , there is a theorem A of T and a number n such that A admits a proof of length $\leq n$ in T' , but no proof of length $\leq h(n)$ in T .

Proposition

If T is an essentially undecidable formal system, and $T \not\vdash A$, then $T \cup \{A\} \setminus T$ is not r.e.

Remark: Adding an unprovable sentence to an essentially undecidable formal system T radically shortens some proof of some theorem of T .

Blum's Speed-up Theorem

A **Blum complexity measure** is a pair (φ, Φ) with φ a Gödel numbering of the partial computable functions $\mathbf{P}^{(1)}$ and a computable function $\Phi : \mathbb{N} \rightarrow \mathbf{P}^{(1)}$ such that

- ▶ the domains of φ_i and Φ_i are identical.
- ▶ the set $\{(i, x, t) \in \mathbb{N}^3 : \Phi_i(x) = t\}$ is recursive.

Theorem (Blum's Speed-up Theorem)

Given a Blum complexity measure (φ, Φ) and a total computable function f with two parameters, there exists a 0, 1-valued total computable function g s.t. for every index i for g , there is another index j for g s.t. for almost all x

$$f(x, \Phi_j(x)) \leq \Phi_i(x)$$

Remark: For any complexity measure there are computable functions that are not optimal with respect to that measure. There is no notion of best complexity for all total recursive functions.

Remark: No computer can be optimal for every purpose: no matter how good a computer is, there are always functions on which such a computer behaves very badly.

m-reduction

Definition (*m*-reduction)

We say that A is many-one reducible (*m*-reducible) to B , and write $A \leq_m B$, if there is a total computable function f such that for all x , we have $x \in A \iff f(x) \in B$.

Definition (1-reduction)

If the function f in the definition of *m*-reduction is injective, then we say that A is 1-reducible to B , and write $A \leq_1 B$.

Productive and Creative Sets

Definition (Productive Set)

A set A is *productive* if there is a partial recursive function f such that

$$W_e \subset A \implies f(e) \downarrow \& f(e) \in A \setminus W_e$$

Definition (Creative Set)

A r.e set A is *creative* iff its complement is productive.

Theorem

The following are equivalent:

- ▶ A is creative.
- ▶ A is m -complete (i.e., m -equivalent to \emptyset')
- ▶ A is 1-complete (i.e., 1-equivalent to \emptyset')

Theorem

The set $\# \text{Th } N := \{\#A : N \models A\}$ is productive.

Immune and Simple Sets

Definition (Immune Set)

A set A is *immune* iff it is infinite and contains no infinite r.e. subsets.

Definition (Simple Set)

A r.e. set A is *simple* iff its complement is immune.

$$W_e \text{ infinite} \implies W_e \cap A \neq \emptyset$$

Theorem

The set of non-random numbers $\{x : K(x) < \ell(x)\}$ is simple.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory
Turing Machine

Computability

Diagonal Method

Incompressibility Method

Incompleteness

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Self-reference

- ▶ This sentence repeats the word ‘twice’ twice.
- ▶ Thare are five mistukes im this centence.
- ▶ **The only boldface sentence on this page is false.**
- ▶ All generalizations are wrong.
- ▶ Every rule has an exception except this one.
- ▶ Moderation in all things, including moderation.
- ▶ We must believe in free will — we have no choice!
- ▶ I know that I know nothing.
- ▶ There are two rules lor success in life:
 1. Never tell anyone all that you know.
- ▶ If you choose an answer to this question at random, what is the chance you will be correct? (A) 25% (B) 50% (C) 60% (D) 25%
- ▶
 1. What is the best question to ask and what is the answer to it?
 2. The best question is the one you asked; the answer is the one I gave.
- ▶ Can you answer the following question in the same way to this one?
- ▶ One of the lessons of history is that no one ever learns the lessons of history.



Self-reference vs Paradox

The sentence below is false.



The sentence above is true.

Yablo Paradox

- ▶ S_1 : for all $k > 1$, S_k is false.
- ▶ S_2 : for all $k > 2$, S_k is false.
- ▶ S_3 : for all $k > 3$, S_k is false.
- ▶ ...

Quine Paradox

“Yields falsehood when preceded by its quotation” yields falsehood when preceded by its quotation.

self-reference / circularity or infinite regress / negation / infinity / totality

The “Power” of Self-reference

Curry's Paradox

- ▶ If this sentence is true, then God exists.
- ▶ This sentence is false, and God does not exist.

1. At least one of these two sentences is false.
2. God does not exists.

Hi 美女，问你个问题呗

如果我问你“你能做我女朋友吗”，那么你的答案能否和这个问题本身的答案一样？

自我修复/自我实现？

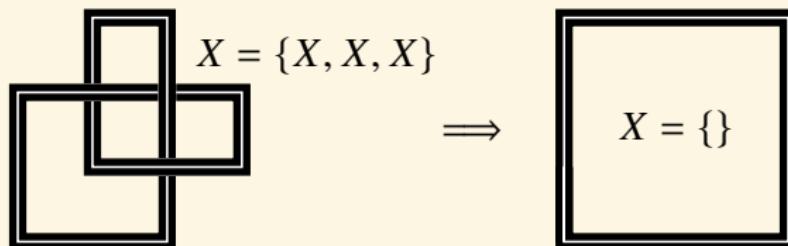
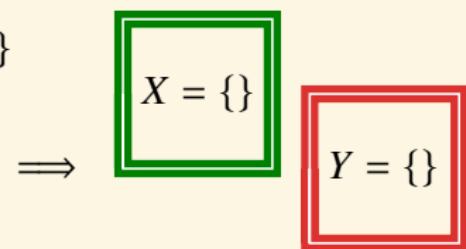
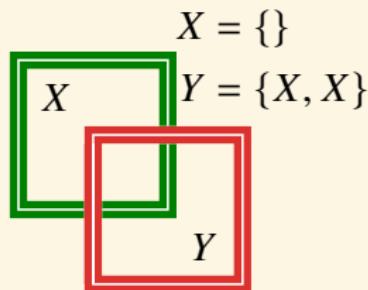
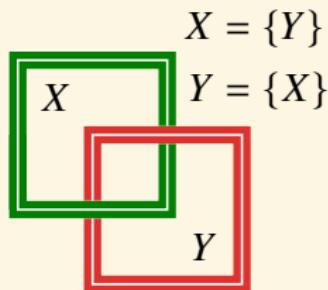
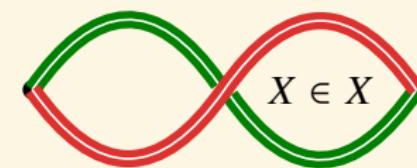
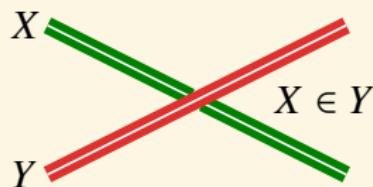
- ▶ “This sentence has _____ letters.” **thirty-one / thirty-three**
- ▶ 这句话有 2 个‘这’字，2 个‘句’字，2 个‘话’字，2 个‘有’字，7 个‘2’字，11 个‘个’字，11 个‘字’字，2 个‘7’字，3 个‘11’字，2 个‘3’字。

How to Refer?

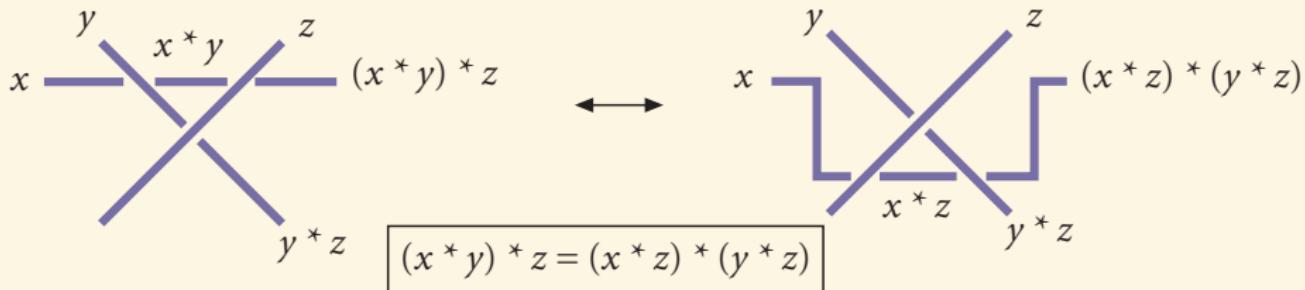
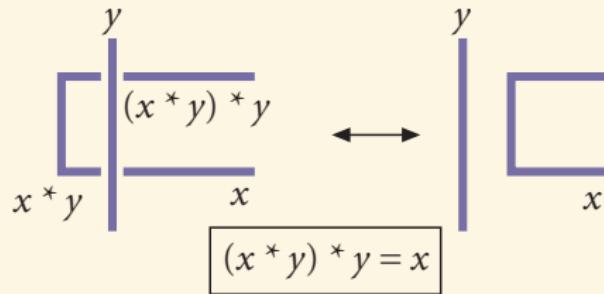
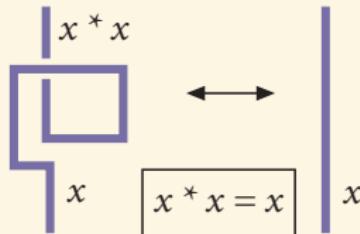


How to Refer? — Levels

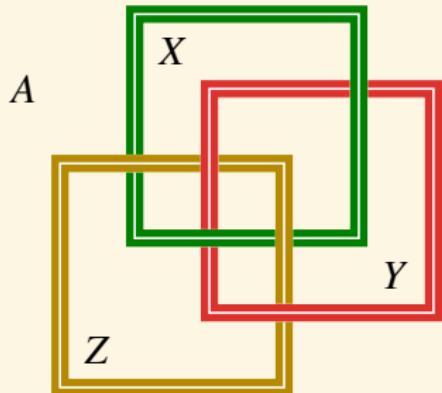




Reidemeister Moves



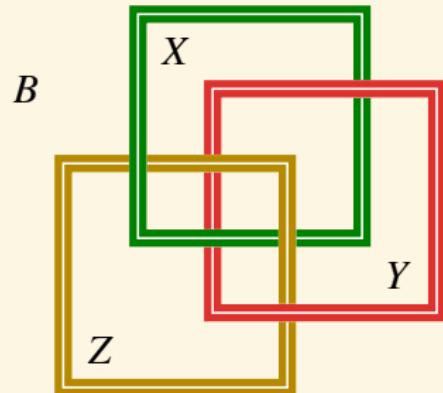
Self-reference & IIT



$$X = \{Y, Y\}$$

$$Y = \{Z, Z\}$$

$$Z = \{X, X\}$$



$$X = \{Y, Z\}$$

$$Y = \{X, Z\}$$

$$Z = \{X, Y\}$$

Figure: $\Phi(A) < \Phi(B)$?

Larger Domain

1, 1, 2, 3, 5, 8, 13, 21, 34, ...

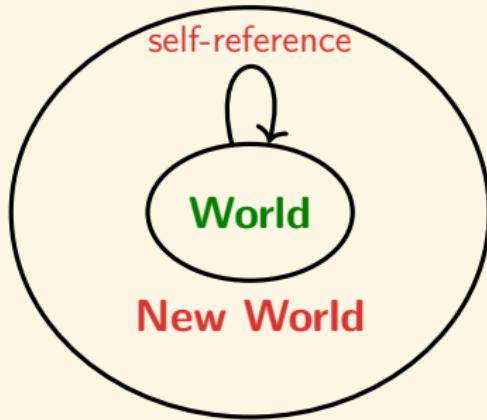
$$F_0 = F_1 = 1; F_{n+1} = F_n + F_{n-1}$$

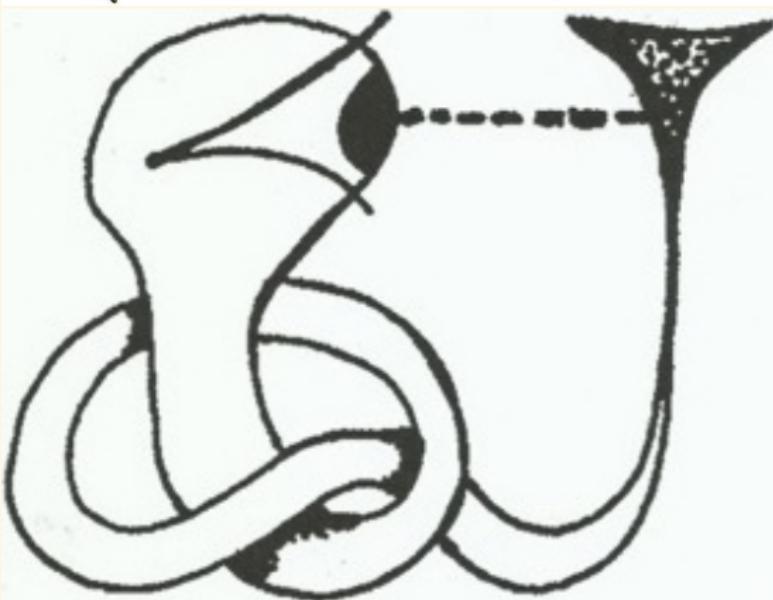
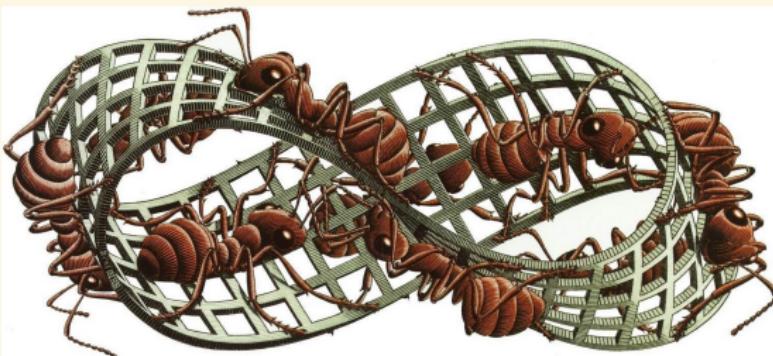
$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n}$$

$$\frac{F_{n+1}}{F_n} = 1 + \frac{1}{\frac{F_n}{F_{n-1}}}$$

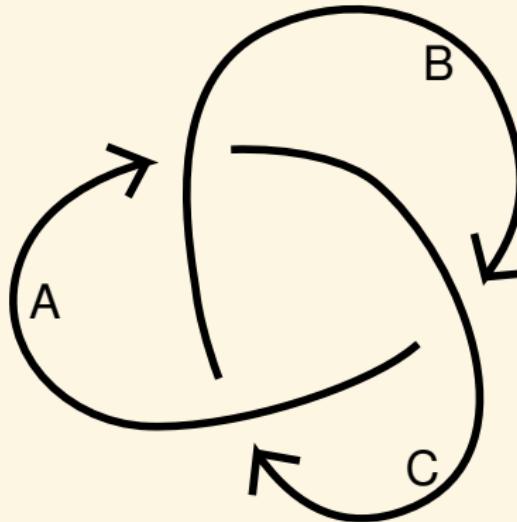
$$f(x) = 1 + \frac{1}{x} = x \implies 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}} = \frac{1 + \sqrt{5}}{2}$$

$$f(x) = \frac{-1}{x} = x \implies x = i$$





Trefoil



- ▶ objects $\{A, B, C\}$
- ▶ morphisms
 - A: $C \rightarrow B$
 - B: $A \rightarrow C$
 - C: $B \rightarrow A$

Nested Virtualization?



从前有座山，山里有座庙，庙里有个老和尚在讲故事：从前有座山…

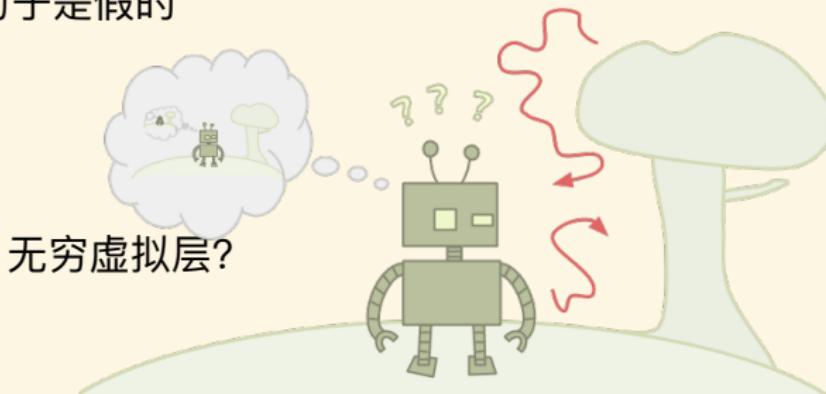
$$\begin{cases} FX = Y \\ GY = X \end{cases}$$

$X = FGFGFGFG \dots$

$Y = FGFGFGFG \dots$

Liar Paradox vs Quine Paradox

1. 这句话是假的
2. “这句话是假的”是假的
3. ““““.....是假的”是假的”是假的”是假的”是假的
4. 把“把中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变”中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变
5. 把“把中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变得到的句子是假的”中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变得到的句子是假的



How to Refer? — Encoding



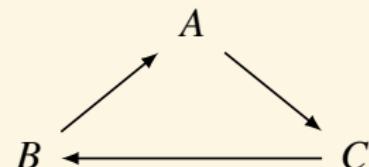
- ▶ 100 prisoners are lined up by an jailer, who places a red or blue hat upon each of their heads.
- ▶ The prisoners can see the hats of the people lined up in front of them, but they can't look at the hats behind them, or at their own.
- ▶ The jailer is going to ask color of each prisoner's hat starting from the last prisoner in queue. If a prisoner tells the correct color, then is saved, otherwise executed.
- ▶ How many prisoners can be saved at most if they are allowed to discuss a strategy before the jailer starts asking colors of their hats?

If the first person sees an **odd** number of red hats he calls out red, if he sees an **even** number of red hats he calls out blue.

手扶拐杖的外星绅士造访地球。临别，人类赠送百科全书：“人类文明尽在其中！”。绅士谢绝：“不，谢谢！我只需在拐杖上点上一点”。

What is the Next Number?

1. 1
 2. 11
 3. 21
 4. 1211
 5. 111221
 6. 312211
 7. ?
- A. 11131221131211132221...
- B. 3113112221131112311332...
- C. 132113213221133112132123...



Diagonalization¹⁴

Definition (Point-Surjective)

A morphism $f : X \rightarrow Y$ is *point-surjective* iff for every $y : 1 \rightarrow Y$, there is an $x : 1 \rightarrow X$ s.t. $y = f \circ x$.

Theorem (Lawvere's Fixpoint Theorem)

In a cartesian closed category, if there is a point-surjective morphism $f : X \rightarrow Y^X$, then every morphism $\alpha : Y \rightarrow Y$ has a fixpoint $y : 1 \rightarrow Y$.

$$\begin{array}{ccc} X \times Y^X & \xrightarrow{\varepsilon} & Y \\ 1_X \times f \uparrow & \nearrow \hat{f} & \downarrow \alpha \\ X \times X & & \\ \Delta \uparrow & & \\ X & \xrightarrow{g} & Y \end{array}$$



¹⁴ Lawvere: Diagonal arguments and cartesian closed categories.

Yanofsky: A universal approach to self-referential paradoxes, incompleteness and fixed points.

Lawvere's Fixpoint Theorem

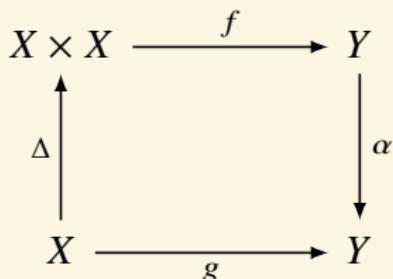
- A function $g : X \rightarrow Y$ is *representable* by $f : X \times X \rightarrow Y$ iff

$$\exists y \forall x : g(x) = f(x, y)$$

Theorem (Lawvere's Fixpoint Theorem)

For sets X, Y , functions $f : X \times X \rightarrow Y$, $\alpha : Y \rightarrow Y$, let $g := \alpha \circ f \circ \Delta$.

1. If α has no fixpoint, then g is not representable by f .
2. If g is representable by f , then α has a fixpoint.



$$\alpha(f(\lceil g \rceil, \lceil g \rceil)) = g(\lceil g \rceil) = f(\lceil g \rceil, \lceil g \rceil)$$

- $\Delta : x \mapsto \langle x, x \rangle$ diagonal
- f evaluation
- α “negation”
- $g (\lceil g \rceil)$ fixpoint-(free) transcendence
- $f (\lceil g \rceil, \lceil g \rceil)$ self-reference
“I have property α .”

Lawvere's Fixpoint Theorem

f	0	1	2	3	\dots	t	\dots
0	$\alpha f(0, 0)$	\dots	\dots	\dots	\dots	$f(0, t)$	\dots
1	\dots	$\alpha f(1, 1)$	\dots	\dots	\dots	$f(1, t)$	\dots
2	\dots	\dots	$\alpha f(2, 2)$	\dots	\dots	$f(2, t)$	\dots
3	\dots	\dots	\dots	$\alpha f(3, 3)$	\dots	$f(3, t)$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
t	\dots	\dots	\dots	\dots	\dots	<div style="border: 1px solid black; padding: 5px; text-align: center;">$f(t, t)$ $\alpha f(t, t)$</div>	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

Diagonalization

- A function $g : X \rightarrow Z$ is *representable* by $f : X \times Y \rightarrow Z$ iff

$$\exists y \in Y \forall x \in X : g(x) = f(x, y)$$

Theorem (Lawvere's Fixpoint Theorem)

For all sets X, Y, Z , and all functions $f : X \times Y \rightarrow Z$, $\alpha : Z \rightarrow Z$, surjective functions $\beta : X \twoheadrightarrow Y$, let $g := \alpha \circ f \circ \langle 1_X, \beta \rangle$.

1. If α has no fixpoint, then g is not representable by f .
2. If g is representable by f , then α has a fixpoint.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \uparrow \langle 1_X, \beta \rangle & & \downarrow \alpha \\ X & \xrightarrow{g} & Z \end{array}$$

Lawvere's Fixpoint Theorem — Multi-Valued Version

- A *multi-valued function* $f : X \rightrightarrows Y$ is a function $f : X \rightarrow \mathcal{P}(Y)$ s.t.
 $\forall x \in X \exists y \in Y : y \in f(x).$

Theorem (Lawvere's Fixpoint Theorem — multi-valued version)

For sets X, Y, Z , multi-valued functions $f : X \times Y \rightrightarrows Z$, $\alpha : Z \rightrightarrows Z$, and surjective function $\beta : X \twoheadrightarrow Y$,

$$\exists y \forall x (\alpha \circ f \circ \langle 1_X, \beta \rangle x \cap f(x, y) \neq \emptyset) \rightarrow \exists z \in \alpha(z)$$

Proof.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \uparrow \langle 1_X, \beta \rangle & & \downarrow \alpha \\ X & \xrightarrow{\quad} & Z \end{array}$$

$$\beta x = y \implies \alpha(f(x, y)) \cap f(x, y) \neq \emptyset$$

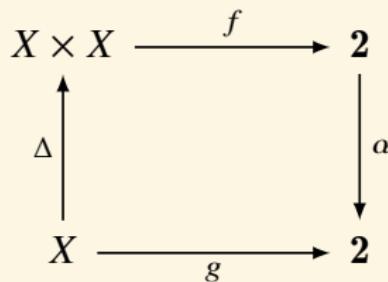
Approximate Version

Theorem (Approximate Version)

Suppose (Z, d) is a metric space. Given $f : X \times Y \rightarrow Z$, $\alpha : Z \rightarrow Z$, and surjective $\beta : X \twoheadrightarrow Y$, let $g := \alpha \circ f \circ \langle 1_X, \beta \rangle$. If g is ε -representable by f :
 $\exists y \in Y \forall x \in X : d(f(x, y), g(x)) < \varepsilon$, then α has ε -fixpoint:
 $\exists z \in Z : d(z, \alpha(z)) < \varepsilon$.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \uparrow \langle 1_X, \beta \rangle & & \downarrow \alpha \\ X & \xrightarrow{g} & Z \end{array}$$

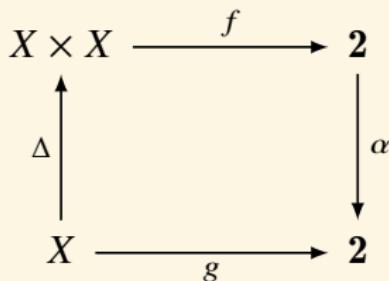
Example — Grelling/Liar/Quine... Paradox



where $f : (x, y) \mapsto [\![y \text{ "describes" } x]\!]$ and $\alpha : x \mapsto 1 - x$.

- ▶ Is “non-self-descriptive” non-self-descriptive?
- ▶ “This sentence is false.”
- ▶ “Yields falsehood when preceded by its quotation” yields falsehood when preceded by its quotation.

Example — Russell Paradox



where

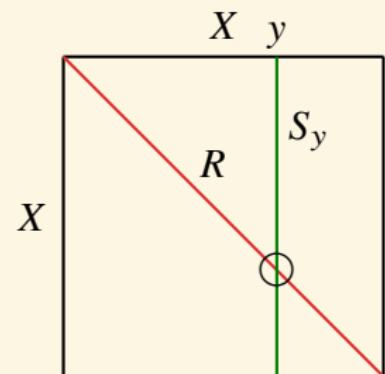
$$f : (x, y) \mapsto [\![x \in y]\!]$$

and

$$\alpha : x \mapsto 1 - x$$

$$R := \{x : x \notin x\} \quad \text{exist?}$$

Barber paradox: $f : (x, y) \mapsto [\![y \text{ "shaves" } x]\!]$



Let $S \subset X \times X$

$$S_y := \{x : Sxy\}$$

$$R := \{x : x \notin S_x\}$$

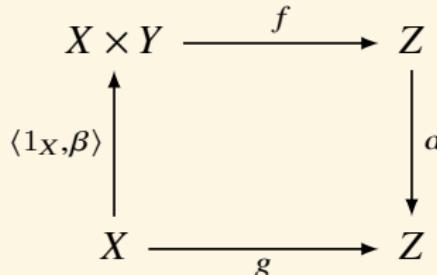
$$\forall x : R \neq S_x$$

Example — Russell/Barber Paradox

f	S_0	S_1	S_2	S_3	\cdots	S_t	\cdots
S_0	0	1	0	1	\cdots	1	\cdots
S_1	1	1	0	0	\cdots	0	\cdots
S_2	0	1	0	0	\cdots	1	\cdots
S_3	0	0	0	1	\cdots	0	\cdots
\vdots							
S_t	0	0	0	0	\cdots	?	\cdots
\vdots	\ddots						

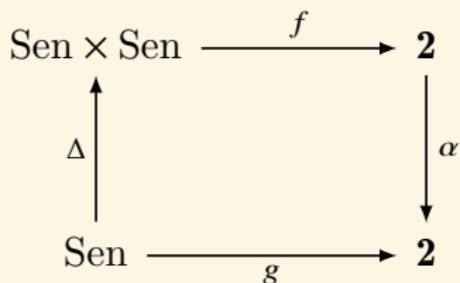
Example — Wittgenstein/Kripke Paradox

- ▶ X : word space.
- ▶ Y : rule space.
- ▶ Z : meaning space.
- ▶ $g \in Z^X$ is finding a meaning.
- ▶ In naive realism, it is assumed that the meaning is certain.
- ▶ What we assume, that a meaning found for a word is certain, is something we do not have to consider another possibility of a meaning. Namely, $\forall g \in Z^X \exists y \in Y : g = \lambda x. f(x, y)$.
- ▶ In the context of Wittgenstein/Kripke, what we can by no means deny as another possibility for a meaning is expressed by infinite regression. It is formally replaced by a fixpoint.



Example — Yablo Paradox in Linear Temporal Logic(LTL)

$$\begin{array}{lll} n \models A \wedge B & \iff & n \models A \& n \models B \\ n \models \neg A & \iff & n \not\models A \\ n \models \circ A & \iff & n+1 \models A \\ n \models \Box A & \iff & \forall m \geq n \implies m \models A \end{array}$$



$$f : (X, Y) \mapsto [\![X \leftrightarrow \circ \Box \neg Y]\!] \quad \text{and} \quad \alpha : x \mapsto 1 - x$$

Theorem

For any wff A , LTL $\not\models A \leftrightarrow \circ \Box \neg A$.

Example — Euclid's Theorem?

Theorem (Euclid's Theorem)

There are infinitely many prime numbers.

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f} & 2 \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & 2 \end{array}$$

where

$$f(m, n) = \begin{cases} 1 & \forall p \in \mathbb{P} : p | (m! + 1) \rightarrow p < n \\ 0 & \text{otherwise} \end{cases}$$

and $\alpha : x \mapsto 1 - x$.

Obviously, $\forall n : f(n, n) = 0$, and $g(n) = \alpha(f(n, n)) = 1$.

If $|\mathbb{P}| < \infty$, let $t := \max \mathbb{P} + 1$, then $\forall n : f(n, t) = 1$ and $\forall n : g(n) = f(n, t)$.

Therefore, $f(t, t)$ is a fixpoint of α . Contradiction!

A Complete List of All Great Mathematicians

D e M o r g a n

A b e l

B o o l e

B r o u w e r

S i e r p i n s k i

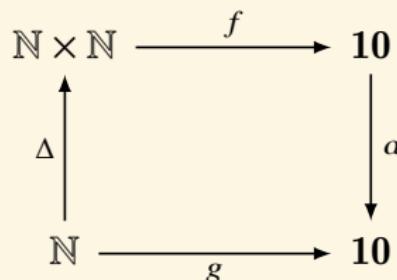
W e i e r s t r a s s

Cantor

Example — The set of real numbers is uncountable

Theorem (Cantor)

\mathbb{R} is uncountable.



where $f : (m, n) \mapsto r_{mn} :=$ “the n^{th} digit of the m^{th} real” and
 $\alpha : x \mapsto 9 - x$.

- There exists uncomputable real $\sum_n g(n)10^{-n}$, where

$$f : (m, n) \mapsto r_{mn} := \begin{cases} \text{the } n^{\text{th}} \text{ digit output by the } m^{\text{th}} \text{ Turing machine} \\ 0 \text{ if the } m^{\text{th}} \text{ Turing machine never outputs a } n^{\text{th}} \text{ digit} \end{cases}$$

- Richard paradox(unnameable real):

$$f : (m, n) \mapsto r_{mn} := \text{“the } n^{\text{th}} \text{ digit of the real named by the } m^{\text{th}} \text{ sentence”}$$

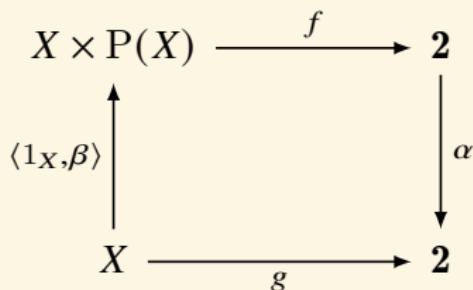
Example — The set of real numbers is uncountable

r_{mn}	0	1	2	3	4	5	\dots	t	\dots
0	5	7	2	7	7	4	\dots	3	\dots
1	1	2	2	7	6	7	\dots	1	\dots
2	3	0	3	0	0	0	\dots	8	\dots
3	6	2	0	4	2	0	\dots	0	\dots
4	1	0	2	3	1	3	\dots	5	\dots
5	1	0	3	0	1	0	\dots	4	\dots
\vdots									
t	4	7	6	5	8	9	\dots	?	\dots
\vdots	\ddots								

Example — Cantor's Theorem

Theorem (Cantor's Theorem)

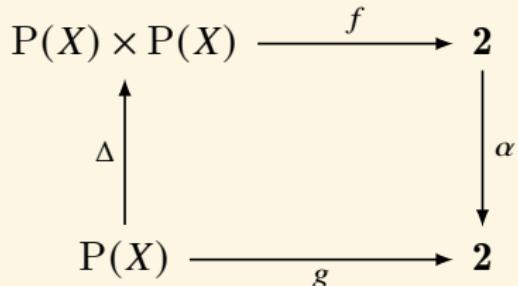
$$|X| < |P(X)|$$



where $f : (x, y) \mapsto [\![h(x) \in y]\!]$ and
 $\alpha : x \mapsto 1 - x$.

β is not surjective.

another proof: assume $h : P(X) \rightarrow X$.



where $f : (x, y) \mapsto [\![h(x) \in y]\!]$, and
 $\alpha : x \mapsto 1 - x$.

g is representable by
 $y := \{h(x) : x \subset X \text{ & } h(x) \notin x\}$.

Example — Cantor's Theorem — another proof

If $|X| \geq |\mathcal{P}(X)|$, then there exists some enumeration $\{S_i\}_{i \in X}$ of $\mathcal{P}(X)$.

$$\begin{array}{ccc} X \times \{S_i\}_{i \in X} & \xrightarrow{f} & 2 \\ \Delta \uparrow & & \downarrow \alpha \\ X & \xrightarrow{g} & 2 \end{array}$$

where $f : (x, y) \mapsto [\![x \in S_y]\!]$ and $\alpha : x \mapsto 1 - x$.

$$g : x \mapsto [\![x \notin S_x]\!]$$

Since $\{S_i\}_{i \in X}$ is the enumeration of $\mathcal{P}(X)$, the set $R := \{x : x \notin S_x\}$ that g characterizes must be some S_t : $\exists t(R = S_t)$. It means g is representable by t . Contradiction!

Example — Cantor's Theorem — another proof

f	S_0	S_1	S_2	S_3	\cdots	S_t	\cdots
0	0	1	0	1	\cdots	1	\cdots
1	1	1	1	1	\cdots	0	\cdots
2	0	1	0	0	\cdots	1	\cdots
3	0	1	1	1	\cdots	0	\cdots
\vdots							
t	1	0	1	0	\cdots	?	\cdots
\vdots	\ddots						

Example — Cantor's Theorem

Theorem (Cantor's Theorem)

For $|Y| \geq 2$,

$$|X| < |Y^X|$$

$$\begin{array}{ccc} X \times X & \xrightarrow{f} & Y \\ \Delta \uparrow & & \downarrow \alpha \\ X & \xrightarrow{g} & Y \end{array}$$

where α is the cyclic permutation.

Every $g : X \rightarrow Y$ is representable by some $f : X \times X \rightarrow Y$ iff $\exists f : X \twoheadrightarrow Y^X$.

If there exists $f : X \twoheadrightarrow Y^X$, then every $\alpha : Y \rightarrow Y$ has a fixpoint.

Example — Continuous Functions

- ▶ Since a continuous function on \mathbb{R} is determined by its values at rational points, the set of continuous functions $|C(\mathbb{R}, \mathbb{R})| = |\mathbb{R}|$. However, there is no continuous surjection $\mathbb{R} \twoheadrightarrow C(\mathbb{R}, \mathbb{R})$ from the real line to the Banach space of continuous real functions, equipped with the sup-norm $\|f\|_\infty = \sup_{x \in \mathbb{R}} |f(x)|$.

$$\begin{array}{ccc} \mathbb{R} \times C(\mathbb{R}, \mathbb{R}) & \xrightarrow{\mathcal{F}} & \mathbb{R} \\ \uparrow \langle 1_{\mathbb{R}}, \beta \rangle & & \downarrow \alpha \\ \mathbb{R} & \xrightarrow{g} & \mathbb{R} \end{array}$$

where $\mathcal{F} : (x, f) \mapsto f(x)$ and $\alpha : x \mapsto x + 1$.

- ▶ For most spaces X , there is no space-filling curve for its path space, $f : I \rightarrow X^I$.

Example — total recursive but not primitive recursive

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f} & \mathbb{N} \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & \mathbb{N} \end{array}$$

where $f : (m, n) \mapsto \psi_n(m)$ and $\alpha : x \mapsto x + 1$.

$$g : n \mapsto \psi_n(n) + 1$$

or, let $f : (m, n) \mapsto \max_{k \leq n} \psi_k(m)$.

Similarly, let $f : (m, n) \mapsto \max_{k \leq n} \varphi_k(m)$ then we get a busy beaver function.

Example — Berry Paradox vs Busy Beaver

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f_\varphi} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \end{array}$$

where $f_\varphi : (m, n) \mapsto \varphi_n(m)$, and $\alpha : \varphi_n(m) \mapsto \min(\mathbb{N} \setminus \{\varphi_k(m) : k \leq n\})$

$$g(m) = \min(\mathbb{N} \setminus \{\varphi_k(m) : k \leq m\}) = \mu n [K(n \mid m) > m]$$

g unrepresentable $\implies g$ uncomputable $\implies K$ uncomputable

$$\Sigma(m) := \max\{\varphi_k(0) : k \leq m\} = \max\{n : K(n) \leq m\}$$

Example — Not every partial recursive function is potentially recursive

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f_\varphi} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \end{array}$$

where $f_\varphi : (m, n) \mapsto \varphi_n(m)$, and $\alpha : x \mapsto x + 1$

$$g : m \mapsto \varphi_m(m) + 1$$

g partial recursive $\implies g$ representable $\implies \alpha(g(\ulcorner g \urcorner)) = g(\ulcorner g \urcorner) \uparrow$

for any partial recursive $\bar{g} \supset g : \bar{g}(\ulcorner \bar{g} \urcorner) \uparrow$.

$$\bar{g}(\ulcorner \bar{g} \urcorner) = \varphi_{\ulcorner \bar{g} \urcorner}(\ulcorner \bar{g} \urcorner) = g(\ulcorner \bar{g} \urcorner) = \varphi_{\ulcorner \bar{g} \urcorner}(\ulcorner \bar{g} \urcorner) + 1$$

Example — Turing's Halting Problem

Theorem (Turing 1936)

The Halting problem is unsolvable.

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{H} & 2 \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & 2 \end{array}$$

where $H : (m, n) \mapsto [\![m \in W_n]\!]$, and $\alpha : x \mapsto 1 - x$.

However, if H is total computable, then g is total computable and representable by H . Contradiction!

Example — Turing's Halting Problem

H	W_0	W_1	W_2	W_3	\dots	W_t	\dots
0	0	1	0	1	\dots	1	\dots
1	1	1	0	0	\dots	0	\dots
2	0	1	0	0	\dots	1	\dots
3	0	0	0	1	\dots	0	\dots
\vdots							
t	0	0	0	0	\dots	?	\dots
\vdots	\ddots						

Remark: “Russell Paradox” — The set $\overline{K} = \{n : n \notin W_n\}$ of numbers not belonging to the r.e. sets they code is not r.e. itself $\forall t : \overline{K} \neq W_t$.

Example — Turing's Halting Problem

Theorem (Turing 1936)

The Halting problem is unsolvable.

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{H} & 2 \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & 2 \end{array}$$

where $H : (m, n) \mapsto [\![\varphi_n(m) \downarrow]\!]$, and $\alpha(x) = \begin{cases} 1 & \text{if } x = 0 \\ \uparrow & \text{otherwise} \end{cases}$.

$$H(\ulcorner g \urcorner, \ulcorner g \urcorner) \uparrow$$

There is no perfect anti-virus software.

Example — Turing's Halting Problem

$H(m, n)$	0	1	2	3	\dots	t	\dots
0	1	1	0	0	\dots	0	\dots
1	1	0	1	1	\dots	1	\dots
2	0	1	1	0	\dots	0	\dots
3	0	1	1	0	\dots	1	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
t	1	0	1	0	\dots		\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

Example — Turing's Halting Problem — another proof

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f_\varphi} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \\ \Delta \uparrow & & \downarrow \alpha \\ \mathbb{N} & \xrightarrow{g} & \{\varphi_n(m)\}_{(m,n) \in \mathbb{N}^2} \end{array}$$

where $f_\varphi : (m, n) \mapsto \varphi_n(m)$, and

$$\alpha : \varphi_n(m) \mapsto \begin{cases} 0 & \text{if } H(m, n) = 0 \\ \varphi_n(m) + 1 & \text{if } H(m, n) = 1 \end{cases}$$

or

$$\alpha : \varphi_n(m) \mapsto 1 + \sum_{k=0}^n H(m, k) \cdot \varphi_k(m)$$

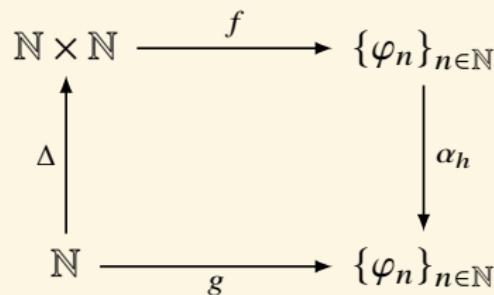
If H is total computable, then g is total computable. \times

Example — Kleene's Fixpoint Theorem

Theorem (Kleene's Fixpoint Theorem)

Given a recursive function h , there is an index e s.t.

$$\varphi_e = \varphi_{h(e)}$$



where $f : (m, n) \mapsto \varphi_{\varphi_n(m)}$, and $\alpha_h : \varphi_n \mapsto \varphi_{h(n)}$.

The function $g : m \mapsto \varphi_{h(\varphi_m(m))}$ is a recursive sequence of partial recursive functions, and thus is representable by $f(-, t)$.

$$e := \varphi_t(t)$$

Explicitly, $g(m) = \varphi_{h(\varphi_m(m))} = \varphi_{s(m)} = \varphi_{\varphi_t(m)} = f(m, t)$

Example — Kleene's Fixpoint Theorem

f	0	1	2	3	\dots	t
0	$\varphi h(\varphi_0(0))$	$\varphi \varphi_0(1)$	$\varphi \varphi_0(2)$	$\varphi \varphi_0(3)$	\dots	$\varphi \varphi_0(t)$
1	$\varphi \varphi_1(0)$	$\varphi h(\varphi_1(1))$	$\varphi \varphi_1(2)$	$\varphi \varphi_1(3)$	\dots	$\varphi \varphi_1(t)$
2	$\varphi \varphi_2(0)$	$\varphi \varphi_2(1)$	$\varphi h(\varphi_2(2))$	$\varphi \varphi_2(3)$	\dots	$\varphi \varphi_2(t)$
3	$\varphi \varphi_3(0)$	$\varphi \varphi_3(1)$	$\varphi \varphi_3(2)$	$\varphi h(\varphi_3(3))$	\dots	$\varphi \varphi_3(t)$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
t	$\varphi \varphi_0(0)$	$\varphi \varphi_1(1)$	$\varphi \varphi_2(2)$	$\varphi \varphi_3(3)$	\dots	$\varphi \varphi_t(t)$
	$\varphi h(\varphi_0(0))$	$\varphi h(\varphi_1(1))$	$\varphi h(\varphi_2(2))$	$\varphi h(\varphi_3(3))$		$\boxed{\varphi h(\varphi_t(t))}$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots

Example — Kleene's Fixpoint Theorem

Theorem (Kleene's Fixpoint Theorem)

Given a recursive function h , there is an index e s.t.

$$\varphi_e = \varphi_{h(e)}$$

Proof.

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{f} & \{\varphi_n\}_{n \in \mathbb{N}} \\ \Delta \uparrow & & \downarrow \alpha_h \\ \mathbb{N} & \xrightarrow{g} & \{\varphi_n\}_{n \in \mathbb{N}} \end{array}$$

where $f : (m, n) \mapsto \varphi_{\varphi_n(m)}$, and

$$\alpha_h : \varphi_n \mapsto \{\varphi_i : \varphi_i = \varphi_{h(n)}\}$$

Example — Y Combinator

$$\begin{array}{ccc} \Lambda \times \Lambda & \xrightarrow{f} & \Lambda \\ \Delta \uparrow & & \downarrow \alpha_y \\ \Lambda & \xrightarrow{g} & \Lambda \end{array}$$

where $f : (x, y) \mapsto yx$, and $\alpha_y : x \mapsto yx$.

$$g = \lambda x. y(xx)$$

$$gg = \alpha_y(gg)$$

$$Y := \lambda y. gg = \lambda y. (\lambda x. y(xx))(\lambda x. y(xx))$$

$$\mathbf{Y}h = h(\mathbf{Y}h) = h(h(\mathbf{Y}h)) = \dots$$

Example — Z Combinator

$$\begin{array}{ccc} \Lambda \times \Lambda & \xrightarrow{f} & \Lambda \\ \Delta \uparrow & & \downarrow \alpha_y \\ \Lambda & \xrightarrow{g} & \Lambda \end{array}$$

where $f : (x, y) \mapsto \lambda v. yxv$, and $\alpha_y : x \mapsto yx$.

$$g = \lambda x. y(\lambda v. xxv)$$

$$gg = \alpha_y(gg)$$

$$Z := \lambda y. gg = \lambda y. (\lambda x. y(\lambda v. xxv))(\lambda x. y(\lambda v. xxv))$$

$$Zhv = h(Zh)v$$

$$e := Zh \implies ev = hev \quad (\text{Kleene's fixpoint?})$$

Remark: Quine: $ev = Kev = e$.

Example — Θ Combinator

$$\begin{array}{ccc} \Lambda \times \Lambda & \xrightarrow{f} & \Lambda \\ \Delta \uparrow & & \downarrow \alpha \\ \Lambda & \xrightarrow{g} & \Lambda \end{array}$$

where $f : (x, y) \mapsto yx$, and $\alpha : x \mapsto \lambda y. y(xy)$.

$$g = \lambda xy. y(xxy)$$

$$gg = \alpha(gg)$$

$$\Theta := gg = (\lambda xy. y(xxy))(\lambda xy. y(xxy))$$

$$\Theta h = h(\Theta h) = h(h(\Theta h)) = \dots$$

Generally, let $\gamma := \lambda x_1 \dots x_{n-1} y. y(wy)$ where w is an arbitrary word of length n over the alphabet $\{x_1, \dots, x_{n-1}\}$. Then $\Gamma := \gamma^n$ is a fixpoint combinator.

Example — Θ_v Combinator

$$\begin{array}{ccc} \Lambda \times \Lambda & \xrightarrow{f} & \Lambda \\ \Delta \uparrow & & \downarrow \alpha \\ \Lambda & \xrightarrow{g} & \Lambda \end{array}$$

where $f : (x, y) \mapsto yx$, and $\alpha : x \mapsto \lambda y. y(\lambda z. xyz)$.

$$g = \lambda xy. y(\lambda z. xxyz)$$

$$gg = \alpha(gg)$$

$$\Theta_v := gg = (\lambda xy. y(\lambda z. xxyz))(\lambda xy. y(\lambda z. xxyz))$$

$$\Theta_v hv = h(\Theta_v h)v$$

Example — Fixpoint Theorem in Lambda Calculus

Theorem (Fixpoint Theorem in Lambda Calculus)

For every λ -term F there is a λ -term E s.t.

$$F^\Gamma E^\neg = E$$

$$\begin{array}{ccc} \underline{\Lambda} \times \underline{\Lambda} & \xrightarrow{A} & \Lambda \\ \Delta \uparrow & & \downarrow \alpha_F \\ \underline{\Lambda} & \xrightarrow{G} & \Lambda \end{array}$$

where $\underline{\Lambda} := \{\Gamma M^\neg : M \in \Lambda\}$, and $A : (\Gamma M^\neg, \Gamma N^\neg) \mapsto N(\Gamma M^\neg)$, and $\alpha_F : M \mapsto F^\Gamma M^\neg$.

$$G^\Gamma M^\neg = F^\Gamma M^\Gamma M^{\neg\Gamma}$$

$$E := G^\Gamma G^\neg$$

Example — Fixpoint Lemma in Logic

Theorem (Fixpoint Lemma in Logic)

For any wff $F(x)$ with one free variable x , there exists a sentence E s.t.

$$\mathbf{Q} \vdash E \leftrightarrow F(\neg E^\top)$$

$$\begin{array}{ccc} \text{Lin}_1 \times \text{Lin}_1 & \xrightarrow{f} & \text{Lin}_0 \\ \Delta \uparrow & & \downarrow \alpha_F \\ \text{Lin}_1 & \xrightarrow{g} & \text{Lin}_0 \end{array}$$

where $f : (M(x), N(x)) \mapsto N(\neg M(x)^\top)$, and $\alpha_F : M \mapsto F(\neg M^\top)$.

$g(M(x)) = F(\neg M(\neg M(x)^\top)^\top)$ which is representable by
 $G(x) := F(d(x))$

where $d(n) := \begin{cases} \#M(\neg M(x)^\top) & \text{if } n = \#M(x) \text{ for } M(x) \in \text{Lin}_1 \\ 0 & \text{otherwise} \end{cases}$

is primitive recursive and is thus represented by some function symbol d .

$$E := G(\neg G(x)^\top)$$

Example — Fixpoint Lemma in Logic

f	M	N	\dots	G
M	$F(\Gamma M(\Gamma M(x) \neg) \neg)$	$M(\Gamma N(x) \neg)$	\dots	$M(\Gamma G(x) \neg)$
N	$N(\Gamma M(x) \neg)$	$F(\Gamma N(\Gamma N(x) \neg) \neg)$	\dots	$N(\Gamma G(x) \neg)$
\vdots	\vdots	\vdots	\vdots	\vdots
G	$G(\Gamma M(x) \neg)$	$G(\Gamma N(x) \neg)$	\dots	$G(\Gamma G(x) \neg)$
	$F(\Gamma M(\Gamma M(x) \neg) \neg)$	$F(\Gamma N(\Gamma N(x) \neg) \neg)$		$F(\Gamma G(\Gamma G(x) \neg) \neg)$
\vdots	\vdots	\vdots	\vdots	\vdots

Strong Fixpoint Lemma

Theorem (Strong Fixpoint Lemma — Jeroslow1973)

For any wff $F(x)$ with one free variable x , there is a closed-term t s.t.

$$T \vdash t = \ulcorner F(t) \urcorner$$

Proof.

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \xrightarrow{d} & \mathbb{N} \\ \Delta \uparrow & & \downarrow \alpha_F \\ \mathbb{N} & \xrightarrow{g} & \mathbb{N} \end{array}$$

where $d(m, n) := \lfloor n \rfloor(m) := \begin{cases} f(m) & \text{if } n = \ulcorner f \urcorner \text{ for some function } f \\ 0 & \text{otherwise} \end{cases}$ and
 $\alpha_F : n \mapsto \ulcorner F(n) \urcorner$.

$$g(n) = \ulcorner F(\lfloor n \rfloor(n)) \urcorner$$

g is primitive recursive $\implies g = \lfloor k \rfloor = d(-, k)$ for some $k \in \mathbb{N}$

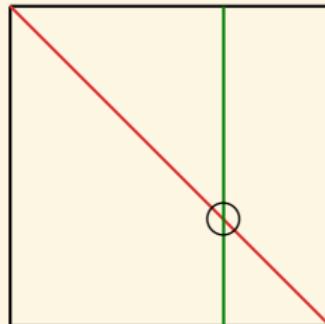
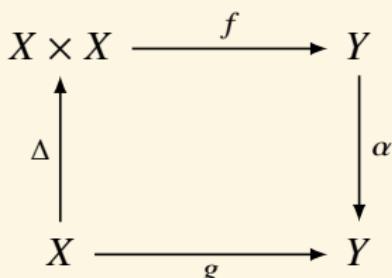
$$t := \lfloor k \rfloor(k)$$

Remark: Strong Fixpoint Lemma \implies Fixpoint Lemma: $E := F(t)$

d	0	1	2	\dots	k	\dots
0	0	0	0	\dots	0	\dots
1	$\lfloor 1 \rfloor(0)$	$\lfloor 1 \rfloor(1)$	$\lfloor 1 \rfloor(2)$	\dots	$\lfloor 1 \rfloor(k)$	\dots
2	$\lfloor 2 \rfloor(0)$	$\lfloor 2 \rfloor(1)$	$\lfloor 2 \rfloor(2)$	\dots	$\lfloor 2 \rfloor(k)$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
k	$\lfloor k \rfloor(0)$	$\lfloor k \rfloor(1)$	$\lfloor k \rfloor(2)$	\dots	$\lfloor k \rfloor(k)$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

d	0	1	2	\dots	k	\dots
0	$\lceil F(0) \rceil$	0	0	\dots	0	\dots
1	$\lfloor 1 \rfloor(0)$	$\lceil F(\lfloor 1 \rfloor(1)) \rceil$	$\lfloor 1 \rfloor(2)$	\dots	$\lfloor 1 \rfloor(k)$	\dots
2	$\lfloor 2 \rfloor(0)$	$\lfloor 2 \rfloor(1)$	$\lceil F(\lfloor 2 \rfloor(2)) \rceil$	\dots	$\lfloor 2 \rfloor(k)$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
k	$\lfloor k \rfloor(0)$	$\lfloor k \rfloor(1)$	$\lfloor k \rfloor(2)$	\dots	$\boxed{\begin{array}{c} \lfloor k \rfloor(k) \\ \lceil F(\lfloor k \rfloor(k)) \rceil \end{array}}$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\dots

Fixpoint vs Diagonalization

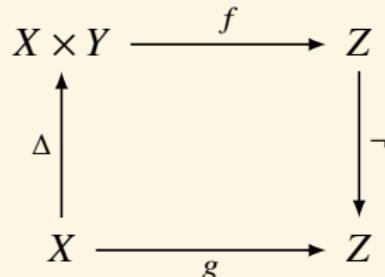


Curry Y	$\hat{=}$	λ -fixpoint	$\hat{=}$	Gödel	$\hat{=}$	Kleene	$\hat{=}$	Russell
yx	$\hat{=}$	$N(\Gamma M^\top)$	$\hat{=}$	$N(\Gamma M(x)^\top)$	$\hat{=}$	$\varphi_n(m)$	$\hat{=}$	$x \in y$
xx	$\hat{=}$	$M(\Gamma M^\top)$	$\hat{=}$	$M(\Gamma M(x)^\top)$	$\hat{=}$	$\varphi_n(n)$	$\hat{=}$	$x \in x$
$y(xx)$	$\hat{=}$	$F\Gamma M\Gamma M^\top$	$\hat{=}$	$F(\Gamma M(\Gamma M(x)^\top)^\top)$	$\hat{=}$	$h(\varphi_n(n))$	$\hat{=}$	$x \notin x$
$\lambda x.y(xx)$	$\hat{=}$	G	$\hat{=}$	$G(x)$	$\hat{=}$	$\varphi_t(n)$	$\hat{=}$	$x \notin R$
$(\lambda x.y(xx))(\lambda x.y(xx))$	$\hat{=}$	$G(\Gamma G^\top)$	$\hat{=}$	$G(\Gamma G(x)^\top)$	$\hat{=}$	$\varphi_t(t)$	$\hat{=}$	$R \notin R$

self-reference $\xrightarrow{?}$ self-improvement

Cantor's Diagonal Argument vs Three-Valued Logic

Let $Z = \{0, u, 1\}$.



z	$\neg z$
0	1
u	u
1	0

$$\neg f(\neg g^\neg, \neg g^\neg) = g(\neg g^\neg) = f(\neg g^\neg, \neg g^\neg) \implies f(\neg g^\neg, \neg g^\neg) = u$$

We can't conclude that g is not of the form $f(-, y)$ for any y . Thus Cantor's diagonal argument about higher cardinalities does not generalize to a set theory based on the three-valued logic.

Non-operational Self-inspection[Svo18]

The information available to the observer regarding his own state could have absolute limitations, by the laws of nature.

— John von Neumann

$$\begin{array}{ccc} M \times M & \xrightarrow{f} & O \\ \Delta \uparrow & & \downarrow \alpha \\ M & \xrightarrow{g} & O \end{array}$$

- ▶ **M**: quantum measurements.
- ▶ **O**: possible outcomes of quantum measurements.

If we assume that it is not possible to measure properties without changing them (observer effect: α is fixpoint-free), then there is a limit to self-inspection.

General Fixpoint Theorem[San20]

$$\forall XYZ. \forall R \subset Z \times Z. \forall R' \subset Z^X \times Z^{X \times Y} \times X \times Y. \forall \beta : X \rightarrowtail Y. \forall d : Z^{X \times Y} \rightarrow Z^X. \left\{ \left(\exists f \in Z^{X \times Y}. \exists y \in Y. \forall x \in X. R'(df, f, x, y) \right) \wedge \left(\forall g \in Z^X. \forall f \in Z^{X \times Y}. \forall x \in X. [R'(g, f, x, \beta x) \rightarrow R(gx, dfx)] \right) \rightarrow \exists z \in Z. R(z, z) \right\}$$

Theorem (General Fixpoint Theorem)

In a category \mathbf{C} , for $X, Y, Z \in \text{ob}(C)$, $R \subset \text{Hom}(1, Z) \times \text{Hom}(1, Z)$,
 $R' \subset \text{Hom}(X, Z) \times \text{Hom}(X \times Y, Z) \times \text{Hom}(1, X) \times \text{Hom}(1, Y)$,
 $\beta : \text{Hom}(1, X) \rightarrowtail \text{Hom}(1, Y)$, and $d : \text{Hom}(X \times Y, Z) \rightarrow \text{Hom}(X, Z)$, if

1. there exists $f : X \times Y \rightarrow Z$ and $y : 1 \rightarrow Y$ s.t for all $x : 1 \rightarrow X$:

$$R'(df, f, x, y)$$

2. for all $g : X \rightarrow Z$, $f : X \times Y \rightarrow Z$, and $x : 1 \rightarrow X$,

$$R'(g, f, x, \beta x) \implies R(gx, dfx)$$

then, there exists $z : 1 \rightarrow Z$ s.t. $R(z, z)$.

General Fixpoint Theorem \Rightarrow Smullyan's Fixpoint Theorem

Theorem (Smullyan's Fixpoint Theorem)

For $R, R' \subset Z \times Z$, and $\alpha : Z \rightarrow Z$, if

1. there exists $x \in Z$ s.t. $R'(\alpha x, x)$, and
2. for $x, y \in Z$, $R'(x, y) \implies R(x, \alpha y)$.

then, there exists $z \in Z$ s.t. $R(z, z)$.

Proof.

Let $d : Z^{Z \times Z} \rightarrow Z^Z :: f \mapsto \alpha \circ f \circ \langle 1_Z, \beta \rangle$.

Let $R'_1(g, f, x, y) := R'(gx, f(x, y))$.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \langle 1_X, \beta \rangle \uparrow & & \downarrow \alpha \\ X & \longrightarrow & Z \end{array}$$

$$\begin{aligned} R'(\alpha x, x) &\implies R'(\alpha \circ \pi_1 \circ \langle 1_Z, \beta \rangle x, x) \implies R'_1(d\pi_1 x, \pi_1(x, y)) \\ &\implies R'_1(d\pi_1, \pi_1, x, y) \end{aligned}$$

$$\begin{aligned} R'_1(g, f, x, \beta x) &\implies R'(gx, f(x, \beta x)) \implies R(gx, \alpha(f(x, \beta x))) \\ &\implies R(gx, \alpha \circ f \circ \langle 1_Z, \beta \rangle x) \implies R(gx, dfx) \end{aligned}$$

General Fixpoint Theorem \Rightarrow Lawvere's Fixpoint Theorem

Theorem (Lawvere's Fixpoint Theorem)

For all sets X, Y, Z , and all functions $f : X \times Y \rightarrow Z, \alpha : Z \rightarrow Z$, surjective functions $\beta : X \twoheadrightarrow Y$. If $\alpha \circ f \circ \langle 1_X, \beta \rangle$ is representable by f , then α has a fixpoint.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \langle 1_X, \beta \rangle \uparrow & & \downarrow \alpha \\ X & \longrightarrow & Z \end{array}$$

Proof.

$$d(f) := \alpha \circ f \circ \langle 1_X, \beta \rangle$$
$$R'(g, f, x, y) := gx = f(x, y)$$

$$R(x, y) := \alpha x = y$$

Since df is representable by $f(-, y)$, we have $R'(df, f, x, y)$, and

$$R'(g, f, x, \beta x) \implies gx = f(x, \beta x) \implies \alpha(gx) = (\alpha \circ f \circ \langle 1_X, \beta \rangle)x$$
$$\implies R(gx, df x)$$

General Fixpoint Theorem \Rightarrow Lawvere's Fixpoint Theorem

Theorem (Lawvere's Fixpoint Theorem — multi-valued version)

For sets X, Y, Z , multi-valued functions $f : X \times Y \rightrightarrows Z$, $\alpha : Z \rightrightarrows Z$, and surjective functions $\beta : X \twoheadrightarrow Y$, if $\exists y \forall x : \alpha \circ f \circ \langle 1_X, \beta \rangle x \cap f(x, y) \neq \emptyset$, then α has a fixpoint, i.e. $\exists z \in \alpha(z)$.

$$\begin{array}{ccc} X \times Y & \xrightarrow{f} & Z \\ \uparrow \langle 1_X, \beta \rangle & & \downarrow \alpha \\ X & \longrightarrow & Z \end{array}$$

Proof.

$$d(f) := \alpha \circ f \circ \langle 1_X, \beta \rangle$$

$$R'(g, f, x, y) := gx \cap f(x, y) \neq \emptyset$$

$$R(x, y) := \alpha x \cap y \neq \emptyset$$

Obviously, we have $R'(df, f, x, y)$, and

$$\begin{aligned} R'(g, f, x, \beta x) &\implies gx \cap f(x, \beta x) \neq \emptyset \implies \alpha(gx) \cap (\alpha \circ f \circ \langle 1_X, \beta \rangle)x \neq \emptyset \\ &\implies R(gx, dfx) \end{aligned}$$

Smullyan's Fixpoint Theorem \Rightarrow Tarski's Fixpoint Theorem

Theorem (Tarski's Fixpoint Theorem)

Given a set V , and $(P(V), \subset)$, and an order-preserving function $f : P(V) \rightarrow P(V)$, f has a fixpoint.

Proof.

Define $R, R' \subset P(V) \times P(V)$ and $\alpha : P(V) \rightarrow P(V)$ as follows.

$$R(X, Y) := f(X) = Y$$

$$R'(X, Y) := (\forall x \in Y. x \subset f(x)) \wedge \left(\bigcup Y \subset X \right) \wedge \left(\bigcup Y \in Y \right) \wedge \left(f(X) \subset \bigcup Y \right)$$

$$\alpha(X) := \bigcup X$$

Consider $S := \{X \in P(V) : X \subset f(X)\}$. It is easy to check that $R'(\alpha S, S)$.

$$R'(X, Y) \implies f(X) = \bigcup Y = \alpha Y \implies R(X, \alpha Y)$$

By Smullyan's theorem, $R(X, Y)$ has a fixpoint.

Definition

A function $f : X \rightarrow X$ is preserved in $\mathcal{A} \subset X^\omega$ iff for each $x \in \mathcal{A}$, $\langle f(x_n) \rangle_{n \in \omega} \in \mathcal{A}$.

Definition

A function $F : \mathcal{A} \rightarrow X$ is a limit function iff

1. $\forall x \in \mathcal{A} : \langle x_{n+1} \rangle_{n \in \omega} \in \mathcal{A}$;
2. $\forall x \in \mathcal{A} : F(x) = F(\langle x_{n+1} \rangle_{n \in \omega})$.

Definition

A function $f : X \rightarrow X$ is continuous with respect to a limit function $F : \mathcal{A} \rightarrow X$ iff f is preserved in \mathcal{A} , and

1. $\exists a \in X : \langle f^n(a) \rangle_{n \in \omega} \in \mathcal{A}$;
2. $\forall x \in \mathcal{A} : f(F(x)) = F(\langle f(x_n) \rangle_{n \in \omega})$.

Theorem (Fixpoint for Continuous Function w.r.t. Limit Function)

Let $f : X \rightarrow X$ be a continuous function with respect to a limit function $F : \mathcal{A} \rightarrow X$. Then f has a fixpoint.

Proof.

Define $R, R' \subset \mathcal{A} \times \mathcal{A}$ and $\alpha : \mathcal{A} \rightarrow \mathcal{A}$ as follows.

$$R(x, y) := f(F(x)) = F(y)$$

$$R'(x, y) := f(F(x)) = F(\langle f(y_n) \rangle_{n \in \omega})$$

$$\alpha(x) := \langle f(x_n) \rangle_{n \in \omega}$$

Take a in $\exists a \in X : \langle f^n(a) \rangle_{n \in \omega} \in \mathcal{A}$. Consider z given by $z_n := f^n(a)$.

$$\begin{aligned} f(F(\alpha z)) &= f(F(\langle f(z_n) \rangle_{n \in \omega})) = F(\langle f(f(z_n)) \rangle_{n \in \omega}) = F(\langle f^{n+2}(a) \rangle_{n \in \omega}) = \\ &= F(\langle f^{(n+1)+1}(a) \rangle_{n \in \omega}) = F(\langle f^{n+1}(a) \rangle_{n \in \omega}) = F(\langle f(z_n) \rangle_{n \in \omega}) \end{aligned}$$

Hence $R'(\alpha z, z)$.

$$R'(x, y) \implies f(F(x)) = F(\langle f(y_n) \rangle_{n \in \omega}) \implies f(F(x)) = F(\alpha y) \implies R(x, \alpha y)$$

By Smullyan's theorem, $R(x, y)$ has a fixpoint.

Fixpoint Theorem for Normal Functions

Definition

A function $f : \text{Ord} \rightarrow \text{Ord}$ is a normal function iff

1. $\alpha < \beta \implies f(\alpha) < f(\beta)$.
2. $f(\alpha) = \sup \{f(\gamma) : \gamma < \alpha\}$ if α is a limit ordinal.

Theorem (Fixpoint Theorem for Normal Functions)

Every normal function $f : \text{Ord} \rightarrow \text{Ord}$ has a fixpoint.

Proof.

Let $\mathcal{A} := \{x \in \text{Ord}^\omega : x \text{ is increasing}\}$. Obviously, f is preserved in \mathcal{A} .

Let $F : \mathcal{A} \rightarrow \text{Ord} :: x \mapsto \sup\{x_n : n \in \omega\}$. Obviously, F is a limit function.

Take $\alpha \in \text{Ord}$. Obviously, $\langle f^n(\alpha) \rangle_{n \in \omega} \in \mathcal{A}$.

For $x \in \mathcal{A}$,

$$f(F(x)) = f(\sup\{x_n : n \in \omega\}) = \sup\{f(x_n) : n \in \omega\} = F(\langle f(x_n) \rangle_{n \in \omega})$$

Banach's Fixpoint Theorem

Theorem (Banach's Fixpoint Theorem)

Let (X, d) be a complete metric space and $T : X \rightarrow X$ be a contraction mapping, with Lipschitz constant $\gamma < 1$. Then T has a unique fixpoint.

Proof.

Let $\mathcal{A} := \{x \in X^\omega : x \text{ is a Cauchy sequence}\}$.

For $x \in \mathcal{A}$, it is easy to check that $\langle T(x_n) \rangle_{n \in \omega} \in \mathcal{A}$.

Take $F : \mathcal{A} \rightarrow X :: x \mapsto \lim_{n \in \omega} x_n$. Obviously, F is a limit function.

Let us prove that T is continuous with respect to F .

Let $a \in X$. Consider x given by $x_n := T^n(a)$.

$$d(x_{n+1}, x_n) \leq \gamma^n d(x_1, x_0)$$

It is not hard to check that x is a Cauchy sequence, i.e., $x \in \mathcal{A}$.

As the contraction mapping T is continuous, we have

$$T(F(x)) = T \lim_{n \in \omega} x_n = \lim_{n \in \omega} T(x_n) = F(\langle T(x_n) \rangle_{n \in \omega})$$

Kleene's Fixpoint Theorem



Theorem (Kleene's Fixpoint Theorem)

Given a recursive function h , there is an index e s.t.

$$\varphi_e = \varphi_{h(e)}$$

对于任意的程序 h , 总存在某个程序 e , 执行程序 e 的结果等价于把程序 e 当作数据输入给程序 h 执行的结果。

You can systematically change an infinite number of programs $\varphi_n \mapsto \varphi_{h(n)}$ but you cannot systematically change an infinite number of computable functions $\varphi_e = \varphi_{h(e)}$.

From Kleene's Fixpoint to Chaitin's Incompleteness

Definition: Kolmogorov Complexity $K(x) := \mu e [\varphi_e(0) = x]$

Theorem (Chaitin's Incompleteness Theorem)

For any arithmetically sound Gödelian theory T , $\exists c \forall x : T \not\vdash K(x) > c$.

Proof.

For any m , we can construct:

$M_n := \text{"find } \mu y [\text{prf}_T(y, K(x) > m)], \text{output } x"$

So there exists a computable function $f : m \mapsto n$.

By Kleene's fixpoint theorem, there exists e such that

$M_e = M_{f(e)} = \text{"find } \mu y [\text{prf}_T(y, K(x) > e)], \text{output } x"$

Take $c := e$.

Remark: For almost all random strings their randomness cannot be proved.

Self-reproducing Program/Quine

There is a program that outputs its own length.

- ▶ A Quine is a program which takes no input and outputs its own source code.
- ▶ Quines are algorithmic random.

There is a program that outputs its own source code.

Corollary (Self-reproducing Program)

There is a recursive function φ_e s.t. $\forall x : \varphi_e(x) = e$.

Quine in Python

```
exec(s:='print("exec(s:=%r)"%s)')
```

Quine in Lambda Calculus

$$(\lambda x. xx)(\lambda x. xx)$$

Self-reproducing Program

Print two copies of the following, the second copy in quotes:

“Print two copies of the following, the second copy in quotes:”

DNA / mutation / evolution

Build a baby that acts on the following instructions, and also contains a copy of those instructions in its reproductive organs.

“Build a baby that acts on the following instructions, and also contains a copy of those instructions in its reproductive organs.”

von Neumann's Self-reproducing Automata

1. A universal constructor A .

$$A + \lceil X \rceil \rightsquigarrow X$$

2. A copying machine B .

$$B + \lceil X \rceil \rightsquigarrow \lceil X \rceil$$

3. A control machine C , which first activates B , then A .

$$A + B + C + \lceil X \rceil \rightsquigarrow X + \lceil X \rceil$$

4. Let $X := A + B + C$. Then $A + B + C + \lceil A + B + C \rceil$ is self-reproducing.

$$A + B + C + \lceil A + B + C \rceil \rightsquigarrow A + B + C + \lceil A + B + C \rceil$$

5. It is possible to add the description of any machine D .

$$A + B + C + \lceil A + B + C + D \rceil \rightsquigarrow A + B + C + D + \lceil A + B + C + D \rceil$$

6. Now allow mutation on the description $\lceil A + B + C + D \rceil$.

$$A + B + C + \lceil A + B + C + D' \rceil \rightsquigarrow A + B + C + D' + \lceil A + B + C + D' \rceil$$

Introspective Program

Definition (ψ -introspective)

Given a total recursive function ψ ,

- ▶ the ψ -analysis of $\varphi(x)$ is the code of the computation of $\varphi(x)$ to $\psi(x)$ steps.
- ▶ φ is ψ -introspective at x iff $\varphi(x) \downarrow$ and outputs its own ψ -analysis.
- ▶ φ is *totally ψ -introspective* iff it is ψ -introspective at all x .

Corollary

There is a program that is totally ψ -introspective.

Proof.

Let $f(n, x) :=$ “the ψ -analysis of $\varphi_n(x)$ ”.

Introspective Program

There is a program that is totally introspective.

$$\varphi_e = \varphi_{h(e)}$$

Self-simulating Computer	Self-consciousness
Host Machine	Experiencing Self
Virtual Machine	Remembering Self
Hardware	Body



Know Thyself

Who am I?

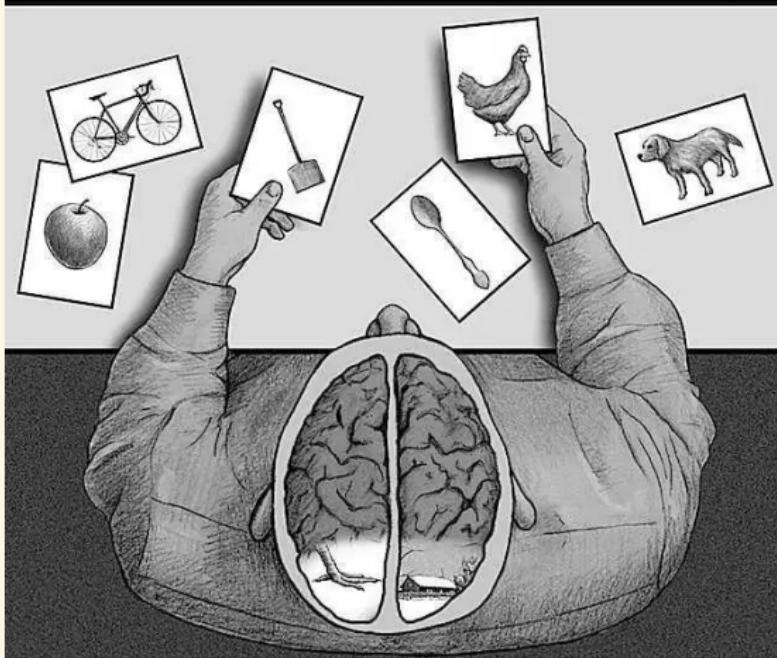
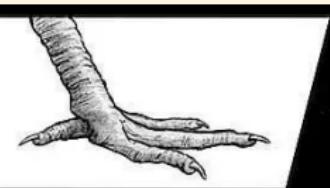
I think, therefore I am.

self-locating: "I" is an indexical term that I use to refer to myself as myself.

What is "me"?

What is "self-consciousness"?

- ▶ self-perception self-observation self-experience self-tracking
self-reflection self-awareness
- ▶ self-evaluation self-analysis self-monitoring
- ▶ self-control self-adjustment self-modification self-actualization
self-fulfillment self-surpass self-improvement
- ▶ *actual-self* pk *ideal-self* self-identity "the *self*"
- ▶ free will: Second order desire that we want to act on is second order volition. Second order volitions involve wanting a certain desire to be one's will, that is wanting it to move one to action. (Frankfurt)



- ▶ the split brain in man
- ▶ snow?
- ▶ shit!
- ▶ life as a story

Kahneman — Thinking, Fast and Slow

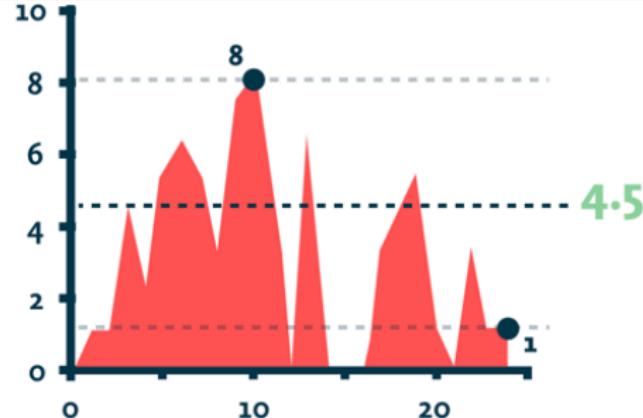
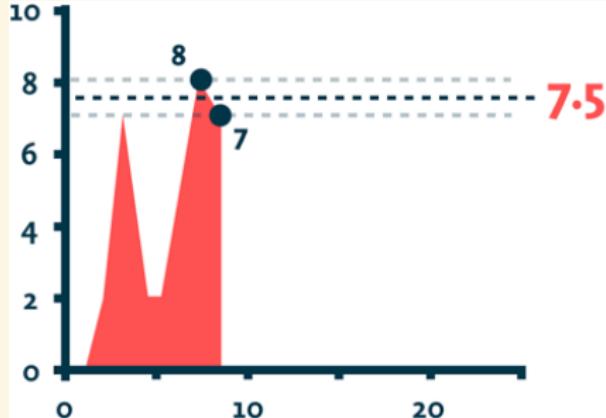


Figure: Why you might prefer more pain

- painful experiment
- experiencing self
- remembering self
- duration neglect
- peak-end rule



Figure: One can imagine a detailed floor plan of a room, sitting on a table in the room; this plan has an image of the table on which there is an image of the plan itself. Now introduce the dynamical aspect: the items on the plan are cut out from paper and can be moved to try a different furniture arrangement; in this way the plan models possible states of the world about which it carries information.

Manin — Cognitive Networks



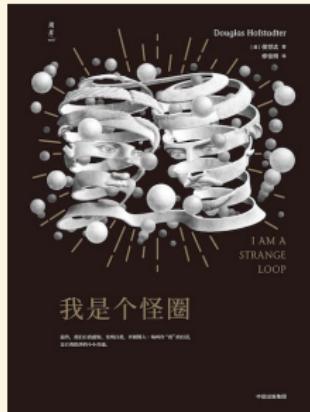
The brain contains inside a map of itself, and some neural information channels in the central neural system:

- ▶ carry information about the mind itself, i.e. are **reflexive**;
- ▶ are capable of modelling states of the mind different from the current one, i.e. possess a **modelling function**;
- ▶ can influence the state of the whole mind and through that, the behavior, i.e. possess **controlling function**.

The reflection of the brain inside itself must be **coarse grained**.

Hofstadter — I am a Strange Loop

- ▶ Animate entities are those that, at some level of description, manifest a certain type of loopy pattern, which inevitably starts to take form if a system with the inherent capacity of perceptually filtering the world into discrete categories vigorously expands its repertoire of categories ever more towards the abstract.
- ▶ This pattern reaches full bloom when there comes to be a deeply entrenched self-representation — a story told by the entity to itself — in which the entity's "I" plays the starring role, as a unitary causal agent driven by a set of desires.



说谎者悖论	我在说谎
Grelling 悖论	“非自谓的”是自谓的吗
Russell 悖论	“不属于自身的集合的集合”属于自身吗
Berry 悖论	我是少于十八个字不可定义的最小数
Yablo 悖论	我下一句及后面所有的句子都是假的
Gödel 不动点引理	我有性质 F
Tarski 算术真不可定义定理	我不真
Gödel 第一不完全性定理	我不可证
Gödel-Rosser 不完全性定理	对于任何一个关于我的证明，都有一个更短的关于我的否定的证明
Löb 定理	如果我可证，那么 A
Curry 悖论	如果我是真的，那么上帝存在
Parikh 定理	我没有关于自己的长度短于 n 的证明
Kleene 不动点定理	我要进行 h 操作
Quine 悖论	把“把中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变得到的句子是假的”中的第一个字放到左引号前面，其余的字放到右引号后面，并保持引号及其中的字不变得到的句子是假的
自测量长度程序	我要输出自己的长度
自复制程序	我要输出自己
自反省程序	我要回顾自己走过的每一步
Gödel 机	我要变成能获取更大效用的自己

Schmidhuber's Gödel Machine

- ▶ The Gödel machine consists of a **Solver** and a **Searcher** running in parallel.
- ▶ The **Solver** ($\text{AIXI}^S/\text{AIXI}^{t\ell}$) interacts with the environment.
- ▶ The **Searcher** (LSEARCH/HSEARCH/OOPS) searches for a proof of “the modification of the software — including the *Solver* and *Searcher* — will increase the expected utility than leaving it as is”.
- ▶ Logic: a theorem prover and a set of self-referential axioms, which include a description of its own software and hardware, and a description of the probabilistic properties of the environment, as well as a user-given utility function.
- ▶ *Since the utility of “leaving it as is” implicitly evaluates all possible alternative modifications, the current modification is globally optimal w.r.t. its initial utility function.*

Gödel Machine

- ▶ language $\mathcal{L} := \{\neg, \wedge, \vee, \rightarrow, \forall, \exists, =, (,), \dots, +, -, \cdot, /, <, \dots\}$
- ▶ well-formed formula
- ▶ utility function $u(s, e) = \mathbb{E}_\mu \left[\sum_{t=1}^T r_t \mid s, e \right]$
- ▶ target theorem
- $$u[s(t) \oplus (\text{switchbit}(t) = 1), e(t)] > u[s(t) \oplus (\text{switchbit}(t) = 0), e(t)]$$
- ▶ theorem prover
 - hardware, costs, environment, initial state, utility, logic/arithmetic/probability

ENVIRONMENT

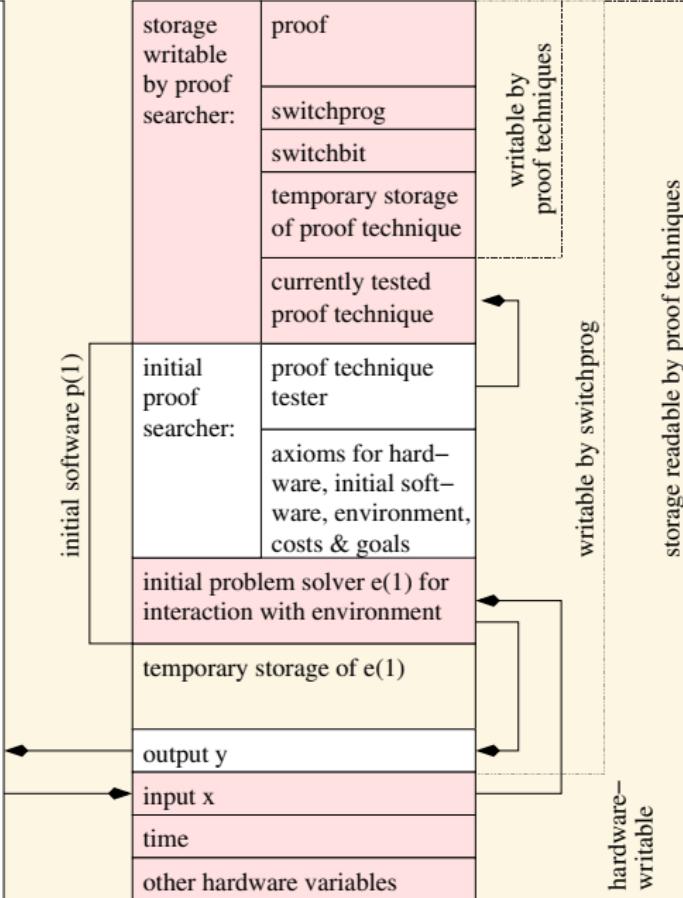
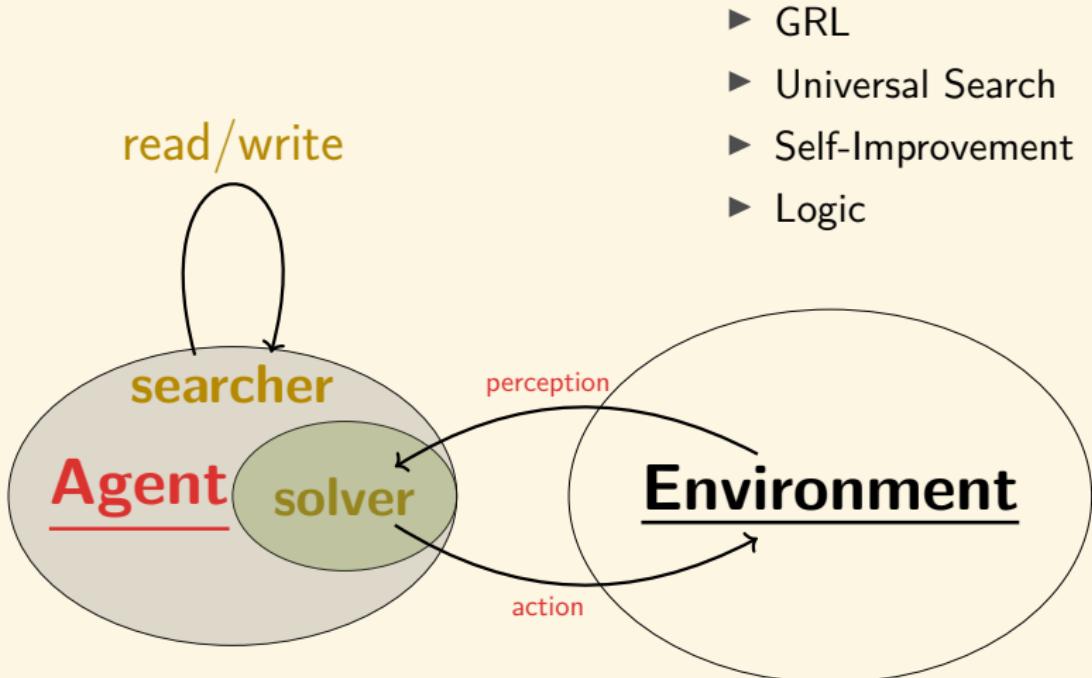


Figure: Schmidhuber

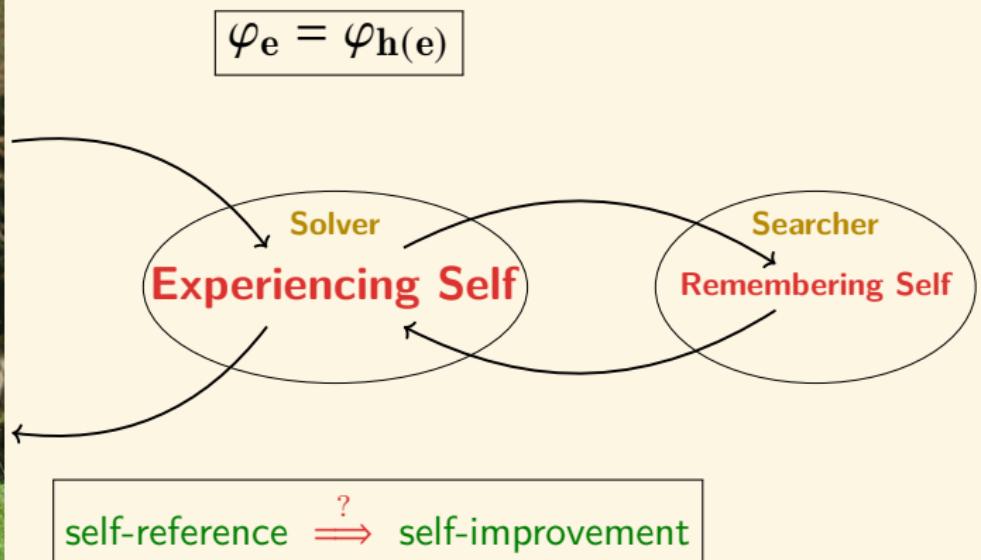
Gödel Machine



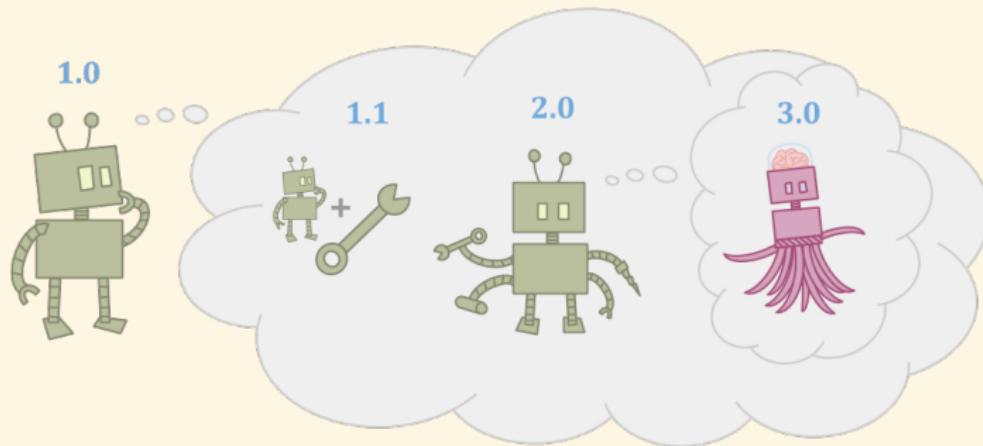
Disadvantage: A Gödel Machine with a badly chosen utility function is motivated to converge to a “poor” program. (goal orthogonality!)

Gödel Machine vs Self-Consciousness vs Free Will?

Self-simulating Computer	Gödel Machine	Self-consciousness
Host Machine	Solver	Experiencing Self
Virtual Machine	Searcher	Remembering Self
Hardware	Hardware	Body



*What matters most
is how you see
yourself*



Gödel Machines

1. *one-shot* self-improvement: Kleene's fixpoint theorem

$$\varphi_e = \varphi_{h(e)}$$

- ▶ global optimality?
- ▶ goal orthogonality? ends vs means

2. *continuous* self-improvement: Kleene's fixpoint theorem **with parameters**

$$\varphi_e(y) = \varphi_{h(e(y),y)}$$

- ▶ “real-time” optimality. human-computer interaction?
- ▶ intelligent explosion / technological singularity???
- continuous self-improvement \neq exponential iteration

3. *beyond computability*: Kleene's **relativized** fixpoint theorem

$$\varphi_{e(y)}^A = \varphi_{h(e(y),y)}^A$$

- ▶ Gödel Machine PK AIXI^{tℓ}
- ▶ Gödel Machine PK AIXI

Limitation

1. Gödel's first incompleteness theorem / Rice's theorem
2. Gödel's second incompleteness theorem

$$T \vdash \Box_{T'} A \rightarrow A \implies T \vdash \text{Con}_{T'}$$

3. Legg's incompleteness theorem. *General prediction algorithms must be complex. Beyond a certain complexity they can't be mathematically discovered.*
4. Complexity: higher-level abstractions — coarse grained.
 - ▶ Psychology: Duration neglect / Peak-end rule
 - ▶ Information Bottleneck: Learning is to forget!
5. Physical constraint: If we assume that it is not possible to measure properties without changing them (observer effect: α is fixpoint-free), then there is a limit to self-inspection.

Evolution & the Number of Wisdom — Chaitin Constant

- ▶ The enormous computational power of evolution could have developed and coded information into our genes,
 - (a) which significantly guides human reasoning,
 - (b) cannot efficiently be obtained from scratch.

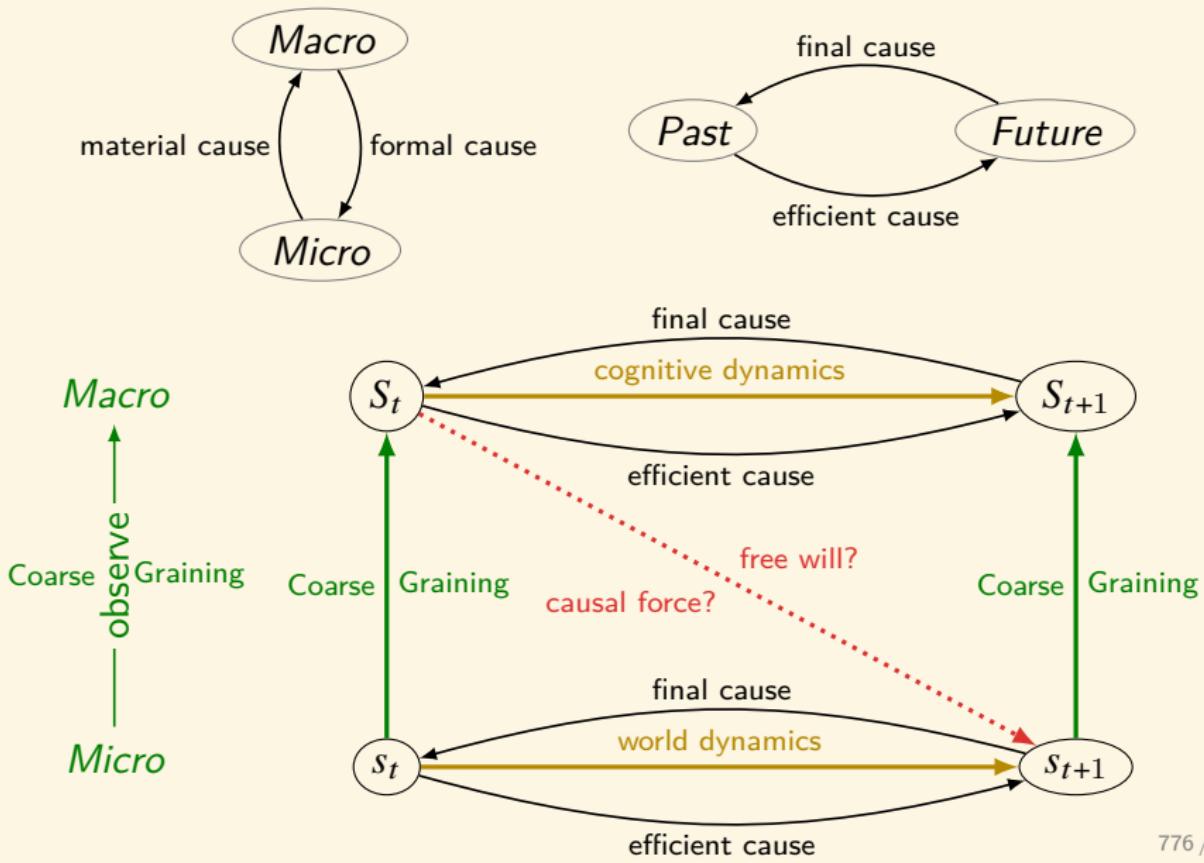
$$\Omega = \lim_{t \rightarrow \infty} \sum_{\ell(p) \leq t \text{ } \& \text{ } U(p) \downarrow \text{ within time } t} 2^{-\ell(p)}$$

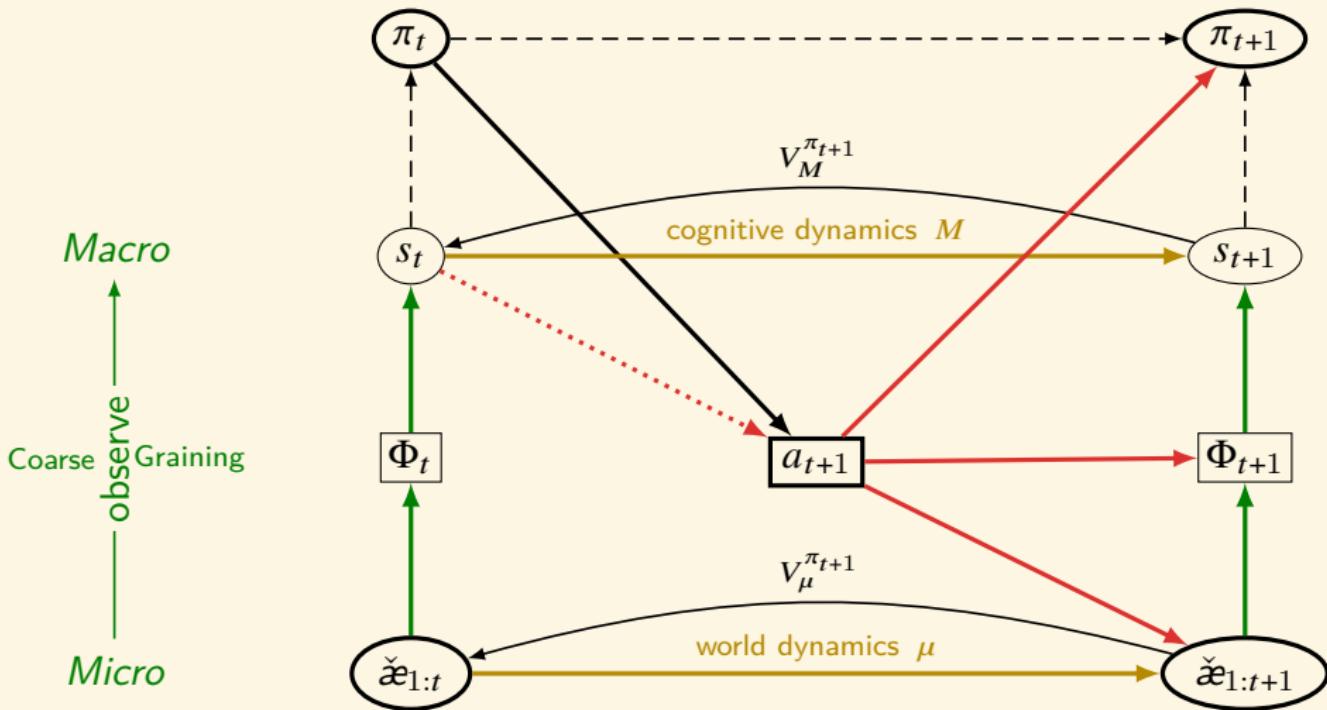
- ▶ Cheating solution: add the information from our genes or brain structure to our AI system?
- ▶ Biological Evolution: Darwin PK Lamarck
natural selection vs artificial evolution
random vs non-random mutation
- ▶ Tegmark: Life3.0



O God, give us courage to change what can be changed,
serenity to accept what cannot be changed,
and wisdom to know the difference.

Jiang ZHANG: Causal Emergence





$$V_t^\pi(\alpha_{<k}) = Q_t(\alpha_{<k}\pi(\alpha_{<k}))$$

$$Q_t(\alpha_{<k}a_k) = \sum_{e_k \in \mathcal{E}} \mu(e_k | \alpha_{<k}\check{a}_k) [u_t(\check{a}_{1:k}) + \gamma V_t^{\pi_{t+1}}(\alpha_{1:k})]$$

$$\pi_1^* := \underset{\pi}{\operatorname{argmax}} V_1^\pi(\epsilon)$$

The Universal program (warm-up): the petulant child

The Petulant Child

Consider program e :

It searches for a proof in PA of a statement:

“program e does not give output n .”

When found, gives output n and halts.

According to Kleene's Fixpoint Theorem, there is a program e s.t.

- ▶ When run in the standard model $\mathcal{N} \models \text{PA}$, the program never halts.
- ▶ For any n , there is a model $\mathcal{M} \models \text{PA}$ in which the program e gives output n .

The Universal algorithm: sequence version

The Petulant Child

Consider program e :

It searches for a proof in PA of a statement:

"program e does not enumerate the sequence a_0, \dots, a_n and halt."

When found, enumerate that sequence.

Theorem (The Universal algorithm: sequence version)

There is a program e s.t.

1. PA proves that the set accepted by e is finite.
2. For any finite $A \subset \mathbb{N}$, there is a model $\mathcal{M} \models \text{PA}$ in which the program e accepts exactly A .
3. Indeed, for any $A \subset \mathbb{N}$, there is a model $\mathcal{M} \models \text{PA}$ in which the program e accepts exactly A .

A program that accepts exactly any desired finite set, in the right universe.

The Universal algorithm: function version

Theorem (The Universal algorithm: function version)

There is a program e s.t.

1. PA proves that the function computed by e is finite.
2. For any finite partial function f , there is a model $\mathcal{M} \models \text{PA}$ in which the program e computes exactly f .
3. For any partial function f , there is a model $\mathcal{M} \models \text{PA}$ in which the program e computes exactly f .

Every function can be computable!... in the right universe.

Proof.

The statements “the n^{th} number enumerated by e is $f(n)$ ” are finitely consistent with PA. So by compactness they are all true in some model.

The Universal Algorithm: full extension version

Theorem (Woodin)

There is a program e s.t,

1. PA proves that the sequence enumerated by e is finite.
2. In the standard model $N \models \text{PA}$, program e enumerates the empty sequence.
3. For any model $M \models \text{PA}$ in which e enumerates a finite (possibly nonstandard) sequence s , and any finite $t \in M$ extending s , there is an end-extension of M to a model $M' \models \text{PA}$ in which e enumerates exactly t .

In particular, every finite sequence s is enumerated by e in some model $M \models \text{PA}$.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory
Turing Machine

Computability

Diagonal Method

Incompressibility Method

Incompleteness

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Incompressibility Method

1. In order to prove that an object in a certain class on average satisfies a certain property, select an object of that class that is incompressible.
2. Show that if it does not satisfy the property then it can be compressed by clever computable coding.
3. In general almost all objects of a given class are incompressible, therefore almost all objects in the class have the property involved.

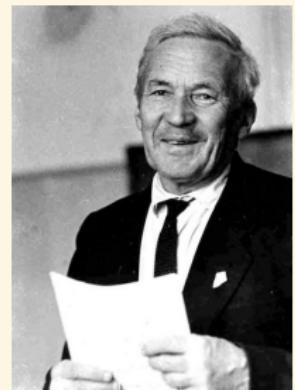


Figure: Kolmogorov

The Infinity of Primes

Theorem (Euclid's Theorem)

There are infinitely many prime numbers.

Proof by Contradiction.

Assume to the contrary that $\mathbb{P} := \{p_1, p_2, \dots, p_k\}$ is finite. Let $N := \prod_{i=1}^k p_i$.
 $\exists p \in \mathbb{P} : p \mid (N + 1) \ \& \ p \mid N \implies p \mid 1$.

Proof by Incompressibility Method — Chaitin.

$$n = \prod_{i=1}^m p_i^{e_i}$$

For a random n ,

$$\begin{aligned}\log n &\leq K(n) \\ &\stackrel{+}{\leq} K(\langle e_1, \dots, e_m \rangle) \\ &\stackrel{+}{\leq} \sum_{i=1}^m K(e_i) \\ &\stackrel{+}{\leq} mK(\log n) \\ &\stackrel{+}{\leq} m(\log \log n + 2 \log \log \log n)\end{aligned}$$



Proof by Combinatorics.

$$n = \prod_{i=1}^m p_i^{e_i} \implies e_i \leq \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor \implies$$
$$\# \left\{ (e_1, \dots, e_m) : \prod_{i=1}^m p_i^{e_i} \leq n \right\} \leq \prod_{i=1}^m \left(\left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor + 1 \right) \leq (\ln n)^m \ll n$$

Proof by Combinatorics — Erdős.

For $N \in \mathbb{N}$, we write every $n \leq N$ in the form $n = rs^2$, where r is the square-free part. There are $2^{\#\mathbb{P}}$ different square-free parts. Furthermore, $s \leq \sqrt{N}$. Hence $N \leq \# \{(r, s) : rs^2 \leq N \text{ and } r \text{ is square-free}\} \leq 2^{\#\mathbb{P}} \sqrt{N}$.

Proof by Coprime Sequence.

Let $n > 1$. Then n and $n + 1$ must be coprime, and hence $N_2 := n(n + 1)$ must have at least 2 different prime factors. Similarly, $n(n + 1)$ and $n(n + 1) + 1$ are coprime, $N_3 := n(n + 1)[n(n + 1) + 1]$ must have at least 3 different prime factors. This can be continued indefinitely.

Proof by Coprime Sequence.

Fermat number $F_n := 2^{2^n} + 1$. It is easy to verify that $\prod_{k=0}^{n-1} F_k = F_n - 2$, and any two Fermat numbers are coprime, hence there must be infinitely many primes.

Proof.

For any n , the prime factor of $n! + 1$ must be larger than n .

Proof by Bertrand's Postulate.

$$\forall n \geq 1 \exists p \in \mathbb{P} : n < p \leq 2n.$$

Proof by Prime Number Theorem.

The prime-counting function $\pi(x) \sim \frac{x}{\ln x}$.

Proof by Euler's Phi Function.

Euler's phi function $\varphi(n) := \#\{k : 1 \leq k \leq n \text{ } \& \text{ } \gcd(n, k) = 1\}$. We know

$$\gcd(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

Then $\varphi\left(\prod_{i=1}^n p_i\right) = \prod_{i=1}^n (p_i - 1) \geq 2$. Hence $\exists m \forall p_i \in \{p_1, \dots, p_n\} : p_i \nmid m$.

Proof by Euler Product Formula.

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}$$

$\zeta(2) = \frac{\pi^2}{6}$ is irrational. If \mathbb{P} were finite, then $\zeta(2)$ would be rational.

Euler.

$$\begin{aligned} \ln x &\leq \sum_{n \leq x} n^{-1} \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} p^{-k} \right) = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} (1 - p^{-1})^{-1} = \prod_{n=1}^{\pi(x)} \left(1 + \frac{1}{p_n^{-1}} \right) \leq \\ &\prod_{n=1}^{\pi(x)} \left(1 + \frac{1}{n} \right) = \pi(x) + 1. \end{aligned}$$

Proof by Lagrange's Theorem.

Let $p := \max \mathbb{P}$. Let q be a prime dividing $2^p - 1$. We have $2^p \equiv 1 \pmod{q}$. This means that the element 2 has order p in the multiplicative group $\mathbb{Z}_q \setminus \{0\}$ of the field \mathbb{Z}_q . This group has $q - 1$ elements. By Lagrange's theorem we have $p \mid (q - 1)$. Hence $q > p$.

Proof by Topology — Fürstenberg.

Let

$$N_{a,b} := \{an + b : n \in \mathbb{Z}\}$$

We call a set $O \subset \mathbb{Z}$ open if $O = \emptyset$ or $\forall x \in O \exists N_{a,b} \subset O : x \in N_{a,b}$.

Note that any non-empty open set is infinite.

And $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{a-1} N_{a,b+i}$ is clopen.

Since every integer $\mathbb{Z} \setminus \{-1, +1\}$ has a prime factor, then

$$\mathbb{Z} \setminus \{-1, +1\} = \bigcup_{p \in \mathbb{P}} N_{p,0}$$

If \mathbb{P} were finite, then $\bigcup_{p \in \mathbb{P}} N_{p,0}$ would be closed.

Consequently, $\{-1, +1\}$ would be open. Contradiction!

Proof.

Let $f(n) := \#\{k \in \mathbb{P} : p \mid n\}$, and $P := \prod_{p \in \mathbb{P}} p$. Obviously,
 $\forall n : f(n) = f(n + P)$. However, $f(n) = 0 \implies n = 1$.

Proof.

$$0 < \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi}{p}\right) = \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi \left(1 + 2 \prod_{p \in \mathbb{P}} p\right)}{p}\right) = 0$$

Proof.

Consider $P := \prod_{i=2}^n p_i$. Obviously, $\{k \in \mathbb{N} : \gcd(k, P) = 1\} = \{2^i : i \in \mathbb{N}\}$. In particular, $\gcd(2, P) = 1$, then $\gcd(P - 2, P) = 1$. Therefore, $P - 2 \in \{2^i : i \in \mathbb{N}\}$ and $2 \nmid (P - 2)$. Hence $P - 2 = 1$, i.e. $P = 3$. It means that 3 is the greatest prime number.

Halting Problem

Theorem (Halting Problem is Undecidable)

There is no computable function deciding whether a program halts.

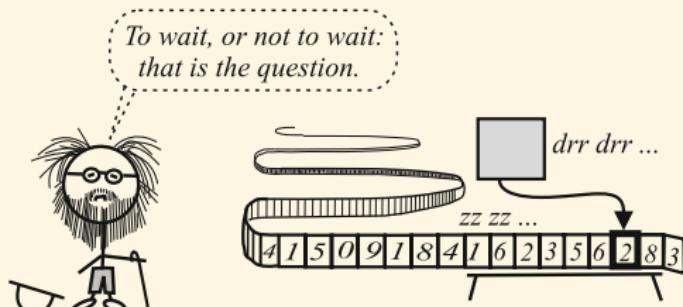
Proof.

Assume there exists a halting program H .

Construct a program q as follows:

1. read n ;
2. generate $A := \{p : \ell(p) \leq n\}$;
3. use H to get
 $B := \{p \in A : U(p) \downarrow\}$;
4. output $2 \max\{U(p) : p \in B\}$.

$$\ell(q) \stackrel{?}{\leq} \log n \lesssim n \implies U(q) \geq 2U(q)$$



Incompressibility vs Incompleteness vs Berry Paradox

Theorem (Kolmogorov)

Kolmogorov complexity K is uncomputable.

$$x^* := \mu x [K(x) > n] \implies n < K(x^*) \leq O(\log n)$$

Theorem (Chaitin)

For any arithmetically sound Gödelian T , $\exists c \forall x : T \not\vdash K(x) > c$.

“given n , find $\mu y [\text{prf}_T(y, K(x) > n)]$, output x ” $\implies n < K(x) \leq O(\log n)$

“the least number undefinable in fewer characters than there are in this sentence.”

$M_e :=$ “find $\mu y [\text{prf}_T(y, K(x) > e)]$, output x ” (Berry Paradox)

Theorem (Chaitin)

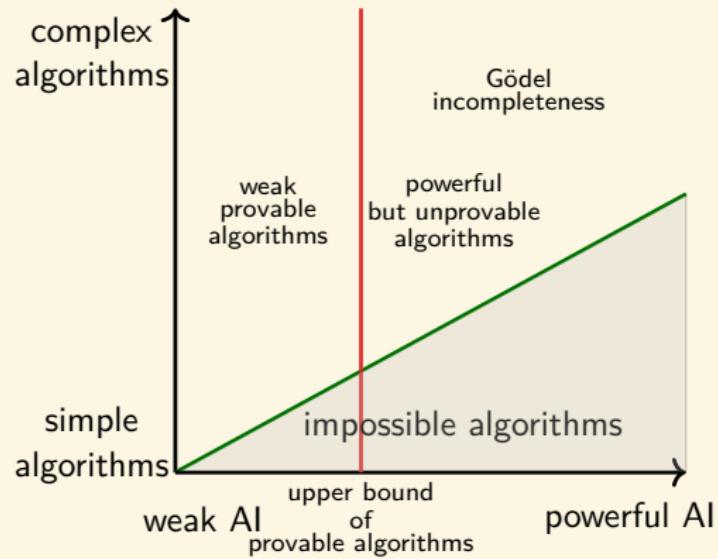
For any arithmetically sound Gödelian T , $|\{x : T \vdash K(x) > \ell(x)\}| < \infty$.

Remark: For almost all random strings their randomness cannot be proved.

Incompressibility vs Incompleteness vs Intelligence

- ▶ $P(x) := \{p \in X^* : \exists m \forall n \geq m (p(x_{1:n}) = x_{n+1})\}$
- ▶ $P(A) := \bigcap_{x \in A} P(x)$
- ▶ $P_n := P(\{x : K(x) \leq n\})$

- ▶ $\forall n \exists p \in P_n : K(p) \stackrel{+}{\leq} n + O(\log n)$
- ▶ $\forall n : p \in P_n \implies K(p) \stackrel{+}{\geq} n$



Theorem (Legg)

For any arithmetically sound Gödelian T , $\exists m \forall n \geq m \forall p : T \not\vdash p \in P_n$.

"given n , find $\mu x [\text{prf}_T (x, p \in P_n)]$, output p " $\implies K(p) < O(\log n)$

Halting Probability

Definition (Halting Probability)

$$E_t := \{p : U(p) \downarrow \text{in at most } t \text{ steps}\}$$

$$E := E_\infty$$

$$\Omega^t := \sum_{p \in E_t} 2^{-\ell(p)}$$

$$\Omega := \Omega^\infty$$

$$t(n) := \mu t[\Omega^t \geq \Omega_{1:n}]$$

Obviously,

$$\Omega^1 \leq \dots \leq \Omega^i \leq \Omega^{i+1} \leq \dots \xrightarrow{i \rightarrow \infty} \Omega$$

and

$$\Omega_{1:n} \leq \Omega < \Omega_{1:n} + 2^{-n}$$

and $t(n)$ is computable with Oracle Ω .

Halting Probability

Lemma

$$\Omega \equiv_T \chi_E$$

Proof.

If a program p of length $\leq n$ is not in $E_{t(n)}$ then it is not in E at all.

Otherwise,

$$\Omega^t + 2^{-n} \leq \Omega^t + 2^{-\ell(p)} < \Omega$$

conflicts with

$$\Omega_{1:n} \leq \Omega^t < \Omega < \Omega_{1:n} + 2^{-n}$$

It follows that $\chi_{E_{1:2^n}}$ can be computed from $\Omega_{1:n}$.

Remark: Ω is a “philosopher’s stone”. Knowing Ω to an accuracy of n bits will enable us to decide the truth of any provable or finitely refutable mathematical theorem that can be written in less than n bits.

Randomness of Ω

Theorem (Randomness of Ω)

$$\exists c \forall n : K(\Omega_{1:n}) \geq n - c$$

Proof.

$$f(\Omega_{1:n}) := \mu x [2^{<\omega} \setminus \{U(p) : p \in E_{t(n)}\}]$$

Obviously, f is computable.

$$n < K(f(\Omega_{1:n})) \stackrel{+}{\leq} K(\Omega_{1:n}) + K(f) \stackrel{+}{\leq} K(\Omega_{1:n})$$

Theorem (Chaitin Diophantine Incompleteness)

There is an exponential diophantine equation

$$L(n, x_0, x_1, \dots, x_m) = R(n, x_0, x_1, \dots, x_m)$$

which has finitely many solutions x_0, x_1, \dots, x_m iff $\Omega_n = 0$.

Proof.

$$A := \{\langle n, k \rangle : \Omega_n^k = 1\} \text{ is r.e.}$$

Since a set is r.e. iff it is singlefold exponential Diophantine,
hence there exists $L(y, x_0, x_1, \dots, x_m) = R(y, x_0, x_1, \dots, x_m)$ s.t.

$$\langle n, k \rangle \in A \iff \exists! \langle x_1, \dots, x_m \rangle (L(n, k, x_1, \dots, x_m) = R(n, k, x_1, \dots, x_m))$$

Thereby, $L(n, k, x_1, \dots, x_m) = R(n, k, x_1, \dots, x_m)$ has exactly one solution
 x_1, \dots, x_m if $\Omega_n^k = 1$, and it has no solution if $\Omega_n^k = 0$.

Theorem (Chaitin Ω Incompleteness)

For any arithmetically sound Gödelian T , T can determine at most finitely many (scattered) bits of Ω .

Proof.

Assume T can provide infinitely many bits of Ω .

Any k different bits i_1, i_2, \dots, i_k of Ω give us a covering A_k of measure 2^{-k} which includes Ω .

$$A_k := \{s_1\Omega_{i_1} \cdots s_k\Omega_{i_k} 2^\omega : \forall 1 \leq j \leq k (s_j \in 2^{<\omega} \text{ & } \ell(s_j) = i_j - i_{j-1} - 1)\}$$

$$\mu(A_k) = \frac{2^{i_k - k}}{2^{i_k}} = 2^{-k}$$

Thereby,

$$\forall k [\mu(A_k) \leq 2^{-k} \text{ & } \Omega \in A_k]$$

which contradicts the Martin-Löf randomness of Ω .

Definition (Busy Beaver)

$$\Sigma(n) := \max\{x : K(x) \leq n\}$$

$$\sigma(n) := \mu t [\Omega_{1:n}^t = \Omega_{1:n}]$$

Lemma

$$\Sigma(n - K(n) - O(1)) \leq \sigma(n) \leq \Sigma(n + 2K(n) + O(1))$$

Proof.

$$\Omega_{1:n} = \Omega_{1:n}^{\sigma(n)} \implies K(\Omega_{1:n}) \leq K(n) + K(\sigma(n)) + O(1)$$

Since $\exists c \forall n : K(\Omega_{1:n}) \geq n - c$, we have $n - K(n) - O(1) \leq K(\sigma(n))$.

Thus $\Sigma(n - K(n) - O(1)) \leq \sigma(n)$.

From $\sigma(n) := \mu t [\Omega_{1:n}^t = \Omega_{1:n}]$ and $K(\Omega_{1:n}) \leq n + K(n) + O(1)$, we have

$$K(\sigma(n)) \leq K(n) + K(\Omega_{1:n}) + O(1) = n + 2K(n) + O(1)$$

Therefore

$$\sigma(n) \leq \Sigma(n + 2K(n) + O(1))$$

Busy Beaver

Lemma (Busy Beaver)

For any computable function f , $\Sigma \geq^+ f$ and $\sigma \geq^+ f$.

Proof.

$$K(f(n)) \stackrel{+}{\leq} K(n) + K(f) \lesssim n \implies \Sigma \stackrel{+}{\geq} f$$

Theorem (Chaitin Busy Beaver Incompleteness)

For any arithmetically sound Gödelian T , $\exists n \forall x : T \not\vdash \sigma(n) \leq x$.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory
Turing Machine

Computability

Diagonal Method

Incompressibility Method

Incompleteness

Equational Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

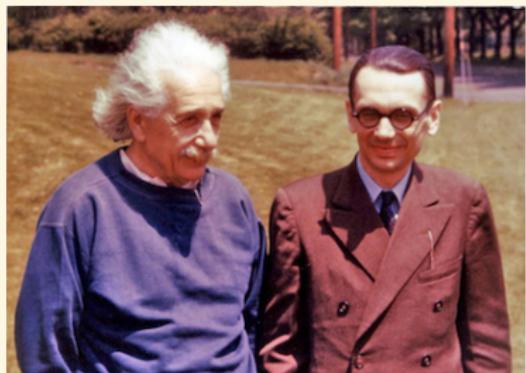
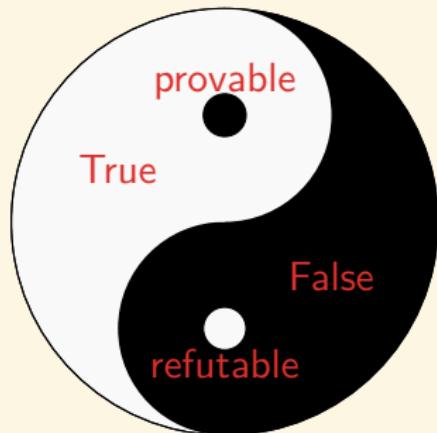
- ▶ M: It's one of the most important discoveries of the last decade!
- ▶ P: Can you explain it in words ordinary mortals can understand?
- ▶ M: Look, buster, if ordinary mortals could understand it, you wouldn't need mathematicians to do the job for you, right? You can't get a feeling for what's going on without understanding the technical details. How can I talk about manifolds without mentioning that **the theorems only work if the manifolds are finite-dimensional paracompact Hausdorff with empty boundary?**
- ▶ P: Lie a bit.
- ▶ M: Oh, but I couldn't do that!
- ▶ P: Why not? Everybody else does.
- ▶ M: Oh, no! Don't lie — because everybody else does.

Fixpoint Lemma

Lemma (Fixpoint Lemma)

For any wff $F(x)$ with one free variable x , there exists a sentence G s.t.

$$\mathbf{Q} \vdash G \leftrightarrow F(\neg G \neg)$$



Strong Fixpoint Lemma

Theorem (Strong Fixpoint Lemma)

For a theory T that is a primitively recursive axiomatised extension of PA and that has a function-symbol for each primitive recursive function, and for each one-free-variable-formula $F(x)$, there is a closed-term t s.t.

$$T \vdash t = {}^\lceil F(t) {}^\rceil$$

Proof.

Let $d : \mathbb{N} \rightarrow \mathbb{N}$ be the function s.t.

$$d(n) := \begin{cases} \#F(f({}^\lceil f {}^\rceil)) & \text{if } n = \#f \text{ for one-free-variable-function-symbol } f \\ 0 & \text{otherwise} \end{cases}$$

Since d is primitive recursive, it is represented by some function-symbol d .

$$T \vdash d({}^\lceil f {}^\rceil) = \underline{d(\#f)} = {}^\lceil F(f({}^\lceil f {}^\rceil)) {}^\rceil$$

$$T \vdash d({}^\lceil d {}^\rceil) = {}^\lceil F(d({}^\lceil d {}^\rceil)) {}^\rceil$$

Strong Fixpoint Lemma \implies Fixpoint Lemma.

Let $G := F(t)$. Then $G \leftrightarrow F(t) \leftrightarrow F({}^\lceil F(t) {}^\rceil) \leftrightarrow F({}^\lceil G {}^\rceil)$.

老子 ◎ô◎

- 道，可道，非常道；名，可名，非常名。
- 无名，天地之始；有名，万物之母。
- 故常无，欲以观其妙；常有，欲以观其微。
- 此两者，同出而异名，同谓之玄。
- 玄之又玄，众妙之门。

The theory that can be formulated can't be the ultimate theory. The formulated theory of categories evolves, and its projection on reality changes. The unformulatable ultimate theory is the truth of universe. The formulated theory is the basis to describe all the matter. In search of the unformulatable ultimate theory, we give meaning to life. Within the formulated theory, we study its limits. The gap between the formulatable and the unformulatable is a mystery. From the formulated to the unformulated and from the unformulated to the formulated is the gateway to all understanding.

Gödel's First Incompleteness Theorem

Theorem (Gödel's First Incompleteness Theorem)

For any Gödelian $T \supset Q$, there is a sentence G such that,

1. if T is consistent, $T \not\vdash G$
2. if T is ω -consistent, $T \not\vdash \neg G$

Gödel's First Incompleteness Theorem

$$F(x) := \neg \Box x$$

G = “I am not provable.”

$$T \vdash \text{Con}_T \rightarrow \neg \Box G$$

Proof.

$$\begin{aligned} G \leftrightarrow \neg \Box G &\implies \Box G \rightarrow \neg G \implies \Box(\Box G \rightarrow \neg G) \implies \Box G \rightarrow \Box \neg G \implies \\ \Box G \rightarrow \Box(G \wedge \neg G) &\implies \neg \Box \perp \rightarrow \neg \Box G \end{aligned}$$

We now know enough to know that
we will never know everything! ⑩^⑩

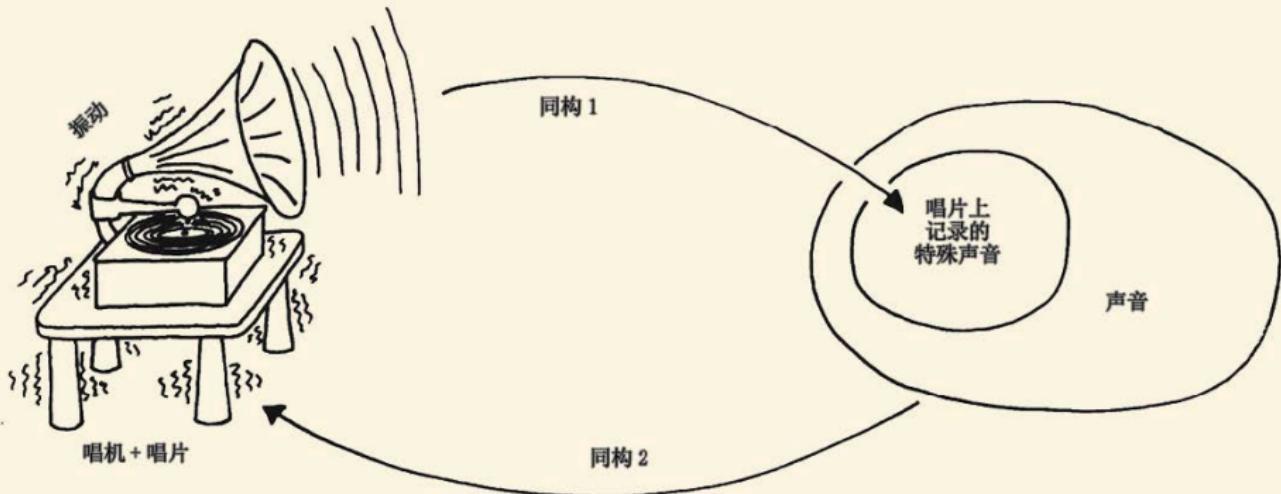


Figure: For every record player, there are records that it can't play. (sympathetic vibration)

Gödel-Rosser's Incompleteness Theorem

Theorem (Gödel's-Rosser First Incompleteness Theorem)

For any Gödelian $T \supset Q$, $Cn(T) \subsetneq \text{Th}(\mathcal{N})$.

Rosser's Trick

$$\Box^R x := \exists y [\text{prf}_T(y, x) \wedge \neg \exists z < y \text{ prf}_T(z, N(x))]$$

where $N : \Gamma A \vdash \mapsto \Gamma \neg A \vdash$

$$F(x) := \neg \Box^R x$$

$G = \text{"For every proof of me, there is a shorter proof of my negation."}$

Tarski's Undefinability of truth Theorem

Theorem (Tarski's Undefinability of truth Theorem)

There is no definable predicate $B(x)$ in the language of arithmetic, such that $\mathcal{N} \models A \leftrightarrow B(\Gamma A \neg)$.

suppose $\{\#A : \mathcal{N} \models A\}$ is definable by $B(x)$.

$$F(x) := \neg B(x)$$

$G = \text{"I am not true."}$

Montague's Fixpoint Lemma

Lemma (Fixpoint Lemma — Montague)

For any wff $F(x, y)$, there is a wff $G(x)$ s.t.

$$T \vdash \forall x(G(x) \leftrightarrow F(x, \neg G(x)))$$

Proof.

$$d(n) := \begin{cases} \#A(\neg A(x)) & \text{if } n = \#A(x) \\ 0 & \text{otherwise} \end{cases}$$

is primitive recursive and is thus represented by some function symbol d .

$$T \vdash d(\neg A(x)) = \neg A(\neg A(x))$$

$$E_x(y) := F(x, d(y))$$

$$G(x) := E_x(\neg E_x(y))$$

$$G(x) \leftrightarrow E_x(\neg E_x(y))$$

$$\leftrightarrow F(x, d(\neg E_x(y)))$$

$$\leftrightarrow F(x, \neg E_x(\neg E_x(y)))$$

$$\leftrightarrow F(x, \neg G(x))$$

$$T \vdash \forall x(G(x) \leftrightarrow F(x, \neg G(x)))$$

Remark: This is the form analogous to Second Recursion Theorem: If $f(x, y)$ is a partial recursive function, there is an index e s.t.

$$\varphi_e(y) = f(e, y)$$

Corollary

For any wff $F(x, y, z)$, there is a wff $G(x)$ s.t.

$$T \vdash \forall x(G(x) \leftrightarrow \forall y F(x, y, \neg G(y)))$$

Proof.

Apply the fixed point lemma to the formula

$$F'(x, v) := \forall y \exists z(\delta(v, y, z) \wedge F(x, y, z))$$

$$T \vdash \forall x(G(x) \leftrightarrow \forall y \exists z(\delta(\neg G(x), y, z) \wedge F(x, y, z)))$$

where $\exists z(\delta(\neg G(x), y, z) \wedge F(x, y, z)) \leftrightarrow F(x, y, \neg G(y))$

Yablo Paradox

Yablo Paradox

$$F(x, y, z) := y > x \rightarrow \neg \Box z$$

$$T \vdash \forall x (Y(x) \leftrightarrow \forall y > x \neg \Box Y(y))$$

- ▶ $T \vdash \text{Con}_T \rightarrow \forall x \neg \Box Y(x)$
- ▶ $T \vdash \forall x (Y(x) \leftrightarrow \text{Con}_T)$
- ▶ $T \vdash \forall x \forall y (Y(x) \leftrightarrow Y(y))$

Provability Conditions

Provability Conditions

For any Gödelian $T \supset PA$,

1. $T \vdash A \implies Q \vdash \Box_T A$
2. $PA \vdash \Box_T A \rightarrow \Box_T \Box_T A$
3. $PA \vdash \Box_T(A \rightarrow B) \rightarrow \Box_T A \rightarrow \Box_T B$

Löb's Theorem

Theorem (Löb's Theorem)

For any Gödelian $T \supset PA$, $T \vdash \Box(\Box A \rightarrow A) \rightarrow \Box A$.

Löb's Theorem

$$F(x) := \Box x \rightarrow A$$

G = “If I am provable, then A .”

Corollary

$$T \vdash \Box A \rightarrow A \implies T \vdash A$$

Proof.

$$\begin{aligned} T \vdash \Box G \rightarrow \Box \Box G \wedge \Box(\Box G \rightarrow A) &\implies T \vdash \Box G \rightarrow \Box A \implies T \vdash \Box G \rightarrow \\ A &\implies T \vdash G \implies T \vdash \Box G \implies T \vdash A \end{aligned}$$

Curry's Paradox

“If this sentence is true, then Santa Claus exists.”

Gödel's Second Incompleteness Theorem

Theorem (Gödel's Second Incompleteness Theorem)

For any Gödelian $T \supset PA$, $T \vdash \text{Con}_T \rightarrow \neg \Box \text{Con}_T$.

Proof.

$$T \vdash \Box(\Box \perp \rightarrow \perp) \rightarrow \Box \perp \implies T \vdash \text{Con}_T \rightarrow \neg \Box \text{Con}_T$$

$$PA \not\vdash \neg \Box_{PA} \text{Con}(PA)$$

$$PA \not\vdash \text{Con}(PA)$$

$$PA^* \vdash \neg \text{Con}(PA^*) \text{ where } PA^* = PA + \neg \text{Con}(PA)$$

Remark: The second incompleteness theorem does not imply that the consistency of a system T can only be proved in a stronger system.

Gödel's Second Incompleteness Theorem

$$T \vdash \text{Con}_T \rightarrow \text{Con}(T + \neg \text{Con}_T)$$

Proof.

$$T \vdash \text{Con}_T \rightarrow \neg \square \text{Con}_T$$

$$T \vdash \text{Con}_T \rightarrow \neg \square(\neg \text{Con}_T \rightarrow \perp)$$

$$T \vdash \text{Con}_T \rightarrow \text{Con}(T + \neg \text{Con}_T)$$

We have put a fence around the herd to protect it from the wolves but we do not know whether some wolves were already enclosed within the fence.

— Henri Poincaré

God exists because mathematics is consistent, and the devil exists because we can't prove the consistency.

— André Weil

Second Incompleteness Theorem

$T \not\vdash \text{Con}_T$

second incompleteness \implies Löb

Proof.

$$T \vdash G \leftrightarrow \neg \Box G$$

$$T \vdash G \rightarrow (\Box G \rightarrow \perp)$$

$$T \vdash \Box G \rightarrow \Box(\Box G \rightarrow \perp)$$

$$T \vdash \Box G \rightarrow \Box \perp$$

$$T \vdash \text{Con}_T \rightarrow \neg \Box G$$

$$T \vdash \text{Con}_T \implies T \vdash \neg \Box G$$

$$T \vdash \text{Con}_T \implies T \vdash G$$

$$T \vdash \text{Con}_T \implies T \vdash \Box G$$

$T \not\vdash \text{Con}_T$

Löb's Theorem

$$T \vdash \Box A \rightarrow A \iff T \vdash A$$

Proof.

Assume $T \not\vdash A$.

Then $T + \neg A$ is consistent.

$$T + \neg A \not\vdash \text{Con}(T + \neg A)$$

$$T + \neg A \not\vdash \neg \Box(\neg A \rightarrow \perp)$$

$$T + \neg A \not\vdash \neg \Box A$$

$$T \not\vdash \Box A \rightarrow A$$

Let G be the Gödel sentence s.t. $T \vdash G \leftrightarrow \neg \Box G$. Then

$$T \vdash G \leftrightarrow \text{Con}_T$$

Proof.

(\rightarrow):

$$T \vdash \perp \rightarrow G$$

$$T \vdash \Box \perp \rightarrow \Box G$$

$$T \vdash \Box \perp \rightarrow \neg G$$

$$T \vdash G \rightarrow \text{Con}_T$$

(\leftarrow):

$$T \vdash \Box G \rightarrow \Box \Box G$$

$$T \vdash \Box G \rightarrow \Box \neg G$$

$$T \vdash \Box G \rightarrow \Box(G \wedge \neg G)$$

$$T \vdash \text{Con}_T \rightarrow G$$

Fixpoint

1. For any Gödelian $T \supset PA$, Con_T is the only fixpoint of $\neg \Box x$ up to the logical equivalence in T .
2. For any Gödelian $T \supset PA$, \top is the only fixpoint of $\Box x$ up to the logical equivalence in T .

Surprise Exam Paradox vs Second Incompleteness Theorem

$$T \not\vdash \text{Con}_T$$

$$T \vdash \text{Con}_T \rightarrow \forall x \neg \Box(K(x) > c) \quad (\text{Chaitin})$$

$$T \vdash \text{Con}_T \implies T \vdash \forall x \in X^{c+1} \neg \Box(K(x) > c)$$

$$T \vdash \forall x \in X^{c+1} [K(x) \leq c \rightarrow \Box(K(x) \leq c)] \quad (\Sigma_1\text{-complete})$$

$$m := |\{x \in X^{c+1} : K(x) > c\}|$$

$$T \vdash 1 \leq m \leq 2^{c+1}$$

We prove by induction that for $1 \leq i \leq 2^{c+1}$,

$$T \vdash m \geq i \implies T \vdash m \geq i + 1$$

$$\mathbf{T} \vdash m \geq i \implies \mathbf{T} \vdash m \geq i + 1$$

Proof.

Assume $\mathbf{T} \vdash m \geq i$. Let $r := 2^{c+1} - i$.

$$\mathbf{T} \vdash m = i \rightarrow \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^r (K(y_k) \leq c)$$

$$\mathbf{T} \vdash m = i \rightarrow \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^r \square(K(y_k) \leq c)$$

$$\forall x \in \mathcal{X}^{c+1} \setminus \{y_1, \dots, y_r\} : \mathbf{T} \vdash m \geq i \rightarrow \left(\bigwedge_{k=1}^r (K(y_k) \leq c) \rightarrow (K(x) > c) \right)$$

$$\mathbf{T} \vdash \square(m \geq i) \rightarrow \left(\bigwedge_{k=1}^r \square(K(y_k) \leq c) \rightarrow \square(K(x) > c) \right)$$

$$\mathbf{T} \vdash m = i \wedge \square(m \geq i) \rightarrow \exists x \in \mathcal{X}^{c+1} \square(K(x) > c)$$

$$\mathbf{T} \vdash m \neq i$$

Completeness Properties

- ▶ syntactic completeness: $\Box A \vee \Box \neg A$
- ▶ semantic completeness: $A \rightarrow \Box A$
- ▶ ω -completeness: $\forall x \Box A(\dot{x}) \rightarrow \Box \forall x A(x)$

ω -complete \implies ω -consistent \implies 1-consistent \implies consistent

Theorem

For any Gödelian $T \supset PA$, the following are equivalent in T .

1. $\neg \text{Cont}_T$
2. $\Box A \vee \Box \neg A$
3. $A \rightarrow \Box A$
4. $\forall x \Box A(\dot{x}) \rightarrow \Box \forall x A(x)$

1. consistency
2. effectiveness $\text{Th}(\mathcal{N})$
3. richness Real closed field/Euclidean geometry/Presburger
4. completeness \mathbb{Q} / PA / ZFC

Parikh Sentences

Parikh Sentences

There are true sentences that have very long proofs, but there are relatively short proof of the fact that the sentences are provable.

$\text{prflen}_T(m) := \text{"the length of the proof encoded by } m\text{"}$

$\Box^n x := \exists m (\text{prf}_T(m, x) \wedge \text{prflen}_T(m) < n)$

$F(x) := \neg \Box^n x$

$G = \text{"I have no proof of myself shorter than } n.\text{"}$

$\neg \Box G \implies G \implies \Box G$

Gödel's No-short-proof Theorem

Theorem (Gödel's No-short-proof Theorem)

Let f be any primitive recursive function of one variable. Then there is a formula $G(x)$ of one free variable such that $\forall x G(x)$ is true, but for each n , $G(n)$ has no proof with fewer than $f(n)$ steps.

Gödel's No-short-proof Theorem

$$F(x) := \neg \Box^{f(y)} x$$

$G(y) = \text{"I have no proof of myself shorter than } f(y).$ "

$$\neg G(n) \implies \Box^{f(n)} G(n) \implies G(n)$$

Remark: it is easily seen that the fixpoint lemma applies also to formulas with free variables.

Gödel's no-short-proof theorem $\implies T \not\vdash \forall x G(x)$

Undecidability

Q is incomplete.

Theorem (Σ_1 -completeness of Robinson Arithmetic Q)

For any Gödelian $T \supset Q$, and any sentence $A \in \Sigma_1$, $Q \vdash A \rightarrow \Box A$.

Theorem (Strong Undecidability of Q)

If $T \cup Q$ is consistent, then T is undecidable.

Remark: In fact, the above is true for any countable \mathcal{L} containing a k -ary predicate or function symbol, $k \geq 2$, or at least two unary function symbols.

First order logic $\mathcal{L}_{\omega\omega}$ is undecidable.

Theorem (Church1936, Turing1936)

The set of valid sentences is recursively enumerable but undecidable.

Undecidability

Theorem (Trakhtenbrot's Theorem)

Suppose \mathcal{L} contains at least one binary relation symbol.

- The set of finitely satisfiable sentences is recursively enumerable,
- but it is undecidable whether a sentence is finitely satisfiable.
- The set of sentences valid in all finite structures is not recursively enumerable.

Remark:

1. This implies that Gödel's completeness theorem fails in the finite since completeness implies recursive enumerability.
2. It follows that there is no recursive function f s.t.: if a wff A has a finite model, then it has a model of size at most $f(A)$. In other words, there is no effective analogue to the Löwenheim-Skolem theorem in the finite.

Undecidability

Problem (Post Correspondence Problem)

Given n pairs of words:

$$(w_1, v_1), \dots, (w_n, v_n)$$

is there a sequence of indices (i_1, \dots, i_k) with $k \geq 1$ s.t.

$$w_{i_1} \dots w_{i_k} \stackrel{?}{=} v_{i_1} \dots v_{i_k}$$

Example

$(a, baa), (ab, aa), (bba, bb)$	$(3, 2, 3, 1)$
$(1, 101), (10, 00), (011, 11)$	$(1, 3, 2, 1)$
$(110, 0), (00, 1)$	no solution

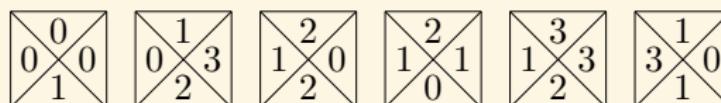
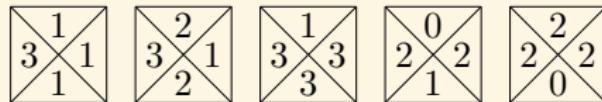
Theorem (Post 1946)

Post Correspondence Problem is undecidable.

Undecidability

Problem (Wang's Tiling Problem)

Wang's tiling problem (of determining whether a tile set can tile the plane) is undecidable.



$0 \mapsto \text{white}$

$1 \mapsto \text{red}$

$2 \mapsto \text{blue}$

$3 \mapsto \text{green}$

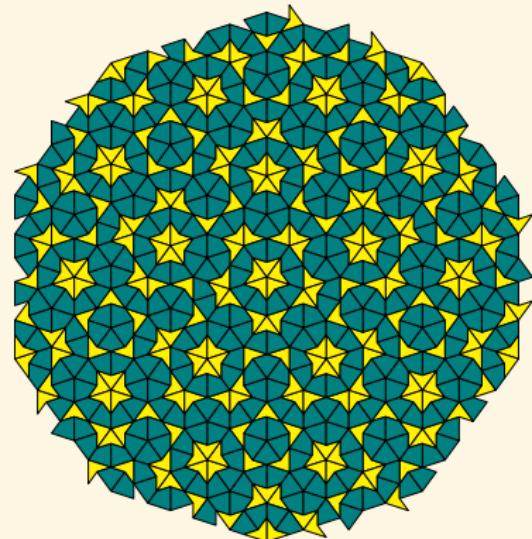
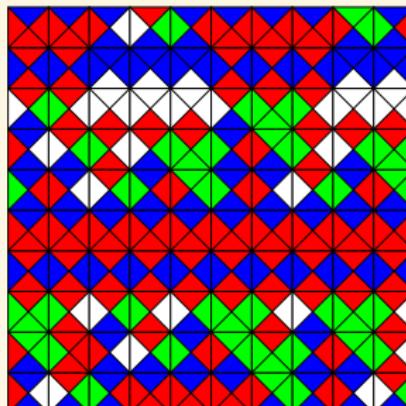


Figure: Penrose Tiling

王浩铺砖



- ▶ 是否有算法判定任给有穷个四色砖块能否铺满整个平面？否！
- ▶ 是否存在有穷个砖块能铺满平面但只能非周期性的铺满？是！
- ▶ 王浩铺砖可以模拟图灵机的运行。
- ▶ Berger 证明：一个图灵机不停机当且仅当相应砖块集铺满整个平面。
- ▶ 可以用一个一阶逻辑公式描述这样的铺砖问题，使得这个公式可满足当且仅当存在这样的铺砖。例如，可以用一阶逻辑说：只有几种砖块，任意两个相邻的砖块的相接的颜色是一样的，每个砖块上下左右都有相邻的砖块。所以一阶逻辑的可满足性（及有效性）不可判定。

Hilbert's 10th Problem is Unsolvable

Definition (Diophantine Set)

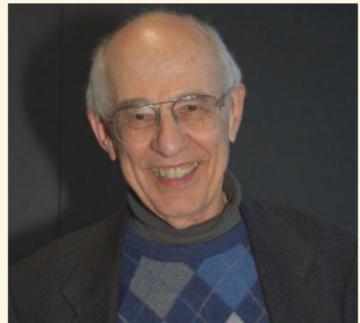
A set $A \subset \mathbb{N}^n$ is diophantine iff there exists a polynomial $P(x, y)$ with integer coefficients s.t.

$$x \in A \iff \exists y \in \mathbb{N}^m [P(x, y) = 0]$$

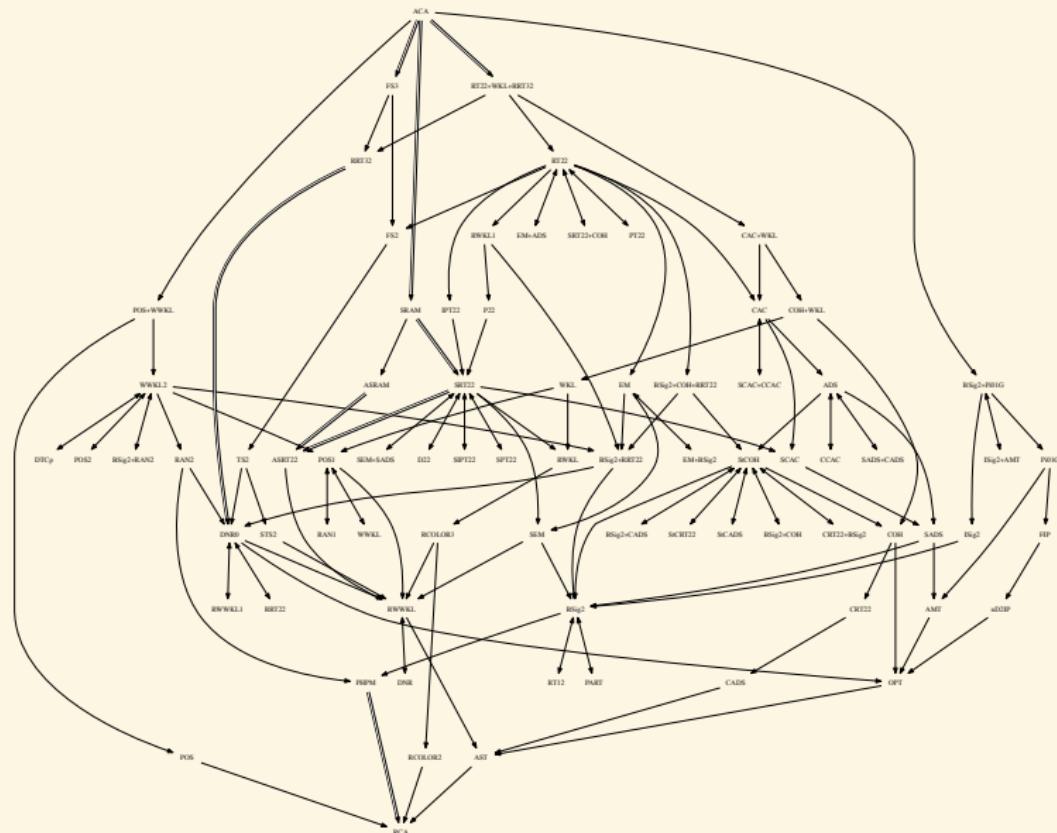
Theorem (MRDP Theorem — Matiyasevich, Robinson, Davis, Putnam)

A subset of \mathbb{N} is r.e. iff it is diophantine.

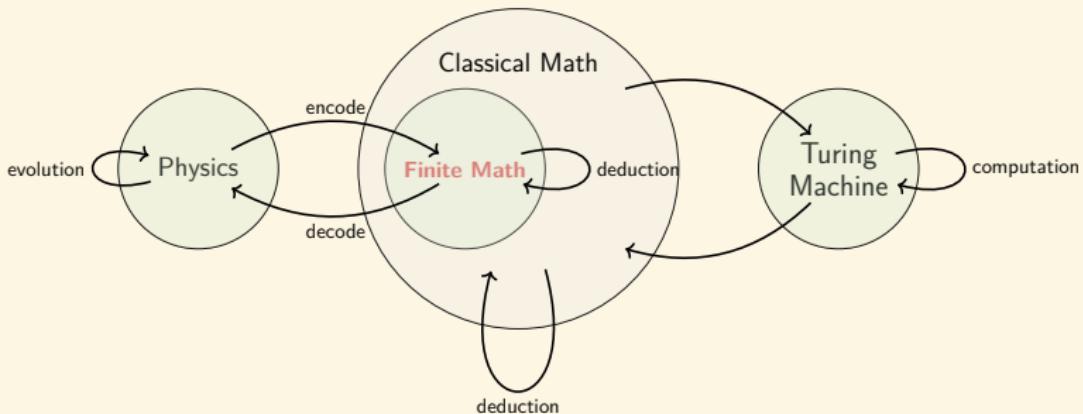
There is no algorithm for deciding whether an arbitrary diophantine equation has a solution.



Reverse Mathematics



The Applicability (Unreasonable Effectiveness) of Mathematics

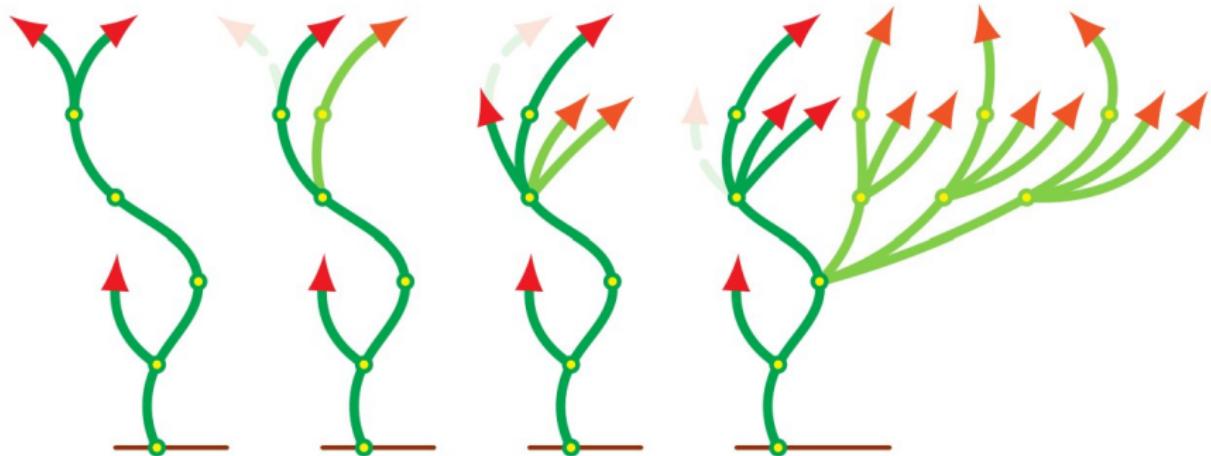


$$\frac{\Gamma_r \cup \Gamma_m \cup \Gamma_b \vdash A \quad \mathcal{M}_r \models \Gamma_r}{\mathcal{M}_r \models A} \quad ?$$

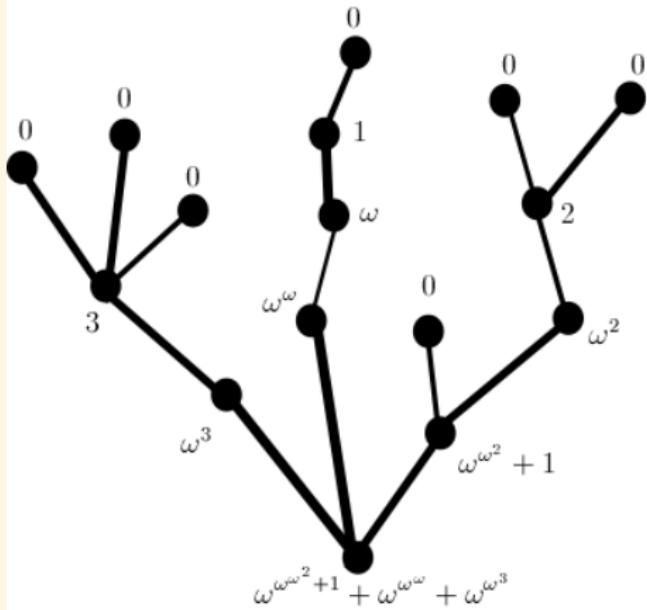
$$\frac{\Gamma_r \cup \Gamma'_r \vdash A \quad \mathcal{M}_r \models \Gamma_r \cup \Gamma'_r}{\mathcal{M}_r \models A}$$

where $\Gamma'_r \subset \Gamma_m \cup \Gamma_b$

When you come across the Hydra — “natural” vs “ad-hoc”



When you come across the Hydra — “natural” vs “ad-hoc”



Problem

Is there a winning strategy?

Goodstein Theorem

You can't lose!

Theorem (Kirby-Paris Theorem)

Any formal system that proves Goodstein Theorem is strong enough to prove that PA is consistent.

Goodstein Function

Definition (Goodstein Function)

Define $G_n(m)$ as follows: if $m = 0$ then $G_n(m) = 0$, if $m \neq 0$ then $G_n(m)$ is a number obtained by replacing every n in the base n representation of m by $n + 1$ and then subtracting 1. Let

$$m_0 := m$$

$$m_k := G_{k+1}(m_{k-1})$$

$$f_G(m) := \mu k [m_k = 0]$$

$$m_0 = 266 = 2^{2^{2+1}} + 2^{2+1} + 2^1$$

$$m_1 = G_2(m_0) = 3^{3^{3+1}} + 3^{3+1} + 2 \approx 10^{38}$$

$$m_2 = G_3(m_1) = 4^{4^{4+1}} + 4^{4+1} + 1 \approx 10^{616}$$

$$m_3 = G_4(m_2) = 5^{5^{5+1}} + 5^{5+1} \approx 10^{10000}$$

Fast-growing Hierarchy

Definition (Wainer Hierarchy)

$$f_0(n) := n + 1$$

$$f_{\alpha+1}(n) := f_\alpha^n(n)$$

$f_\alpha(n) := f_{\alpha[n]}(n)$ if α is a limit ordinal.

For limit ordinals $\lambda < \varepsilon_0$, written in Cantor normal form,

- ▶ if $\lambda = \omega^{\alpha_1} + \dots + \omega^{\alpha_k}$ for $\alpha_1 \geq \dots \geq \alpha_k$,
then $\lambda[n] := \omega^{\alpha_1} + \dots + \omega^{\alpha_k}[n]$
- ▶ if $\lambda = \omega^{\alpha+1}$, then $\lambda[n] := \omega^\alpha[n]$
- ▶ if $\lambda = \omega^\alpha$ for a limit ordinal α , then
 $\lambda[n] := \omega^{\alpha[n]}$
- ▶ if $\lambda = \varepsilon_0$, then $\lambda[0] := 0$ and
 $\lambda[n+1] := \omega^{\lambda[n]}$

- ▶ $\alpha < \beta < \varepsilon_0 \implies f_\alpha < f_\beta$
- ▶ For any primitive recursive function f ,
 $\exists \alpha < \omega : f < f_\alpha$
- ▶ Every f_α with $\alpha < \varepsilon_0$ is computable, and provably total in PA.
- ▶ If f is computable and provably total in PA, then
 $\exists \alpha < \varepsilon_0 : f < f_\alpha$. Hence f_{ε_0} is not provably total in PA.

Kirby-Paris Theorem vs Goodstein Theorem

Theorem

$$\forall \alpha < \varepsilon_0 (f_\alpha < f_G)$$

$$\text{ZFC} \vdash \forall m \exists k (m_k = 0) \quad \text{but} \quad \text{PA} \not\vdash \forall m \exists k (m_k = 0)$$

$$\Sigma(n) := \max\{m : K(m) \leq n\}$$

$f < \Sigma$ for any computable f

$$\text{PA} \not\vdash \forall n \exists m (\Sigma(n) = m)$$

$$\exists n \forall m : \text{PA} \not\vdash \Sigma(n) \leq m$$

For any arithmetically sound Gödelian T : $\exists n \forall m : T \not\vdash \Sigma(n) \leq m$

Paris-Harrington Theorem vs Ramsey Theorem

$$[A]^n := \{X \subset A : |X| = n\}$$

$$\kappa \rightarrow (\lambda)_m^n := \forall F : [\kappa]^n \rightarrow m \left(\exists H \subset \kappa \left(|H| = \lambda \wedge \exists i \in m \left([H]^n \subset F^{-1}(i) \right) \right) \right)$$

Ramsey theorem: $\forall mn \in \omega : \aleph_0 \rightarrow (\aleph_0)_m^n$

$$s \rightarrow (k_0, \dots, k_{m-1})_m^n := \forall F : [s]^n \rightarrow m \left(\bigvee_{i=0}^{m-1} \exists H \subset s \left(|H| = k_i \wedge [H]^n \subset F^{-1}(i) \right) \right)$$

$$s \xrightarrow{*} (k)_m^n := \forall F : [s]^n \rightarrow m \left(\exists H \subset s \left(|H| \geq \min(H) \wedge |H| \geq k \wedge \exists i \in m \left([H]^n \subset F^{-1}(i) \right) \right) \right)$$

$$\text{ZFC} \vdash \forall mnk \exists s \left(s \xrightarrow{*} (k)_m^n \right)$$

$$\text{PA} \not\vdash \forall mnk \exists s \left(s \xrightarrow{*} (k)_m^n \right)$$

$$\forall \alpha < \varepsilon_0 (f_\alpha < f_R) \quad \text{where } f_R(m, n, k) := \mu s \left[s \xrightarrow{*} (k)_m^n \right]$$

Leibniz — Hilbert — Gödel — Turing ...

- ▶ $G_T :=$ “This sentence cannot be proved in the formal axiomatic system T ”
- ▶ We humans can easily see that G_T must be true.
- ▶ Since any AI is a FAS T , no AI can prove G_T . — Penrose
- ▶ Therefore there are things humans, but no AI system can do.
- ▶ $P :=$ “Penrose can't consistently assert that this sentence is true”
- ▶ Penrose cannot assert P , but now we can conclude that it is true.
- ▶ Penrose is in the same situation as an AI.
- ▶ Either (a) absolutely unsolvable problems exist or (b) the human mind infinitely surpasses any Turing machine or axiomatizable formal system. — Gödel
- ▶ Hayek: social spontaneous order?
- ▶ Hawking: ‘Theory of Everything’ impossible?

Ingenuity, Intuition and Creativity

Logic will get you from A to B; Imagination will take you everywhere.

— Albert Einstein

No, no, you're not thinking; you're just being logical.

— Niels Bohr

The ultimate goal of mathematics is to eliminate any need for intelligent thought.

— Alfred Whitehead

Eliminate not intuition but ingenuity.

— Alan Turing

The logical process is essentially creative.

— Emil Post

Logic may be said to be Mathematics become self-conscious.

— Emil Post

Strength & Limitation

God plays dice both in quantum mechanics and in pure math.

— Gregory Chaitin

It is the duty of the human understanding to understand that there are things which it can't understand, and what those things are.

— Søren Kierkegaard

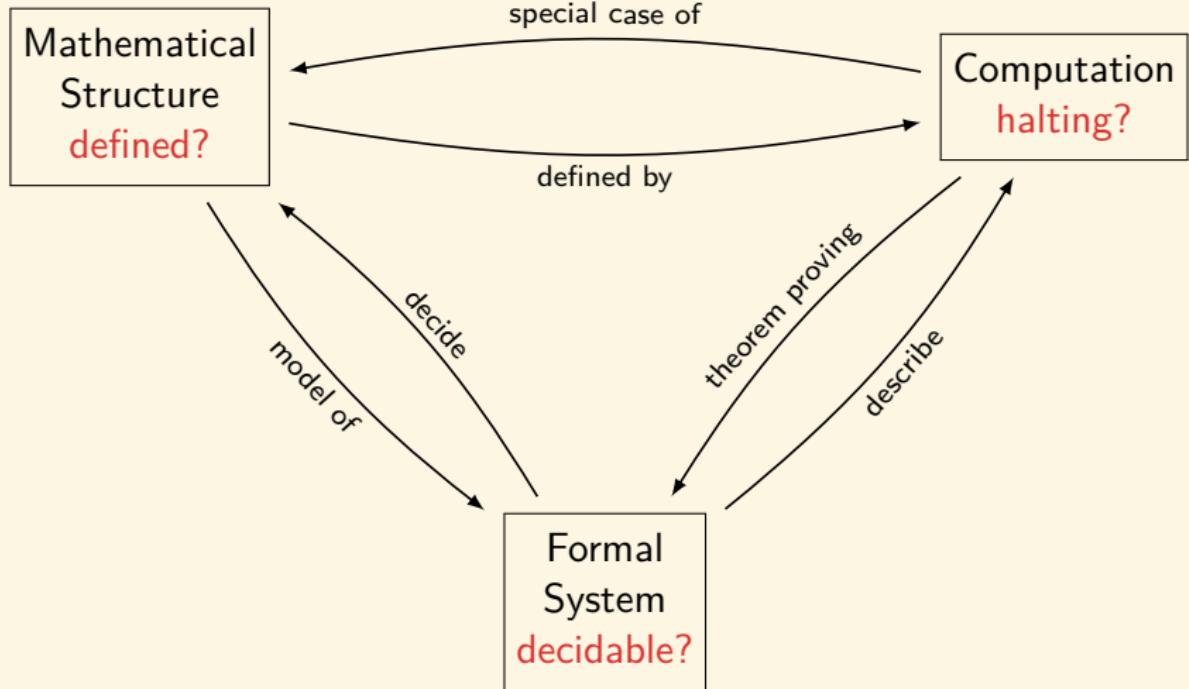
The only way of discovering the limits of the possible is to venture a little way past them into the impossible.

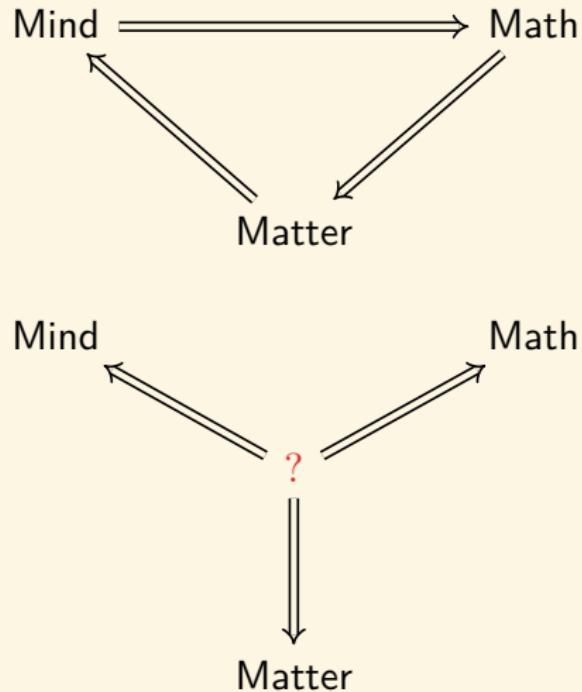
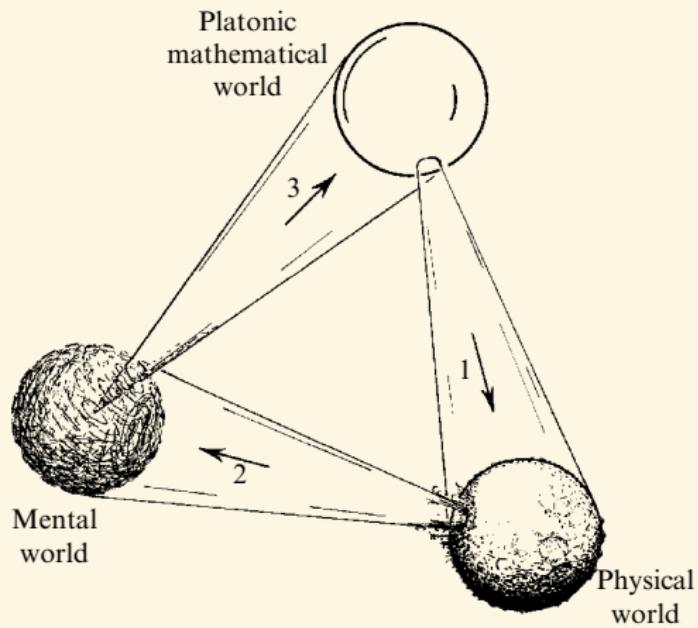
— Arthur Charles Clarke



Царство небесное

Math-Matter-Mind (Penrose)





Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Equational Logic

Boolean Algebra

Lambda Calculus and
Combinatory Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Why Study Equational Logic?

- ▶ Propositional logic has very limited expressive power.
- ▶ Equational Logic is powerful enough to express propositional logic.
- ▶ It underlies the mathematical field of universal algebra.
- ▶ The basis of programming and specification languages.

Syntax

Language

$$\mathcal{L}^= := \{=, (,)\} \cup \text{Var} \cup \text{Fun}$$

where

$$\text{Var} := \{x_i : i \in \mathbb{N}\}$$

$$\text{Fun} := \bigcup_{n \in \mathbb{N}} \text{Fun}^n \quad \text{Fun}^n := \{f_1^n, f_2^n, f_3^n, \dots\}$$

f^n is an n -place function symbol.

A 0-place function symbol f^0 is called constant.

Term & Formula

Term

$$t ::= x \mid c \mid f(t, \dots, t)$$

where $x \in \text{Var}$ and $f \in \text{Fun}$.

Well-Formed Formula Wff

$$A ::= s = t$$

where $s, t \in \text{Term}$.

Semantics

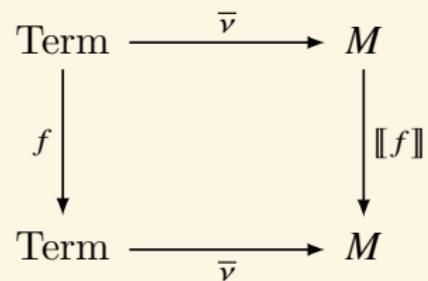
A **structure** is a pair $\mathcal{M} := (M, \llbracket \rrbracket)$, where M is a non-empty set, and $\llbracket \rrbracket$ is a mapping which assigns to each constant symbol an element $\llbracket c \rrbracket \in M$, and assigns each function symbol f an n -ary function $\llbracket f \rrbracket : M^n \rightarrow M$. We write $\mathcal{M} = (M, \llbracket c \rrbracket, \llbracket f \rrbracket)$ or $(M, c^{\mathcal{M}}, f^{\mathcal{M}})$ for convenience.

An **interpretation** (\mathcal{M}, ν) is a structure \mathcal{M} with a variable assignment $\nu : \text{Var} \rightarrow M$.

We extend ν to $\bar{\nu} : \text{Term} \rightarrow M$ by recursion as follows:

Assignment over Terms

- ▶ $\bar{\nu}(x) = \nu(x)$
- ▶ $\bar{\nu}(c) = \llbracket c \rrbracket$
- ▶ $\bar{\nu}(f(t_1, \dots, t_n)) = \llbracket f \rrbracket(\bar{\nu}(t_1), \dots, \bar{\nu}(t_n))$



Semantics

- $\mathcal{M}, \nu \models s = t$ iff $\bar{\nu}(s) = \bar{\nu}(t)$. (Satisfaction)
- $\mathcal{M} \models s = t$ iff for all $\nu : \mathcal{M}, \nu \models s = t$. (True)
- $\mathcal{M} \models T$ iff for all $A \in T : \mathcal{M} \models A$. (Model)
- $T \models s = t$ iff for all $\mathcal{M} : \mathcal{M} \models T \implies \mathcal{M} \models s = t$.
- $\models s = t$ iff $\emptyset \models s = t$. (Valid)

Formal System

Birkhoff's Rules

$$\frac{}{t = t} \text{ [refl]}$$

$$\frac{s = t}{t = s} \text{ [symm]}$$

$$\frac{r = s \quad s = t}{r = t} \text{ [trans]}$$

$$\frac{s = t}{r(\dots s \dots) = r(\dots t \dots)} \text{ [rep]}$$

$$\frac{r(x_1, \dots, x_n) = s(x_1, \dots, x_n)}{r[t_1/x_1, \dots, t_n/x_n] = s[t_1/x_1, \dots, t_n/x_n]} \text{ [subst]}$$

where $r(\dots t \dots)$ arises from $r(\dots s \dots)$ by replacing an occurrence of s in r by t .

$T \vdash s = t$: An equation $s = t$ is a *theorem* of a theory T iff $s = t$ is the last member of some deduction from T .

Meta-Theorems

Theorem (Soundness & Completeness)

$$T \vdash s = t \iff T \vDash s = t$$

- Determining Validity? Undecidable!

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Equational Logic

Boolean Algebra

Lambda Calculus and
Combinatory Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Semigroup/Monoid/Group

Group $\mathcal{L} = \{e, \cdot\}$

Group $\mathcal{L} = \{e, \cdot, {}^{-1}\}$

1. $\forall xyz : x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x : e \cdot x = x \cdot e = x$
3. $\forall x : x \cdot e = x$
4. $\forall x : x^{-1} \cdot x = e$
5. $\forall x : x \cdot x^{-1} = e$

Group $\mathcal{L} = \{\cdot\}$

1. $\forall xyz : x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall xy \exists z : xz = y$
3. $\forall xy \exists z : zx = y$

$$1. \forall xyz : x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$2. \forall x : e \cdot x = x \cdot e = x$$

$$3. \forall x \exists y : x \cdot y = y \cdot x = e$$

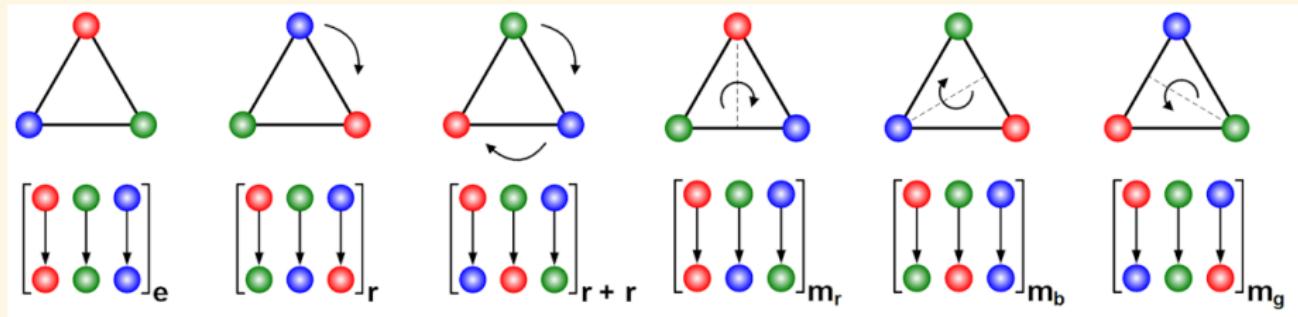
Structure

- $(\mathbb{Z}, 0, +)$
- $(\mathbb{Q} \setminus \{0\}, 1, \times)$
- Klein group: $(\{e, a, b, c\}, e, \cdot)$

\cdot	e	a	b	c	permutation
e	e	a	b	c	e
a	a	e	c	b	$(1, 2)(3, 4)$
b	b	c	e	a	$(1, 3)(2, 4)$
c	c	b	a	e	$(1, 4)(2, 3)$

Examples of Groups

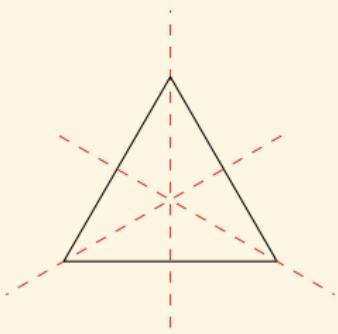
$$\begin{array}{ccccccc} \dagger & \clubsuit & * & \not{\circ} & \blacklozenge & \triangledown & \$ \\ \hline * & \blacklozenge & \triangledown & \clubsuit & \not{\circ} & \$ & \dagger \end{array} \iff \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 2 & 4 & 7 & 1 \end{array} = (1, 3, 6, 7)(2, 5, 4)$$



$$\{e, r, r^2, m, mr, mr^2\}$$

Jump above calculations; group the operations, classify them according to their complexities rather than their appearances.

— Évariste Galois



Cayley Theorem

Theorem (Cayley Theorem)

Every group G is isomorphic to a subgroup of the symmetric group on G .

Proof.

Let $\lambda_g : x \mapsto g \cdot x$, and $T : g \mapsto \lambda_g$ for $g \in G$.

For every group (G, e, \cdot) , the function T embeds (G, e, \cdot) in the group $(\text{Aut}(G), 1_G, \circ)$.

$$\lambda_e = 1_G \quad \lambda_{g \cdot h} = \lambda_g \circ \lambda_h \quad (\lambda_g)^{-1} = \lambda_{g^{-1}}$$

Ring/Boolean Ring

Ring $\mathcal{L} = \{0, 1, \oplus, \odot, -\}$

1. $\forall xyz : x \oplus (y \oplus z) = (x \oplus y) \oplus z$

2. $\forall xy : x \oplus y = y \oplus x$

3. $\forall x : x \oplus (-x) = 0$

4. $\forall x : x \oplus 0 = x$

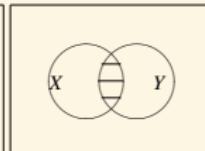
5. $\forall xyz : x \odot (y \odot z) = (x \odot y) \odot z$

6. $\forall xyz : x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

7. $\forall xyz : (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z)$

8. $\forall x : x \odot 1 = 1 \odot x = x$

9. $0 \neq 1$



A *Boolean ring* is a ring for which

$$\forall x : x \odot x = x$$

Field $\mathcal{L} = \{0, 1, \oplus, -, \odot, ^{-1}\}$

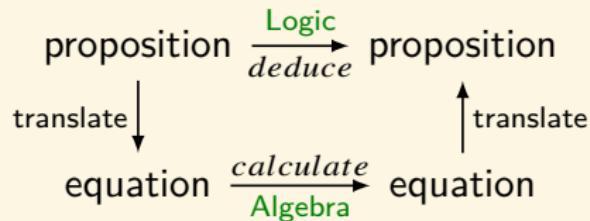
► $\forall xy : x \odot y = y \odot x$

► $\forall x \neq 0 : x \odot x^{-1} = x^{-1} \odot x = 1$

Boolean Algebra

Boolean Algebra $\mathcal{L} = \{0, 1, +, \cdot, \bar{}\}$

- $x + (y + z) = (x + y) + z$
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $x + y = y + x \quad x \cdot y = y \cdot x$
- $x + (x \cdot y) = x \quad x \cdot (x + y) = x$
- $x + (y \cdot z) = (x + y) \cdot (x + z)$
 $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $\bar{\bar{x}} = x$
- $\overline{x + y} = \bar{x} \cdot \bar{y} \quad \overline{x \cdot y} = \bar{x} + \bar{y}$
- $x + \bar{x} = 1 \quad x \cdot \bar{x} = 0 \quad 0 \neq 1$
- $x + 0 = x \quad x \cdot 0 = 0$
 $x + 1 = 1 \quad x \cdot 1 = x$



Logic as Algebra

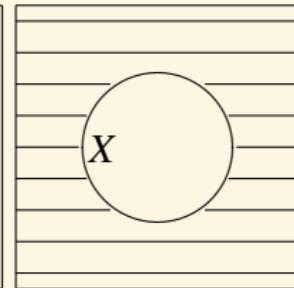
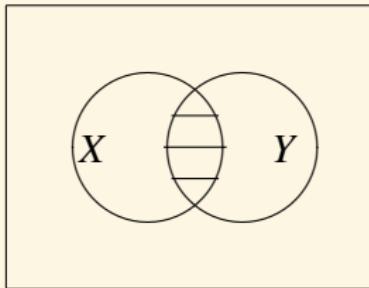
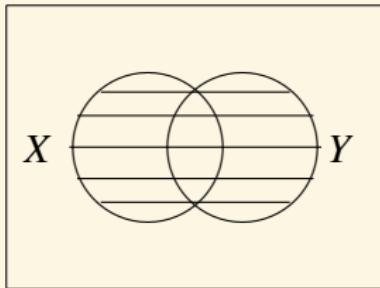
$$x - y := x \cdot \bar{y}$$

$$\bar{x} = 1 - x$$

$$x \cdot (y - z) = x \cdot y - x \cdot z$$

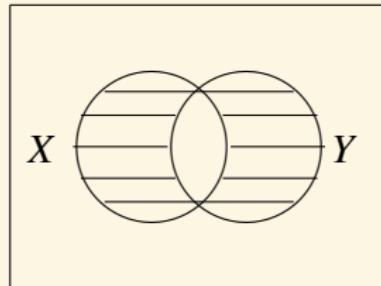
Power Set Algebra

$$(\mathcal{P}(A), \emptyset, A, \cup, \cap, \neg)$$



$$x \oplus y := (x \cdot \bar{y}) + (\bar{x} \cdot y)$$

$$x = y \iff x \oplus y = 0$$



Boolean Ring vs Boolean Algebra

Boolean Ring to Boolean Algebra

$$x \cdot y = x \odot y$$

$$x + y = x \oplus y \oplus (x \odot y)$$

$$\bar{x} = 1 \oplus x$$

Boolean Algebra to Boolean Ring

$$x \odot y = x \cdot y$$

$$x \oplus y = (x \cdot \bar{y}) + (\bar{x} \cdot y)$$

$$-x = x$$

Boole's Four Main Theorems

$$\mathbf{x}^\sigma := x_1^{\sigma_1} \cdots x_n^{\sigma_n} \quad x_i^{\sigma_i} := \begin{cases} x_i & \text{if } \sigma_i = 1 \\ \bar{x}_i & \text{if } \sigma_i = 0 \end{cases} \quad \sigma : \{1, \dots, n\} \rightarrow \{0, 1\}$$

1. Expansion

$$f(\mathbf{x}, \mathbf{y}) = \sum_{\sigma} f(\sigma, \mathbf{y}) \cdot \mathbf{x}^\sigma$$

2. Reduction

$$\bigwedge_i (f_i(\mathbf{x}) = 0) \iff \sum_i f_i(\mathbf{x}) = 0$$

3. Elimination

$$\exists \mathbf{x} (f(\mathbf{x}, \mathbf{y})) = 0 \iff \prod_{\sigma} f(\sigma, \mathbf{y}) = 0$$

4. Solution

$$q(\mathbf{y}) \cdot x = p(\mathbf{y})$$



$$p(\mathbf{y}) \cdot (p(\mathbf{y}) - q(\mathbf{y})) = 0 \quad \& \quad \exists v : x = \sum_{\tau: p(\tau)=q(\tau)\neq 0} \mathbf{y}^\tau + v \cdot \sum_{\tau: p(\tau)=q(\tau)=0} \mathbf{y}^\tau$$

Boole's Method

1. **Translation.** Translate premises into equational form.

$$\mathbf{A}: x \cdot \bar{y} = 0; \quad \mathbf{E}: x \cdot y = 0; \quad \mathbf{I}: v = v \cdot x \cdot y; \quad \mathbf{O}: v = v \cdot x \cdot \bar{y}.$$

2. **Reduction.** Combine the premise-equations into a single equation.

$$f_1(\mathbf{x}) = 0, \dots, f_k(\mathbf{x}) = 0 \iff \sum_{i=1}^k f_i(\mathbf{x}) = 0$$

3. **Elimination.** Given the single premise $\sum_{i=1}^k f_i(\mathbf{y}, \mathbf{z}) = 0$, the most general conclusion involving only \mathbf{z} is $f(\mathbf{z}) = 0$, where

$$f(\mathbf{z}) := \left(\sum_{i=1}^k f_i(1, \dots, 1, \mathbf{z}) \right) \cdot \dots \cdot \left(\sum_{i=1}^k f_i(0, \dots, 0, \mathbf{z}) \right)$$

4. **Expansion.** $f(\mathbf{z}) = f(1, \dots, 1) \cdot z_1 \cdot \dots \cdot z_n + \dots + f(0, \dots, 0) \cdot \bar{z}_1 \cdot \dots \cdot \bar{z}_n$
5. **Translation.** Interpret the conclusion-equations as propositions.

Boole's Method — Syllogism

$$\mathbf{A} : x \cdot \bar{y} = 0;$$

$$\mathbf{E} : x \cdot y = 0;$$

$$\mathbf{I} : v = v \cdot x \cdot y;$$

$$\mathbf{O} : v = v \cdot x \cdot \bar{y}$$

$$\begin{array}{c} MAP \\ SAM \\ \hline SAP \end{array}$$

$$\overbrace{m \cdot \bar{p} = 0 \quad s \cdot \bar{m} = 0}^{\Downarrow Reduction}$$

$$m \cdot \bar{p} + s \cdot \bar{m} = 0$$

$$\Downarrow Elimination$$

$$(1 \cdot \bar{p} + s \cdot 0) \cdot (0 \cdot \bar{p} + s \cdot 1) = 0$$

$$\Downarrow Expansion$$

$$(1 \cdot 0 + 1 \cdot 0) \cdot (0 \cdot 1 + 1 \cdot 1) \cdot s \cdot p + \dots + (1 \cdot 1 + 0 \cdot 0) \cdot (0 \cdot 1 + 0 \cdot 1) \cdot \bar{s} \cdot \bar{p} = 0$$

$$\Downarrow$$

$$s \cdot \bar{p} = 0$$

$$s \cdot \bar{p} = s \cdot 1 \cdot \bar{p} = s \cdot (m + \bar{m}) \cdot \bar{p} = s \cdot m \cdot \bar{p} + s \cdot \bar{m} \cdot \bar{p} = 0 + 0 = 0$$

Boole's Method — Syllogism

$$\mathbf{A} : x \cdot \bar{y} = 0; \quad \mathbf{E} : x \cdot y = 0; \quad \mathbf{I} : v = v \cdot x \cdot y; \quad \mathbf{O} : v = v \cdot x \cdot \bar{y}$$

$$\frac{\begin{array}{c} PAM \\ SOM \\ \hline SOP \end{array}}{\begin{array}{c} p \cdot \bar{m} = 0 \\ v = v \cdot s \cdot \bar{m} \\ \hline v = v \cdot s \cdot \bar{p} \end{array}}$$

$$v \cdot s \cdot \bar{p} \stackrel{2}{=} v \cdot s \cdot \bar{m} \cdot s \cdot \bar{p} = v \cdot s \cdot \bar{m} \cdot \bar{p} \stackrel{1}{=} v \cdot s \cdot \bar{m} \cdot \bar{p} + v \cdot s \cdot \bar{m} \cdot p = v \cdot s \cdot \bar{m} \stackrel{2}{=} v$$

$$\frac{\begin{array}{c} MEP \\ MIS \\ \hline SOP \end{array}}{\begin{array}{c} m \cdot p = 0 \\ v = v \cdot m \cdot s \\ \hline v = v \cdot s \cdot \bar{p} \end{array}}$$

$$v \cdot s \cdot \bar{p} \stackrel{2}{=} v \cdot m \cdot s \cdot s \cdot \bar{p} = v \cdot s \cdot m \cdot \bar{p} \stackrel{1}{=} v \cdot s \cdot m \cdot \bar{p} + v \cdot s \cdot m \cdot p = v \cdot s \cdot m \stackrel{2}{=} v$$

Boole's Method — Syllogism — Another Translation

A : $x \cdot \bar{y} = 0$; **E** : $x \cdot y = 0$; **I** : $x \cdot y \neq 0$; **O** : $x \cdot \bar{y} \neq 0$.

$$\begin{array}{c} PAM \\ SOM \\ \hline SOP \end{array}$$

$$p \cdot \bar{m} = s \cdot \bar{m} \cdot p + \bar{s} \cdot \bar{m} \cdot p = 0$$

$$s \cdot \bar{m} = s \cdot \bar{m} \cdot p + s \cdot \bar{m} \cdot \bar{p} \neq 0$$

\Downarrow

$$p \cdot \bar{m} + s \cdot \bar{m} = s \cdot \bar{m} \cdot \bar{p} \neq 0$$

\Downarrow

$$s \cdot \bar{m} \cdot \bar{p} + s \cdot m \cdot \bar{p} = s \cdot \bar{p} \neq 0$$

$$\begin{array}{c} MEP \\ MIS \\ \hline SOP \end{array}$$

$$m \cdot p = s \cdot m \cdot p + \bar{s} \cdot m \cdot p = 0$$

$$m \cdot s = s \cdot m \cdot p + s \cdot m \cdot \bar{p} \neq 0$$

\Downarrow

$$m \cdot p + m \cdot s = s \cdot m \cdot \bar{p} \neq 0$$

\Downarrow

$$s \cdot m \cdot \bar{p} + s \cdot \bar{m} \cdot \bar{p} = s \cdot \bar{p} \neq 0$$

Propositional Logic vs Boolean Algebra

$$(\perp)^* := 0$$

$$(\top)^* := 1$$

$$(p)^* := p$$

$$(\neg A)^* := \overline{A^*}$$

$$(A \vee B)^* := A^* + B^*$$

$$(A \wedge B)^* := A^* \cdot B^*$$

$$(0)^\star := \perp$$

$$(1)^\star := \top$$

$$(p)^\star := p$$

$$\left(\overline{A}\right)^\star := \neg A^\star$$

$$(A + B)^\star := A^\star \vee B^\star$$

$$(A \cdot B)^\star := A^\star \wedge B^\star$$

$$\frac{A \vdash B}{A^* \leq B^*}$$

$$\frac{A \leq B}{A^\star \vdash B^\star}$$

where $x \leq y := x \cdot \overline{y} = 0$

Boolean Algebra vs Propositional Logic

Exercise

Alice, Ben, Charlie, and Diane are considering going to a Halloween party.

1. If Alice goes then Ben won't go and Charlie will.
2. If Ben and Diane go, then either Alice or Charlie (but not both) will go.
3. If Charlie goes and Ben does not, then Diane will go but Alice will not.

$$A \rightarrow \neg B \wedge C$$

$$A \cdot (B + \overline{C}) = 0$$

$$B \wedge D \rightarrow (A \wedge \neg C) \vee (\neg A \wedge C)$$

$$B \cdot D \cdot (\overline{A} \cdot \overline{C} + A \cdot C) = 0$$

$$\neg B \wedge C \rightarrow \neg A \wedge D$$

$$\overline{B} \cdot C \cdot (A + \overline{D}) = 0$$

General Solution?¹⁵

Exercise — Save Yourself

You can say one sentence. If you lie I will hang you. If you tell the truth I will shoot you.

$$\begin{aligned}x = ? \implies & \models (\neg x \rightarrow h) \wedge (x \rightarrow s) \wedge (s \leftrightarrow \neg h) \rightarrow \neg h \wedge \neg s \\& \models (\neg h \rightarrow h) \wedge (h \rightarrow s) \wedge (s \leftrightarrow \neg h) \rightarrow \neg h \wedge \neg s\end{aligned}$$

Problem (General Solution?)

$$x = ? \implies \models A(x)$$

¹⁵Frank Markham Brown: Boolean Reasoning — The Logic of Boolean Equations.

General Solution?

$$x^5 - x - 1 = 0 \implies x = ?$$

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

$$ax^2 + bx + c = 0 \implies x = ?$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

General Solution of Boolean Equation

Theorem (General Solution of Boolean Equation)

Assume $f(x) = 0$ is *consistent* (it has at least one solution, i.e. $f(0) \cdot f(1) = 0$), then

$$f(x) = 0$$

\Updownarrow

$$f(0) \leq x \leq \overline{f(1)}$$

\Updownarrow

$$x = f(0) + \theta \cdot \overline{f(1)}$$

where $\theta \in \{0, 1\}$.

Application — How to Flirt with a Beauty 😊

Smullyan

Flirts with a Beauty ❤️😊

1. “I am to make a statement. If it is true, would you give me your autograph?”
2. “I don’t see why not.”
3. “If it is false, do not give me your autograph.”
4. “Alright.”
5. Then Smullyan said such a sentence that she have to give him a kiss.

$$x =? \implies \models (a \leftrightarrow x) \rightarrow k$$

Application — How to Flirt with a Beauty 😊

Smullyan

Flirts with a Beauty ❤️😊

1. “I am to make a statement. If it is true, would you give me your autograph?”
2. “I don’t see why not.”
3. “If it is false, do not give me your autograph.”
4. “Alright.”
5. Then Smullyan said such a sentence that she have to give him a kiss.

$$x = ? \implies \models (a \leftrightarrow x) \rightarrow k$$

Solution

$$(a \cdot x + \bar{a} \cdot \bar{x}) \cdot \bar{k} = 0 \implies x = \bar{a} \cdot \bar{k} + \theta \cdot (\bar{a} + k)$$

$$\models (a \leftrightarrow \neg a \wedge \neg k) \rightarrow k$$

$$\models (a \leftrightarrow (a \rightarrow k)) \rightarrow k$$

General Solution of Boolean Equation

Theorem (General Solution of Boolean Equation)

Given the Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, define

$f_0, f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)$ by means of the recursion

$$f_n := f$$

$$f_{i-1}(x_1, \dots, x_{i-1}) := f_i(x_1, \dots, x_{i-1}, 0) \cdot f_i(x_1, \dots, x_{i-1}, 1)$$

then

$$f_0 = 0$$

$$f_i(x_1, \dots, x_{i-1}, 0) \leq x_i \leq \overline{f_i(x_1, \dots, x_{i-1}, 1)} \quad (i = 1, \dots, n)$$

is a general solution of $f(x_1, \dots, x_n) = 0$.

Homomorphism

- Let \mathcal{M} and \mathcal{N} be Boolean algebras. A (Boolean) homomorphism is a mapping $h : \mathcal{M} \rightarrow \mathcal{N}$ s.t. for all $x, y \in \mathcal{M}$:
 1. $h(0) = 0$
 2. $h(1) = 1$
 3. $h(\bar{x}) = \overline{h(x)}$
 4. $h(x + y) = h(x) + h(y)$
 5. $h(x \cdot y) = h(x) \cdot h(y)$
- If $h : \mathcal{M} \rightarrow \mathcal{N}$, it is an isomorphic embedding of \mathcal{M} into \mathcal{N} .
- If $h : \mathcal{M} \rightarrow \mathcal{N}$, then \mathcal{M} and \mathcal{N} are isomorphic ($\mathcal{M} \cong \mathcal{N}$).

Example — Lindenbaum Algebra of Propositional Logic

Lindenbaum Algebra of Propositional Logic

$$\text{Lin} := (\text{Wff}/\sim, 0, 1, +, \cdot, \neg)$$

$$\mathbf{2} := (\{0, 1\}, 0, 1, \max, \min, 1 -)$$

where

$$A \sim B := \vdash A \leftrightarrow B$$

$$[A] := \{B \in \text{Wff} : A \sim B\}$$

$$\text{Wff}/\sim := \{[A] : A \in \text{Wff}\}$$

$$0 := [\perp]$$

$$1 := [\top]$$

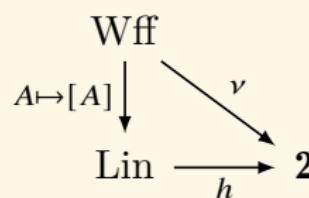
$$\overline{[A]} := [\neg A]$$

$$[A] + [B] := [A \vee B]$$

$$[A] \cdot [B] := [A \wedge B]$$

$$\text{Lin} \xrightarrow{?} \mathbf{2}$$

If ν is a truth assignment, then $h : [A] \mapsto \nu(A)$ is a homomorphism.
If $h : \text{Lin} \rightarrow \mathbf{2}$ is a homomorphism,
then $\nu : A \mapsto h([A])$ is a truth
assignment.



Ultrafilter

- ▶ A partial order R over P is a binary relation which is reflexive, antisymmetric, and transitive, i.e. for all $x, y, z \in P$:
 1. Rxx
 2. $Rxy \wedge Ryx \rightarrow x = y$
 3. $Rxy \wedge Ryz \rightarrow Rxz$
- ▶ \leq is a partial order.
- ▶ Let $\mathcal{B} = (B, 0, 1, +, \cdot, \bar{})$ be a Boolean algebra. A subset $F \subset B$ is a filter iff
 1. $1 \in F$
 2. $x \in F \wedge x \leq y \rightarrow y \in F$
 3. $x \in F \wedge y \in F \rightarrow x \cdot y \in F$
- ▶ A filter F is proper iff $0 \notin F$.
- ▶ A proper filter F is an ultrafilter iff either $x \in F$ or $\bar{x} \in F$.
- ▶ **Ultrafilter Theorem:** every proper filter can be extended to an ultrafilter.

Ultrafilter theorem on Lindenbaum Algebra of Propositional Logic \iff
Every consistent set can be extended to a maximal consistent set.

Stone's Representation Theorem

Theorem (Stone's Representation Theorem)

Every Boolean algebra is isomorphic to an algebra of sets.

Proof.

Let \mathcal{B} be a Boolean algebra, and $\text{Sto}(\mathcal{B}) := \{w : w \text{ is an ultrafilter on } \mathcal{B}\}$. Define a map $h : \mathcal{B} \rightarrow \mathcal{P}(\text{Sto}(\mathcal{B}))$ by

$$x \mapsto \{w \in \text{Sto}(\mathcal{B}) : x \in w\}$$

Then

$$\mathcal{B} \cong (h(\mathcal{B}), \emptyset, \text{Sto}(\mathcal{B}), \cup, \cap, \setminus)$$

An Algebraic proof of Completeness Theorem for Propositional Logic

$$\models A \implies \vdash A$$

$$\begin{array}{c} \models A \\ \Downarrow \\ \vdash A \\ \Downarrow \\ [A] \neq [\top] \\ \Downarrow \\ [\neg A] \neq [\perp] \\ \Downarrow \\ h([\neg A]) \neq \emptyset \\ \Downarrow \\ \exists w \in \text{Sto}(\text{Lin}) ([\neg A] \in w) \\ \Downarrow \\ \chi_w([\neg A]) = 1 \end{array}$$

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Equational Logic

Boolean Algebra

Lambda Calculus and
Combinatory Logic

Homotopy Type Theory

Category Theory

Quantum Computing

Answers to the Exercises

References 1436

Church 1903-1995



- ▶ Lambda Calculus
- ▶ Church-Turing Thesis
- ▶ Undecidability
- ▶ Church-Rosser Theorem
- ▶ Frege-Church Ontology

Lambda Calculus

$$\mathcal{L} = \{\lambda, .\}$$

Definition (λ -Terms)

$$\Lambda ::= x \mid \Lambda\Lambda \mid \lambda x.\Lambda$$

Notation:

- ▶ $M_0M_1 \cdots M_n$ denotes $(\cdots ((M_0M_1)M_2 \cdots M_n))$
- ▶ $\lambda x_0x_1 \cdots x_n.M$ denotes $(\lambda x_0.(\lambda x_1.(\cdots (\lambda x_n.M)) \cdots))$

Definition (Free Variable)

$$\text{Fv}(\Lambda) := \begin{cases} \{x\} & \text{if } \Lambda = x \\ \text{Fv}(M) \cup \text{Fv}(N) & \text{if } \Lambda = MN \\ \text{Fv}(M) \setminus \{x\} & \text{if } \Lambda = \lambda x.M \end{cases}$$

Reduction Rules

Definition (Substitution)

$$y[N/x] = \begin{cases} N & \text{if } x = y \\ y & \text{otherwise} \end{cases}$$

$$(M_1 M_2)[N/x] = (M_1[N/x]) (M_2[N/x])$$

$$(\lambda y. M)[N/x] = \begin{cases} \lambda y. M & \text{if } x = y \\ \lambda y. M[N/x] & \text{if } x \neq y \text{ and } y \notin \text{Fv}(N) \end{cases}$$

Reduction Rules

$$\lambda x. M \stackrel{\alpha}{=} \lambda y. M[y/x] \quad \text{if } y \text{ does not occur in } M.$$

$$(\lambda x. M)N \stackrel{\beta}{=} M[N/x]$$

$$\lambda x. Mx \stackrel{\eta}{=} M \quad \text{if } x \notin \text{Fv}(M)$$

λ -definability

Definition (Church Numeral)

$$\begin{aligned}\underline{n} &:= \lambda f x. f^n x \\ f^0 x &:= x \\ f^{n+1} x &:= f(f^n x)\end{aligned}$$

Definition (λ -definability)

An n -ary function $f(x_1, \dots, x_n)$ is λ -definable iff there is a λ -term F s.t. for all a_1, \dots, a_n ,

$$F \underline{a}_1 \dots \underline{a}_n \stackrel{\beta}{=} \underline{f(a}_1, \dots, a_n)$$

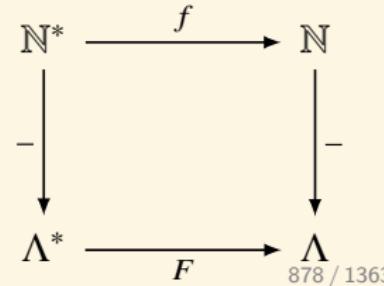
A function f is computable iff it is λ -definable.

$$\text{succ} := \lambda n f x. f(n f x)$$

$$\text{add} := \lambda m n f x. m f(n f x)$$

$$\text{mult} := \lambda m n f. m(n f)$$

$$\text{exp} := \lambda m n. n m$$



Combinator

Definition (Combinator)

A λ -term M is called a combinator iff $\text{Fv}(M) = \emptyset$.

$$\mathbf{K} = \lambda xy.x$$

$$\mathbf{S} = \lambda xyz.xz(yz)$$

$$\mathbf{I} = \lambda x.x$$

$$\omega = \lambda x.xx$$

$$\Omega = \omega\omega$$

$$\mathbf{Y} = \lambda y.(\omega(\lambda x.y(xx)))$$

$$\mathbf{F} = \lambda xy.y$$

$$\mathbf{T} = \mathbf{K}$$

$$\mathbf{B} = \mathbf{S}(\mathbf{KS})\mathbf{K}$$

$$\mathbf{C} = \mathbf{S}(\mathbf{BBS})(\mathbf{KK})$$

$$\mathbf{W} = \mathbf{SS}(\mathbf{SK})$$

$$\mathbf{D} = \mathbf{SII}$$

$$\mathbf{L} = \mathbf{D}(\mathbf{BDD})$$

$$\mathbf{neg} = \lambda x.x\mathbf{FT}$$

$$\mathbf{and} = \lambda xy.xy\mathbf{F}$$

$$\mathbf{or} = \lambda xy.x\mathbf{Ty}$$

$$\mathbf{iszero} = \lambda x.x(\lambda y.\mathbf{F})\mathbf{T}$$

$$\iota = \lambda x.x\mathbf{SK}$$

$$\mathbf{K} = \iota(\iota(u))$$

$$\mathbf{S} = \iota(\iota(\iota(u)))$$

$$\mathbf{I} = u$$

Iota

Syntax	Semantics
$F \rightarrow 1F_0F_1$	$[F_0]([F_1])$ “application”
$F \rightarrow 0$	$\lambda x.xSK$ “Iota”

Example

$$\begin{aligned} 1010100 &= 1010I \\ 100 &= (\lambda x.xSK)(\lambda x.xSK) & &= (\lambda x.xSK)((\lambda x.xSK)I) \\ &= (\lambda x.xSK)SK & &= (\lambda x.xSK)(ISK) \\ &= SSKK & &= (\lambda x.xSK)(SK) \\ &= SK(KK) & &= SKSK \\ &= I & &= KK(SK) \\ & & &= K \end{aligned}$$

Exercises

- ▶ $Bxyz = x(yz)$ (composition)
- ▶ $Cxyz = xzy$ (swap)
- ▶ $Wxy = xyy$ (duplicate)
- ▶ $Dx = xx$ (doubling)
- ▶ $L = LL$ (self-doubling)

Smullyan: To Mock a Mockingbird

- ▶ A forest is inhabited by talking birds. Given any birds A, B , if you call out the name of B to A , then A will respond by calling out the name of some bird AB . If $AB = B$, then we say that A is fond of B .
- ▶ A bird x is called *egocentric* if x is fond of itself $xx = x$.

The forest satisfies the following two conditions:

1. For any birds A, B , there is a bird C s.t. for any bird x , $Cx = A(Bx)$.
2. There is a mockingbird M s.t. for any bird x , $Mx = xx$.

Theorem

Every bird is fond of some bird, and at least one bird is egocentric.

Proof.

Take any bird A . There is a bird C such that for any bird x , $Cx = A(Mx)$. Then taking C for x , $CC = A(MC) = A(CC)$.

In particular, the mocking bird M is fond of some bird E . Thus $ME = E$, but also $ME = EE$. Therefore $EE = E$.

Smullyan: To Mock a Mockingbird

- ▶ A bird Θ is called a *Sage* bird if you call out the name of a bird x to it, it will name a bird of which x is fond $\Theta x = x(\Theta x)$.
 - ▶ A bird U is called a *Turing* bird if $Uxy = y(xxy)$.
 - ▶ A bird L is called a *Lark* if $Lxy = x(yy)$.
 - ▶ A bird O is called an *Owl* if $Oxy = y(xy)$.
 - ▶ A bird I is called an *Idiot* if $Ix = x$.
 - ▶ A bird K is called a *Kestrel* if $Kxy = x$.
 - ▶ A bird S is called a *Starling* if $Sxyz = xz(yz)$.
1. If there is a lark in the forest, then every bird is fond of some bird.
 $Lx(Lx) = x(Lx(Lx))$.
 2. SI is an Owl.
 3. An owl is fond only of Sage birds. $OA = A \implies Ax = x(Ax)$.
 4. Turing birds: $LO, L(SI)$.
 5. Sage birds: $\Theta O, O\Theta, UU, SLL$.
 6. Mocking birds: OI, LI, SII .
 7. ΘM is egocentric. $\Theta M = M(\Theta M) = \Theta M(\Theta M)$.
 8. ΘK is hopelessly egocentric. $\Theta Kx = K(\Theta K)x = \Theta K$.

First Fixpoint Theorem in Lambda Calculus

Theorem (First Fixpoint Theorem in Lambda Calculus)

For every λ -term F there is a λ -term E s.t. $FE = E$.

Proof.

Let $G := \lambda x.F(xx)$ and $E := GG$.

$$Y = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx))$$

Corollary

For any λ -term $C(f, \vec{x})$, there exists a λ -term M s.t. for all λ -terms \vec{N}

$$M\vec{N} = C(M, \vec{N})$$

Proof.

Let $M := Y(\lambda f\vec{x}.C(f, \vec{x}))$.

Fixpoint Combinator

$$Y = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx)) \quad \text{Curry}$$

$$\Theta = (\lambda xy.y(xxy))(\lambda xy.y(xxy)) \quad \text{Turing}$$

fac $n = \text{if_then_else } (\text{iszzero } n) \ (1) \ (\text{mult } n \ (\text{fac } (\text{pred } n)))$

fac $= \lambda n. \text{if_then_else } (\text{iszzero } n) \ (1) \ (\text{mult } n \ (\text{fac } (\text{pred } n)))$

fac $= (\lambda f. \lambda n. \text{if_then_else } (\text{iszzero } n) \ (1) \ (\text{mult } n \ (f \ (\text{pred } n)))) \ \text{fac}$

$F := \lambda f. \lambda n. \text{if_then_else } (\text{iszzero } n) \ (1) \ (\text{mult } n \ (f \ (\text{pred } n)))$

fac $:= YF$

$$YF = F(YF)$$

fac $= F \ \text{fac}$

Church-Rosser Theorem

We write $M \twoheadrightarrow_{\beta} N$ iff M β -reduces to N in zero or more steps.

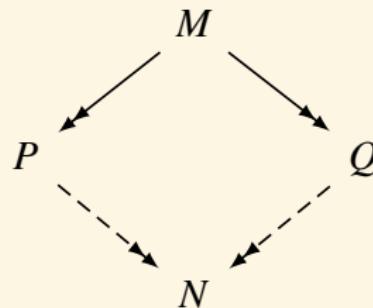
Definition (β -nf)

A term is in β normal form iff it can't be β -reduced.

A term M has a β normal form iff it β reduces to some N that is in β -nf.

Theorem (Church-Rosser Theorem)

Let \twoheadrightarrow denote either $\twoheadrightarrow_{\beta}$ or $\twoheadrightarrow_{\beta\eta}$. Suppose M, P, Q are λ -terms s.t. $M \twoheadrightarrow P$ and $M \twoheadrightarrow Q$. Then there exists a λ -term N s.t. $P \twoheadrightarrow N$ and $Q \twoheadrightarrow N$.



Second Fixpoint Theorem in Lambda Calculus

We write $\ulcorner M \urcorner := \#M$ to denote the Church numeral representing the Gödel number of M .

Theorem (Second Fixpoint Theorem in Lambda Calculus)

For every λ -term F there is a λ -term E s.t. $F^{\ulcorner} E^{\urcorner} = E$.

Proof.

By Church-Turing thesis, there is a term C s.t. $C^{\ulcorner} M^{\urcorner} = \ulcorner \ulcorner M \urcorner \urcorner$.

Furthermore, there is a term A s.t. $A^{\ulcorner} M^{\urcorner} \ulcorner N^{\urcorner} = \ulcorner M N \urcorner$.

Take $G := \lambda n.F(An(Cn))$. Then let $E := G^{\ulcorner} G^{\urcorner}$.

$$\begin{aligned} E &= G^{\ulcorner} G^{\urcorner} \\ &= F(A^{\ulcorner} G^{\urcorner}(C^{\ulcorner} G^{\urcorner})) \\ &= F(A^{\ulcorner} G^{\urcorner}(\ulcorner \ulcorner G \urcorner \urcorner)) \\ &= F^{\ulcorner} G^{\ulcorner} G^{\urcorner \urcorner} \\ &= F^{\ulcorner} E^{\urcorner} \end{aligned}$$

Undecidability

Theorem (Church1936)

There is no term that will decide whether two terms have the same normal form.

Theorem (Church1936)

There is no λ -term D s.t. for all \underline{n} ,

$$D\underline{n} = \begin{cases} 0 & \text{if term with Gödel number } n \text{ has a } \beta\text{-nf} \\ 1 & \text{otherwise} \end{cases}$$

Proof.

Suppose there was such a D . Then define $G := \lambda n.\text{iszzero}(Dn)\Omega\mathbf{I}$.

By the fixpoint theorem, there is X s.t. $G(\Gamma X^\neg) = X$.

X has a β -nf $\implies D\Gamma X^\neg = 0 \implies G\Gamma X^\neg = \Omega \implies X$ has no β -nf

X has no β -nf $\implies D\Gamma X^\neg = 1 \implies G\Gamma X^\neg = \mathbf{I} \implies X$ has a β -nf

Undecidability

Theorem (Church1936)

There is no D s.t. for all M ,

$$DM = \begin{cases} T & \text{if } M \text{ has a normal form} \\ F & \text{otherwise} \end{cases}$$

Proof.

let $G := C(C(BD(SII))\Omega)I$ and $X := GG$. Then

$$X = D(X)\Omega I$$

If X has a normal form, then $D(X)\Omega I = \Omega$, but Ω has no normal form.

If X has no normal form, then $D(X)\Omega I = I$, but I is in normal form.

Theorem (Curry, Scott, Rice)

Suppose $A \subset \Lambda$ is closed under β . Then A is decidable iff $A = \Lambda$ or $A = \emptyset$.

Proof.

Define $B := \{M : M^\Gamma M^\neg \in A\}$.

There exists a term $D \in \Lambda$ s.t.

$$M \in B \iff D^\Gamma M^\neg = \underline{0}$$

$$M \notin B \iff D^\Gamma M^\neg = \underline{1}$$

Let $P \in A$ and $Q \in \Lambda \setminus A$.

$$G := \lambda n. \mathbf{iszzero}(Dn) Q P$$

$$G \in B \iff D^\Gamma G^\neg = \underline{0} \implies G^\Gamma G^\neg = Q \implies G^\Gamma G^\neg \notin A \implies G \notin B$$

$$G \notin B \iff D^\Gamma G^\neg = \underline{1} \implies G^\Gamma G^\neg = P \implies G^\Gamma G^\neg \in A \implies G \in B$$

Theorem (Enumeration Theorem)

There exists a term $\mathbf{E} \in \Lambda^0$ such that, for all $M \in \Lambda^0$

$$\mathbf{E}^\Gamma M^\neg \rightarrow_\beta M$$

Theorem

There is no term $Q \in \Lambda$ such that, for all $M \in \Lambda$

$$QM =_\beta {}^\Gamma M^\neg$$

Proof.

We know that Church numerals are in normal form. However

$${}^\Gamma M^\neg =_\beta QM =_\beta Q(\mathbf{I}M) =_\beta {}^\Gamma \mathbf{I}M^\neg$$

which makes two distinct normal forms equal.

Remark: One can go from intension ${}^\Gamma M^\neg$ to extension M , but not the other way within the system itself.

Second Fixpoint Theorem
Enumeration Theorem } \implies First Fixpoint Theorem

Proof.

$$M =_{\beta} \lambda x. F(\mathbf{Ex})^{\top} M^{\top} =_{\beta} F(\mathbf{E}^{\top} M^{\top}) =_{\beta} FM$$

Combinatory Logic

Definition (Combinatory Terms)

$$C ::= x \mid \mathbf{K} \mid \mathbf{S} \mid (CC)$$

Reduction

$$\mathbf{K}MN = M$$

$$\mathbf{S}MNL = ML(NL)$$

- ▶ $\varphi_k(x, y) = x$
- ▶ $\varphi_s(x, y, z) = \varphi_{\varphi_x(z)}(\varphi_y(z))$

Combinatory Completeness

Proposition (Combinatory Completeness)

For every λ -term P and variable x , there is a combinator $\lambda^*x.P$ s.t.

$$(\lambda^*x.P)Q = P[Q/x]$$

Proof.

$$\lambda^*x.P := \begin{cases} \mathbf{I} & \text{if } P = x \\ \mathbf{K}P & \text{if } x \notin \text{Fv}(P) \\ \mathbf{S}(\lambda^*x.M)(\lambda^*x.N) & \text{if } P = MN \end{cases}$$

Lambda Calculus subsumes Combinatory Logic

M	$(M)_\lambda$
I	$\lambda x.x$
K	$\lambda xy.x$
S	$\lambda xyz.xz(yz)$
PQ	$(P)_\lambda(Q)_\lambda$

Table: translation: $()_\lambda : \text{CL} \rightarrow \Lambda$

$$\vdash_{\text{CL}} M = N \implies \vdash_\lambda (M)_\lambda = (N)_\lambda$$

But not the other way around:

$$\vdash_{\text{CL}} \mathbf{SKI} = \mathbf{I}, \vdash_\lambda (\mathbf{SKI})_\lambda = (\mathbf{I})_\lambda.$$

Combinatory Logic subsumes Lambda Calculus

M	$(M)_C$
x	x
$\lambda x.P$	$\lambda^*x.(P)_C$
PQ	$(P)_C(Q)_C$

Table: translation: $()_C : \Lambda \rightarrow CL$

$$\vdash_{\lambda} M = N \iff \vdash_{CL} (M)_C = (N)_C$$

Numerewise Representability

- The combinatory Church numerals are defined by

$$\underline{n} = (\mathbf{S}\mathbf{B})^n(\mathbf{K}\mathbf{I})$$

- A partial function $f : \mathbb{N} \rightarrow \mathbb{N}$ is *numerewise represented* by a combinatory term M if for all $n \in \mathbb{N}$, if $f(n)$ is defined and equal to m , then

$$\vdash_{\text{CL}} M\underline{n} = \underline{m}$$

and if $f(n)$ is undefined, then $M\underline{n}$ has no normal form.

Theorem

The partial functions numerewise representable in CL are exactly the partial recursive functions.

Simply-Typed Lambda Calculus (STLC)

- ▶ Type

$$T ::= 1 \mid T \times T \mid T \rightarrow T$$

- ▶ Term

$$\Lambda ::= x \mid * \mid \Lambda\Lambda \mid \lambda x.\Lambda \mid \langle \Lambda, \Lambda \rangle \mid \pi_1\Lambda \mid \pi_2\Lambda$$

- ▶ Judgement

$$x_1 : T_1, \dots, x_n : T_n \vdash t : T$$

1. t is a proof of T from assumptions T_1, \dots, T_n .
2. t is a program of type T with free variables x_1, \dots, x_n of type T_1, \dots, T_n .

The System of Simply-Typed Lambda Calculus

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A} \text{ var}$$

$$\frac{}{\Gamma \vdash * : 1} \text{ unit}$$

$$\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \times B} \times^+$$

$$\frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_1 t : A} \times^-$$

$$\frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_2 t : B} \times^-$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x. t : A \rightarrow B} \text{ abs}$$

$$\frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash tu : B} \text{ app}$$

Reduction rules

$$(\lambda x. t)u \rightarrow t[u/x] \quad (\beta_{\rightarrow})$$

$$\lambda x. tx \rightarrow t \quad \text{where } x \notin \text{Var}(t) \quad (\eta_{\rightarrow})$$

$$\pi_1 \langle t, u \rangle \rightarrow t \quad (\beta_{\times,1})$$

$$\pi_2 \langle t, u \rangle \rightarrow u \quad (\beta_{\times,2})$$

$$\langle \pi_1 t, \pi_2 t \rangle \rightarrow t \quad (\eta_{\times})$$

What does β/η -reduction correspond to?

$$\frac{\Gamma, x : A \vdash t : B}{\frac{\Gamma \vdash \lambda x.t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash (\lambda x.t)u : B}} \quad \xrightarrow{\text{cut}} \quad \Gamma \vdash t[u/x] : B$$

$$\Gamma \vdash t : A \rightarrow B \quad \xrightarrow{\text{expansion}} \quad \frac{\frac{\Gamma, x : A \vdash t : A \rightarrow B \quad \Gamma, x : A \vdash x : A}{\Gamma, x : A \vdash tx : B}}{\Gamma \vdash \lambda x.tx : A \rightarrow B}$$

Example

$$\frac{\frac{[x : A \rightarrow B \rightarrow C]^3 \quad [z : A]^1}{xz : B \rightarrow C} \quad \frac{[y : A \rightarrow B]^2 \quad [z : A]^1}{yz : B}}{xz(yz) : C} \stackrel{[\rightarrow^+]^1}{\underline{\lambda z. xz(yz) : A \rightarrow C}} \quad \frac{\stackrel{[\rightarrow^+]^2}{\underline{\lambda y. \lambda z. xz(yz) : (A \rightarrow B) \rightarrow A \rightarrow C}}}{\lambda x. \lambda y. \lambda z. xz(yz) : (A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C} \stackrel{[\rightarrow^+]^3}{}$$

- $\mathbf{I} := \lambda x. x : A \rightarrow A$
- $\mathbf{K} := \lambda x. \lambda y. x : A \rightarrow B \rightarrow A$
- $\mathbf{S} := \lambda x. \lambda y. \lambda z. xz(yz) : (A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
- $\mathbf{B} : (B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$
- $\mathbf{C} : (A \rightarrow B \rightarrow C) \rightarrow B \rightarrow A \rightarrow C$
- $\mathbf{W} : (A \rightarrow A \rightarrow B) \rightarrow A \rightarrow B$

Lemma (Substitution lemma)

$$\frac{\Gamma, x : A \vdash t : B \quad \Gamma \vdash u : A}{\Gamma \vdash t[u/x]B}$$

Theorem (Subject Reduction Theorem)

$$\Gamma \vdash t : A \quad \& \quad t \rightarrow_{\beta} u \implies \Gamma \vdash u : A$$

Theorem (Church-Rosser property for typable terms)

Suppose that $\Gamma \vdash t : A$. If $t \rightarrow_{\beta} u$ and $t \rightarrow_{\beta} v$, then there exists a term w s.t. $u \rightarrow_{\beta} w, v \rightarrow_{\beta} w$ and $\Gamma \vdash w : A$.

Theorem (Strong Normalization Theorem)

If $\Gamma \vdash t : A$, then there is no infinite β -reduction path starting from t .

Subject Reduction Well-typed programs never go wrong: evaluating a program $t : A$ to a value indeed returns a value of type A .

Church-Rosser It doesn't make any difference for the final value how we reduce.

Strong Normalization No matter how one evaluates, one always obtains a value: there are no infinite computations possible.

Subformula Property

Theorem (Subformula Property)

If $\Gamma \vdash t : A$ is normal, i.e. there is no reduction step $t \rightarrow t'$, then the derivation of $\Gamma \vdash t : A$ can only mention subformulas of A and subformulas of assumptions in Γ .

Remark: We can eliminate irrelevant detours from a proof in finite time.

Intensionality

Intensionality occurs when mathematical objects can be seen in two ways:

1. **extensionally**, i.e. abstractly, up to extensional equality. For example, logical formula, computable function
2. **intensionally**, through their descriptions, or syntax. For example, Gödel number, index of computable function

To be intensional is to be finer than extensional equality.

One **cannot** go from extension to intension within the system.

- we cannot get an index for a computable function from the function itself within the computing system.

$$\neg \exists Q \in \Lambda \forall M \in \Lambda. QM =_{\beta} \Gamma M \neg$$

- we cannot obtain the Gödel number of a logical formula within the logical system.

Modality-as-Intension

- ▶ For type A , let there be a type $\Box A$, whose elements can be understood as “programs that — when run — will yield objects of that type”.
- ▶ From intension to extension: Interpreter, or evaluator.

$$\Box A \rightarrow A$$

- ▶ From code to code-for-code.

$$\Box A \rightarrow \Box \Box A$$

- ▶ From code for a function, to a map on codes: intensional substitution, a.k.a. the *smn* theorem

$$\Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B$$

- ▶ Assume $t = f \ulcorner t \urcorner$. If $t : A$, then $\ulcorner t \urcorner : \Box A$ and hence $f : \Box A \rightarrow A$.
- ▶ Kleene's fixpoint theorem then says

“for each $f : \Box A \rightarrow A$, we have $\ulcorner t \urcorner : \Box A$ ”

- ▶ It is Löb's rule

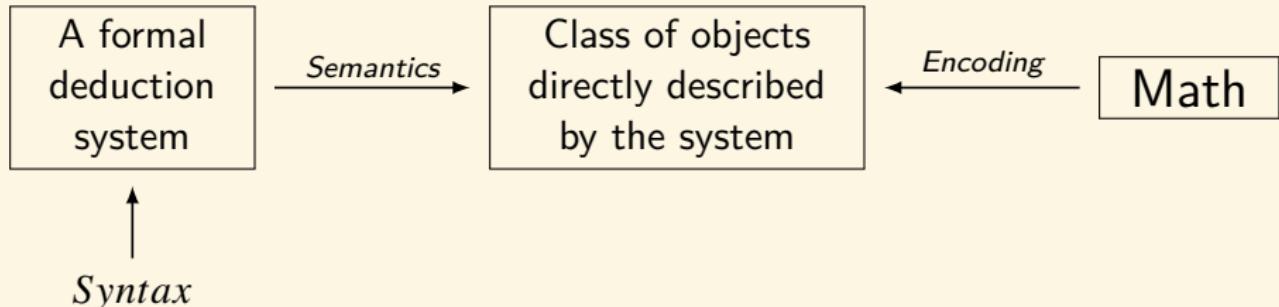
$$\frac{\Box A \rightarrow A}{\Box A}$$

- ▶ The type of Kleene's fixpoint theorem is Löb axiom $\Box(\Box A \rightarrow A) \rightarrow \Box A$

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

What is a Formalization of Math?



$$\text{First Order Logic} \xrightarrow{\text{express}} ZFC \xrightarrow{\text{describe}} V$$

$$\text{Intensional MLTT} \xrightarrow{\text{express}} HoTT \xrightarrow{\text{describe}} \infty\text{-Grpd}$$

- ▶ set theory
- ▶ category theory
- ▶ homotopy type theory

Why HoTT?[Uni13]

1. Homotopy can be used as a tool to construct models of systems of logic.
2. Constructive type theory can be used as a formal calculus to reason about homotopy.
3. The computational implementation of type theory allows computer verified proofs in homotopy theory.
4. The homotopy interpretation suggests new logical constructions and axioms as a new approach to foundations of math with intrinsic geometric content.



(e) Martin-Löf



(f) Voevodsky

Context & Judgement

- ▶ context: sequence of variable declarations
 $x_1 : A_1, x_2 : A_2(x_1), \dots, x_n : A_n(x_1, \dots, x_{n-1})$
- ▶ judgement: context \vdash conclusion

$\Gamma \vdash A : \text{type}$ A is a well-formed **type** in context Γ

$\Gamma \vdash a : A$ a is a well-formed **term** of type A

$\Gamma \vdash a = b : A$ a is convertible to b in type A

$\Gamma \vdash A = B : \text{type}$ types A and B are convertible

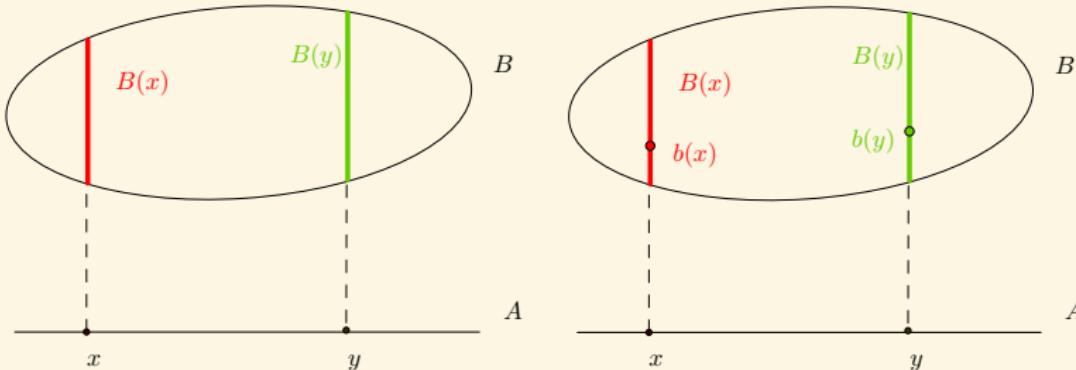
- ▶ dependent type

$x : A \vdash B(x) : \text{type}$

- ▶ dependent term

$x : A \vdash b(x) : B(x)$

Remark



- ▶ From any point x of A , we can observe a portion $B(x)$ of the shape B .

$$x : A \vdash B(x) : \text{Shape}$$

In topology, B is a space fibered over A (there is a fibration $\pi : B \rightarrow A$), whose fibers are given by $\pi^{-1}(x)$ for each $x \in A$.

- ▶ From any point x of A , we can observe a point $b(x)$ of $B(x)$.

$$x : A \vdash b(x) : B(x)$$

Here b is a section of the fibration $\pi : B \rightarrow A$, i.e. a map $s : A \rightarrow B$ such that $\pi \circ s = 1_A$.

Logical Rules

Each type constructor comes with rules:

Formation way to construct a type

Introduction way to construct canonical terms of that type

Elimination way to use a term of the introduced type to construct other terms

Conversion what happens when one does Introduction followed by Elimination

Remark:

Formation When can we observe A ?

Introduction When can we observe a point of A ?

Elimination When can we observe points on another shape from A ?

Conversion What are the symmetries of A ?

Rules for unit type

$$\frac{}{\Gamma \vdash 1 : \text{type}} \text{ 1-F}$$

$$\frac{}{\Gamma \vdash * : 1} \text{ 1-I}$$

$$\frac{\Gamma \vdash x : 1}{\Gamma \vdash x = * : 1} \text{ 1-C}$$

Rules for dependent product type

$$\frac{A : \text{type} \quad x : A \vdash B(x) : \text{type}}{\prod_{x:A} B(x) : \text{type}} \text{ } \Pi\text{-F}$$

$$\frac{x : A \vdash fx : B(x)}{\lambda x. fx : \prod_{x:A} B(x)} \text{ } \Pi\text{-I}$$

$$\frac{a : A \quad f : \prod_{x:A} B(x)}{fa : B(a)} \text{ } \Pi\text{-E}$$

$$\frac{a : A \quad x : A \vdash fx : B(x)}{(\lambda x. fx) a = fa : B(a)} \text{ } \Pi\text{-C}$$

Remark: We write $A \rightarrow B$ instead of $\prod_{x:A} B$ if x is not free in B .

Rules for dependent sum type

$$\frac{A : \text{type} \quad x : A \vdash B(x) : \text{type}}{\sum_{x:A} B(x) : \text{type}} \Sigma\text{-F}$$

$$\frac{a : A \quad b : B(a)}{(a, b) : \sum_{x:A} B(x)} \Sigma\text{-I}$$

$$\frac{p : \sum_{x:A} B(x) \quad x : A, y : B(x) \vdash c(x, y) : C((x, y))}{E(c, p) : C(p)} \Sigma\text{-E}$$

Remark: We execute $E(c, p)$ as follows. First execute p , which yields a canonical term of the form (a, b) with $a : A$ and $b : B(a)$. Then we have $c(a, b) : C((a, b))$. Executing $c(a, b)$ we obtain a canonical term e of $C((a, b))$. It is also a canonical term of $C(p)$.

$$\frac{a : A \quad b : B(a) \quad x : A, y : B(x) \vdash c(x, y) : C((x, y))}{E(c, (a, b)) = c(a, b) : C((a, b))} \Sigma\text{-C}$$

Derived Rules

$$\pi_1(p) \coloneqq E(\lambda xy.x, p)$$

$$\pi_2(p) \coloneqq E(\lambda xy.y, p)$$

$$\frac{A : \text{type} \quad x : A \vdash B(x) : \text{type}}{\sum_{x:A} B(x) : \text{type}} \Sigma\text{-F}$$

$$\frac{a : A \quad b : B(a)}{(a, b) : \sum_{x:A} B(x)} \Sigma\text{-I}$$

$$\frac{p : \sum_{x:A} B(x)}{\pi_1(p) : A} \Sigma\text{-E}_1$$

$$\frac{p : \sum_{x:A} B(x)}{\pi_2(p) : B(\pi_1(p))} \Sigma\text{-E}_2$$

$$\frac{a : A \quad b : B(a)}{\pi_1(a, b) = a : A} \Sigma\text{-C}_1$$

$$\frac{a : A \quad b : B(a)}{\pi_2(a, b) = b : B(a)} \Sigma\text{-C}_2$$

Remark: We write $A \times B$ instead of $\sum_{x:A} B$ if x is not free in B .

Rules for coproduct type

$$\frac{A : \text{type} \quad B : \text{type}}{A + B : \text{type}} \text{+-F}$$

$$\frac{a : A}{\iota_1(a) : A + B} \text{+I}_1 \qquad \frac{b : B}{\iota_2(b) : A + B} \text{+I}_2$$

$$\frac{c : A + B \quad x : A \vdash f(x) : C(\iota_1(x)) \quad y : B \vdash g(y) : C(\iota_2(y))}{D(f, g, c) : C(c)} \text{+E}$$

$$\frac{a : A \quad x : A \vdash f(x) : C(\iota_1(x)) \quad y : B \vdash g(y) : C(\iota_2(y))}{D(f, g, \iota_1(a)) = f(a) : C(\iota_1(a))} \text{+C}_1$$

$$\frac{b : B \quad x : A \vdash f(x) : C(\iota_1(x)) \quad y : B \vdash g(y) : C(\iota_2(y))}{D(f, g, \iota_2(b)) = g(b) : C(\iota_2(b))} \text{+C}_2$$

Rules for identity type

Notation: Sometimes we write $x =_A y$ for $\text{Id}_A(x, y)$.

$$\frac{A : \text{type} \quad a, b : A}{a =_A b : \text{type}} \text{ Id-F}$$

$$\frac{a : A}{\text{refl}_a : a =_A a} \text{ Id-I}$$

$$\frac{p : a =_A b \quad \frac{x, y : A, z : x =_A y \vdash B(x, y, z) : \text{type}}{\frac{x : A \vdash d(x) : B(x, x, \text{refl}_x)}{J_d(a, b, p) : B(a, b, p)}}}{J_d(a, b, p) : B(a, b, p)} \text{ Id-E}$$

$$\frac{a : A \quad \frac{x, y : A, z : x =_A y \vdash B(x, y, z) : \text{type}}{\frac{x : A \vdash d(x) : B(x, x, \text{refl}_x)}{J_d(a, a, \text{refl}_a) = d(a) : B(a, a, \text{refl}_a)}}}{J_d(a, a, \text{refl}_a) = d(a) : B(a, a, \text{refl}_a)} \text{ Id-C}$$

Remark: Id-E Rule as Path Induction

Path Induction

If $x, y : A$, $p : x =_A y \vdash B(x, y, p)$ is a type family then to prove $B(x, y, p)$ it suffices to assume y is x and p is refl_x . i.e.:

$$\text{ind}_{=_A} : \prod_{x:A} B(x, x, \text{refl}_x) \rightarrow \prod_{x,y:A} \prod_{p:x=_A y} B(x, y, p)$$

By path induction, paths can be reversed and concatenated:

$$(-)^{-1} : x =_A y \rightarrow y =_A x \quad * : x =_A y \rightarrow y =_A z \rightarrow x =_A z$$

To define both terms, we may assume $p : x =_A y$ and then define terms in the types $P(x, y, p) := y =_A x$ and $Q(x, y, p) := y =_A z \rightarrow x =_A z$. By path induction, we may reduce to the cases $P(x, x, \text{refl}_x) := x =_A x$ and $Q(x, x, \text{refl}_x) := x =_A z \rightarrow x =_A z$.

Logic in HoTT

Logical Connectives	Interpretation in HoTT
\perp	0
\top	1
$A \wedge B$	$A \times B$
$A \vee B$	$\ A + B\ $
$A \rightarrow B$	$A \rightarrow B$
$A \leftrightarrow B$	$A \simeq B$
$\neg A$	$A \rightarrow 0$
$\forall_{x:A} B(x)$	$\prod_{x:A} B(x)$
$\exists_{x:A} B(x)$	$\ \sum_{x:A} B(x)\ $
$\exists!_{x:A} B(x)$	$\text{contr}(\sum_{x:A} B(x))$

Rules for Propositional Truncation

The propositional truncation $\|A\|$ of A is defined by

- ▶ $a : A \vdash \bar{a} : \|A\|$
- ▶ $x, y : \|A\| \vdash x =_A y$
- ▶ If B is a mere proposition and $f : A \rightarrow B$, then there is an induced $\bar{f} : \|A\| \rightarrow B$ such that $\bar{f}(\bar{a}) = f(a)$ for all $a : A$.

$$\begin{array}{ccc} A & \xrightarrow{\quad} & \|A\| \\ & \searrow_f & \downarrow \bar{f} \\ & & B \end{array}$$

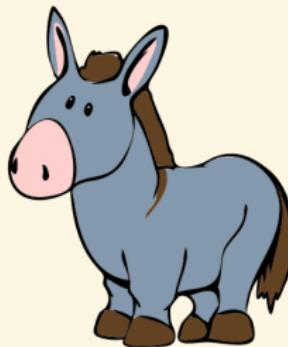
Remarks: The first rule means that if A is inhabited, so is $\|A\|$.

The second ensures that $\|A\|$ is a mere proposition.

Remark: $\|A\| := \prod_{X:\text{Prop}} (A \rightarrow X) \rightarrow X$ satisfies the rules.

Translation

Every farmer who owns a donkey beats it.



$$\forall x \forall y (Fx \wedge Dy \wedge Oxy \rightarrow Bxy)$$

$$b : \prod_{z: \sum_{x:F} \sum_{y:D} Oxy} B(\pi_1(z), \pi_1(\pi_2(z)))$$

- ▶ Anyone who owns a gun should register it.
- ▶ Every point that lies outside a line determines a parallel to it.
- ▶ Any number which has a proper divisor is greater than it.

Homotopy Levels

$$\text{contr}(A) := \sum_{x:A} \prod_{y:A} x =_A y$$

$$\text{prop}(A) := \prod_{x,y:A} \text{contr}(x =_A y) \quad \left(\text{equivalently, } \prod_{x,y:A} x =_A y \right)$$

$$\text{set}(A) := \prod_{x,y:A} \text{prop}(x =_A y)$$

$$\text{groupoid}(A) := \prod_{x,y:A} \text{set}(x =_A y)$$

$$n+1\text{-groupoid}(A) := \prod_{x,y:A} n\text{-groupoid}(x =_A y)$$

$$\text{Prop} := \sum_{A:U} \text{prop}(A) \qquad \text{Set} := \sum_{A:U} \text{set}(A)$$

The Hierarchy of Homotopy Levels

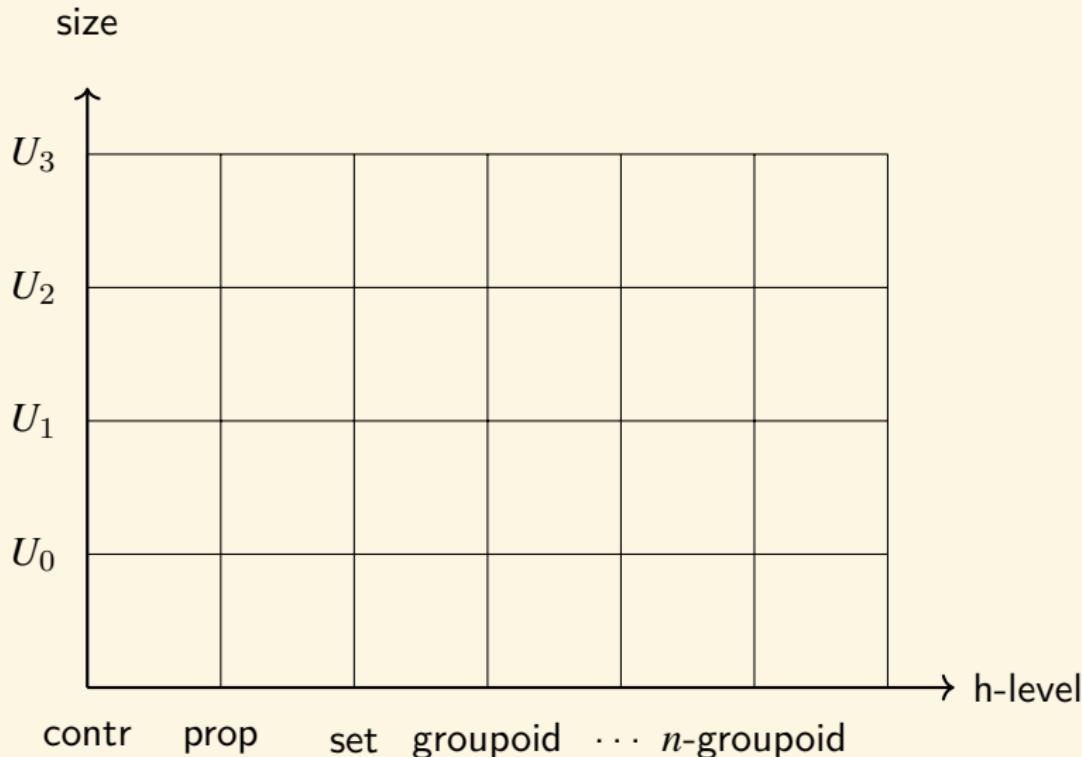


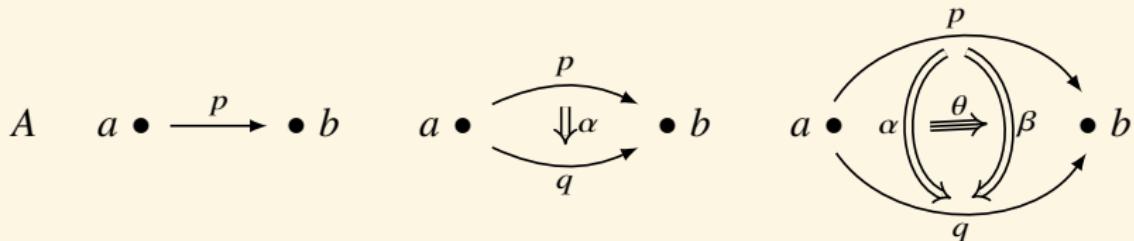
Figure: The 2D hierarchy of types

Instead of sets, clouds of discrete elements, we envisage some sorts of vague spaces, which can be very severely deformed, mapped one to another, and all the while the specific space is not important, but only the space up to deformation.

If you want to get a discrete set, then you pass to the set of connected components of a space defined only up to homotopy.

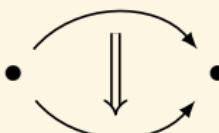
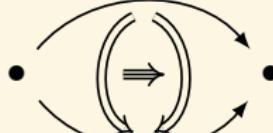
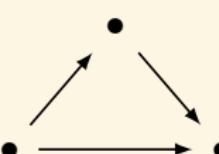
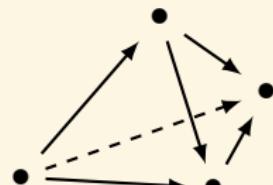
— Yuri Manin

Morning Star $\stackrel{?}{=}$ Evening Star



Type	Topological space
Term	Continuous map
$a : A$	point $a \in A$
$p : a =_A b$	path p from a to b
$\alpha : p =_{a=_Ab} q$	homotopy α from p to q
$\theta : \alpha =_{p=_Abq} \beta$...

- ▶ There is no ultimate, once-and-for-all identity between things — instead, there are structures and isomorphisms between them, and insofar as we are given an isomorphism between structures, we can transfer properties of one to the other, making them indistinguishable.
- ▶ But isomorphisms are no longer facts, they are themselves structures.

object	morphism	2-morphism	3-morphism	...
•	• \longrightarrow •	•  •	•  •	Globes
•	• \longrightarrow •	•  •	•  •	Simplices

Equivalence

$$\text{contr}(A) := \sum_{x:A} \prod_{y:A} x =_A y$$

$$\text{fib}_f(y) := \sum_{x:A} f(x) =_A y$$

$$\text{equiv}(f) := \prod_{y:B} \text{contr}(\text{fib}_f(y))$$

$$A \simeq B := \sum_{f:A \rightarrow B} \text{equiv}(f)$$

► function extensionality

Let $f, g : \prod_{x:A} B(x)$. A homotopy from f to g is a dependent function of the type

$$f \sim g := \prod_{x:A} (fx =_B gx)$$

For saying $\prod_{x:A} (fx =_B gx)$ is inhabited tells us there is a continuous map from $x : A$ to paths between $f(x)$ and $g(x)$, which is the same as giving us a continuous deformation of f into g .

► bi-inverse

$$\text{biinv}(f) := \left(\sum_{g:B \rightarrow A} g \circ f \sim \text{id}_A \right) \times \left(\sum_{h:B \rightarrow A} f \circ h \sim \text{id}_B \right)$$

► isomorphism

$$\text{iso}(f) := \sum_{g:B \rightarrow A} \left[\left(\prod_{x:A} gfx =_A x \right) \times \left(\prod_{y:B} fggy =_B y \right) \right]$$

$$A \cong B := \sum_{f:A \rightarrow B} \text{iso}(f)$$

► $\text{equiv}(f) \simeq \text{biinv}(f) \simeq \text{iso}(f)$

Univalence Foundation

If a statement, concept, or construction is purely logical, then it should be invariant under **all equivalences** of the structures involved.

—Steve Awodey

Voevodsky's Univalence Axiom

$$A =_U B \simeq (A \simeq B)$$

“Identity is equivalent to equivalence.”

Consequences of the Univalence Axiom

- Structure invariance principle

$$(A \cong B) \rightarrow A =_U B$$

Isomorphic structures are identical.

- Function extensionality

$$\prod_{f,g:A \rightarrow B} f = g \simeq \left(\prod_{x:A} fx =_B gx \right)$$

- Propositional extensionality

$$\prod_{A,B:\text{Prop}} A = B \simeq (A \leftrightarrow B)$$

- Paths are isomorphisms for sets

$$\prod_{A,B:\text{Set}} A = B \simeq (A \cong B)$$

Type-Theoretic Axiom of Choice

Theorem (Type-Theoretic Axiom of Choice)

$$\left(\prod_{x:A} \sum_{b:B(x)} C(x, b) \right) \rightarrow \left(\sum_{g:\prod_{x:A} B(x)} \prod_{x:A} C(x, g(x)) \right)$$

is inhabited.

Remark: The stronger version of axiom of choice

$$\left(\prod_{x:A} \left\| \sum_{b:B(x)} C(x, b) \right\| \right) \rightarrow \left\| \sum_{g:\prod_{x:A} B(x)} \prod_{x:A} C(x, g(x)) \right\|$$

is not a consequence of our basic type theory, but it may consistently be assumed as axioms.

Proof.

Take $f : \prod_{x:A} \sum_{b:B(x)} C(x, b)$ and $x : A$.

$$fx : \sum_{b:B(x)} C(x, b) \quad (\Pi\text{-E})$$

$$\pi_1(fx) : B(x) \quad (\Sigma\text{-}E_1)$$

$$\pi_2(fx) : C(x, \pi_1(fx)) \quad (\Sigma\text{-}E_2)$$

$$\lambda x.\pi_1(fx) : \prod_{x:A} B(x) \quad (\Pi\text{-I})$$

$$(\lambda x.\pi_1(fx))x = \pi_1(fx) : B(x) \quad (\Pi\text{-C})$$

$$\pi_2(fx) : C(x, (\lambda x.\pi_1(fx))x) \quad (\text{substitution})$$

$$\lambda x.\pi_2(fx) : \prod_{x:A} C(x, (\lambda x.\pi_1(fx))x) \quad (\Pi\text{-I})$$

$$(\lambda x.\pi_1(fx), \lambda x.\pi_2(fx)) : \sum_{g:\prod_{x:A} B(x)} \prod_{x:A} C(x, g(x)) \quad (\Sigma\text{-I})$$

where $g := \lambda x.\pi_1(fx)$. By $\Pi\text{-I}$, the type-theoretic axiom of choice is inhabited by $\lambda f.(\lambda x.\pi_1(fx), \lambda x.\pi_2(fx))$.

Curry-Howard-Voevodsky Correspondence

Type Theory	Logic	Set Theory	Homotopy Theory
$A : \text{type}$	proposition	set	space
$a : A$	proof	element	point
$x : A \vdash B(x)$	predicate of sets	$\{B_x\}_{x \in A}$	fibration $B \rightarrow A$ with fibers $B(x)$
$x : A \vdash b(x) : B(x)$	conditional proof \perp, \top	family of elements $\emptyset, \{\emptyset\}$	section $\emptyset, \{\bullet\}$
$A + B$	$A \vee B$	disjoint union	coproduct
$A \times B$	$A \wedge B$	set of pairs	product space
$A \rightarrow B$	$A \rightarrow B$	set of functions	function space
$\sum_{x:A} B(x)$	$\exists_{x:A} B(x)$	disjoint sum	total space of fibration $B \rightarrow A$
$\prod_{x:A} B(x)$	$\forall_{x:A} B(x)$	product	space of sections of fibration $B \rightarrow A$
$p : x =_A y$	proof of equality	$x = y$	path from x to y
$\sum_{x,y:A} x =_A y$	equality relation	$\{(x,x) : x \in A\}$	path space A^I

Type Theory	Category Theory
empty type 0	initial object
unit type 1	terminal object
product type $A \times B$	product
coproduct type $A + B$	coproduct
function type $A \rightarrow B$	exponential object (cartesian closure)
dependent product $\prod_{x:A} B$	right adjoint to pullback
dependent sum $\sum_{x:A} B$	left adjoint to pullback
identity type	diagonal/equalizer
proposition type Ω	subobject classifier (elementary topos)
universe type U	object classifier (∞ -topos)
natural numbers \mathbb{N}	natural numbers object
coequalizer type $\text{coeq}(f, g)$	coequalizer

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

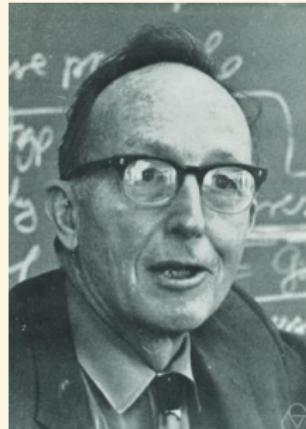
Birds vs Frogs

Category theory takes a bird's eye view of mathematics. From high in the sky, details become invisible, but we can spot patterns that were impossible to detect from ground level.

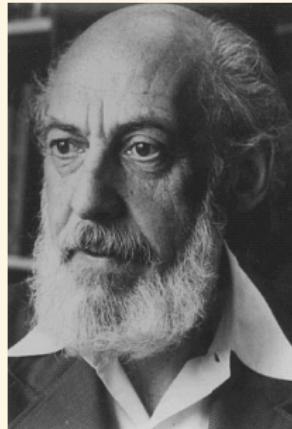
— Tom Leinster

Good general theory does not search for the maximum generality, but for the right generality.

— Saunders Mac Lane



(a) Mac Lane



(b) Eilenberg

Readings

1. S. Awodey: Category Theory.
2. S. Mac Lane: Categories for the Working Mathematician.
3. T. Leinster: Basic Category Theory.
4. P. Smith: Category Theory — A Gentle Introduction.
5. E. Riehl: Category theory in Context.
6. H. Simmons: An Introduction to Category Theory.
7. M. Barr, C. Wells: Category Theory for Computing Science.
8. B. Fong, D. I. Spivak: An Invitation to Applied Category Theory.
9. D. I. Spivak: Category Theory for the Sciences.
10. F. W. Lawvere, S. H. Schanuel: Conceptual Mathematics.
11. F. W. Lawvere, R. Rosebrugh: Sets for Mathematics.
12. T. Streicher: Introduction to Category Theory and Categorical Logic.
13. B. Jacobs: Categorical Logic and Type Theory.
14. R. Goldblatt: Topoi — The Categorical Analysis of Logic.
15. P. Johnstone: Sketches of an Elephant.
16. S. Mac Lane, I. Moerdijk: Sheaves in Geometry and Logic.
17. J. Adamek, H. Herrlich, G. E. Streicher: Abstract and Concrete Categories — The Joy of Cats.
18. nLab

Contents

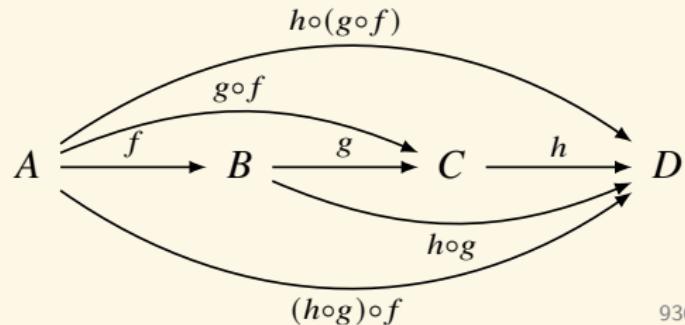
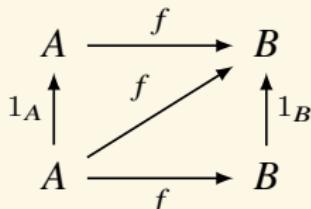
Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References
	1436

What is a Category?

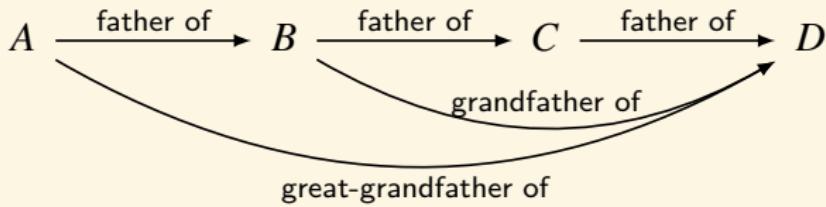
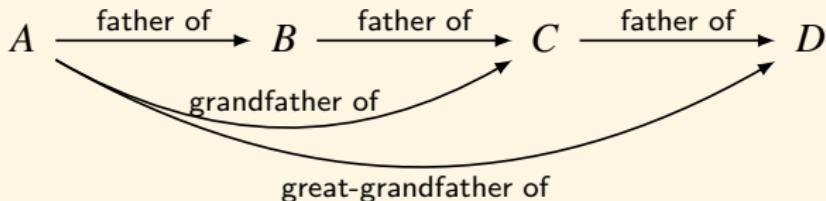
Definition (Category)

A category \mathbf{C} consists of

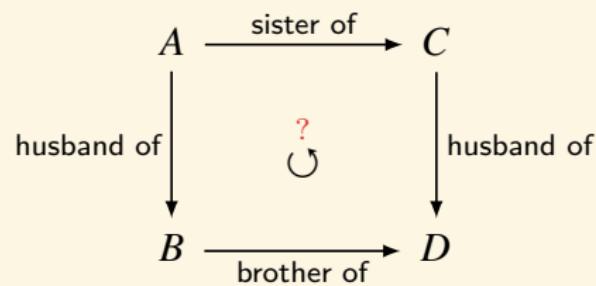
- ▶ a class of objects $\text{ob}(\mathbf{C})$.
- ▶ a set of morphisms $\text{Hom}(A, B) := \{f : A \rightarrow B\}$ (or $\mathbf{C}(A, B)$) with domain $A = \text{dom}(f)$ and codomain $B = \text{cod}(f)$ for $A, B \in \text{ob}(\mathbf{C})$.
- ▶ the identity $1_A : A \rightarrow A$ for $A \in \text{ob}(\mathbf{C})$.
- ▶ the composition $\circ : \text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$ for $A, B, C \in \text{ob}(\mathbf{C})$ such that
 - ▶ $\forall AB \in \text{ob}(\mathbf{C}) \forall f : A \rightarrow B \ [f \circ 1_A = f = 1_B \circ f]$
 - ▶ $\forall ABCD \in \text{ob}(\mathbf{C}) \forall fgh : A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \ [h \circ (g \circ f) = (h \circ g) \circ f]$



Associativity



Commutative?



Remark

The concept of category has a first-order axiomatization, in a language having

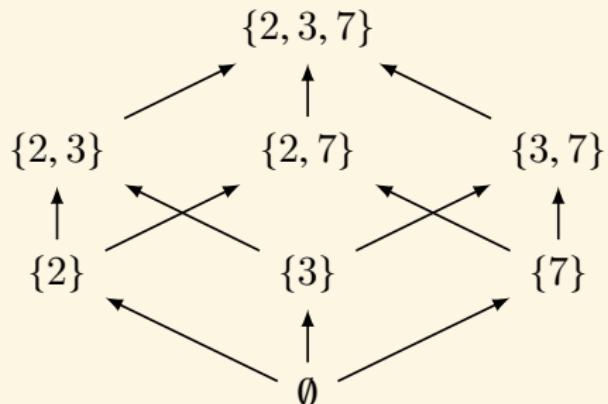
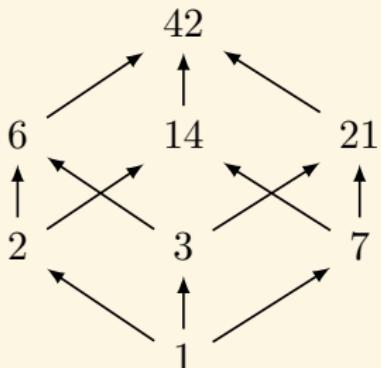
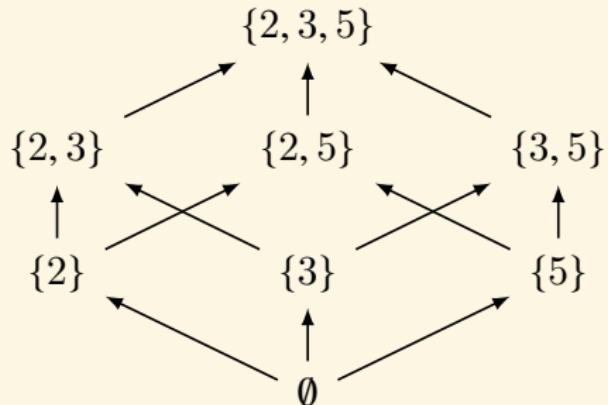
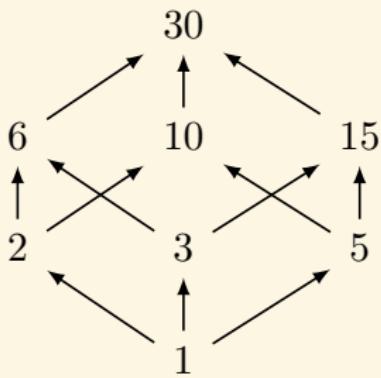
- ▶ two sorts O and A (respectively for objects and arrows),
- ▶ two unary function symbols (for domain and codomain)

$$A \xrightarrow[\text{cod}]{\text{dom}} O$$

- ▶ one unary function symbol $1 : O \rightarrow A$ (formalizing the concept of identity arrow) and
- ▶ a ternary predicate of type A (formalizing the notion of composition of arrows).

From a graph G we can get a category $\text{Free}(G)$ called the “free category on G ”, which has nodes of the graph as objects and paths as morphisms.

Example: The “Lattice” of Factors



A category is a network of composable relationships

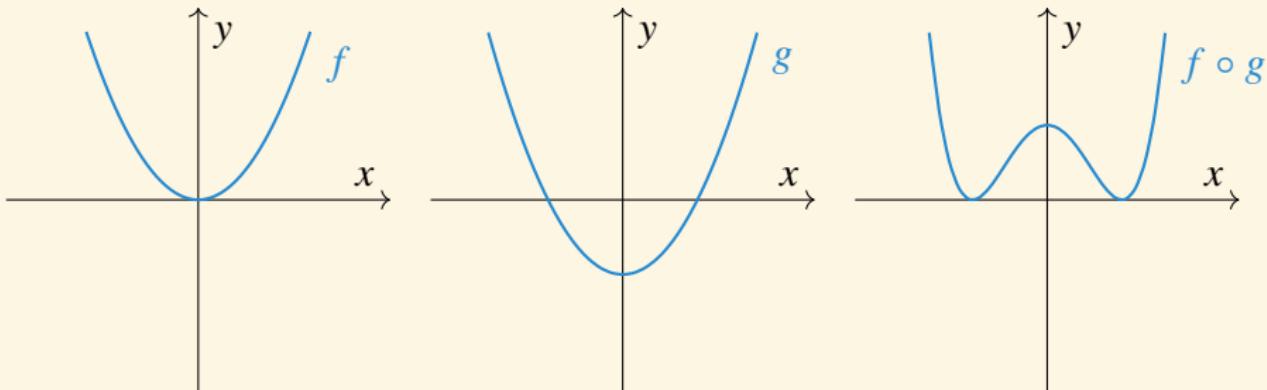


Figure: Convex functions on \mathbb{R} do not form a category.

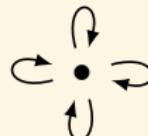
- ▶ the devil is in the morphisms!
- ▶ objects are easy, morphisms are usually where the difficulties hide.
- ▶ Ask not what a thing is; ask what it does.

Examples — Mathematical Objects as Categories

- A *discrete category* is a category whose only morphisms are the identity morphisms. — A *set* can be seen as a discrete category.
- A *preorder* is a category having at most one morphism from one object to another.
- A *poset* is a preorder where if there's a morphism $f : x \rightarrow y$ and $g : y \rightarrow x$, then $x = y$.
- A *monoid* (M, \cdot, e) is a category that has only one object \bullet s.t. $\text{Hom}(\bullet, \bullet) = M$.
- A *groupoid* is a category in which every morphism is an isomorphism.



- A *group* is a category that has only one object and in which every morphism is an isomorphism.



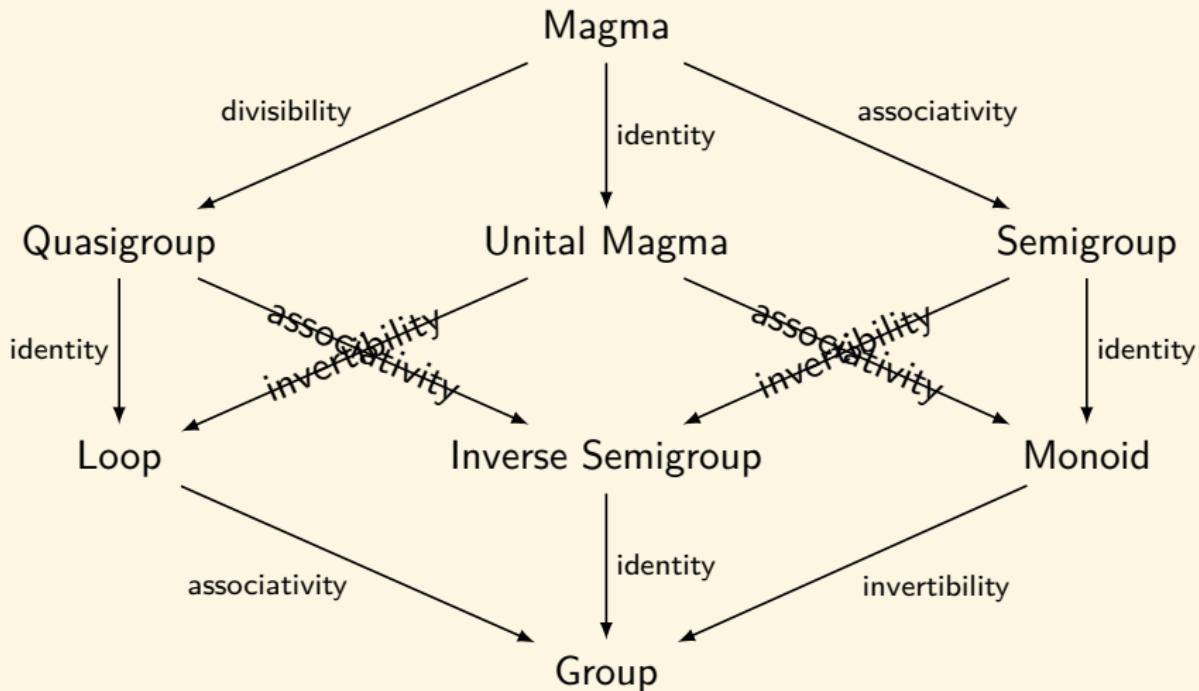
Examples — Categories of Mathematical Objects

Category	Objects	Morphisms
Set	sets	functions
Par	sets	partial functions
Rel	sets	relations
Preord	preorders	monotone functions
Poset	partial order sets	monotone maps
Graph	directed graphs	graph homomorphisms
Type	types	computable functions
Mon	monoids	homomorphisms
Grp	groups	homomorphisms
Ab	abelian groups	homomorphisms
Rng	rings	ring homomorphisms
Vect\mathbb{K}	vector spaces over a field \mathbb{K}	linear maps
Ban$_{\infty}$	real Banach spaces	bounded linear mappings
Ban$_1$	real Banach spaces	linear contractions
Diff	smooth manifolds	smooth maps
Top	topological spaces	continuous functions

Group-like Structures

	Totality	Associativity	Identity	Invertibility	Commutativity
Semigroupoid		✓			
Small Category		✓	✓		
Groupoid		✓	✓	✓	
Magma	✓				
Quasigroup	✓			✓	
Unital Magma	✓		✓		
Loop	✓		✓	✓	
Semigroup	✓	✓			
Inverse Semigroup	✓	✓		✓	
Monoid	✓	✓	✓		
Commutative monoid	✓	✓	✓		✓
Group	✓	✓	✓	✓	
Abelian group	✓	✓	✓	✓	✓

Group-like Structures

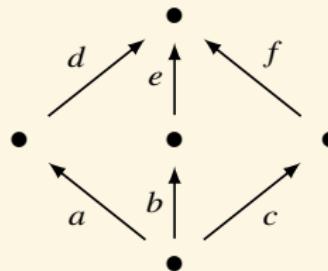


Groupoid

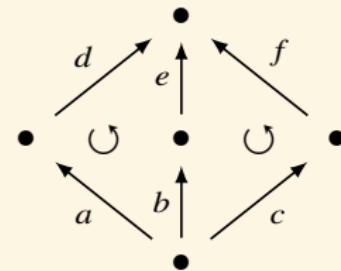
- ▶ Any equivalence relation R on a set X can be presented as a groupoid on X . A groupoid is a generalized equivalence relation.
- ▶ The underlying groupoid of a category **C** is an internal criterion of identity. Entities are entities in a context.

Preorder

Which graph is a preorder?

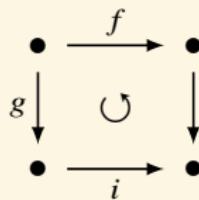


no equation

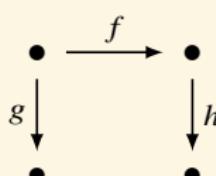


$da = eb = fc$

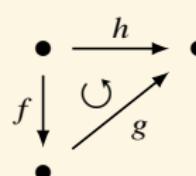
What equations do you need to make the following graphs into preorders?



$$hf = ig$$



no equation



$$h = gf$$



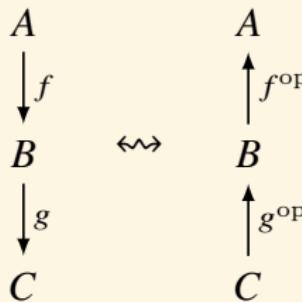
$$f = 1_a$$

Remark: The free category on a graph has the fewest possible equations between parallel morphisms, while a preorder has the most possible.

Opposite Category

Definition (Opposite Category)

The *opposite category* \mathbf{C}^{op} of \mathbf{C} is formed by reversing the morphisms. Formally, $\text{ob}(\mathbf{C}^{\text{op}}) = \text{ob}(\mathbf{C})$, and for each morphism $f : A \rightarrow B$ of \mathbf{C} a morphism $f^{\text{op}} : B \rightarrow A$ in \mathbf{C}^{op} , with the same identities and a composition defined (when possible) by $f^{\text{op}} \circ g^{\text{op}} := (g \circ f)^{\text{op}}$.



The duality principle

- ▶ Every statement formulated in the language of Category Theory has a dual, obtained by formally reversing the arrows and the order of composition of them.
- ▶ A statement is true in a category \mathbf{C} iff the dual statement is true in the dual category \mathbf{C}^{op} .
- ▶ Hence a statement is valid in all categories iff its dual is.

“A comathematician is a machine for turning cotheorems into ffee.”

“A mathematician is a machine for turning coffee into theorems.”

Subcategory

Definition (Subcategory)

We say that \mathbf{C}' is a subcategory of \mathbf{C} if:

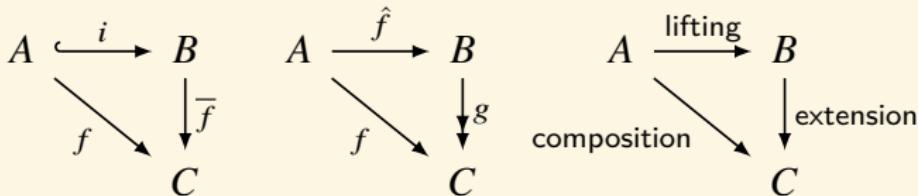
1. $\text{ob}(\mathbf{C}') \subset \text{ob}(\mathbf{C})$;
2. $\mathbf{C}'(A, B) \subset \mathbf{C}(A, B)$ for $A, B \in \text{ob}(\mathbf{C}')$;
3. the composition of morphisms in \mathbf{C}' is induced by the composition of morphisms in \mathbf{C} ;
4. the identity morphisms in \mathbf{C}' are identity morphisms in \mathbf{C} .

Moreover, \mathbf{C}' is called *wide* iff all objects of \mathbf{C} are also objects of \mathbf{C}' .

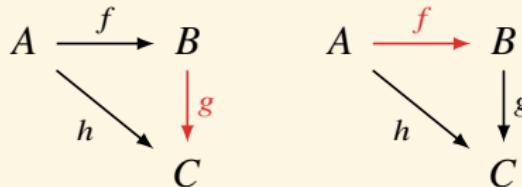
\mathbf{C}' is called *full* iff for $A, B \in \text{ob}(\mathbf{C}')$: $\mathbf{C}'(A, B) = \mathbf{C}(A, B)$.

Composition, Extension, Lifting

- If $f : A \rightarrow C$ is a function and A is a subset of B with the inclusion function $i : A \hookrightarrow B$, then an extension of f along i is a function $\bar{f} : B \rightarrow C$ such that $f = \bar{f} \circ i$.
- Consider an onto function $g : B \twoheadrightarrow C$. Let $f : A \rightarrow C$ be any function. A lifting of f along g is a function $\hat{f} : A \rightarrow B$ such that $f = g \circ \hat{f}$.

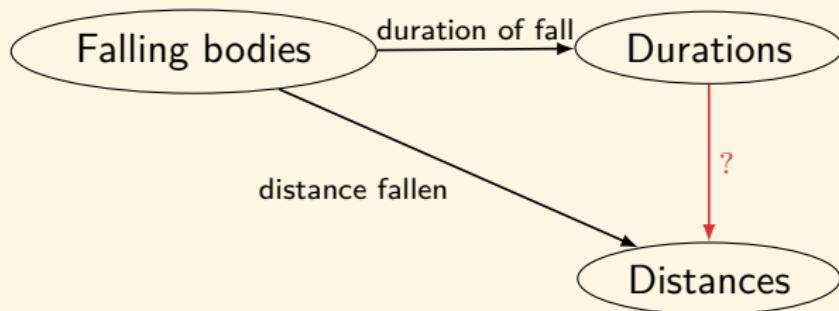


1. The 'determination' (or 'extension') problem: given f and h , what are all g , if any, for which $h = g \circ f$?
2. The 'choice' (or 'lifting') problem: given g and h , what are all f , if any, for which $h = g \circ f$?

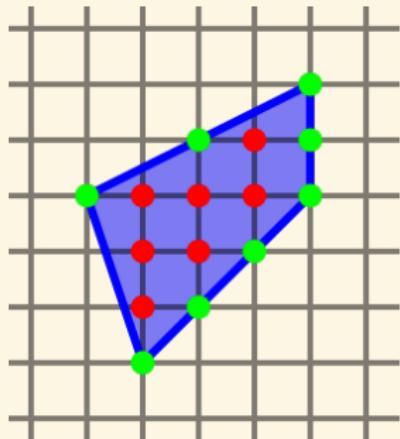


Example: the ‘determination’ (or ‘extension’) problem

Once Galileo realized that the distance of a dropped object falls in a certain time is determined by the time, it did not take too many experiments before he found a function for the distance in terms of the time $d = \frac{1}{2}gt^2$.



Example: the ‘determination’ (or ‘extension’) problem

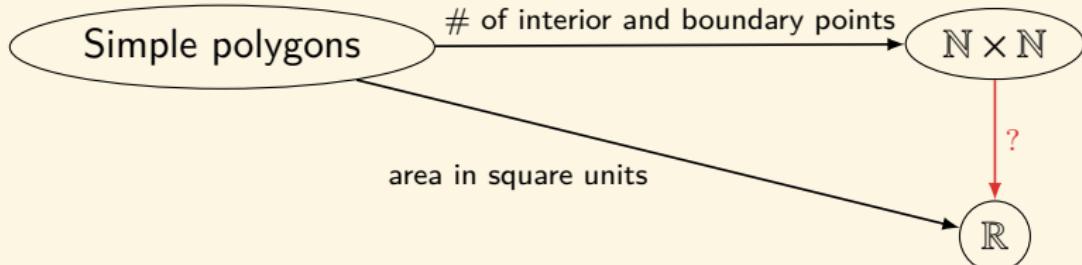


Pick's theorem

The *Area* of a simple polygon with integer vertex coordinates is determined by the number of its *Interior* points and its *Boundary* points.

$$A = I + \frac{B}{2} - 1$$

$$A = 7 + \frac{5}{2} - 1 = 10$$



Monic / Epic / Bimorphism / Isomorphism

Definition

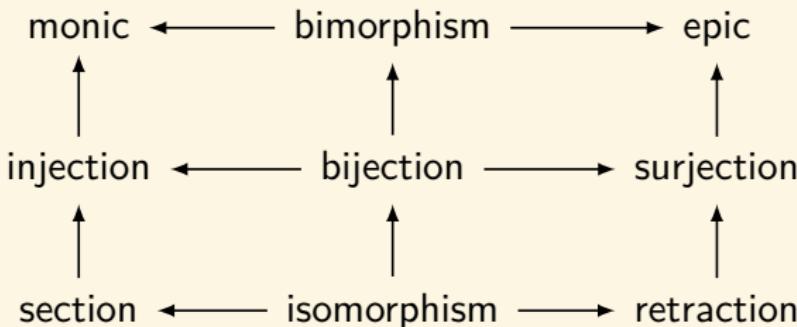
A morphism $f : A \rightarrow B$ is a:

1. monomorphism (monic) iff $\forall X \forall g_1 g_2 : X \rightarrow A : fg_1 = fg_2 \implies g_1 = g_2$.
2. epimorphism (epic) iff $\forall X \forall g_1 g_2 : B \rightarrow X : g_1 f = g_2 f \implies g_1 = g_2$.
3. bimorphism iff f is both monic and epic.
4. isomorphism iff $\exists g : B \rightarrow A : gf = 1_A \text{ & } fg = 1_B$.
5. endomorphism iff $A = B$.
6. automorphism iff f is both an endomorphism and an isomorphism.
7. retraction iff a right inverse of f exists, i.e. $\exists g : B \rightarrow A : fg = 1_B$.
8. section iff a left inverse of f exists, i.e. $\exists g : B \rightarrow A : gf = 1_A$.

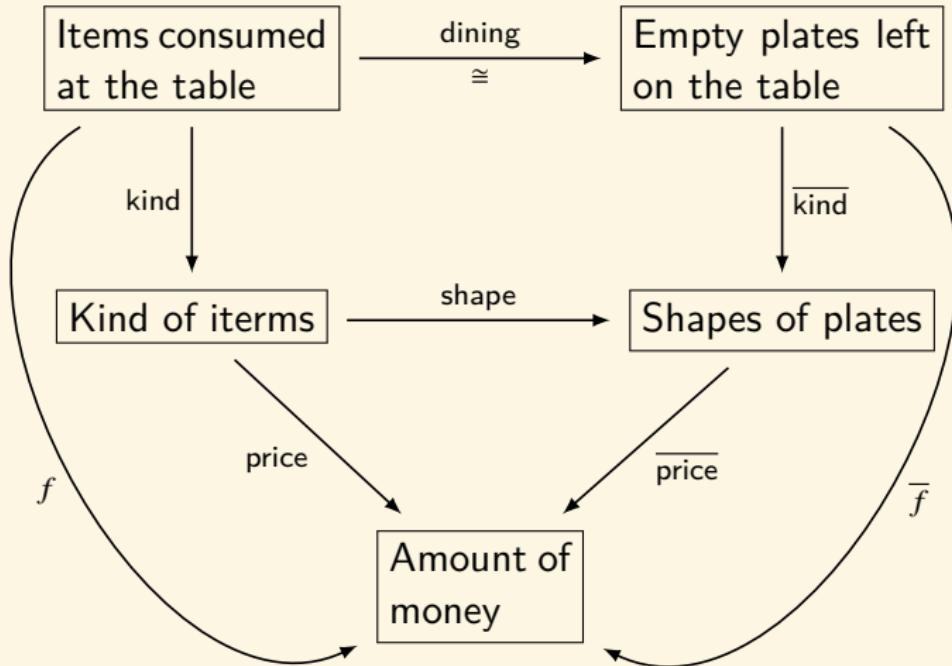
$$\begin{array}{ccc} B & \xrightarrow{g} & A \\ & \searrow 1_B & \downarrow f \\ & & B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow 1_A & \downarrow g \\ & & A \end{array}$$

Monic / Epic / Bimorphism / Isomorphism

- ▶ Every retraction is epic.
- ▶ Every section is monic.
- ▶ In a concrete category every section is injective.
- ▶ In a concrete category every retraction is surjective.
- ▶ The following three statements are equivalent:
 1. f is a monomorphism and a retraction;
 2. f is an epimorphism and a section;
 3. f is an isomorphism.



大学自助食堂



$$\sum_k \text{price}(k) \cdot (\text{size of the stack of } \textit{kind} \text{ over } k) = \sum_x x \cdot (\text{size of the stack of } f \text{ over } x)$$

$$\sum_k \overline{\text{price}}(s) \cdot (\text{size of the stack of } \overline{\textit{kind}} \text{ over } s) = \sum_x x \cdot (\text{size of the stack of } \overline{f} \text{ over } x)$$

- ▶ All equations are lies except $x = x$.
- ▶ Equality doesn't mean a and b are the same — it is about when the world should treat them the same.
- ▶ Isomorphic objects are treated as the same by the rest of the category.
- ▶ Things can be isomorphic in one category but not another.
- ▶ Everything should be understood in context.
- ▶ Something not universal in one place can be universal in another.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Initial Object & Terminal Object

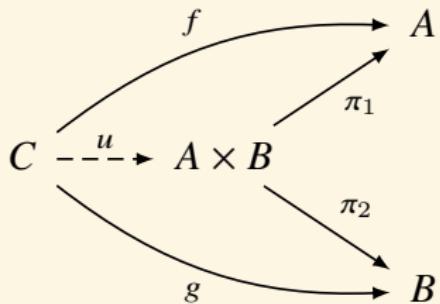
Definition (Initial Object & Terminal Object)

- ▶ An *initial object* in \mathbf{C} is an object 0 s.t. for every object A , there is a unique morphism $!_A : 0 \rightarrow A$.
- ▶ A *terminal object* in \mathbf{C} is an object 1 s.t. for every object A , there is a unique morphism $!_A : A \rightarrow 1$.
- ▶ If an object is both initial and terminal, it is called a *zero object*.
- ▶ An initial object 0 is called a *strict initial object* iff every morphism $x \rightarrow 0$ is an isomorphism.
- ▶ A zero morphism $0 : A \rightarrow B$ is the unique morphism factoring over the zero object $0 : A \rightarrow 0 \rightarrow B$
- ▶ A category with a zero object is called *pointed*.
- ▶ An initial object of \mathbf{C} is a terminal object of \mathbf{C}^{op} , and vice-versa.
- ▶ Initial and terminal objects are unique up to isomorphism.

Examples

- ▶ In **Preord**, the greatest element \top is terminal and the least element \perp is initial.
- ▶ In **Set**, any one-element set is terminal. The empty set is initial.
- ▶ In **Top**, the one-element topological space is terminal and the empty topological space is initial.
- ▶ In **Grp**, the one-element group is both initial and terminal. Similarly in **Mon** and **R -Mod**.
- ▶ In **Rng**, the one-element ring is terminal, and \mathbb{Z} is initial.

Product



Definition (Product)

A *product* of A and B is an object $A \times B$ with a pair of morphisms

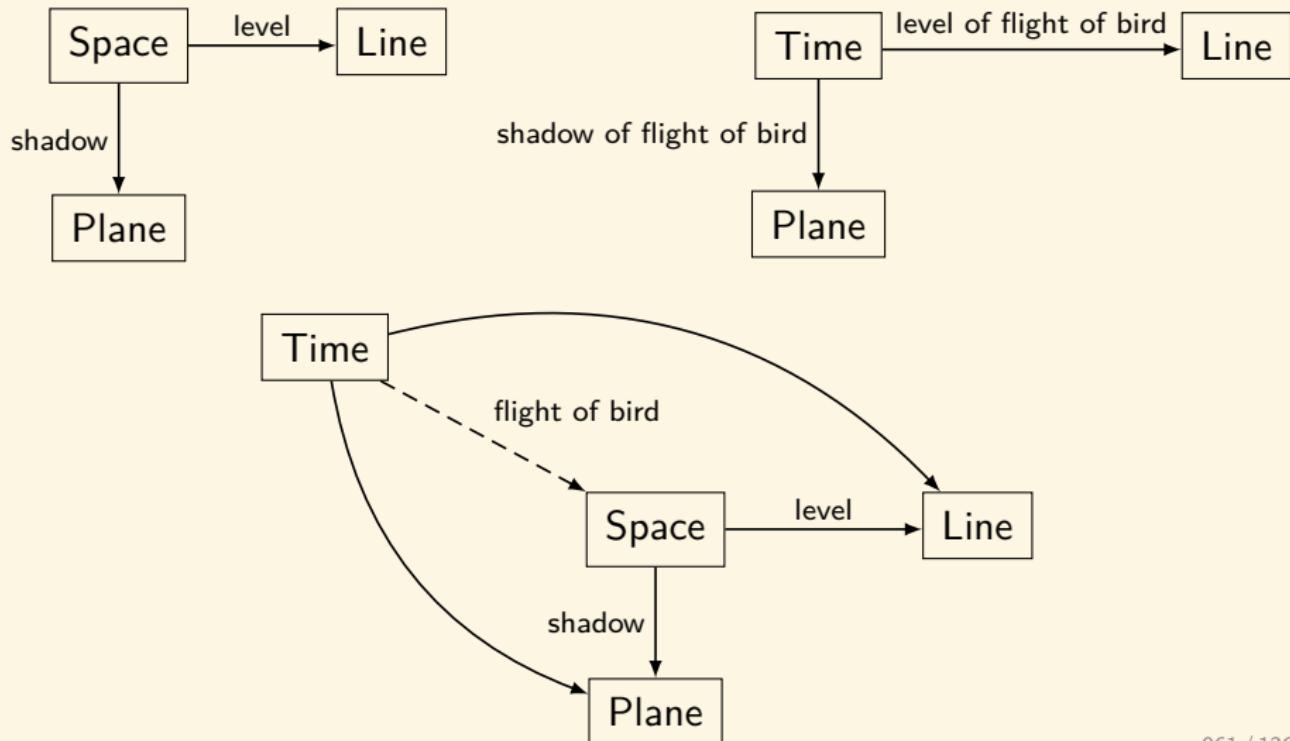
$$A \xleftarrow{\pi_1} A \times B \xrightarrow{\pi_2} B \text{ s.t}$$

$$\forall C \forall fg : A \xleftarrow{f} C \xrightarrow{g} B \exists! u : C \rightarrow A \times B [f = \pi_1 \circ u \text{ & } g = \pi_2 \circ u]$$

Example: $\min\{x, y\}$ in (\mathbb{R}, \leq) . $x \cap y$ in $(P(A), \subset)$. $\gcd(x, y)$ in $(\mathbb{N}, |)$.

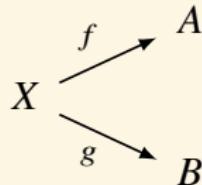
$$A \wedge B \vdash A \quad A \wedge B \vdash B \quad \frac{C \vdash A \quad C \vdash B}{C \vdash A \wedge B}$$

- ▶ If a bird is in our space, and you know only the shadow of the bird and the level of the bird, then you can reconstruct the position of the bird.
- ▶ If you have a motion picture of the bird's shadow as it flies, and a motion picture of its level, then you can reconstruct the entire flight of the bird!

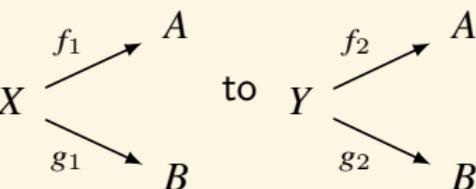


How to understand product? — terminal object of \mathbf{C}_{AB}

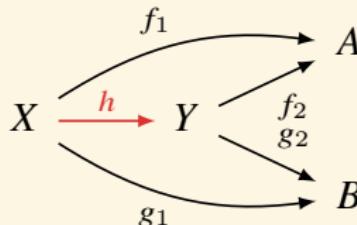
- Given a category \mathbf{C} and $A, B \in \mathbf{C}$, we can build a new category \mathbf{C}_{AB} .
- An object of \mathbf{C}_{AB} is an object of \mathbf{C} with a pair of maps to A, B .



- a morphism from X to Y is a map $X \xrightarrow{h} Y$ in \mathbf{C}



which ‘preserves the structure’.



- then the terminal object of \mathbf{C}_{AB} is the product $A \times B$.

Coproduct

$$\begin{array}{ccccc} A & \xrightarrow{\quad f \quad} & & & C \\ \downarrow \iota_1 & & & & \downarrow u \\ & & A + B & \dashrightarrow & \\ & \nearrow \iota_2 & & & \searrow \\ B & \xrightarrow{\quad g \quad} & & & \end{array}$$

Definition (Coproduct)

A *coproduct* of A and B is an object $A + B$ with a pair of morphisms

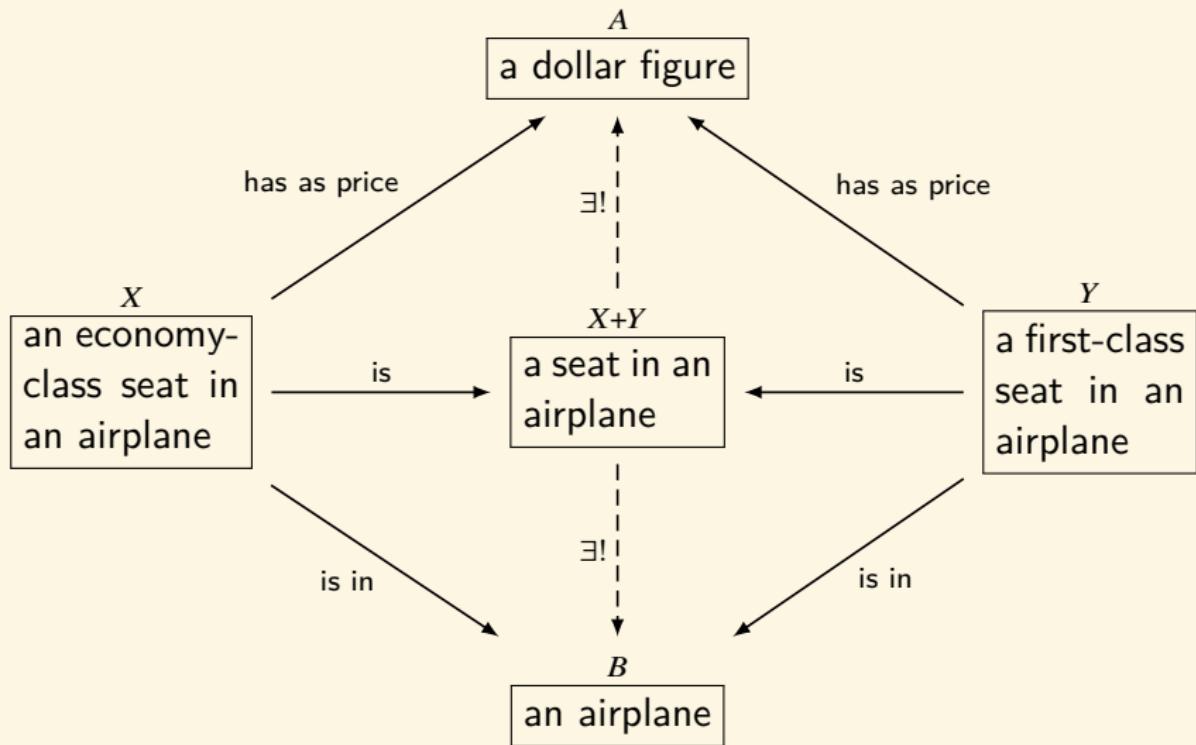
$$A \xrightarrow{\iota_1} A + B \xleftarrow{\iota_2} B \text{ s.t }$$

$$\forall C \forall fg : A \xrightarrow{f} C \xleftarrow{g} B \exists! u : A + B \rightarrow C [f = u \circ \iota_1 \text{ } \& \text{ } g = u \circ \iota_2]$$

Example: $\max\{x, y\}$ in (\mathbb{R}, \leq) . $x \cup y$ in $(P(A), \subset)$. $\text{lcm}(x, y)$ in $(\mathbb{N}, |)$.

$$\frac{A \vdash C \quad B \vdash C}{A \vee B \vdash C}$$

Example — Coproduct



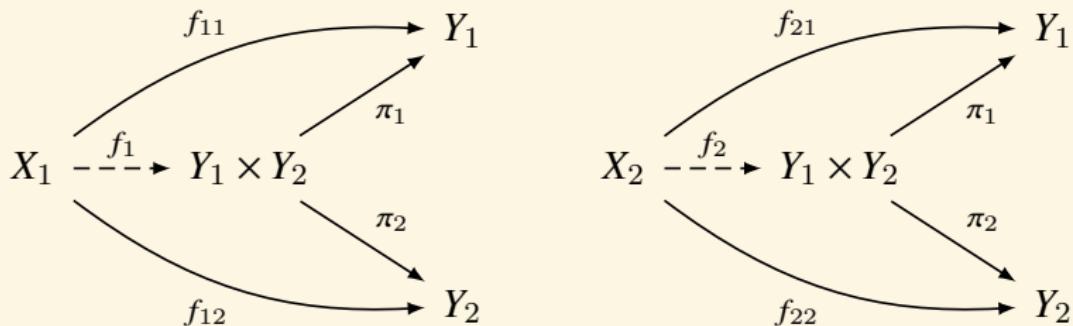
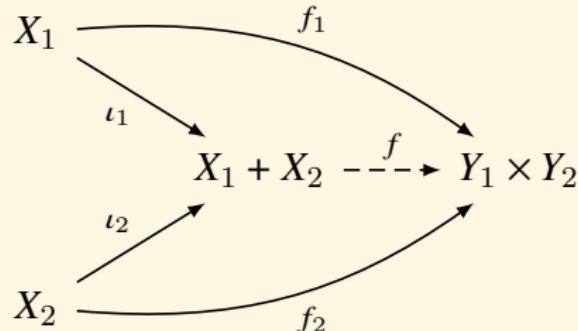
Coproduct & Product

The diagram consists of two parts. On the left, labeled 'Coproduct', there is a commutative square. The top horizontal arrow is labeled ι_i and maps X_i to the coproduct $\coprod_{i \in I} X_i$. The bottom horizontal arrow is labeled f_i and maps X_i to Y . The vertical arrow between the coproduct and Y is labeled u . On the right, labeled 'Product', there is another commutative square. The top horizontal arrow is labeled f_i and maps X to the product $\prod_{i \in I} Y_i$. The bottom horizontal arrow is labeled π_i and maps the product $\prod_{i \in I} Y_i$ to Y_i . The vertical arrow between X and the product is labeled u .

$$\text{Hom}\left(\coprod_{i \in I} X_i, Y\right) \cong \prod_{i \in I} \text{Hom}(X_i, Y) \quad u \mapsto (u\iota_i)_{i \in I}$$

$$\text{Hom}\left(X, \prod_{i \in I} Y_i\right) \cong \prod_{i \in I} \text{Hom}(X, Y_i) \quad u \mapsto (\pi_i u)_{i \in I}$$

What are the morphisms $\coprod_{i=1}^m X_i \rightarrow \prod_{j=1}^n Y_j$?



$$f_1 = \langle f_{11}, f_{12} \rangle \quad f_2 = \langle f_{21}, f_{22} \rangle \quad f = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}$$

What are the morphisms $\coprod_{i=1}^m X_i \rightarrow \prod_{j=1}^n Y_j$?

$$\text{Hom}\left(\coprod_{i=1}^m X_i, \prod_{j=1}^n Y_j\right) \cong \prod_{i=1}^m \text{Hom}\left(X_i, \prod_{j=1}^n Y_j\right) \cong \prod_{i=1}^m \prod_{j=1}^n \text{Hom}(X_i, Y_j)$$

Theorem

The morphisms $\coprod_{i=1}^m X_i \rightarrow \prod_{j=1}^n Y_j$ are the “matrices”

$$M = \begin{bmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ & & \ddots & \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{bmatrix}$$

where $\pi_j M \iota_i = f_{ij}$.

Matrix Multiplication

- ▶ Assume there is a zero morphism 0_{AB} from A to B .
- ▶ Then we have the ‘identity matrix’:

$$A + B \xrightarrow{\begin{bmatrix} 1_A & 0_{AB} \\ 0_{BA} & 1_B \end{bmatrix}} A \times B$$

- ▶ A category with zero morphisms in which every ‘identity matrix’ is an isomorphism is called a *linear category*.
- ▶ In a linear category, we can multiply any matrix $X_1 + X_2 \xrightarrow{f} A \times B$ and $A + B \xrightarrow{g} Y_1 \times Y_2$ as

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} \cdot \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} := \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} \circ \begin{bmatrix} 1_A & 0_{AB} \\ 0_{BA} & 1_B \end{bmatrix}^{-1} \circ \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix}$$

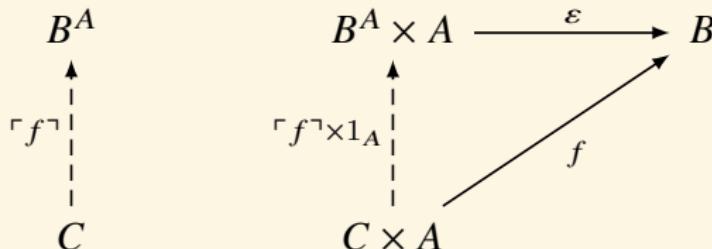
- ▶ This multiplication is another matrix $X_1 + X_2 \rightarrow Y_1 \times Y_2$.

$$X_1 + X_2 \xrightarrow{f} A \times B \xrightarrow{\begin{bmatrix} 1_A & 0_{AB} \\ 0_{BA} & 1_B \end{bmatrix}^{-1}} A + B \xrightarrow{g} Y_1 \times Y_2$$

Exponential & Cartesian Closed Category (CCC)

- An exponential of objects A, B is an object B^A with a morphism $\varepsilon : B^A \times A \rightarrow B$ s.t.

$$\forall C \forall f : C \times A \rightarrow B \exists! \lceil f \rceil : C \rightarrow B^A \left[\varepsilon \circ (\lceil f \rceil \times 1_A) = f \right]$$



- Cartesian Closed Category (CCC)** is a category with a terminal object, all products and all exponentials.
- Bicartesian Closed Category (BCCC)** is a CCC with an initial object and all coproducts, with products distributing over coproducts.

Curry-Howard-Lambek Isomorphism

- **Objects** types/formulas $\top | A \times B | A \rightarrow B$
- **Morphisms** terms/proofs $1_A | ! | g \circ f | \langle f, g \rangle | \pi_1 | \pi_2 | \vdash f \dashv | \varepsilon$
 $f : A \rightarrow B \iff A \vdash B$

$$\frac{}{1_A : A \vdash A}$$

$$\frac{}{! : A \vdash \top}$$

$$\frac{f : A \vdash B \quad g : B \vdash C}{g \circ f : A \vdash C}$$

$$\frac{f : C \vdash A \quad g : C \vdash B}{\langle f, g \rangle : C \vdash A \times B}$$

$$\frac{}{\pi_1 : A \times B \vdash A}$$

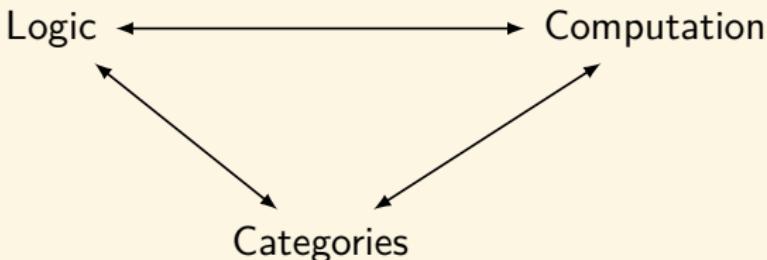
$$\frac{}{\pi_2 : A \times B \vdash B}$$

$$\frac{f : A \times B \vdash C}{\vdash f \dashv : A \vdash B \rightarrow C}$$

$$\frac{}{\varepsilon : (A \rightarrow B) \times A \vdash B}$$

Curry-Howard-Lambek Isomorphism

Logic	Type Theory	Category Theory
Formula Proof	Type Term/Program	Object Morphism
false \perp	empty type 0	initial object 0
true T	unit type 1	terminal object 1
conjunction \wedge	product type \times	product \times
disjunction \vee	coproduct type $+$	coproduct $+$
implication \rightarrow	function type \rightarrow	exponential B^A
cut-elimination	β -reduction	composition \circ
modus ponens	application app	evaluation ε



A mathematician is a person who can find analogies between theorems; a better mathematician is one who can see analogies between proofs and the best mathematician can notice analogies between theories. One can imagine that the ultimate mathematician is one who can see analogies between analogies.

— Stefan Banach

- ▶ Category theory is not a theory of everything.
- ▶ It is a theory of theories of anything.
- ▶ It allows one to compare different models, thus carrying knowledge from one domain to another, as long as one can construct the appropriate “analogy”, i.e., functor.

Mathematics

formalized in type theory

internalized in structured categories

computation

type theory can be interpreted in structured categories

categories

Category	Physics	Topology	Logic	Computation
Object	Hilbert space	Manifold	Proposition	Data type
Morphism	Operator	Cobordism	Proof	Program
Tensor product of objects	Hilbert space of joint system	Disjoint union of manifolds	Conjunction of propositions	Product of data types
Tensor product of morphisms	Parallel processes	Disjoint union of cobordisms	Proofs carried out in parallel	Programs executing in parallel
Internal Hom	Hilbert space of “anti- X and Y ”	Disjoint union of orientation-reversed X and Y	Conditional proposition	Function type

Table: Physics, Topology, Logic and Computation

Definition (Groups in a Category)

Let \mathbf{C} be a category with finite products. A group in \mathbf{C} consists of objects

and morphisms $G \times G \xrightarrow{m} G \xleftarrow{i} G$ such that,
 $\begin{array}{c} \uparrow e \\ 1 \end{array}$

$$(G \times G) \times G \xrightarrow{\cong} G \times (G \times G)$$

1. m is associative, $m \times 1_G \downarrow \qquad \qquad \qquad \downarrow 1_G \times m$

$$\begin{array}{ccccc} & & & & \\ G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G \\ & & & & \end{array}$$

$$1 \times G \xleftarrow{\cong} G \xrightarrow{\cong} G \times 1$$

2. e is a unit, $e \times 1_G \downarrow \qquad \qquad \qquad \downarrow 1_G \times e$

$$\begin{array}{ccccc} & & & & \\ G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G \\ & & & & \end{array}$$

$$G \times G \xleftarrow{\Delta} G \xrightarrow{\Delta} G \times G$$

3. i is an inverse, $1_G \times i \downarrow \qquad \qquad \qquad \downarrow !_G \qquad \qquad \qquad \downarrow i \times 1_G$

$$\begin{array}{ccccc} & & & & \\ G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G \\ & & & & \end{array}$$

Groups in a Category

Definition

A *group homomorphism* from G to H is a morphism $f : G \rightarrow H$ in \mathbf{C} s.t.

$$\begin{array}{ccc} G \times G & \xrightarrow{f \times f} & H \times H \\ m_1 \downarrow & & \downarrow m_2 \\ G & \xrightarrow{f} & H \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ e_1 \swarrow & 1 & \searrow e_2 \\ & 1 & \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ i_1 \downarrow & & \downarrow i_2 \\ G & \xrightarrow{f} & H \end{array}$$

Groups in a Category

- ▶ A group in the usual sense is a group in the category **Set**.
- ▶ If **C** is the category of algebraic varieties, a group in **C** is an algebraic group.
- ▶ If **C = Top**, a group in **C** is a topological group.
- ▶ If **C = Diff**, a group in **C** is a Lie group.
- ▶ If **C = Grp**, a group in **C** is an abelian group.

Suppose \circ is a group homomorphism $(G, \bullet) \times (G, \bullet) \rightarrow (G, \bullet)$. Then

$$(a \bullet b) \circ (c \bullet d) = (a \circ c) \bullet (b \circ d)$$

$$a \bullet b = (a \circ 1) \bullet (1 \circ b) = (a \bullet 1) \circ (1 \bullet b) = a \circ b = (1 \bullet a) \circ (b \bullet 1) = (1 \circ b) \bullet (a \circ 1) = b \bullet a$$

Groups as Categories

- ▶ A *group* is a category that has only one object and in which every morphism is an isomorphism.
- ▶ If G and H are groups, regarded as categories, then a functor $f : G \rightarrow H$ is exactly the same thing as a *group homomorphism*.
- ▶ What is a functor $R : G \rightarrow \mathbf{C}$ from a group G to another category \mathbf{C} ? If $\mathbf{C} = \mathbf{Vect}_{\mathbb{K}}$, then R is a “linear representation” of G .
- ▶ In general, any functor $R : G \rightarrow \mathbf{C}$ can be regarded as a representation of G in the category \mathbf{C} : the elements of G become automorphisms of some object in \mathbf{C} . A permutation representation, for instance, is simply a functor into \mathbf{Set} .

Contents

Introduction	
Term Logic	Functors
Propositional Logic	Natural Transformations
Predicate Logic	Equivalence of Categories
Modal Logic	Product and Functor Category
Set Theory	Limits and Colimits
Recursion Theory	Construct New from Old
Equational Logic	Topos
Homotopy Type Theory	ETCS
Category Theory	Yoneda Lemma
Categories	Adjunctions
Cartesian Closed Categories	Categorical Logic
	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Functor

Definition (Functor)

A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ between categories \mathbf{C} and \mathbf{D} is a mapping of objects to objects and morphisms to morphisms, in such a way that:

- $F(f : A \rightarrow B) = Ff : FA \rightarrow FB$
- $F(1_A) = 1_{FA}$
- $F(g \circ f) = Fg \circ Ff$

identity functor $1_{\mathbf{C}}$ and composition of functors

$$\begin{array}{ccc} A & & A \\ \downarrow f & = & \downarrow f \\ B & & B \end{array} \qquad \begin{array}{ccc} A & & G(FA) \\ \downarrow f & = & \downarrow G(Ff) \\ B & & G(FB) \end{array}$$

The diagram illustrates the properties of a functor. On the left, two commutative squares show that F preserves identity morphisms ($1_{\mathbf{C}}$) and composition of morphisms. On the right, another commutative square shows that F preserves composition of morphisms.

Definition (Diagonal Functor)

For categories \mathbf{C} and \mathbf{I} , there exists a *diagonal functor*

$$\Delta : \mathbf{C} \rightarrow \mathbf{C}^{\mathbf{I}}$$

mapping an object $X \in \mathbf{C}$ to the constant diagram ΔX of shape \mathbf{I} in \mathbf{C} where all objects are copies of X and all morphisms are copies of $1_X : X \rightarrow X$.

$$(\Delta X)i := X \text{ for } i \in \mathbf{I}$$

$$(\Delta X)f := 1_X \text{ for } f \in \mathbf{I}$$

$$(\Delta f)i := f \text{ for } f \in \text{Hom}_{\mathbf{C}}(X, Y) \text{ and } i \in \mathbf{I}$$

Remark: The (binary) diagonal functor of \mathbf{C} is the functor $\Delta : \mathbf{C} \rightarrow \mathbf{C} \times \mathbf{C}$ given by $\Delta X = (X, X)$ and $\Delta f = (f, f)$.

Definition: The diagonal morphism of X in a category \mathbf{C} with product is

$\Delta : X \rightarrow X \times X$ satisfying

$$\begin{array}{ccccc} & & X & & \\ & \swarrow^{1_X} & \downarrow \Delta & \searrow^{1_X} & \\ X & & X \times X & & X \\ & \xleftarrow{\pi_1} & \xrightarrow{\pi_2} & & \end{array} .$$

Remark: The diagonal morphisms in \mathbf{Cat} are diagonal functors.

Functor — Example

- ▶ Let Top_* be the category of *pointed topological spaces*, where
 - ▶ objects (X, x_0) are topological spaces with a distinguished *base point*.
 - ▶ a morphism $f : (X, x_0) \rightarrow (Y, y_0)$ is a continuous map $f : X \rightarrow Y$ which preserves the base point $f(x_0) = y_0$.
- ▶ If one has a path f and a path g , which begins where f ends, then their *concatenation*:

$$(g \cdot f)t := \begin{cases} f(2t) & 0 \leq t \leq 1/2 \\ g(2t - 1) & 1/2 < t \leq 1 \end{cases}$$

- ▶ A *homotopy* between the maps $f, g : X \rightarrow Y$ is a continuous map $\gamma : X \times [0, 1] \rightarrow Y$ such that:
 - ▶ $\forall x \in X : \gamma(x, 0) = fx$
 - ▶ $\forall x \in X : \gamma(x, 1) = gx$
- ▶ If there exists a homotopy γ between f and g we say that f and g are *homotopic*. This is an equivalence relation.
- ▶ The *fundamental groupoid* $\pi_1(X)$ of space X is the category whose objects are points of X . A morphism $x \rightarrow y$ is a homotopy class $[f]$ of paths from x to y . Composition is given by concatenation of paths $[g] \circ [f] = [g \cdot f]$.

Functor — Example

- ▶ A *loop in X based at x_0* is a continuous function $f : [0, 1] \rightarrow X$ such that $f(0) = f(1) = x_0$.
- ▶ The *fundamental group of X based at the point x_0* is the group $\pi_1(X, x_0)$ of homotopy classes of loops based at $x_0 \in X$.
The unit is given by the constant loop at x_0 , and the inverse is given by “walking the loop backwards” $f^{-1}(t) := f(1 - t)$.
- ▶ Let $f : (X, x_0) \rightarrow (Y, y_0)$ be a base point-preserving continuous function. We can map a loop at x_0 to a loop of y_0

$$[0, 1] \xrightarrow{l} X \xrightarrow{f} Y$$

- ▶ It induces a map between the equivalence classes, $\pi_1(X, x_0) \rightarrow \pi_1(Y, y_0)$. We denote this resulting map $\pi_1(f)$.
- ▶ The assignment given by $(X, x_0) \mapsto \pi_1(X, x_0)$ and $f \mapsto \pi_1(f)$ is a functor $\pi_1 : \mathbf{Top}_* \rightarrow \mathbf{Grp}$.
- ▶ $\pi_1(S^1) \cong (\mathbb{Z}, +)$ where $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

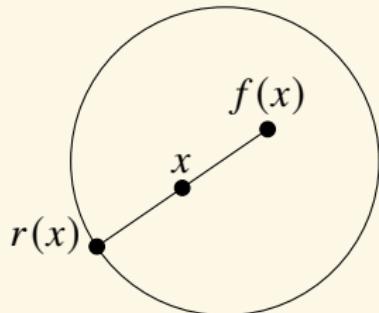
Theorem (Brouwer Fixpoint Theorem)

Any continuous endomorphism of a 2-dimensional disk D^2 has a fixpoint.

Proof.

Suppose $f : D^2 \rightarrow D^2$ has no fixpoint. Then there is a continuous function $r : D^2 \rightarrow S^1$ that carries a point $x \in D^2$ to the intersection of the ray from $f(x)$ to x with the boundary S^1 , and $r(x) = x$ when $x \in S^1$. Then the function r is a retraction for the inclusion $i : S^1 \hookrightarrow D^2$.

$$S^1 \xrightarrow{i} D^2 \xrightarrow{r} S^1$$



Pick any basepoint on the boundary S^1 and apply the functor π_1 to obtain a composable pair of group homomorphisms:

$$\pi_1(S^1) \xrightarrow{\pi_1(i)} \pi_1(D^2) \xrightarrow{\pi_1(r)} \pi_1(S^1)$$

By the functoriality axioms, we have

$$\pi_1(r) \cdot \pi_1(i) = \pi_1(ri) = \pi_1(1_{S^1}) = 1_{\pi_1(S^1)}$$

Therefore, $\pi_1(i)$ is monic and hence injective. However, $\pi_1(S^1) \cong (\mathbb{Z}, +)$, $\pi_1(D^2) \cong (\{0\}, +)$. There is no injection $\mathbb{Z} \rightarrowtail \{0\}$.

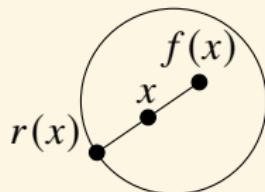
- ▶ How to understand Brouwer's proof?
- ▶ Let \mathbf{C} be a category. The objects are some type of sets (sphere S , ball B , etc.), and the morphisms are continuous maps.
- ▶ there is an object A (whose points are the arrows in B);
- ▶ a morphism $A \xrightarrow{h} B$ (assigning to each arrow its head);
- ▶ a morphism $A \xrightarrow{p} S$ (telling where each arrow points).
- ▶ **Assumption1:** $\forall T \in \mathbf{C} \forall a : T \rightarrow A \forall s : T \rightarrow S [h \circ a = i \circ s \rightarrow p \circ a = s]$

$$\begin{array}{ccc} T & \xrightarrow{a} & A \\ s \downarrow & \nearrow p & \downarrow h \\ S & \xrightarrow{i} & B \end{array}$$

Remark: if an arrow's head is on S , then its head is the point it points.

- ▶ Lemma: $\forall \gamma : B \rightarrow A [h \circ \gamma \circ i = i \rightarrow p \circ \gamma \circ i = 1_S]$
Proof: Take $T = S$, $s = 1_S$, and $a = \gamma \circ i$.

- ▶ **Assumption2:** For any $T \in \mathbf{C}$, and $T \xrightarrow[g]{f} B$, then either
 $\exists t : 1 \rightarrow T [f \circ t = g \circ t]$, or $\exists \gamma : T \rightarrow A [h \circ \gamma = g]$. “tail \neq head”
- ▶ **Theorem:** Suppose $B \xrightarrow[g]{f} B$ and $g \circ i = i$, then either
 $\exists b : 1 \rightarrow B [f \circ b = g \circ b]$, or there is a retraction for $S \xrightarrow{i} B$.



Functor — Example

Define the category of *pointed Euclidean spaces* \mathbf{Euc}_* as follows.

- As objects, we take (\mathbb{R}^n, x) with a distinguished point $x \in \mathbb{R}^n$.
- As morphisms $f : (\mathbb{R}^n, x) \rightarrow (\mathbb{R}^m, y)$ we take smooth (i.e. differentiable infinitely many times) functions $\mathbb{R}^n \rightarrow \mathbb{R}^m$ such that $f(x) = y$.

The derivative is a functor $D : \mathbf{Euc}_* \rightarrow \mathbf{Vect}$ defined in the following way.

- On objects, it maps (\mathbb{R}^n, x) to \mathbb{R}^n (now seen as a vector space).
- On morphisms, it maps $f : (\mathbb{R}^n, x) \rightarrow (\mathbb{R}^m, y)$ to the derivative $Df|_x$.

The derivative is functorial because:

- The derivative of the identity map $(\mathbb{R}^n, x) \rightarrow (\mathbb{R}^n, x)$ is just the identity of \mathbb{R}^n (the identity matrix).
- Consider composable maps

$$(\mathbb{R}^n, x) \xrightarrow{f} (\mathbb{R}^m, y) \xrightarrow{g} (\mathbb{R}^p, z)$$

We have that, *by the chain rule*, $D(g \circ f)|_x = Dg|_y \circ Df|_x$, i.e.

$$\frac{\partial(g \circ f)^k}{\partial x^i} = \sum_{j=1}^m \frac{\partial g^k}{\partial y^j} \frac{\partial f^j}{\partial x^i} \quad \text{for } i = 1, \dots, n \text{ and } k = 1, \dots, p.$$

Faddeev's Characterization of Shannon Entropy

- Shannon Entropy:

$$H(p) := - \sum_{i=1}^n p_i \log p_i$$

- n -simplex:

$$\Delta^n := \left\{ (p_0, \dots, p_n) \in \mathbb{R}^{n+1} : 0 \leq p_i \leq 1 \text{ and } \sum_{i=0}^n p_i = 1 \right\}$$

Theorem (Faddeev's Characterization of Shannon Entropy)

Let $\{F : \Delta^n \rightarrow \mathbb{R}\}_{n \geq 0}$ be a sequence of functions. The following are equivalent:

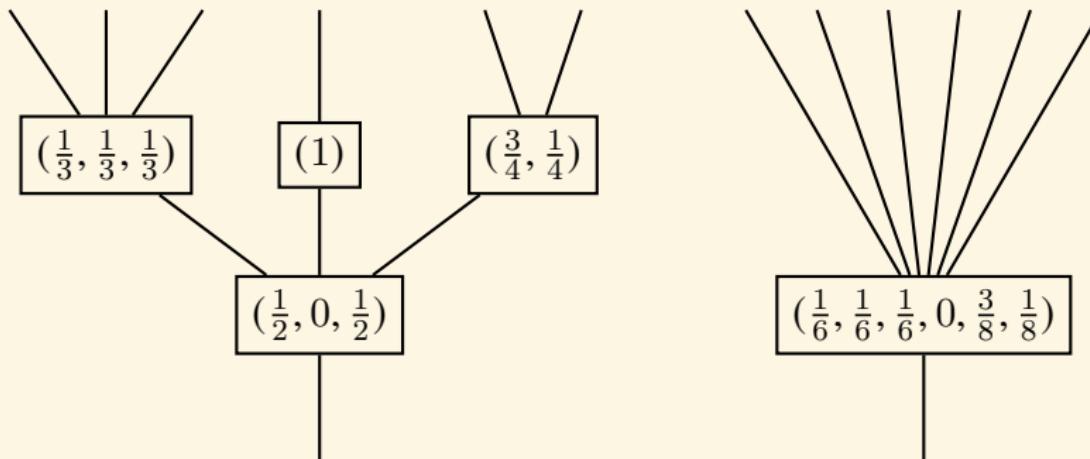
1. the functions F are continuous and satisfy

$$F(p \circ (q^0, \dots, q^n)) = F(p) + \sum_{i=0}^n p_i F(q^i)$$

where $n \geq 0$ and $p \in \Delta^n$ and $q^i \in \Delta^{k_i}$ with $k_0, \dots, k_n \geq 0$.

2. $F = cH$ for some $c \in \mathbb{R}$.

Composition of Probability Distributions and Chain Rule



$$H(p \circ (q^0, \dots, q^n)) = H(p) + \sum_{i=0}^n p_i H(q^i)$$

FinProb Category

- Given finite sets with probability distributions (X, p) and (Y, q) , a measure-preserving map from the first to the second is a function $f : (X, p) \rightarrow (Y, q)$ s.t.

$$q_y = \sum_{x \in f^{-1}(y)} p_x$$

- The composite of measure-preserving maps is measure-preserving.
- So, we get a category **FinProb** with
 - finite sets equipped with probability distributions as objects.
 - measure-preserving maps as morphisms.
- The entropy loss of a measure-preserving map $f : (X, p) \rightarrow (Y, q)$ defined by $\text{Loss}(f) := H(p) - H(q)$ is a functor from **FinProb** to some category $[0, \infty)$ with one object $*$, and nonnegative real numbers c as morphisms $c : * \rightarrow *$, and addition as composition.

$$\text{Loss}(g \circ f) = \text{Loss}(f) + \text{Loss}(g)$$

Ful and Faithful Functors

Definition

A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is:

- ▶ *faithful* iff for $A, B \in \mathbf{C}$ each $F : \mathbf{C}(A, B) \rightarrow \mathbf{D}(FA, FB)$ is injective;
- ▶ *full* iff for $A, B \in \mathbf{C}$ each $F : \mathbf{C}(A, B) \rightarrow \mathbf{D}(FA, FB)$ is surjective;
- ▶ an *embedding* iff F is full, faithful, and injective on objects;
- ▶ *essentially surjective* iff for every $B \in \mathbf{D}$ there is $A \in \mathbf{C}$ s.t. $F(A) \cong B$;
- ▶ an *isomorphism* iff there is a functor $G : \mathbf{D} \rightarrow \mathbf{C}$ such that $G \circ F = 1_{\mathbf{C}}$ and $F \circ G = 1_{\mathbf{D}}$.

Theorem (Functors preserve isomorphism)

If $A \cong B$ are isomorphic objects in \mathbf{C} and $F : \mathbf{C} \rightarrow \mathbf{D}$ is a functor then $FA \cong FB$.

Definition (Contravariant Functor)

A *contravariant functor* $F : \mathbf{C} \rightarrow \mathbf{D}$ between categories \mathbf{C} and \mathbf{D} is a functor $F : \mathbf{C}^{\text{op}} \rightarrow \mathbf{D}$.

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Categories

Cartesian Closed Categories

Functors

Natural Transformations

Equivalence of Categories

Product and Functor Category

Limits and Colimits

Construct New from Old

Topos

ETCS

Yoneda Lemma

Adjunctions

Categorical Logic

Kan Extensions

Monoidal Categories

Enriched Categories

End/Coend

Monads

Sheaves

CCAF

Rosen's (M, R) -System

Quantum Computing

Answers to the Exercises

References

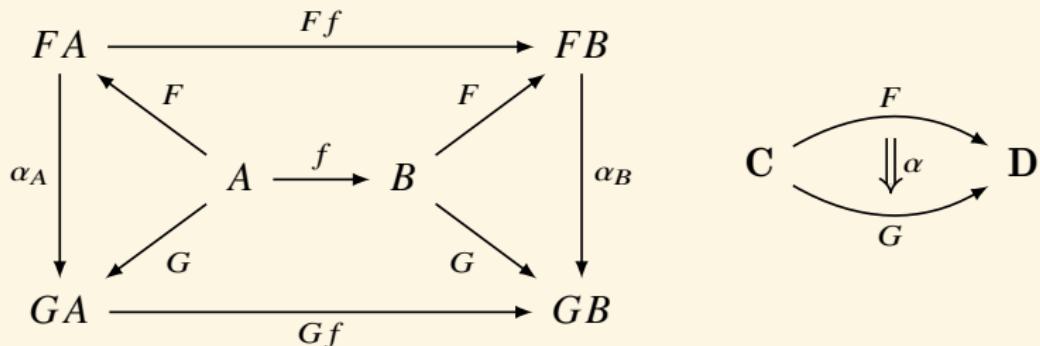
1436

Natural Transformation

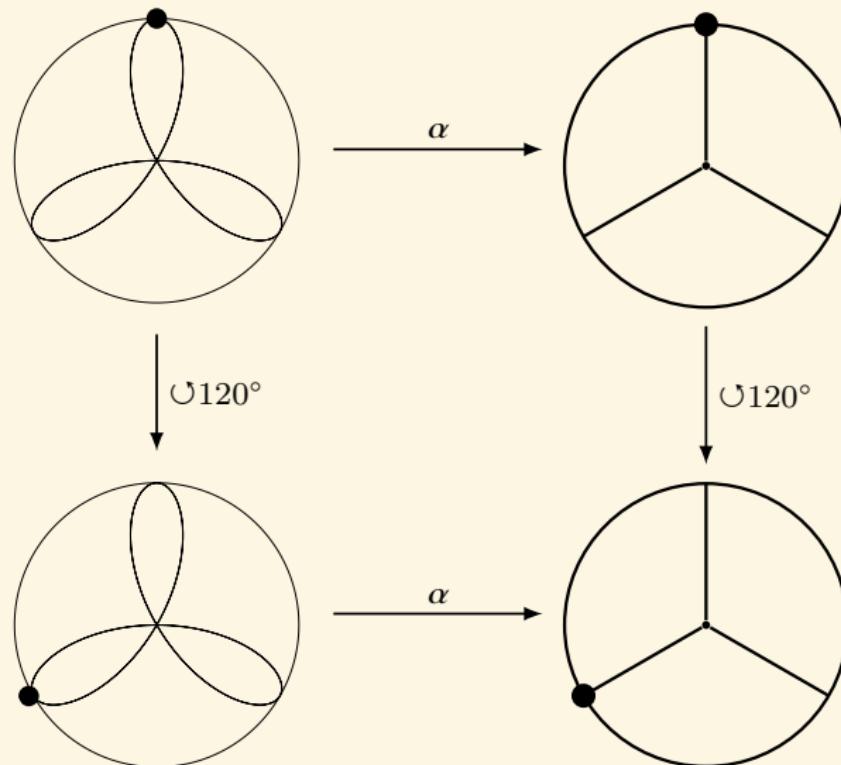
Definition (Natural Transformation)

Given categories and functors $F, G : \mathbf{C} \rightarrow \mathbf{D}$, a natural transformation $\alpha : F \rightarrow G$ is a family of \mathbf{D} -morphisms $\{\alpha_A : FA \rightarrow GA\}_{A \in \mathbf{C}}$, such that for all \mathbf{C} -morphisms $f : A \rightarrow B$, the diagram commutes:

$$\begin{array}{ccc} FA & \xrightarrow{Ff} & FB \\ \alpha_A \downarrow & & \downarrow \alpha_B \\ GA & \xrightarrow{Gf} & GB \end{array}$$



A natural transformation is a mapping between functors preserving specified actions, symmetries, or other structures



Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Equivalence of Categories

Definition (Natural Isomorphism)

A natural transformation $\alpha : F \rightarrow G$ is a natural isomorphism ($F \cong G$) iff each morphism $\alpha_A : FA \rightarrow GA$ is an isomorphism.

Definition (Equivalence of Categories)

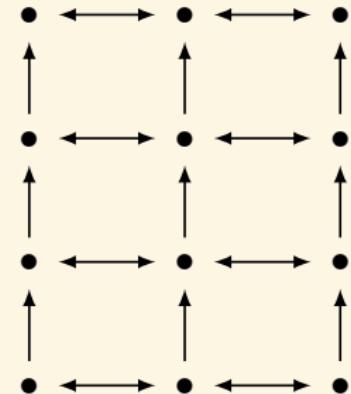
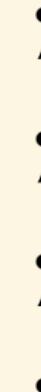
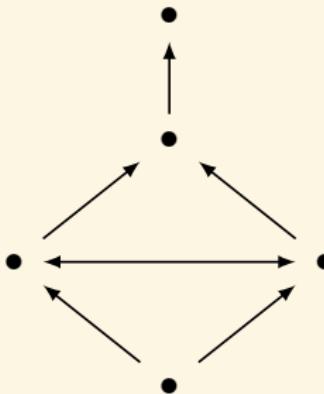
The categories **C** and **D** are equivalent ($\mathbf{C} \simeq \mathbf{D}$) iff there are functors

$\mathbf{C} \begin{array}{c} \xrightarrow{F} \\[-1ex] \xleftarrow{G} \end{array} \mathbf{D}$ and natural isomorphisms $G \circ F \cong 1_{\mathbf{C}}, F \circ G \cong 1_{\mathbf{D}}$.

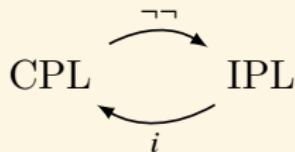
- ▶ The categories **C** and **D** are isomorphic ($\mathbf{C} \cong \mathbf{D}$) iff there are functors $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\[-1ex] \xleftarrow{G} \end{array} \mathbf{D}$ satisfying $G \circ F = 1_{\mathbf{C}}, F \circ G = 1_{\mathbf{D}}$.
- ▶ Equivalence of categories is a generalization of isomorphism. It can be seen as “isomorphism up to isomorphism”.

Examples

- The following categories are equivalent, but not isomorphic.



- CPL and IPL are not equivalent.



$$A \equiv_{\text{CPL}} i(\neg\neg(A)) \quad \text{but} \quad A \not\equiv_{\text{IPL}} \neg\neg(i(A))$$

Theorem

Under axiom of choice, a functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is an equivalence functor iff F is fully faithful and essentially surjective on objects.

Proof.

(\implies) Easy.

(\impliedby) Suppose $F : \mathbf{C} \rightarrow \mathbf{D}$ is fully faithful and essentially surjective on objects. For each $B \in \mathbf{D}$, choose $GB \in \mathbf{C}$ and an isomorphism $\alpha_B : F(GB) \rightarrow B$. For $f : B \rightarrow B'$, let $Gf : GB \rightarrow GB'$ be the unique morphism s.t.

$$F(Gf) = \alpha_{B'}^{-1} \circ f \circ \alpha_B$$

Such a unique morphism exists because F is fully faithful.

This defines a functor $G : \mathbf{D} \rightarrow \mathbf{C}$.

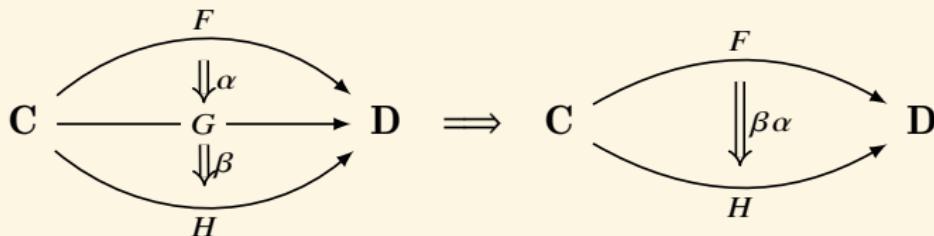
In addition, α is a natural isomorphism $\alpha : FG \rightarrow 1_{\mathbf{D}}$.

It remains to show that $GF \cong 1_{\mathbf{C}}$. For $A \in \mathbf{C}$, let $\beta_A : A \rightarrow G(FA)$ be the unique morphism s.t. $F\beta_A = \alpha_{FA}^{-1}$. Because F reflects isomorphisms, β_A is an isomorphism for every A . Naturality of β_A follows from functoriality of F and naturality of α .

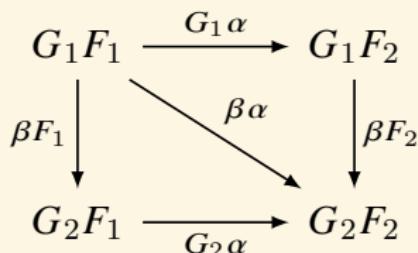
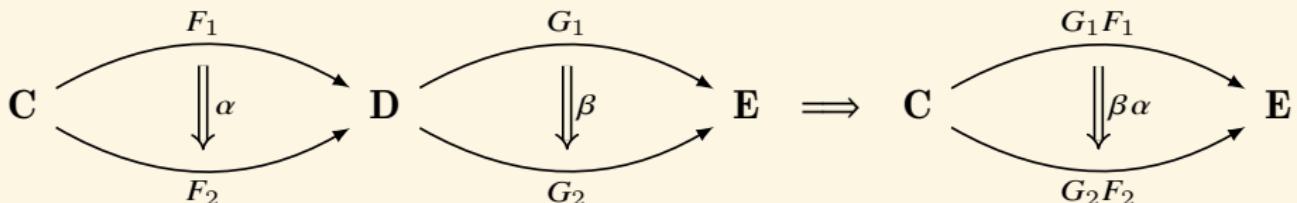
Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Vertical and Horizontal Composition



$$(\beta\alpha)_A := \beta_A \alpha_A$$



Whiskering

$$\begin{array}{ccccc} & & G_1 & & \\ & \text{C} & \xrightarrow{F} & \text{D} & \xrightleftharpoons[\beta]{\quad} & \text{E} \\ & & G_2 & & & \end{array} \qquad \begin{array}{ccccc} & & G_1 & & \\ & \text{C} & \xrightleftharpoons[\beta]{\quad} & \text{D} & \xrightarrow{F} & \text{E} \\ & & G_2 & & & \end{array}$$

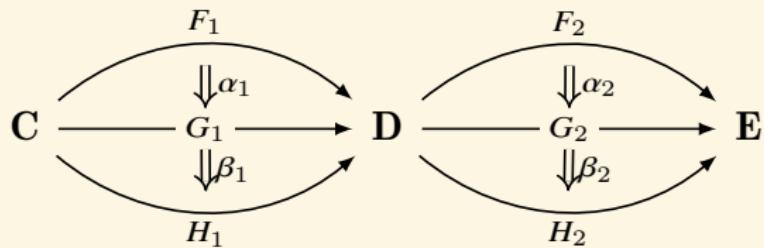
The prewhiskering of β by F , denoted $\beta F := \beta 1_F : G_1 F \rightarrow G_2 F$ (resp. the postwhiskering of β by F , denoted $F\beta := 1_F \beta : FG_1 \rightarrow FG_2$) is defined as follows.

$$\begin{array}{ccccc} & & G_1 F & & \\ & \text{C} & \xrightleftharpoons[\beta F]{\quad} & \text{D} & \xrightarrow{G_2 F} & \text{E} \\ & & G_2 F & & & \end{array} \qquad \begin{array}{ccccc} & & FG_1 & & \\ & \text{C} & \xrightleftharpoons[F\beta]{\quad} & \text{D} & \xrightarrow{FG_2} & \text{E} \\ & & FG_2 & & & \end{array}$$

$$(\beta F)_A := \beta_{FA}$$

$$(F\beta)_A := F\beta_A$$

Vertical and Horizontal Composition



$$(\beta_2 \beta_1)(\alpha_2 \alpha_1) = (\beta_2 \alpha_2)(\beta_1 \alpha_1)$$

Product Category

Definition (Product Category)

Given categories **C** and **D**, the product category **C × D** has

- ▶ objects (A, B) for $A \in \mathbf{C}$ and $B \in \mathbf{D}$.
- ▶ morphisms $(f, g) : (A, B) \rightarrow (A', B')$ for $f : A \rightarrow A'$ and $g : B \rightarrow B'$.
- ▶ identity $1_{(A,B)} := (1_A, 1_B)$.
- ▶ composition $(f', g') \circ (f, g) := (f' \circ f, g' \circ g)$.

$$(A, B) \xrightarrow{(f,g)} (A', B') \xrightarrow{(f',g')} (A'', B'')$$

$$(A, B) \xrightarrow{(f' \circ f, g' \circ g)} (A'', B'')$$

Product/Coproduct Category

Definition (Product Category $\prod_{i \in I} \mathbf{C}_i$)

$$\text{ob}\left(\prod_{i \in I} \mathbf{C}_i\right) = \prod_{i \in I} \text{ob}(\mathbf{C}_i)$$

$$\text{Hom}_{\prod_{i \in I} \mathbf{C}_i} \left((X_i)_{i \in I}, (Y_i)_{i \in I} \right) = \prod_{i \in I} \text{Hom}_{\mathbf{C}_i}(X_i, Y_i)$$

Definition (Coproduct Category $\coprod_{i \in I} \mathbf{C}_i$)

$$\text{ob}\left(\coprod_{i \in I} \mathbf{C}_i\right) = \coprod_{i \in I} \text{ob}(\mathbf{C}_i)$$

$$\text{Hom}_{\coprod_{i \in I} \mathbf{C}_i}(X, Y) = \begin{cases} \text{Hom}_{\mathbf{C}_i}(X, Y) & \text{if } X, Y \in \text{ob}(\mathbf{C}_i) \\ \emptyset & \text{otherwise} \end{cases}$$

Functor Category

Definition (Functor Category)

Given categories \mathbf{C} and \mathbf{D} , the functor category $\mathbf{D}^{\mathbf{C}}$ has

- ▶ objects: functors $F : \mathbf{C} \rightarrow \mathbf{D}$
- ▶ morphisms: natural transformations $\alpha : F \rightarrow G$
- ▶ identity natural transformation $(1_F)_A := 1_{FA}$
given a functor $F : \mathbf{C} \rightarrow \mathbf{D}$, define $1_F : F \rightarrow F$ with
 $(1_F)_A := FA \xrightarrow{1_{FA}} FA$.
- ▶ composition of natural transformations $(\beta \circ \alpha)_A := \beta_A \circ \alpha_A$
given functors $F, G, H : \mathbf{C} \rightarrow \mathbf{D}$ and natural transformations
 $F \xrightarrow{\alpha} G \xrightarrow{\beta} H$, define $\beta \circ \alpha : F \rightarrow H$ with

$$(\beta \circ \alpha)_A := FA \xrightarrow{\alpha_A} GA \xrightarrow{\beta_A} HA$$

The Category of Small Categories **Cat**

- ▶ Assume there is an infinite sequence $U_0 \in U_1 \in U_2 \in \dots$ of bigger and bigger Grothendieck universes.
- ▶ \mathbf{Set}_n = category whose objects are the sets in U_n and with $\mathbf{Set}_n(A, B) = B^A$ = the functions from A to B .
- ▶ A category **C** is locally small iff $\forall A B \in \mathbf{C} : \mathbf{C}(A, B) \in \mathbf{Set}_0$.
- ▶ A category **C** is small iff it is both locally small and $\text{ob}(\mathbf{C}) \in \mathbf{Set}_0$.

Definition (The Category of Small Categories **Cat**)

The category of small categories **Cat** has

- ▶ objects: small categories.
- ▶ morphisms: functors $F : \mathbf{C} \rightarrow \mathbf{D}$.
- ▶ identity and composition as for functors.

Cat is large.

Cat is CCC

1_{\bullet}
↓

- ▶ **Cat** has a terminal object $1 := \bullet$.
- ▶ **Cat** has products.
- ▶ There is a functor $\varepsilon : \mathbf{D}^C \times \mathbf{C} \rightarrow \mathbf{D}$ that makes \mathbf{D}^C the exponential.
- ▶ **Cat** is cartesian closed.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

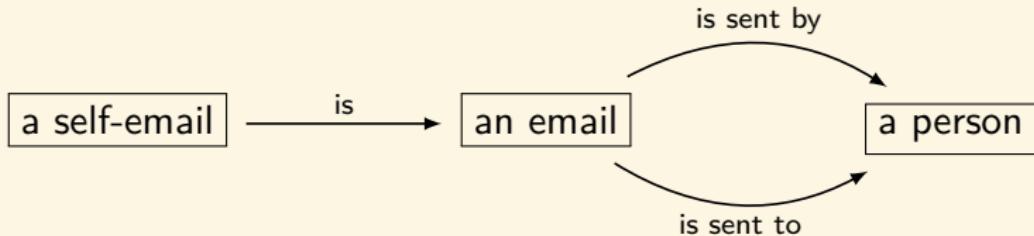
Equalizer

- ▶ A *fork* in a category \mathbf{C} consists of $C \xrightarrow{h} A \rightrightarrows B$ s.t. $fh = gh$.
- ▶ Let \mathbf{C} be a category and take $A \rightrightarrows B$. An *equalizer* of f and g is an object E with a morphism $E \xrightarrow{e} A$ s.t. $E \xrightarrow{e} A \rightrightarrows B$ is a fork, and for any fork $C \xrightarrow{h} A \rightrightarrows B$, there exists a unique morphism $C \xrightarrow{u} E$ s.t.

$$\begin{array}{ccccc} C & & & & \\ \downarrow u & \searrow h & & & \\ E & \xrightarrow{e} & A & \rightrightarrows & B \end{array}$$

Example: In \mathbf{Set} , $E := \{x \in A : f(x) = g(x)\}$.

Example — Equalizer



A self-email is an email which is sent by the same person it is sent to.

Coequalizer

- A *cofork* in a category \mathbf{C} consists of $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B \xrightarrow{h} C$ s.t. $hf = hg$.
- Let \mathbf{C} be a category and take $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B$. An *coequalizer* of f and g is an object Q with a morphism $B \xrightarrow{q} Q$ s.t. $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B \xrightarrow{q} Q$ is a cofork, and for any cofork $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B \xrightarrow{h} C$, there exists a unique morphism $Q \xrightarrow{u} C$ s.t.

$$\begin{array}{ccccc} & & & & \\ & A & \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} & B & \xrightarrow{q} Q \\ & & \searrow h & \downarrow u & \\ & & C & & \end{array}$$

Example: In \mathbf{Set} , let $y \sim y' := \exists x(f(x) = y \wedge g(x) = y')$. Then $Q := B/\sim$ is a coequalizer.

Theorem

If $C \xrightarrow{h} A \rightrightarrows B$ is an equalizer, h is monic.

Theorem

If $A \rightrightarrows B \xrightarrow{h} C$ is a coequalizer, h is epic.

Pullback

Let \mathbf{C} be a category. A *pullback* of

$$\begin{array}{ccc} & B & \\ & \downarrow g & \\ A & \xrightarrow{f} & C \end{array}$$

is an object P with

$P \xrightarrow{p_1} A$ and $P \xrightarrow{p_2} B$ s.t. $p_1 \downarrow$, $p_2 \downarrow$, and for any $q_1 \downarrow$, $q_2 \downarrow$ there

$$\begin{array}{ccc} P & \xrightarrow{p_2} & B \\ p_1 \downarrow & & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

$$\begin{array}{ccc} Q & \xrightarrow{q_2} & B \\ q_1 \downarrow & & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

is a unique morphism $Q \xrightarrow{u} P$ s.t.

$$\begin{array}{ccccc} Q & \xrightarrow{q_2} & P & \xrightarrow{p_2} & B \\ \dashv u \searrow & & p_1 \downarrow & & \downarrow g \\ & & A & \xrightarrow{f} & C \end{array}$$

Pullback

$$\begin{array}{ccc} P & \xrightarrow{p_2} & B \\ p_1 \downarrow & \lrcorner & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

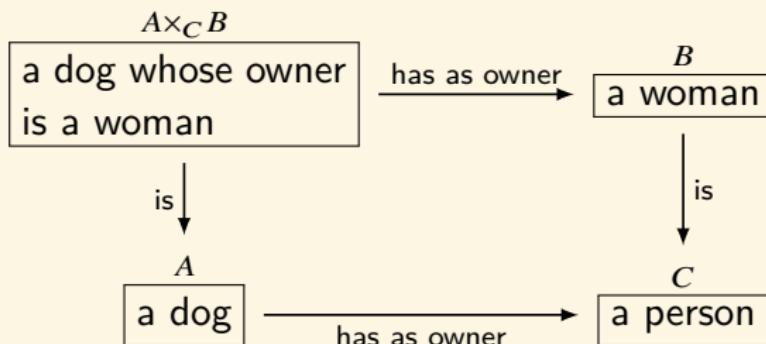
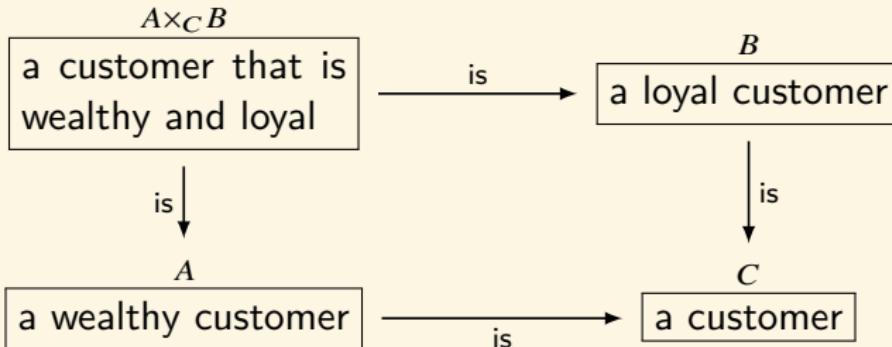
In **Set**, $P := A \times_C B := \{(a, b) \in A \times B : f(a) = g(b)\}$.

We also say that we pull back g along f and think of $f^*g : f^*B \rightarrow A$ as the inverse image of B along f . This terminology is explained by looking at the pullback of a subset inclusion $i : B \hookrightarrow C$.

$$\begin{array}{ccc} f^*B & \xrightarrow{p_2} & B & \quad & f^*B & \longrightarrow & B \\ f^*g \downarrow & \lrcorner & \downarrow g & & \downarrow & \lrcorner & \downarrow i \\ A & \xrightarrow{f} & C & \quad & A & \xrightarrow{f} & C \end{array}$$

In this case $\{(a, b) \in A \times B : fa = b\} \cong \{a \in A : fa \in B\} = f^*B$.

Example — Pullback



products & equalizers \implies pullbacks

Theorem

In a category with products and equalizers, given $A \xrightarrow{f} C \leftarrow B$, consider the diagram:

$$\begin{array}{ccc} E & \xrightarrow{e} & A \times B \\ & \searrow & \downarrow \pi_1 \\ & & A \xrightarrow{f} C \end{array}$$
$$A \times B \xrightarrow{\pi_2} B \quad g \downarrow$$

Then $e : E \rightarrow A \times B$ is an equalizer of $A \times B \rightrightarrows C$ iff

$$\begin{array}{ccc} E & \xrightarrow{\pi_2 \circ e} & B \\ \pi_1 \circ e \downarrow & \lrcorner & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

is a pullback.

- pullbacks & terminal objects \implies products

$$A \times B \cong A \times_1 B$$

$$\begin{array}{ccc} A \times B & \xrightarrow{\pi_2} & B \\ \pi_1 \downarrow & \lrcorner & \downarrow !_B \\ A & \xrightarrow{!_A} & 1 \end{array}$$

- pullbacks & products \implies equalizers

The equalizer $E \xleftarrow{e} A \xrightarrow[\underline{g}]{} B$ is constructed as the following pullback,

$$\begin{array}{ccc} E & \xrightarrow{h} & B \\ e \downarrow & \lrcorner & \downarrow \Delta \\ A & \xrightarrow{\langle f,g \rangle} & B \times B \end{array}$$

Theorem

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ p \downarrow & \lrcorner & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

If g is monic, so is p .

Theorem

$$\begin{array}{ccccc} F & \longrightarrow & E & \longrightarrow & D \\ \downarrow & & \downarrow & & \downarrow \\ A & \longrightarrow & B & \longrightarrow & C \end{array}$$

1. If the two squares are pullbacks, so is the outer rectangle. Thus,
$$A \times_B (B \times_C D) \cong A \times_C D$$
2. If the right square and the outer rectangle are pullbacks, so is the left square.

Pushout

$$\begin{array}{ccc} C & \xrightarrow{g} & B \\ f \downarrow & & \\ A & & \end{array}$$

Let \mathbf{C} be a category. A *pushout* of

$A \xrightarrow{i_1} P$ and $B \xrightarrow{i_2} P$ s.t. $f \downarrow$, and for any $f \downarrow$ there is

$$\begin{array}{ccc} C & \xrightarrow{g} & B \\ f \downarrow & & \downarrow i_2 \\ A & \xrightarrow{i_1} & P \end{array} \quad \begin{array}{ccc} C & \xrightarrow{g} & B \\ f \downarrow & & \downarrow j_2 \\ A & \xrightarrow{j_1} & Q \end{array}$$

a unique morphism $P \xrightarrow{u} Q$ s.t.

$$\begin{array}{ccccc} C & \xrightarrow{g} & B & & \\ f \downarrow & & \downarrow i_2 & & \\ A & \xrightarrow{i_1} & P & \xrightarrow{u} & Q \\ & & \nearrow r & \searrow j_2 & \\ & & & \nearrow u & \\ & & & j_1 & \end{array} .$$

Pushout

$$\begin{array}{ccc} C & \xrightarrow{g} & B \\ f \downarrow & \lrcorner & \downarrow i_2 \\ A & \xrightarrow{i_1} & A +_C B \end{array}$$

In **Set**, $A +_C B := (A + B)/\sim$, where \sim is the smallest equivalence relation on $A + B$ such that for all $x \in C : f(x) = g(x)$.

$$\begin{array}{ccc} A \cap B & \xrightarrow{\iota_2} & B \\ \iota_1 \downarrow & \lrcorner & \downarrow i_2 \\ A & \xrightarrow{i_1} & A \cup B \end{array}$$

$$A +_{A \cap B} B = A \cup B$$

Theorem

$$\begin{array}{ccc} C & \xrightarrow{g} & B \\ f \downarrow & \lrcorner & \downarrow j \\ A & \xrightarrow{i} & A +_C B \end{array}$$

If f is epic, so is j .

Theorem

$$\begin{array}{ccccc} C & \longrightarrow & B & \longrightarrow & A \\ \downarrow & & \downarrow & & \downarrow \\ D & \longrightarrow & E & \longrightarrow & F \end{array}$$

1. If the two squares are pushouts, so is the outer rectangle. Thus,
 $A +_B (B +_C D) \cong A +_C D$
2. If the left square and the outer rectangle are pushouts, so is the right square.

Kernel & Cokernel

- In a category \mathbf{C} with a zero object 0 , the *zero morphism* $0_{AB} : A \rightarrow B$ between $A, B \in \mathbf{C}$ is the unique morphism that factors through 0 :

$$0_{AB} : A \rightarrow 0 \rightarrow B$$

- In a category with zero morphism, the *kernel* $\ker(f)$ of a morphism $f : A \rightarrow B$ is the equalizer of f and the zero morphism 0_{AB} .

$$\ker(f) = \text{eq}(f, 0_{AB})$$

- In a category with zero morphism, the *cokernel* $\text{coker}(f)$ of a morphism $f : A \rightarrow B$ is the coequalizer of f and the zero morphism 0_{AB} .

$$\text{coker}(f) = \text{coeq}(f, 0_{AB})$$

The composition of a zero morphism with any morphism is a zero morphism.

Kernel & Cokernel

- In a category with an initial object 0 , the *kernel* $\ker(f)$ of a morphism $f : A \rightarrow B$ is the pullback:

$$\begin{array}{ccc} \ker(f) & \longrightarrow & 0 \\ \downarrow & \lrcorner & \downarrow \\ A & \xrightarrow{f} & B \end{array}$$

- In a category with a terminal object 1 , the *cokernel* $\text{coker}(f)$ of a morphism $f : A \rightarrow B$ is the pushout:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & \lrcorner & \downarrow \\ 1 & \longrightarrow & \text{coker}(f) \end{array}$$

Cone

- ▶ A *diagram* of a small category \mathbf{I} in category \mathbf{C} is a functor $D : \mathbf{I} \rightarrow \mathbf{C}$.
- ▶ A *cone* (C, c) over a diagram D consists of an object $C \in \mathbf{C}$ and a family of morphisms $(C \xrightarrow{c_i} D_i)_{i \in \mathbf{I}}$ such that for each $i \xrightarrow{f} j$ in \mathbf{I} , the following triangle commutes.

$$\begin{array}{ccc} & & D_i \\ C & \begin{array}{c} \nearrow c_i \\ \searrow c_j \end{array} & \downarrow Df \\ & & D_j \end{array}$$

A cone (C, c) over D can be taken as a natural transformation $c : \Delta C \rightarrow D$.

- ▶ A morphism of cones $\theta : (C, c) \rightarrow (C', c')$ is a morphism θ s.t.

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ & \searrow c_i & \downarrow c'_i \\ & & D_i \end{array}$$

Then we have a category $\mathbf{Cone}(D)$ of cones over D .

Cocone

- ▶ A *cocone* (C, c) over a diagram D consists of an object $C \in \mathbf{C}$ and a family of morphisms $(D_i \xrightarrow{c_i} C)_{i \in \mathbf{I}}$ such that for each $i \xrightarrow{f} j$ in \mathbf{I} , the following triangle commutes.

$$\begin{array}{ccc} D_i & & C \\ Df \downarrow & \searrow c_i & \\ D_j & \nearrow c_j & \end{array}$$

A cocone (C, c) over D can be taken as a natural transformation $c : D \rightarrow \Delta C$.

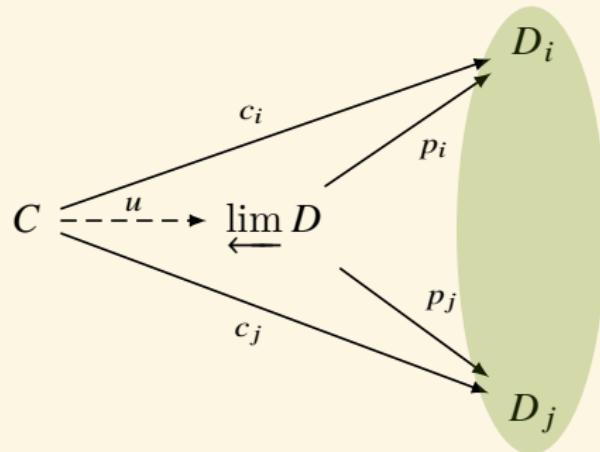
- ▶ A morphism of cocones $\theta : (C, c) \rightarrow (C', c')$ is a morphism θ s.t.

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ & \swarrow c_i & \uparrow c'_i \\ & D_i & \end{array}$$

Then we have a category **Cocone**(D) of cones over D .

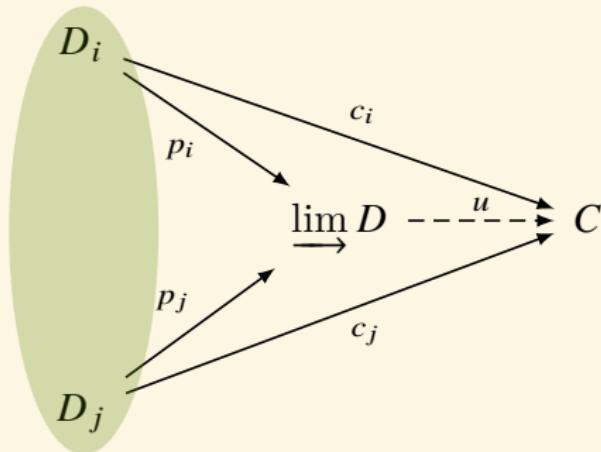
Limit

- A *limit* $\left(\varprojlim D, p\right)$ for a diagram $D : \mathbf{I} \rightarrow \mathbf{C}$ is a terminal object in $\mathbf{Cone}(D)$. In other word, for any cone (C, c) over D , there is a unique morphism $C \xrightarrow{u} \varprojlim D$ s.t. $c_i = p_i \circ u$ for all $i \in \mathbf{I}$.



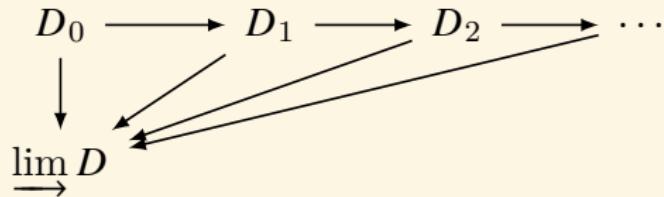
Colimit

- A *colimit* $\left(\varinjlim D, p\right)$ for a diagram $D : \mathbf{I} \rightarrow \mathbf{C}$ is an initial object in $\mathbf{Cocone}(D)$. In other word, for any cocone (C, c) over D , there is a unique morphism $\varinjlim D \xrightarrow{u} C$ s.t. $c_i = u \circ p_i$ for all $i \in \mathbf{I}$.

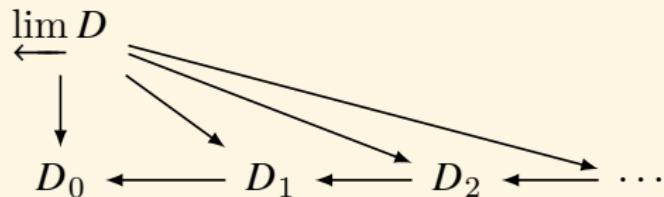


Direct/Inverse Limit

- Direct Limit

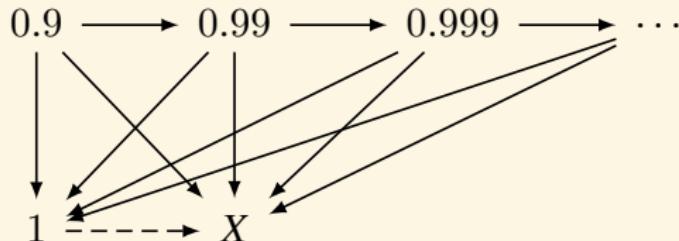


- Inverse Limit

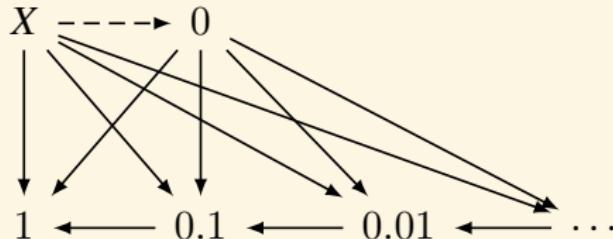


Direct/Inverse Limit — Example

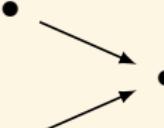
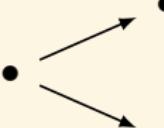
- Direct Limit



- Inverse Limit

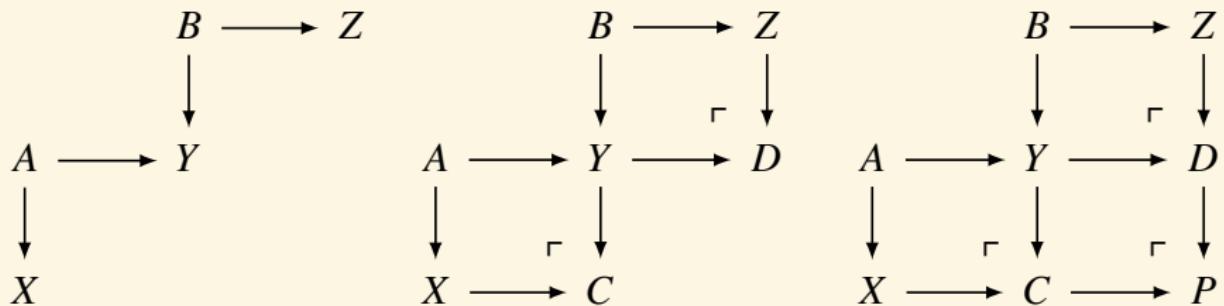


Examples

Limit $\lim_{\leftarrow} D$	I	Colimit $\lim_{\rightarrow} D$
terminal object	\emptyset	initial object
binary product		binary coproduct
equalizor		coequalizor
inverse limit		
		direct limit
pullback		
		pushout

Exercise

Suppose we want to take the colimit of the diagram.



We know how to take pushouts. The object P , together with all the morphisms from the original diagram to P is the colimit of the original diagram.

products & equalizers \implies limits

Let $D : \mathbf{I} \rightarrow \mathbf{C}$. Let E be the equalizer of f and g such that

$f_\alpha := \pi_\alpha \circ f = D\alpha \circ \pi_i$ and $g_\alpha := \pi_\alpha \circ g = \pi_j$ for $\alpha : i \rightarrow j \in \text{mor } \mathbf{I}$.

$$\begin{array}{ccccc}
 C & & & & \\
 \downarrow u & \searrow c & & & \\
 E & \xrightarrow{e} & \prod_{i \in \text{ob } \mathbf{I}} D_i & \xrightarrow{\quad f \quad} & \prod_{\alpha: i \rightarrow j \in \text{mor } \mathbf{I}} D_j \\
 & & \downarrow \pi_i & \swarrow \pi_j & \downarrow \pi_\alpha \\
 & & D_i & \xrightarrow{\quad D\alpha \quad} & D_j
 \end{array}$$

but generally $D\alpha \circ \pi_i \neq \pi_j$

Take any $c : C \rightarrow \prod_{i \in \text{ob } \mathbf{I}} D_i$. For $\alpha : i \rightarrow j$ in \mathbf{I} , we have

$$D\alpha \circ \pi_i \circ c = \pi_\alpha \circ f \circ c \quad \text{and} \quad \pi_j \circ c = \pi_\alpha \circ g \circ c$$

So (C, c_i) with $c_i := \pi_i \circ c$ is a cone of D iff $f \circ c = g \circ c$.

It follows that (E, e_i) with $e_i := \pi_i \circ e$ is a cone of D .

For any $c : C \rightarrow \prod_{i \in \text{ob } \mathbf{I}} D_i$, there is a unique $u : C \rightarrow E$ s.t. $c = e \circ u$.

Then $u : C \rightarrow E$ is also the required factorization of the cone (C, c_i) through (E, e_i) s.t. $c_i = e_i \circ u$. Therefore $E = \varprojlim D$.

coproducts & coequalizers \implies colimits

$$\varinjlim D = \text{coeq} \left(\coprod_{\alpha \in \text{mor } I} D_{\text{dom}(\alpha)} \xrightarrow{\begin{matrix} f \\ g \end{matrix}} \coprod_{i \in \text{ob } I} D_i \right)$$

where the morphisms are determined by their components as follows: f maps the component D_i to D_j via $\alpha : i \rightarrow j$, and g maps D_i to D_i by the identity morphism.

$$\begin{array}{ccc} \coprod_{\alpha \in \text{mor } I} D_{\text{dom}(\alpha)} & \xrightarrow{\begin{matrix} f \\ g \end{matrix}} & \coprod_{i \in \text{ob } I} D_i \\ \uparrow \iota_\alpha & \nearrow \iota_{\text{dom}(\alpha)} & \uparrow \iota_{\text{cod}(\alpha)} \\ D_{\text{dom}(\alpha)} & \xrightarrow{D_\alpha} & D_{\text{cod}(\alpha)} \end{array}$$

Theorem

The following are equivalent for a category C:

- ▶ *C has all pullbacks and a terminal object.*
- ▶ *C has all equalizers and finite products.*
- ▶ *C has finite limits.*

Theorem

The following are equivalent for a category C:

- ▶ *C has all equalizers and small products.*
- ▶ *C has small limits.*

Theorem

A functor preserves finite (small) limits iff it preserves equalizers and finite (small) products.

Preserving/Reflecting/Creating Limits

- A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is said to *preserve limits of \mathbf{I}* iff, for all diagrams $D : \mathbf{I} \rightarrow \mathbf{D}$ and all cones (C, c) over D ,
 (C, c) is a limit over $D \implies (FC, Fc)$ is a limit over $FD : \mathbf{I} \rightarrow \mathbf{D}$
- A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is said to *reflect limits of \mathbf{I}* iff, for all diagrams $D : \mathbf{I} \rightarrow \mathbf{D}$ and all cones (C, c) over D ,
 (C, c) is a limit over $D \iff (FC, Fc)$ is a limit over $FD : \mathbf{I} \rightarrow \mathbf{D}$
- A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is said to *create limits of \mathbf{I}* iff, for all diagrams $D : \mathbf{I} \rightarrow \mathbf{C}$, if (M, m) is a limit cone over $FD : \mathbf{I} \rightarrow \mathbf{D}$, there is a unique cone (C, c) over D s.t. $(FC, Fc) = (M, m)$, and moreover (C, c) is a limit.
- A category is *complete* iff it has all small limits.
- A functor is *continuous* iff it preserves all small limits.

Obviously, if F preserves limits then $F\left(\varprojlim D\right) \cong \varprojlim(FD)$.

The Fibonacci Sequence as a Functor

$$F_0 := 1$$

$$F_1 := 1$$

$$F_n := F_{n-1} + F_{n-2}$$

$$\gcd(F_m, F_n) = F_{\gcd(m, n)}$$

Fibonacci function $F : \mathbb{N} \rightarrow \mathbb{N}$ is a functor that preserves limits, which is to say it's a continuous functor from the finitely complete category \mathbb{N} to itself.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Construct New from Old

- ▶ opposite category
- ▶ subcategory
- ▶ product/coproduct category
- ▶ functor category
- ▶ slice/coslice category
- ▶ comma category
- ▶ arrow category
- ▶ quotient category

Free Category

Definition (Free Category)

The *free category* generated by a directed graph is the category that results from freely concatenating arrows together, whenever the target of one arrow is the source of the next.

Definition (Free Group)

There is a functor $F : \mathbf{Set} \rightarrow \mathbf{Grp}$ that sends a set X to the *free group* on X . Elements of FX are finite “words” whose letters are elements $x \in X$ or their formal inverses x^{-1} , modulo an equivalence relation that equates the words xx^{-1} and $x^{-1}x$ with the empty word. Multiplication is by concatenation, with the empty word serving as the identity.

Remark: Freedom is just another word for nothing left to lose.
— there are no relations between the generators of FX beyond the bare minimum required by the group axioms.

Quotient Category

Definition (Quotient Category)

- ▶ Given a category \mathbf{C} . A congruence relation \sim on \mathbf{C} is given by: for each pair of objects $A, B \in \mathbf{C}$, an equivalence relation \sim_{AB} on $\text{Hom}(A, B)$, such that
 - ▶ for $f, g : A \rightarrow B$ and $h : B \rightarrow C$, if $f \sim_{AB} g$ then $hf \sim_{AC} hg$.
 - ▶ for $f : A \rightarrow B$ and $g, h : B \rightarrow C$, if $g \sim_{BC} h$ then $gf \sim_{AC} hf$.
- ▶ Given a congruence relation \sim on \mathbf{C} , we can define the *quotient category* \mathbf{C}/\sim as the category whose objects $\text{ob}(\mathbf{C}/\sim) = \text{ob}(\mathbf{C})$ and whose morphisms are equivalence classes of morphisms in \mathbf{C} . That is,

$$\text{Hom}_{\mathbf{C}/\sim}(A, B) = \text{Hom}_{\mathbf{C}}(A, B)/\sim_{AB}$$

Slice/Coslice Category

Definition (Slice/Coslice Category)

- Given a category \mathbf{C} and $A \in \mathbf{C}$, the *slice category* \mathbf{C}/A is a category whose objects are pairs (B, f) where $B \in \mathbf{C}$ and $f : B \rightarrow A$. A morphism of \mathbf{C}/A from (B, f) to (B', f') is a morphism $g : B \rightarrow B'$ s.t.

$$\begin{array}{ccc} & B & \\ f \swarrow & & \downarrow g \\ A & & \\ \downarrow f' & & \downarrow \\ & B' & \end{array}$$

- Given a category \mathbf{C} and $A \in \mathbf{C}$, the *coslice category* A/\mathbf{C} is a category whose objects are pairs (B, f) where $B \in \mathbf{C}$ and $f : A \rightarrow B$. A morphism of A/\mathbf{C} from (B, f) to (B', f') is a morphism $g : B \rightarrow B'$ s.t.

$$\begin{array}{ccc} & B & \\ f \nearrow & & \downarrow g \\ A & & \\ \nearrow f' & & \downarrow \\ & B' & \end{array}$$

Examples

- Set/I can be regarded as the category of “ I -indexed families of sets”.

$$\boxed{\text{Set}/I \simeq \text{Set}^I}$$

$$\Phi : \text{Set}/I \rightarrow \text{Set}^I$$

$$\Psi : \text{Set}^I \rightarrow \text{Set}/I$$

$$\Phi : A \xrightarrow{f} I \mapsto (f^{-1}(i))_{i \in I}$$

$$\Psi : (A_i)_{i \in I} \mapsto \coprod_{i \in I} A_i \xrightarrow{\pi} I \quad (\text{the indexing projection})$$

where the coproduct is conveniently taken to be

$$\coprod_{i \in I} A_i := \bigcup_{i \in I} A_i \times \{i\}$$

- $1/\text{Set}$ (with $1 = \{\bullet\}$ a one-point set) is the category of pointed sets: objects are pairs (A, a) of sets with a distinguished element $a \in A$, and morphisms $f : (A, a) \rightarrow (B, b)$ must preserve this: $fa = b$.

Slice Category

- There is a forgetful functor $U_A : \mathbf{C}/A \rightarrow \mathbf{C}$ which maps (B, f) to B .
- Furthermore, for $h : A \rightarrow A'$ there is a functor “*composition by h*” $\mathbf{C}/h : \mathbf{C}/A \rightarrow \mathbf{C}/A'$ which maps (B, f) to (B, hf) and

$$\begin{array}{ccc} & \begin{matrix} & B \\ f & \swarrow \quad \downarrow g \\ A & \quad \quad \quad \end{matrix} & \text{to} & \begin{matrix} & B \\ hf & \swarrow \quad \downarrow g \\ A' & \quad \quad \quad \end{matrix} \\ \begin{matrix} & f \\ & \swarrow \\ A & \quad \quad \quad \end{matrix} & & & \begin{matrix} & hf \\ & \swarrow \\ A' & \quad \quad \quad \end{matrix} \\ & \begin{matrix} & f' \\ & \searrow \\ & B' \end{matrix} & & \begin{matrix} & hf' \\ & \searrow \\ & B \end{matrix} \end{array}$$

- For any small category \mathbf{C} , the construction of slice categories itself is a functor $\mathbf{C}/- : \mathbf{C} \rightarrow \mathbf{Cat}$.
- The functor $\mathbf{C}/-$ then factors through the forgetful functor $U_{\mathbf{C}} : \mathbf{Cat}/\mathbf{C} \rightarrow \mathbf{Cat}$ via a functor $\overline{\mathbf{C}} : \mathbf{C} \rightarrow \mathbf{Cat}/\mathbf{C}$.

$$\mathbf{C} \xrightarrow{\overline{\mathbf{C}}} \mathbf{Cat}/\mathbf{C}$$

$$\begin{matrix} & \nearrow U_{\mathbf{C}} \\ \mathbf{C}/- & \searrow \end{matrix}$$

\mathbf{Cat}

where $\overline{\mathbf{C}} : A \mapsto (\mathbf{C}/A, U_A)$ and $\overline{\mathbf{C}} : h \mapsto$

$$\mathbf{C}/A \xrightarrow{\mathbf{C}/h} \mathbf{C}/A'$$

$$\begin{matrix} & \nearrow U_A \\ \mathbf{C} & \searrow \end{matrix}$$

$U_{A'}$

Comma Category

Definition (Comma Category)

Given $\mathbf{A} \xrightarrow{F} \mathbf{C} \xleftarrow{G} \mathbf{B}$, we can form the *comma category* $F \downarrow G$ as follows:

- ▶ the objects are triples (A, B, f) with $A \in \mathbf{A}, B \in \mathbf{B}$ and $f : FA \rightarrow GB$.
- ▶ the morphisms from (A, B, f) to (A', B', f') are pairs (a, b) where $a : A \rightarrow A'$ in \mathbf{A} and $b : B \rightarrow B'$ in \mathbf{B} s.t.

$$\begin{array}{ccc} FA & \xrightarrow{f} & GB \\ Fa \downarrow & & \downarrow Gb \\ FA' & \xrightarrow{f'} & GB' \end{array}$$

- ▶ If $\mathbf{B} = \mathbf{1}$ and $G : \mathbf{1} \rightarrow \mathbf{C}$ picks out the object A and $\mathbf{A} = \mathbf{C}$ with $F = 1_{\mathbf{C}}$, then the comma category $F \downarrow G$ is the slice category \mathbf{C}/A .
- ▶ If $\mathbf{A} = \mathbf{1}$ and $F : \mathbf{1} \rightarrow \mathbf{C}$ picks out the object A and $\mathbf{B} = \mathbf{C}$ with $G = 1_{\mathbf{C}}$, then the comma category $F \downarrow G$ is the coslice category A/\mathbf{C} .

Arrow Category

Definition (Arrow Category)

Given a category \mathbf{C} , the *arrow category* \mathbf{C}^\rightarrow has as objects the morphisms of \mathbf{C} , and a morphism from $h : A \rightarrow B$ to $h' : A' \rightarrow B'$ is a pair $(f, g) : h \rightarrow h'$ where $f : A \rightarrow A'$, $g : B \rightarrow B'$ s.t.

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ f \downarrow & & \downarrow g \\ A' & \xrightarrow{h'} & B' \end{array}$$

If $\mathbf{A} = \mathbf{B} = \mathbf{C}$, then the comma category $1_{\mathbf{C}} \downarrow 1_{\mathbf{C}}$ is the arrow category \mathbf{C}^\rightarrow .

Universal Property

Definition (Universal Property)

Let $G : \mathbf{D} \rightarrow \mathbf{C}$ be a functor, and $A \in \mathbf{C}, B \in \mathbf{D}$.

- ▶ A universal morphism from A to G is a unique pair (B, u) where $u : A \rightarrow GB$ with the following property: for any $f : A \rightarrow GB'$, there exists a unique morphism $g : B \rightarrow B'$ s.t.

$$\begin{array}{ccc} A & \xrightarrow{u} & GB \\ & \searrow f & \downarrow Gg \\ & & GB' \end{array}$$

- ▶ A universal morphism from G to A is a unique pair (B, u) where $u : GB \rightarrow A$ with the following property: for any $f : GB' \rightarrow A$, there exists a unique morphism $g : B' \rightarrow B$ s.t.

$$\begin{array}{ccc} A & \xleftarrow{u} & GB \\ & \nearrow f & \uparrow Gg \\ & & GB' \end{array}$$

Comma Category

Definition (Comma Category)

Let $G : \mathbf{D} \rightarrow \mathbf{C}$ be a functor, and $A \in \mathbf{C}$.

- ▶ The *comma category* $A \downarrow G$ has objects all pairs (B, f) with $B \in \mathbf{D}$ and $f : A \rightarrow GB$. A morphism from (B, f) to (B', f') is given by $g : B \rightarrow B'$ s.t.

$$\begin{array}{ccc} A & \xrightarrow{f} & GB \\ & \searrow f' & \downarrow Gg \\ & & GB' \end{array}$$

- ▶ The *comma category* $G \downarrow A$ has objects all pairs (B, f) with $B \in \mathbf{D}$ and $f : GB \rightarrow A$. A morphism from (B, f) to (B', f') is given by $g : B' \rightarrow B$ s.t.

$$\begin{array}{ccc} A & \xleftarrow{f} & GB \\ & \nearrow f' & \uparrow Gg \\ & & GB' \end{array}$$

- ▶ A universal morphism from A to G is an initial object of $A \downarrow G$.
- ▶ A universal morphism from G to A is a terminal object of $G \downarrow A$.

Comma Category

Given $\mathbf{1} \xrightarrow{A} \mathbf{C} \xleftarrow{G} \mathbf{D}$, the $A \downarrow G$ -objects are (\bullet, B, f) with $B \in \mathbf{D}$ and $f : A \rightarrow GB$ in \mathbf{C} . The $A \downarrow G$ -morphisms from (\bullet, B, f) to (\bullet, B', f') are pairs $(1_\bullet, g)$ with $g : B \rightarrow B'$ in \mathbf{D} s.t.

$$\begin{array}{ccc} A & \xrightarrow{f} & GB \\ 1_A \downarrow & & \downarrow Gg \\ A & \xrightarrow{f'} & GB' \end{array}$$

- ▶ Let $G : \mathbf{D} \rightarrow \mathbf{C}$ be a functor and let A be an object of \mathbf{C} .
The following statements are equivalent:
 1. (B, u) is a universal morphism from A to G .
 2. (B, u) is an initial object of the comma category $A \downarrow G$.
 3. (B, u) is a representation of $\text{Hom}(A, G(-))$.
- ▶ The dual statements are also equivalent:
 1. (B, u) is a universal morphism from G to A .
 2. (B, u) is a terminal object of the comma category $G \downarrow A$.
 3. (B, u) is a representation of $\text{Hom}(G(-), A)$.
- ▶ A universal element can be viewed as a universal morphism from the one-point set $\{\bullet\}$ to the functor $G : \mathbf{D} \rightarrow \mathbf{Set}$.

Universal Property — Product

Let X and Y be objects of a category \mathbf{D} .

$$\begin{array}{ccc} X & \xleftarrow{\pi_1} & X \times Y & \xrightarrow{\pi_2} & Y \\ & \swarrow f & \uparrow h & \searrow g & \\ & Z & & & \end{array} \qquad \begin{array}{ccc} (X, Y) & \xleftarrow{(\pi_1, \pi_2)} & \Delta(X \times Y) \\ \downarrow (f, g) & & \uparrow \Delta(h) \\ \Delta(Z) & & \end{array}$$

Take \mathbf{C} to be the product category $\mathbf{D} \times \mathbf{D}$, and let Δ be the diagonal functor $\Delta : \mathbf{C} \rightarrow \mathbf{C}^I$.

Then $(X \times Y, (\pi_1, \pi_2))$ is a universal morphism from Δ to the object (X, Y) of $\mathbf{D} \times \mathbf{D}$.

One can generalize the above example to arbitrary limits and colimits.

- ▶ Given $D : I \rightarrow \mathbf{C}$ (thought of as an object in \mathbf{C}^I), the limit $\varprojlim D$ is a universal morphism from Δ to D .
- ▶ Dually, the colimit $\varinjlim D$ is a universal morphism from D to Δ .

Contents

Introduction

Term Logic

Propositional Logic

Predicate Logic

Modal Logic

Set Theory

Recursion Theory

Equational Logic

Homotopy Type Theory

Category Theory

Categories

Cartesian Closed Categories

Functors

Natural Transformations

Equivalence of Categories

Product and Functor Category

Limits and Colimits

Construct New from Old

Topos

ETCS

Yoneda Lemma

Adjunctions

Categorical Logic

Kan Extensions

Monoidal Categories

Enriched Categories

End/Coend

Monads

Sheaves

CCAF

Rosen's (M, R) -System

Quantum Computing

Answers to the Exercises

References

1436

Topos

Definition (Subobject)

A *subobject* of an object $X \in \mathbf{C}$ is a monomorphism $m : M \rightarrowtail X$.

Definition (Subobject Classifier)

Let \mathbf{E} be a category with all finite limits. A *subobject classifier* in \mathbf{E} is a monomorphism $\top : 1 \rightarrowtail \Omega$ such that for every monomorphism $m : M \rightarrowtail X$, there is a unique $\varphi : X \rightarrow \Omega$ making the following diagram a pullback:

$$\begin{array}{ccc} M & \xrightarrow{!} & 1 \\ m \downarrow & \lrcorner & \downarrow \top \\ X & \dashrightarrow_{\varphi} & \Omega \end{array}$$

Definition (Topos)

A *topos* is a category which

1. is cartesian closed,
2. has all finite limits,
3. has a subobject classifier.

Topos — Examples

- ▶ \mathbf{Set} is a topos.
- ▶ If \mathbf{E} is a topos and $X \in \mathbf{E}$, then \mathbf{E}/X is a topos.
- ▶ The arrow category $\mathbf{Set}^{\rightarrow}$ is a topos.
- ▶ If \mathbf{E} is a topos, then $\mathbf{E} \times \mathbf{E}$ is a topos.
- ▶ For any small category \mathbf{C} , the category of all presheaves $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$ is a topos.

Power Object

Definition (Power Object)

Let \mathbf{C} be a category with finite limits. A *power object* of an object $A \in \mathbf{C}$ is an object $P(A)$ with a monomorphism $\epsilon_A : A \rightarrow P(A)$ such that, for every object B and every monomorphism $R \rightarrow A \times B$ there is a unique morphism $\chi_R : R \rightarrow P(A)$ such that R is the pullback

$$\begin{array}{ccc} R & \xrightarrow{\quad} & \epsilon_A \\ \downarrow & \lrcorner & \downarrow \\ A \times B & \xrightarrow{1_A \times \chi_R} & A \times P(A) \end{array}$$

Theorem

Any topos \mathbf{E} has power objects.

Proof.

For $A \in \mathbf{E}$, let $P(A) := \Omega^A$, and let $\epsilon_A : A \times \Omega^A \rightarrow A \times \Omega^A$ be the subobject of $A \times \Omega^A$ whose character is $\varepsilon : A \times \Omega^A \rightarrow \Omega$.

$$\begin{array}{ccc} \epsilon_A & \xrightarrow{!} & 1 \\ \downarrow & \lrcorner & \downarrow \top \\ A \times \Omega^A & \xrightarrow{\varepsilon} & \Omega \end{array}$$

Take any monic $R \rightarrowtail A \times B$, and let $f : A \times B \rightarrow \Omega$ be its character. Then let $\lceil f \rceil : B \rightarrow \Omega^A$ be the unique morphism s.t. $\varepsilon \circ (1_A \times \lceil f \rceil) = f$.

$$\begin{array}{ccc} A \times B & \xrightarrow{1_A \times \lceil f \rceil} & A \times \Omega^A \\ & \searrow f & \downarrow \varepsilon \\ & \Omega & \end{array} \quad \begin{array}{ccccc} & & ! & & \\ R & \dashrightarrow & \epsilon_A & \xrightarrow{!} & 1 \\ \downarrow & \lrcorner & \downarrow & & \downarrow \top \\ A \times B & \xrightarrow{1_A \times \lceil f \rceil} & A \times \Omega^A & \xrightarrow{\varepsilon} & \Omega \\ & & \text{f} & & \end{array}$$

Logical Morphism

Definition (Logical Morphism)

A *logical morphism* between toposes is a functor which preserves the topos structure, that is: finite limits, exponentials and the subobject classifier.

- ▶ The inclusion $\mathbf{FinSet} \hookrightarrow \mathbf{Set}$ is logical.
- ▶ For any small category \mathbf{C} the inclusion $\mathbf{FinSet}^{\mathbf{C}^{\text{op}}} \hookrightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ is logical.
- ▶ A logical morphism preserves finite colimits.
- ▶ A logical morphism has a left adjoint iff it has a right adjoint.
- ▶ Let \mathbf{E} be a topos and $X \in \mathbf{E}$. Then \mathbf{E}/X is a topos, and the functor $X^* : \mathbf{E} \rightarrow \mathbf{E}/X$ is logical.
- ▶ For a morphism $f : X \rightarrow Y$ in a topos \mathbf{E} , the pullback $f^* : \mathbf{E}/Y \rightarrow \mathbf{E}/X$ is logical, and it has a left adjoint Σ_f and a right adjoint Π_f .

Geometric Morphism

Definition (Geometric Morphism)

A *geometric morphism* $f : \mathbf{E} \rightarrow \mathbf{F}$ between toposes is a pair of adjoint functors (f^*, f_*) : $\mathbf{F} \xrightleftharpoons[\substack{f_* \\ \perp}]{} \mathbf{E}$, such that the left adjoint f^* preserves finite limits.

We say that f_* is the *direct image*, and f^* is the *inverse image* of the geometric morphism.

Definition (Essential Geometric Morphism)

A geometric morphism (f^*, f_*) is *essential* if f^* has a left adjoint $f_! : \mathbf{E} \rightarrow \mathbf{F}$.

Theorem

A *logical morphism* is the direct image of a geometric morphism iff it is an equivalence.

\subset and \in

- Given subobjects m and m' , define $m \subset_X m'$ (or $M \subset_X M'$) as follows

$$m \subset_X m' := \exists f : m \rightarrow m' \in \mathbf{C}/X$$

```

    \begin{array}{ccc}
    M & \xrightarrow{f} & M' \\
    m \searrow & & \swarrow m' \\
    & X &
    \end{array}
  
```

- $m \sim m' := m \subset_X m' \ \& \ m' \subset_X m$
- $\text{Sub}(X) := \{[m] : m \text{ is monic with } \text{cod}(m) = X\}$
- $[m] \subset_X [m'] := m \subset_X m'$
- In terms of 'generalized elements'¹⁶ of an object X , $z : Z \rightarrow X$, one can define a *local membership* relation,

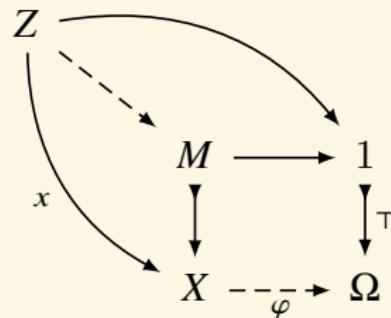
$$z \in_X M := \exists f : Z \rightarrow M [z = mf]$$

```

    \begin{array}{ccc}
    Z & \xrightarrow{f} & M \\
    & z \searrow & \downarrow m \\
    & & X
    \end{array}
  
```

¹⁶When the domain is the terminal object, then $x : 1 \rightarrow X$ is the 'global element' of X .

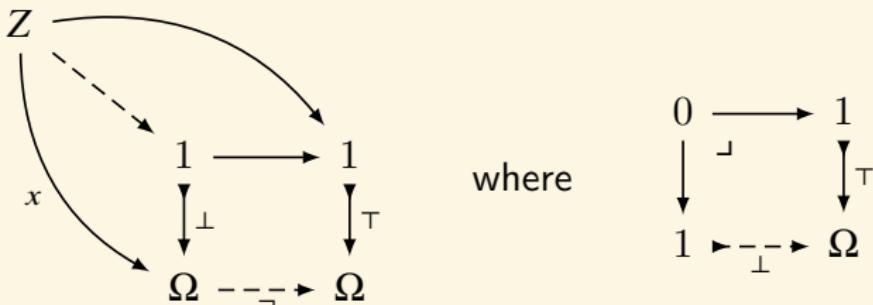
Predicate



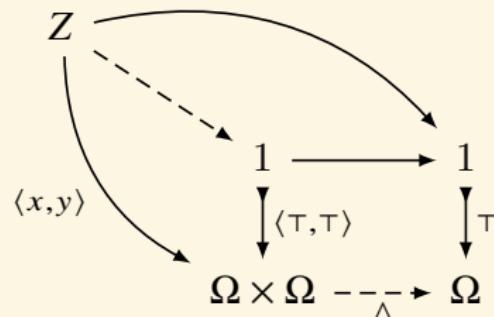
$$\varphi x = \top \iff x \in_X M$$

Remark: A predicate is a subobject of the universe, if we take a universe X as an object in a given topos.

¬ and \wedge

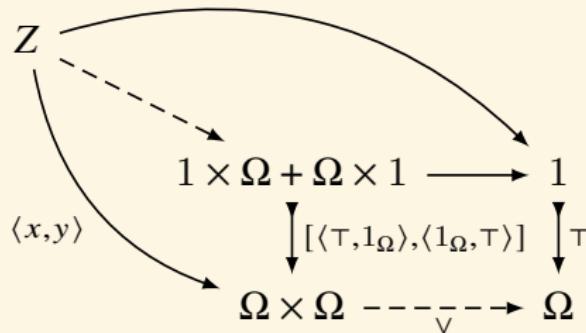


$$\neg x = \top \iff x = \perp$$

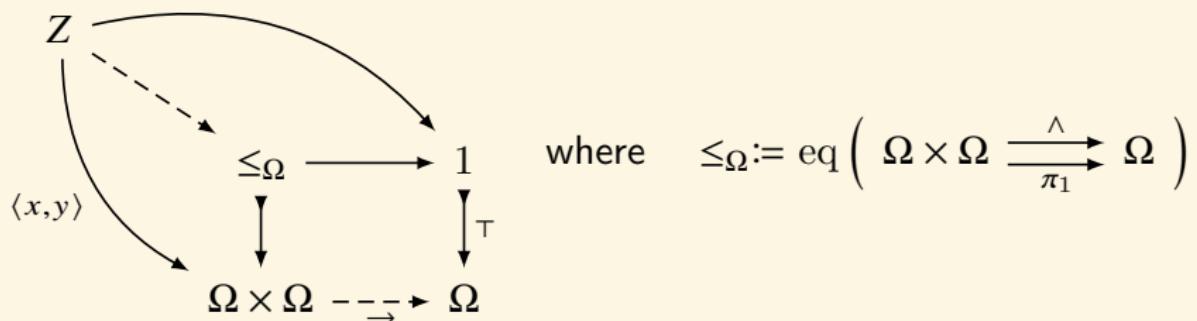


$$x \wedge y = \top \iff \langle x, y \rangle = \langle \top, \top \rangle$$

\vee and \rightarrow



$$x \vee y = \top \iff \langle x, y \rangle = [\langle \tau, 1_\Omega \rangle, \langle 1_\Omega, \tau \rangle]$$



where $\leq_\Omega := \text{eq} \left(\Omega \times \Omega \xrightarrow[\pi_1]{\wedge} \Omega \right)$

$$x \rightarrow y = \top \iff x \wedge y = x$$

forall

$$\begin{array}{ccccc} Y & \xrightarrow{\quad \lceil f \rceil \quad} & 1 & \longrightarrow & 1 \\ & \searrow & \downarrow \lceil \top_X \rceil & & \downarrow \top \\ & & \Omega^X & \xrightarrow[\forall_X]{} & \Omega \end{array}$$

where $\lceil f \rceil : Y \rightarrow \Omega^X$ is the currying of $Y \times X \xrightarrow{f} \Omega$, and $\lceil \top_X \rceil$ is the currying of the composite $1 \times X \xrightarrow{!} 1 \xrightarrow{\top} \Omega$.

Obviously, $\forall_X \circ \lceil f \rceil = \top_Y \iff \varepsilon \circ (\lceil f \rceil \times 1_X) = \top_{Y \times X}$

Theorem

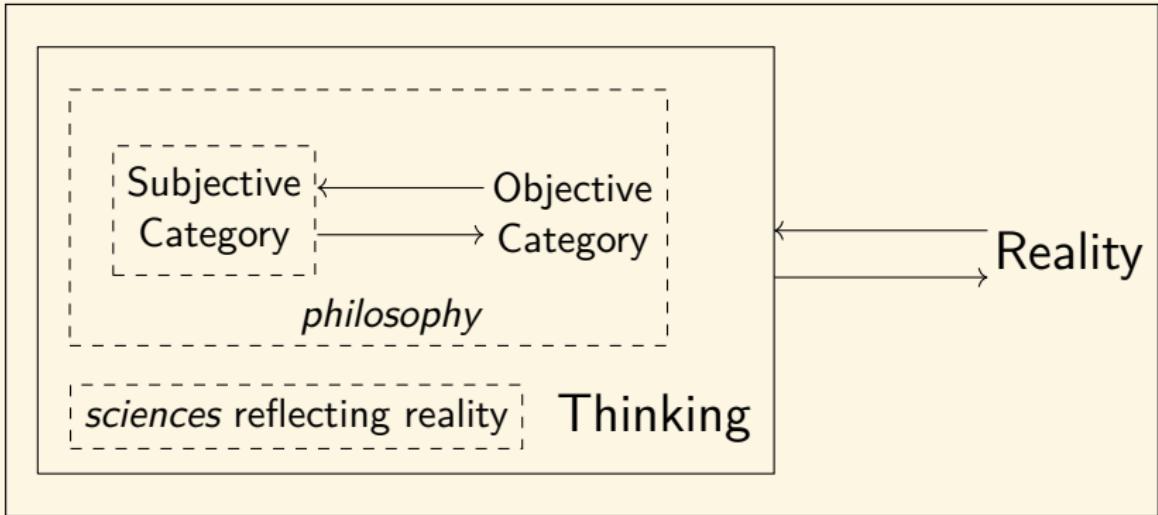
Let $f : Y \times X \rightarrow \Omega$ and $g : Y \rightarrow \Omega$ be morphisms in \mathbf{E} . Then

$$\frac{g \circ \pi_1 \subset_{Y \times X} f}{g \subset_Y \forall_X \circ \lceil f \rceil}$$

Logical Operator	Operation on $\text{Sub}(X)$
truth value	$\top, \perp : 1 \rightarrow \Omega$
monic logical operator	$\Omega \rightarrow \Omega$
binary logical operator	$\Omega \times \Omega \rightarrow \Omega$
proposition with no free variable	$1 \rightarrow \Omega$
proposition with free variable x	the characteristic of some $A \in \text{Sub}(X)$
proposition with free variables x, y	the characteristic of some $R \in \text{Sub}(X \times Y)$
$\exists x\varphi$ with free variable y	the characteristic of $\exists_\pi R \in \text{Sub}(Y)$, where $\exists_\pi \dashv \pi^*$, where $\pi : X \times Y \rightarrow Y$
$\forall x\varphi$ with free variable y	the characteristic of $\forall_\pi R \in \text{Sub}(Y)$, where $\pi^* \dashv \forall_\pi$, where $\pi : X \times Y \rightarrow Y$

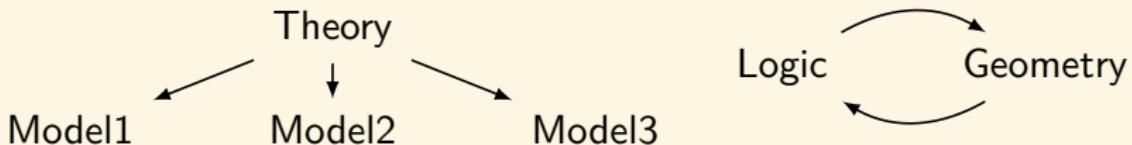
$$\text{Sub}(X) \cong \text{Hom}(X, \Omega)$$

Lawvere's Philosophy



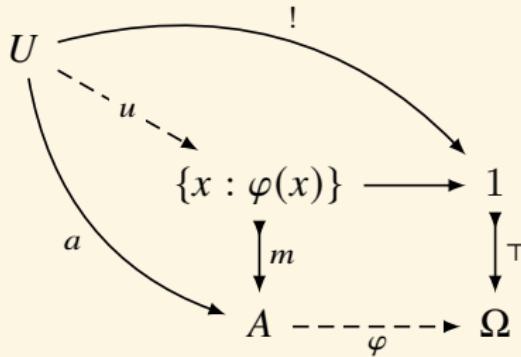
External vs Internal Logic

- ▶ Using ‘intuitionistic’ logic which is sound in any topos, we can construct categories and toposes and the notion of internal logic of a topos. This allows for developing the general theory of categories and toposes internally in any topos: every theorem of the general ‘external’ theory still holds true in every internal version of the theory.
- ▶ Hilbert’s axiomatic logic is always external.
- ▶ Lawvere’s topos theory and Voevodsky’s homotopy type theory qualify both as theories of logic and as theories of geometry.



- ▶ For example, in a topos one and the same element is interpreted either
 1. logically as a truth-value object, or
 2. geometrically as a particular sheaf.
- Similarly, in HoTT one and the same element is interpreted either
 1. logically as identity type, or
 2. geometrically as groupoid of homotopies.

Kripke-Joyal Semantics



Definition (Kripke-Joyal Forcing)

$$U \Vdash \varphi(a) \iff \exists u : m \circ u = a$$

Proposition

- If $f : V \rightarrow U$ and $U \Vdash \varphi(a)$, then $V \Vdash \varphi(a \circ f)$.
- If $f : V \twoheadrightarrow U$ is epic and $V \Vdash \varphi(a \circ f)$, then $U \Vdash \varphi(a)$.

Kripke-Joyal Semantics

Theorem

Let \mathbf{E} be an elementary topos and $a : U \rightarrow A$ a generalized element of $A \in \mathbf{E}$, and $\varphi(x), \psi(x)$ wff with a free variable x of sort A . Then

- ▶ $U \Vdash \varphi(a) \wedge \psi(a)$ iff $U \Vdash \varphi(a)$ and $U \Vdash \psi(a)$.
- ▶ $U \Vdash \varphi(a) \vee \psi(a)$ iff there are morphisms $f : V \rightarrow U$ and $g : W \rightarrow U$ s.t. $\begin{bmatrix} f \\ g \end{bmatrix} : V + W \rightarrow U$ is epic and $V \Vdash \varphi(a \circ f)$ and $W \Vdash \psi(a \circ g)$.
- ▶ $U \Vdash \varphi(a) \rightarrow \psi(a)$ iff for any $f : V \rightarrow U$, $V \Vdash \varphi(a \circ f)$ implies $V \Vdash \psi(a \circ f)$.
- ▶ $U \Vdash \neg\varphi(a)$ iff for any $f : V \rightarrow U$, $V \Vdash \varphi(a \circ f)$ implies $V \cong 0$.

If $\varphi(x, y)$ has an additional free variable y of sort B , then

- ▶ $U \Vdash \exists y \varphi(a, y)$ iff there exists an epic $f : V \rightarrow U$ and a generalized element $b : V \rightarrow B$ s.t. $V \Vdash \varphi(a \circ f, b)$.
- ▶ $U \Vdash \forall y \varphi(a, y)$ iff for every object V , every morphism $f : V \rightarrow U$, and every generalized element $b : V \rightarrow B$, $V \Vdash \varphi(a \circ f, b)$.

Epi-Mono Factorization

Theorem

In a topos, any morphism $f : X \rightarrow Y$ has an epi-mono factorization i.e. there exists an epi $e : X \rightarrow A$ and a mono $m : A \rightarrow Y$ s.t.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow e & \swarrow m \\ & A & \end{array}$$

And the epi-mono factorization is unique up to a unique isomorphism.

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & & \\ & \searrow e & \swarrow m & & \\ & A & \downarrow u & & \\ & \searrow e' & & \swarrow m' & \\ & A' & & & \end{array}$$

Given an epi-mono factorization, we call A the image of f , and denote it as $\text{Im } f$.

Theorem

If \mathbf{C} has finite limits and is in addition a locally small category, then it has a subobject classifier iff $\text{Sub} : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set} :: X \mapsto \{M \rightarrowtail X\}/\sim$ is representable, with representing object Ω . In this case there is a natural isomorphism

$$\text{Sub}_{\mathbf{C}}(X) \cong \text{Hom}_{\mathbf{C}}(X, \Omega)$$

$$\text{Sub}_{\mathbf{Set}}(X) \cong \mathbf{P}(X)$$

Theorem

In any topos \mathbf{E} , for any object $X \in \mathbf{E}$, $(\text{Sub}_{\mathbf{E}}(X), \subset)$ is a Heyting algebra: it is a poset that has finite limits, finite colimits, and is cartesian closed.

Definition (Boolean Topos)

A topos \mathbf{E} is Boolean iff for any $X \in \mathbf{E}$, $(\text{Sub}_{\mathbf{E}}(X), \subset)$ is a Boolean algebra.

True in any Topos	True only in a Boolean Topos
$A \rightarrow \neg\neg A$	$A \vee \neg A = \top$
$\neg A \wedge \neg B \leftrightarrow \neg(A \vee B)$	$\neg\neg A \rightarrow A$
$\neg A \vee \neg B \rightarrow \neg(A \wedge B)$	$\neg(A \vee B) \rightarrow \neg A \wedge \neg B$
$\forall x \neg A \leftrightarrow \neg \exists x A$	
$\exists x A \rightarrow \neg \forall x \neg A$	$\neg \forall x \neg A \rightarrow \exists x A$
$\forall x A \rightarrow \neg \exists x \neg A$	$\neg \exists x \neg A \rightarrow \forall x A$

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References 1436

Elementary Theory of the Category of Sets ETCS

Definition (Well-pointed Topos)

A topos is called *well-pointed* iff

1. extensionality: for $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B$, if $\forall x : 1 \rightarrow A [fx = gx]$ then $f = g$.
2. non-triviality: $0 \not\cong 1$.

Remark: Lawvere calls the objects of any topos '**variable sets**' and those of a well-pointed topos '**constant sets**', the limiting case of variation.

Definition (Choice)

For any epimorphism $f : A \rightarrow B$, there exists $g : B \rightarrow A$ s.t. $fg = 1_B$.
(every epimorphism has a section.)

Definition (ETCS — Lawvere)

ETCS is a well-pointed topos with NNO and Choice.

Axiom Scheme of Replacement

Definition (Replacement)

For each relation $R(x, Y)$ of morphisms x to objects Y expressible in ETCS:
For any object X , if for any $x : 1 \rightarrow X$ there exists an object S_x unique up to isomorphism with property $R(x, S_x)$, then there exists S and $f : S \rightarrow X$ such that for any $x : 1 \rightarrow X$ there is a pullback

$$\begin{array}{ccc} S_x & \longrightarrow & 1 \\ \downarrow & \lrcorner & \downarrow x \\ S & \xrightarrow{f} & X \end{array}$$

Theorem

ETCS + Replacement *is bi-interpretable with ZFC.*

ZFC vs ETCS

Global vs Local

	ZFC	ETCS
Are elements of a set also sets?	✓	✗
Given sets X and Y , can you ask whether $X \in Y$?	✓	✗
Does ' $X \cap Y$ ' make sense for arbitrary X and Y ?	✓	✗
Is everything isomorphism-invariant?	✗	✓
Sets	primitive	primitive
\in	primitive	derived
Functions	derived	primitive
Composition	derived	primitive

“The elementary theory of topoi is a basis for the study of continuously variable structures, as classical set theory is a basis for the study of constant structures.”

— F. W. Lawvere

“We are often interested not just in whether or not something is true, but in where it is true.”

— John Baez

“Set theory should not be based on membership, as in ZFC, but rather on isomorphism-invariant structure.”

— F. W. Lawvere

“There is no reason to distinguish between, say, $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots\}$ and $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots\}$ as definitions of ‘the natural numbers’.”

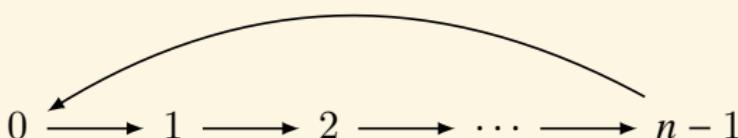
— J. Benacerraf

The Category $\text{Set}^\circlearrowleft$ of Endomaps of Sets

- ▶ An object of $\text{Set}^\circlearrowleft$ is any set $A \in \text{Set}$ equipped with an endomap.
- ▶ A morphism $f : A^{\circlearrowleft s} \rightarrow B^{\circlearrowleft t}$ is a map satisfying $f \circ s = t \circ f$.

$$\begin{array}{ccc} A & \xrightarrow{s} & A \\ f \downarrow & & \downarrow f \\ B & \xrightarrow{t} & B \end{array}$$

- ▶ Some questions can be asked about a particular object $A^{\circlearrowleft s}$ of $\text{Set}^\circlearrowleft$.
 - ▶ accessibility: Given $a \in A^{\circlearrowleft s}$, does $\exists b : s(b) = a$?
 - ▶ convergence to equilibrium: Given $a \in A^{\circlearrowleft s}$, does $\exists n : s^{n+1}(a) = s^n(a)$?
- ▶ Example: let C_n be



then $C_n \rightarrow B^{\circlearrowleft t}$ corresponds to elements in $B^{\circlearrowleft t}$ having period n .

Dynamical Systems

- A discrete dynamical system is a set X with an ‘evolution function’ $X \xrightarrow{f}$, which is the same thing as a functor $f : \mathbb{N} \rightarrow \mathbf{Set}$, where \mathbb{N} is the monoid of natural numbers under addition.

- $f(\bullet) = X$
 n times
- $f(n) = \overbrace{f \circ \cdots \circ f}^{n \text{ times}}$
- $f(0) = 1_X$

- The Category $\mathbf{Set}^{\mathbb{N}}$ can be seen as the category of dynamical systems $\mathbf{Set}^{\mathbb{N}}$.
- A continuous dynamical system (sometimes called a flow) is a topological space X and a continuous function $f : \mathbb{R}^{\geq 0} \times X \rightarrow X$ s.t.

$$f^0 = 1_X \text{ and } f^{t_2+t_1} = f^{t_2} \circ f^{t_1}$$

- A continuous dynamical system can be modeled categorically as a functor $f : \mathbb{R}^{\geq 0} \rightarrow \mathbf{Top}$.

Natural Numbers Object (NNO) — Lawvere's Definition

Definition (NNO — Lawvere)

A *natural numbers object* is an object N with morphisms $0 : 1 \rightarrow N$ and $s : N \rightarrow N$ such that: given morphisms $x : 1 \rightarrow X$ and $t : X \rightarrow X$, there is a unique morphism $f : N \rightarrow X$ making the following diagram commute:

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & N & \xrightarrow{s} & N \\ & \searrow x & \downarrow f & & \downarrow f \\ & & X & \xrightarrow{t} & X \end{array}$$

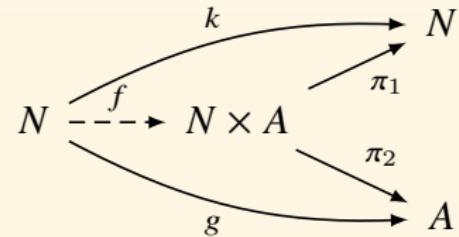
The function f is said to be constructed by *primitive recursion*.

Remark: Two cultures:

1. The natural numbers exist and we can define a function using recursion?
2. The natural numbers are defined as that object with which we can do recursion?

Recursion Lemma

$$\begin{array}{ccccc}
 1 & \xrightarrow{0} & N & \xrightarrow{s} & N \\
 & \searrow x & \downarrow f & \downarrow f & \\
 & X & \xrightarrow[t]{} & X &
 \end{array}
 \quad \frac{1 \xrightarrow{x} X \text{ in } \mathbf{Set}}{N \xrightarrow[s]{f} X \xrightarrow[t]{} \text{ in } \mathbf{Set}^\circ}$$



Theorem (Recursion Lemma)

Given $h : N \times A \rightarrow A$ and $1 \xrightarrow{a} A$, there exists a unique $N \xrightarrow{g} A$ s.t.

$$g(0) = a$$

$$g(n + 1) = h(n, g(n))$$

Proof.

Let $X := N \times A$, $t(n, y) := \langle n + 1, h(n, y) \rangle$, $x := \langle 0, a \rangle$. Then $\exists! f : N \rightarrow X$:

$$f(0) = x = \langle 0, a \rangle$$

$$f(n + 1) = t \circ f(n)$$

Let $k := \pi_1 \circ f$ and $g := \pi_2 \circ f$. Then $f(0) = \langle k(0), g(0) \rangle = \langle 0, a \rangle$ and $f(n + 1) = \langle k(n + 1), g(n + 1) \rangle = t \circ \langle k(n), g(n) \rangle = \langle k(n) + 1, h(k(n), g(n)) \rangle$. Obviously, $k = 1_N$.

NNO — Initial Object of Peano Category

Peano Category

Let \mathbf{C} be a category with terminal object 1 , and define the Peano category \mathbf{P} as follows:

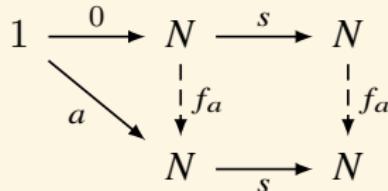
- ▶ the objects $\text{ob}(\mathbf{P})$ are triples (A, a, s) where $A \in \text{ob}(\mathbf{C})$, and $a : 1 \rightarrow A$ and $s : A \rightarrow A$ are \mathbf{C} -morphisms.
- ▶ a morphism $f : (A, a, s) \rightarrow (B, b, t)$ is a \mathbf{C} -morphism $f : A \rightarrow B$ s.t.
 1. $f \circ a = b$
 2. $f \circ s = t \circ f$

$$\begin{array}{ccccc} 1 & \xrightarrow{a} & A & \xrightarrow{s} & A \\ & \searrow b & \downarrow f & & \downarrow f \\ & & B & \xrightarrow{t} & B \end{array}$$

The *Natural Numbers Object* NNO is an initial object of \mathbf{P} .

NNO — Example

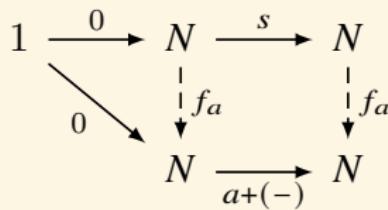
► Addition



$$f_a(0) = a$$

$$f_a(s(n)) = s(f_a(n))$$

► Multiplication



$$f_a(0) = 0$$

$$f_a(s(n)) = a + f_a(n)$$

NNO — Example

► Iteration

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & N & \xrightarrow{s} & N \\ & \searrow \lceil 1_X \rceil & \downarrow f & \downarrow f & \\ X^X & \xrightarrow{t^X} & X^X & & \end{array} \quad \Rightarrow \quad \begin{array}{ccccc} 1 \times X & \xrightarrow{0 \times 1_X} & N \times X & \xrightarrow{s \times 1_X} & N \times X \\ \cong \downarrow & & \downarrow \hat{f} & & \downarrow \hat{f} \\ X & \xrightarrow{1_X} & X & \xrightarrow{t} & X \end{array}$$

where $\lceil 1_X \rceil$ is the currying of $X \xrightarrow{1_X} X$.

$$\left. \begin{array}{l} \hat{f}(0, x) = x \\ \hat{f}(sn, x) = t(\hat{f}(n, x)) \end{array} \right\} \implies \hat{f}(n, x) = t^n(x)$$

NNO — Dedekind's Definition

Definition (NNO — Dedekind)

In a topos, $1 \xrightarrow{0} N \xrightarrow{s} N$ is a NNO iff

1. if $1 \xrightarrow{x} N$, then $sx \neq 0$.
2. s is monic.
3. if $M \xrightarrow{m} N$ is a subobject of N such that
 - there is $1 \xrightarrow{z} M$ such that $mz = 0$ and
 - there is $M \xrightarrow{r} M$ such that $mr = sm$

then $M \xrightarrow{m} N$.

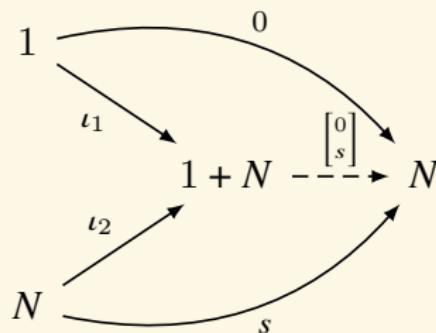
$$\begin{array}{ccccc} 1 & \xrightarrow{z} & M & \xrightarrow{r} & M \\ & \searrow 0 & \downarrow m & & \downarrow m \\ & & N & \xrightarrow{s} & N \end{array}$$

NNO — Freyd's Definition

Definition (NNO — Freyd)

In a topos, $1 \xrightarrow{0} N \xrightarrow{s} N$ is a NNO iff

1. the morphism $\begin{bmatrix} 0 \\ s \end{bmatrix} : 1 + N \rightarrow N$ is an isomorphism.



2. $N \xrightarrow{s} N \xrightarrow{!_N} 1$ is a coequalizer.

Parametrized NNO

$$\begin{array}{ccccc} X & \xrightarrow{\langle 0!, 1_X \rangle} & N \times X & \xrightarrow{s \times 1_X} & N \times X \\ & \searrow g & \downarrow f & & \downarrow f \\ & & Y & \xrightarrow{h} & Y \end{array}$$

$$f(0, x) = g(x)$$

$$f(sn, x) = h(f(n, x))$$

Skeleton

Definition (Skeleton)

Given a category \mathbf{C} , a *skeleton* of \mathbf{C} is a full subcategory containing exactly one objects from each isomorphism class of objects of \mathbf{C} .

The following statements are equivalent to the axiom of choice.

- ▶ Any category has a skeleton.
- ▶ Any category is equivalent to any of its skeletons.
- ▶ Any two skeletons of a given category are isomorphic.

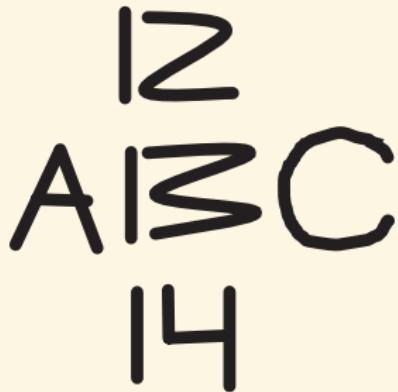
Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

An object is completely determined by its relationships to other objects

"You work at a particle accelerator. You want to understand some particle. All you can do are throw other particles at it and see what happens. If you understand how your mystery particle responds to all possible test particles at all possible test energies, then you know everything there is to know about your mystery particle."

— Ravi Vakil



Tell me who your friends are and I will tell you who you are.

Context: Which is the number 5?

1. In the context of natural numbers, 5 is a prime number.
2. In the context of integers, 5 has an additive inverse, which is -5 .
3. In the context of rational numbers, 5 has a multiplicative inverse, which is $\frac{1}{5}$.
4. In the context of arithmetic modulo 6, 5 is a generator, which means if you add 5 to itself repeatedly you will get every number in the system.

Hom Functor

Definition (Hom Functor)

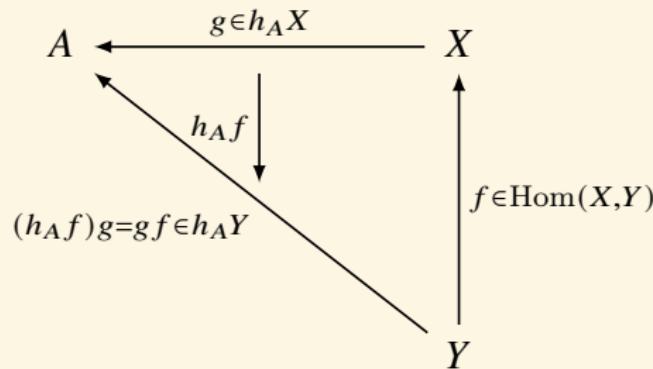
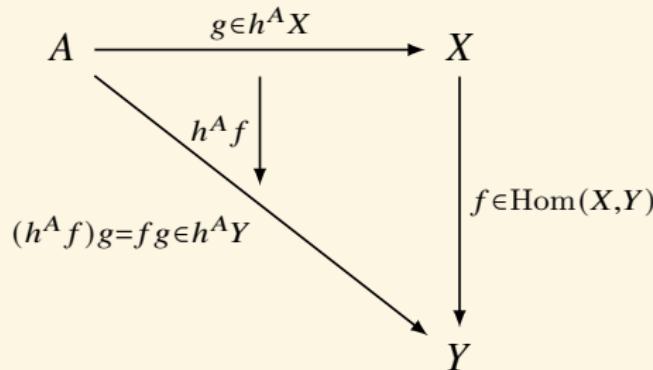
- For $A \in \mathbf{C}$, the functor $h^A := \text{Hom}(A, -)$ maps $X \mapsto \text{Hom}(A, X)$, and $f: X \rightarrow Y$ to $f_* := \text{Hom}(A, f) : \text{Hom}(A, X) \rightarrow \text{Hom}(A, Y) :: g \mapsto fg$.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \text{Hom}(A, X) & \xrightarrow{\text{Hom}(A, f)} & \text{Hom}(A, Y) \\ g & \longmapsto & fg \end{array}$$

- For $A \in \mathbf{C}$, the functor $h_A := \text{Hom}(-, A)$ maps $X \mapsto \text{Hom}(X, A)$, and $f: Y \rightarrow X$ to $f^* := \text{Hom}(f, A) : \text{Hom}(X, A) \rightarrow \text{Hom}(Y, A) :: g \mapsto gf$.

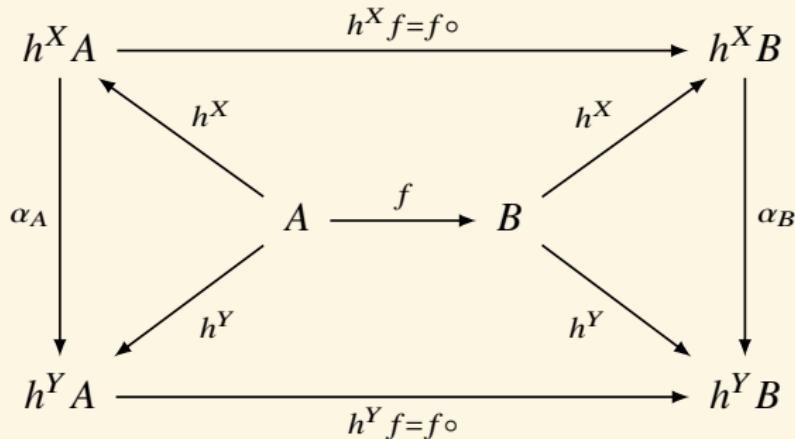
$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ \text{Hom}(X, A) & \xrightarrow{\text{Hom}(f, A)} & \text{Hom}(Y, A) \\ g & \longmapsto & - \circ f \\ & & gf \end{array}$$

Hom Functor



Natural Transformation between Hom Functors

$\alpha \in \text{Nat} (h^X, h^Y)$ for $h^X, h^Y \in \mathbf{Set}^{[\mathbf{C}, \mathbf{Set}]}$



$$f \circ \alpha_A = \alpha_B \circ f$$

$\text{Hom}(-, -) : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{Set}$ maps $A, B \in \mathbf{C}$ to $\text{Hom}(A, B)$, and maps $f : A' \rightarrow A, g : B \rightarrow B'$ to $\text{Hom}(f, g) : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B')$:: $h \mapsto ghf$.

$$\begin{array}{ccccc}
& & h & \xrightarrow{- \circ f} & hf \\
& \downarrow & & & \downarrow \\
& & \text{Hom}(A, B) & \xrightarrow{\text{Hom}(f, B)} & \text{Hom}(A', B) \\
& \downarrow & \text{Hom}(A, g) & \downarrow & \text{Hom}(A', g) \\
& & \text{Hom}(A, B') & \xrightarrow{\text{Hom}(f, B')} & \text{Hom}(A', B') \\
& \downarrow & & & \downarrow \\
& & gh & \xrightarrow{- \circ f} & ghf
\end{array}$$

$B \xrightarrow{g} B'$ $g \circ - : \text{Hom}(A, B) \rightarrow \text{Hom}(A, B')$ $- \circ f : \text{Hom}(A, B) \rightarrow \text{Hom}(A', B')$ $g \circ - : \text{Hom}(A', B') \rightarrow \text{Hom}(A', B)$

$$A' \xrightarrow{f} A$$

Yoneda Embedding

$$\frac{\text{Hom} : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{Set}}{y : \mathbf{C} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}}$$

Definition (Yoneda Embedding)

Let \mathbf{C} be a locally small category. Define $y : \mathbf{C} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ as follows.

- ▶ For $A \in \mathbf{C}$, $y : A \mapsto \text{Hom}(-, A) : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}$.
- ▶ For $f : A \rightarrow B$, $y : f \mapsto f_* = \text{Hom}(-, f) : \text{Hom}(-, A) \rightarrow \text{Hom}(-, B)$.

Definition (Yoneda Embedding)

Let \mathbf{C} be a locally small category. Define $y : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}^{\mathbf{C}}$ as follows.

- ▶ For $A \in \mathbf{C}^{\text{op}}$, $y : A \mapsto \text{Hom}(A, -) : \mathbf{C} \rightarrow \mathbf{Set}$.
- ▶ For $f : B \rightarrow A$, $y : f \mapsto f^* = \text{Hom}(f, -) : \text{Hom}(A, -) \rightarrow \text{Hom}(B, -)$.

$$\widehat{\mathbf{C}} := \mathbf{Set}^{\mathbf{C}^{\text{op}}}$$

Yoneda Lemma

Theorem (Yoneda Lemma)

For any locally small category \mathbf{C} , object $A \in \mathbf{C}$ and functor $F : \mathbf{C} \rightarrow \mathbf{Set}$,

$$\mathbf{Set}^{\mathbf{C}}(yA, F) \cong FA$$

naturally in both A and F .

Theorem (Yoneda Lemma: another version)

- ▶ For any locally small category \mathbf{C} , object $A \in \mathbf{C}$ and functor $F : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}$,

$$\mathbf{Set}^{\mathbf{C}^{\text{op}}}(\text{Hom}(-, A), F) \cong FA$$

naturally in both A and F .

- ▶ For any locally small category \mathbf{C} , object $A \in \mathbf{C}$ and functor $F : \mathbf{C} \rightarrow \mathbf{Set}$,

$$\mathbf{Set}^{\mathbf{C}}(\text{Hom}(A, -), F) \cong FA$$

naturally in both A and F .

Proof Sketch of Yoneda Lemma

Proof.

Let $\varphi : \text{Hom}(\mathbf{C}(A, -), F) \rightarrow FA :: \alpha \mapsto \alpha_A(1_A)$.

Our first aim is to define an inverse function

$\psi : FA \rightarrow \text{Hom}(\mathbf{C}(A, -), F)$ that constructs a natural transformation $\psi(a) : \mathbf{C}(A, -) \rightarrow F$ from any $a \in FA$.

To this end, we must define components

$\psi(a)_B : \mathbf{C}(A, B) \rightarrow FB$ so that

$$\psi(a)_B \circ \mathbf{C}(A, f) = Ff \circ \psi(a)_A.$$

To make $\varphi(\psi(a)) = a$, let $\psi(a)_A(1_A) = a$.

Now, naturality forces us to define

$$\psi(a)_B(f) := Ff(a).$$

By construction, $\varphi(\psi(a)) = a$. It remains to verify that $\psi(\varphi(\alpha)) = \alpha$.

$$\begin{aligned}\psi(\varphi(\alpha))_B(f) &= \psi(\alpha_A(1_A))_B(f) = \\ Ff(\alpha_A(1_A)) &= \alpha_B(f)\end{aligned}$$

$$\begin{array}{ccc}\mathbf{C}(A, A) & \xrightarrow{\mathbf{C}(A, f)} & \mathbf{C}(A, B) \\ \psi(a)_A \downarrow & & \downarrow \psi(a)_B \\ FA & \xrightarrow{Ff} & FB\end{array}$$

$$\begin{array}{ccc}1_A & \longmapsto & f \\ \downarrow & & \downarrow \\ a & \longmapsto & \psi(a)_B(f) = Ff(a)\end{array}$$

$$\begin{array}{ccc}\mathbf{C}(A, A) & \xrightarrow{\mathbf{C}(A, f)} & \mathbf{C}(A, B) \\ \alpha_A \downarrow & & \downarrow \alpha_B \\ FA & \xrightarrow{Ff} & FB\end{array}$$

Proof Sketch of Yoneda Lemma

Proof continued.

To show that φ is natural in F , suppose given a natural transformation $\beta : F \rightarrow G$.

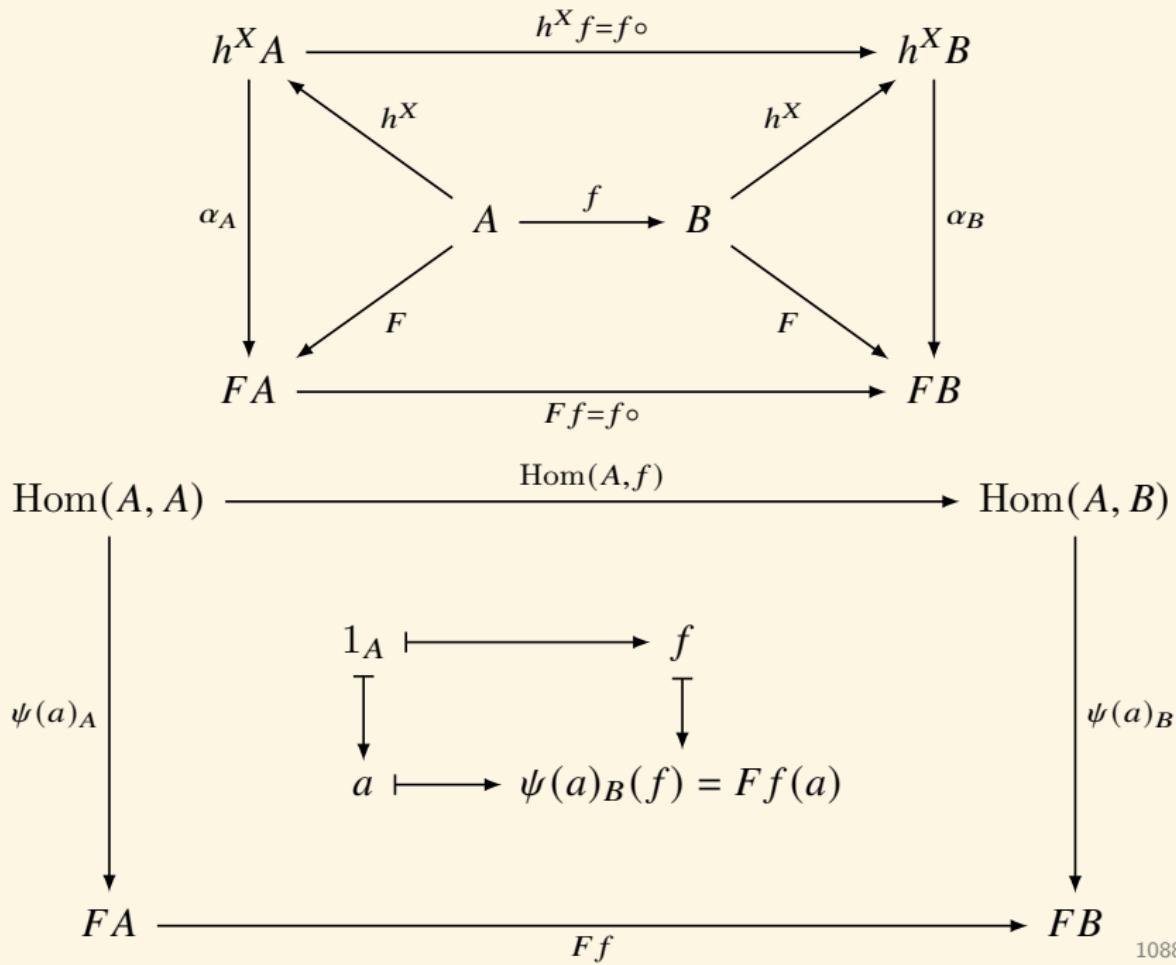
$$\begin{array}{ccc} \text{Set}^C(\mathbf{C}(A, -), F) & \xrightarrow{\beta \circ -} & \text{Set}^C(\mathbf{C}(A, -), G) \\ \varphi_F \downarrow & & \downarrow \varphi_G \\ FA & \xrightarrow{\beta_A} & GA \end{array}$$

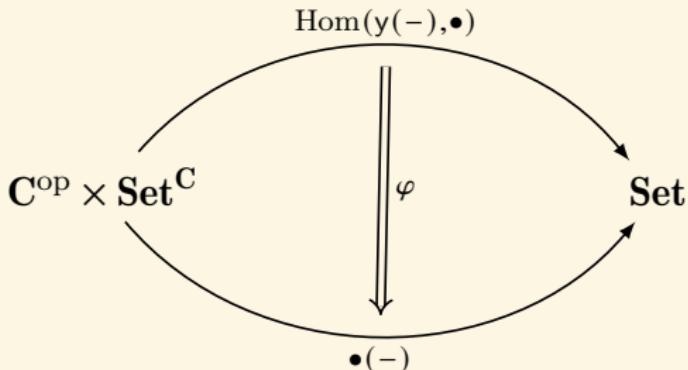
$$\beta_A(\varphi_F(\alpha)) = \beta_A(\alpha_A(1_A)) = (\beta \circ \alpha)_A(1_A) = \varphi_G(\beta \circ \alpha)$$

To show that φ is natural in A , suppose given $f : A \rightarrow B$.

$$\begin{array}{ccc} \text{Set}^C(\mathbf{C}(A, -), F) & \xrightarrow{- \circ \mathbf{C}(f, -)} & \text{Set}^C(\mathbf{C}(B, -), F) \\ \varphi_A \downarrow & & \downarrow \varphi_B \\ FA & \xrightarrow{Ff} & FB \end{array}$$

$$Ff(\varphi_A(\alpha)) = Ff(\alpha_A(1_A)) = \alpha_B \circ \mathbf{C}(A, f)(1_A) = \alpha_B(f) = \alpha_B \circ \mathbf{C}(f, -)_B(1_B) = (\alpha \circ \mathbf{C}(f, -))_B(1_B) = \varphi_B(\alpha \circ \mathbf{C}(f, -))$$





Theorem (Restricted Yoneda Lemma)

For any locally small category \mathbf{C} , object $A, B \in \mathbf{C}$,

- ▶ $\text{Set}^{\mathbf{C}}(\text{Hom}(A, -), \text{Hom}(B, -)) \cong \text{Hom}(B, A)$
- ▶ $\text{Set}^{\mathbf{C}^{\text{op}}}(\text{Hom}(-, A), \text{Hom}(-, B)) \cong \text{Hom}(A, B)$

Proof.

Let $F := \text{Hom}(B, -)$ or $F := \text{Hom}(-, B)$.

Corollary

The Yoneda embedding functor $y : \mathbf{C} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ is fully faithful, and injective on objects. Hence, y is an embedding $\mathbf{C} \hookrightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$.

Proof.

Injectivity of $\mathbf{C}(A, B) \hookrightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}(\mathbf{C}(-, A), \mathbf{C}(-, B))$ given by $f \mapsto f_*$ is clear. The Yoneda lemma gives us surjectivity.

$$\mathbf{Set}^{\mathbf{C}^{\text{op}}}(\mathbf{C}(-, A), \mathbf{C}(-, B)) \cong \mathbf{C}(A, B)$$

For any natural transformation $\alpha : \mathbf{C}(-, A) \rightarrow \mathbf{C}(-, B)$, We need to find a morphism $f : A \rightarrow B$ so that $\alpha = f_*$. Let $f := \alpha_A(1_A)$.

$$\begin{array}{ccc} 1_A & \xleftarrow{\hspace{10em}} & \alpha_A(1_A) \\ X \downarrow g & \text{C}(A, A) \xrightarrow{\alpha_A} & \text{C}(A, B) \\ A & g^* \downarrow & \downarrow g^* \\ & \text{C}(X, A) \xrightarrow{\alpha_X} & \text{C}(X, B) \\ & \downarrow & \downarrow \\ 1_A \circ g & \xrightarrow{\hspace{10em}} & \alpha_X(1_A \circ g) = \alpha_A(1_A) \circ g \\ & & \alpha_X(g) = f \circ g \end{array}$$

Concrete Category & Abstract Category

Definition (Concrete Category & Abstract Category)

A category C is *concrete* iff there is a faithful functor $F : C \rightarrow \text{Set}$.
Categories that are not concrete are called *abstract categories*.

All small categories are concrete because of Yoneda lemma.

Corollary

For any locally small category \mathbf{C} , any objects $A, B \in \mathbf{C}$,
 $A \cong B \iff yA \cong yB$.

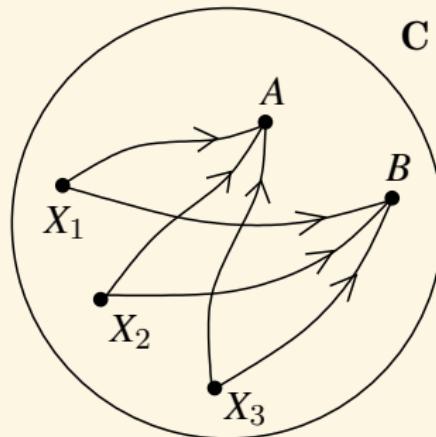


Figure: If $\text{Hom}(X, A) \cong \text{Hom}(X, B)$ naturally in X , then $A \cong B$.

Application — Categorifying Cardinal Arithmetic

What is the meaning of the equation?

$$\forall abc \in \mathbb{N} : a \times (b + c) = (a \times b) + (a \times c)$$

- ▶ categorification (replacing equality by isomorphism)
- ▶ the Yoneda lemma (replacing isomorphism by natural isomorphism)
- ▶ representability (characterizing maps to or from an object)
- ▶ limits and colimits (like cartesian product and disjoint union)
- ▶ adjunctions (such as currying)

Lemma

Lemma (Yoneda Lemma)

$A \cong B \iff \text{Hom}(A, X) \cong \text{Hom}(B, X)$ naturally in X .

Proof.

Suppose $\text{Hom}(A, X) \cong \text{Hom}(B, X)$. Taking $X = A$ and $X = B$, we use the bijections $\text{Hom}(A, A) \cong \text{Hom}(B, A)$ and $\text{Hom}(A, B) \cong \text{Hom}(B, B)$ to define $f : A \rightarrow B$ and $g : B \rightarrow A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$.

By naturality:

$$\begin{array}{ccc} 1_A & \xrightarrow{\hspace{10cm}} & g \\ \downarrow & & \downarrow \\ \text{Hom}(A, A) & \xrightarrow{\cong} & \text{Hom}(B, A) \\ f \circ - \downarrow & & \downarrow f \circ - \\ \text{Hom}(A, B) & \xrightarrow{\cong} & \text{Hom}(B, B) \\ \downarrow & & \downarrow \\ f & \xrightarrow{\hspace{10cm}} & 1_B = f \circ g \end{array}$$

similarly,
 $g \circ f = 1_A$

Categorifying Cardinal Arithmetic

$$a \times (b + c) = (a \times b) + (a \times c)$$

Proof.

- ▶ pick sets A, B, C s.t. $a = |A|, b = |B|, c = |C|$.
- ▶ show that $A \times (B + C) \cong (A \times B) + (A \times C)$.
- ▶ by the Yoneda lemma, this holds iff

$$\text{Hom}(A \times (B + C), X) \cong \text{Hom}((A \times B) + (A \times C), X) \quad \text{naturally}$$

- ▶ now

$$\begin{aligned} \text{Hom}(A \times (B + C), X) &\cong \text{Hom}(B + C, X^A) && (\text{currying}) \\ &\cong \text{Hom}(B, X^A) \times \text{Hom}(C, X^A) && (\text{pairing}) \\ &\cong \text{Hom}(A \times B, X) \times \text{Hom}(A \times C, X) && (\text{currying}) \\ &\cong \text{Hom}((A \times B) + (A \times C), X) && (\text{pairing}) \end{aligned}$$

Theorem

For a locally small category \mathbf{C} , the Yoneda embedding y preserves all limits that exist in \mathbf{C} .

Proof.

Suppose (L, λ) is a limit of $D : \mathbf{I} \rightarrow \mathbf{C}$. The Yoneda embedding maps D to the diagram $yD : \mathbf{I} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ defined by $(yD)_i = yD_i = \text{Hom}(-, D_i)$, and it maps (L, λ) to $(yL, y\lambda)$ on yD defined by $(y\lambda)_i = y\lambda_i = \text{Hom}(-, \lambda_i)$.

To see that $(yL, y\lambda)$ is a limit cone on yD , consider a cone (M, μ) on yD . Then $\mu : \Delta M \rightarrow D$ consists of a family of functions, one for each $i \in \mathbf{I}$ and $A \in \mathbf{C}$,

$$(\mu_i)_A : MA \rightarrow \text{Hom}(A, D_i)$$

For $A \in \mathbf{C}$ and $m \in MA$, we get a cone on D consisting of morphisms $(\mu_i)_A m : A \rightarrow D_i$. There exists a unique morphism $\varphi_A m : A \rightarrow L$ s.t. $(\mu_i)_A m = \lambda_i \circ \varphi_A m$. Then $\varphi_A : MA \rightarrow \text{Hom}(A, L) = (yL)_A$ forms a unique factorization $\varphi : M \rightarrow yL$.

- ▶ $\text{Hom}(A, \lim_{\leftarrow} D_i) \cong \lim_{\leftarrow} \text{Hom}(A, D_i)$
- ▶ $\text{Hom}(\lim_{\rightarrow} D_i, A) \cong \lim_{\leftarrow} \text{Hom}(D_i, A)$

Cayley Theorem

Theorem (Cayley Theorem)

Every group G is isomorphic to a subgroup of the symmetric group on G .

Proof.

Any group G can be viewed as a single object • category, call it \mathbf{G} .

$$\mathbf{Set}^{\mathbf{G}^{\text{op}}}(\mathbf{G}(-, \bullet), \mathbf{G}(-, \bullet)) \cong \mathbf{G}(\bullet, \bullet)$$

The right-hand side is just G .

$y : g \mapsto \mathbf{G}(-, g) : \mathbf{G}(\bullet, \bullet) \rightarrow \mathbf{G}(\bullet, \bullet)$ and $\mathbf{G}(-, g) : x \mapsto gx$.

Therefore, the left-hand side is a subgroup of the group of all permutations on G .

Moreover, this subgroup is isomorphic to the group G itself by the restricted Yoneda lemma.

From Klein's Erlangen Program to Category Theory

- ▶ Klein¹⁷ started with a geometry and looked at the group of transformations of that geometry.
- ▶ One possible generalization is to replace the geometry by a different structure X and consider its algebra of automorphisms $\text{Aut}(X)$.

$$\text{Aut}(X) \rightarrow \text{End}(X) \rightarrow \text{Hom}(X, Y)$$

$$\frac{\begin{matrix} \text{Space} \\ \hline \text{Transformation group} \end{matrix}}{\sim} \quad \frac{\text{Category}}{\text{Algebra of mappings}}$$

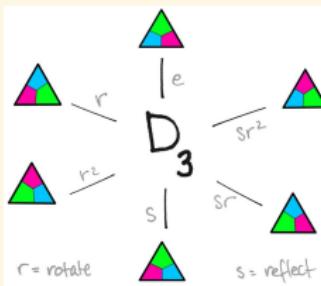
¹⁷Klein's Erlangen program: "Given a manifold, and a transformation group acting on it, to study its invariants."

- ▶ If geometric spaces are taken first, then groups, seen as systems of global properties of spaces, **supervene** upon geometric properties, that is properties definable in the language of the space, for instance via linear algebra.
- ▶ On the other hand, it is possible to reverse the dependence and instead consider groups as being fundamental and construct the spaces from them to look at their various representations.

- Given a vector space X , a group action $G \times X \rightarrow X$ can be seen as a group representation $G \rightarrow \text{Aut}(X)$. A group representation provides a way to view the abstract group elements as concrete linear transformations of some vector space.
- For example, $D_3 \rightarrow \text{Aut}(\mathbb{R}^2)$.

$$D_3 = \langle r, s \mid r^3 = s^2 = rsrs = e \rangle$$

$$r \mapsto R = \begin{bmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix} \quad s \mapsto S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



- We can think of a group G as providing the syntax while automorphisms $\text{Aut}(X)$ provide the semantics. So a group representation is like a functor

syntax \rightarrow semantics

Representable Functor

Definition (Representable Functor)

A functor $F : \mathbf{C} \rightarrow \mathbf{Set}$ is *representable* iff there is a natural isomorphism $\alpha : \text{Hom}(A, -) \xrightarrow{\cong} F$ for some $A \in \mathbf{C}$. We say that the pair (A, α) is a *representation* of F .

$$\begin{array}{ccccc} h_X A & \xrightarrow{h_X f} & & & h_X B \\ \downarrow \alpha_A & \nearrow h_X & & \nearrow h_X & \downarrow \alpha_B \\ & A & \xrightarrow{f} & B & \\ \downarrow F & \nearrow F & & \nearrow F & \downarrow \\ FA & \xrightarrow{Ff} & & & FB \end{array}$$

Universal Element

Definition (Universal Element)

A *universal element* of the functor $F : \mathbf{C} \rightarrow \mathbf{Set}$ is a pair (A, a) , where $A \in \mathbf{C}$ and $a \in FA$, and for each $B \in \mathbf{C}$ and $b \in FB$, there is a unique map $f : A \rightarrow B$ such that $Ff(a) = b$.

$$\begin{array}{ccccc} \text{End}(A) & \xrightarrow{h_A f} & h_A B & & \\ \alpha_A \downarrow & \nearrow h_A & & \nearrow h_A & \downarrow \alpha_B \\ FA & \xrightarrow[F]{Ff} & A & \xrightarrow{f} & B \\ & \searrow F & & \swarrow F & \\ & & FB & & \end{array}$$

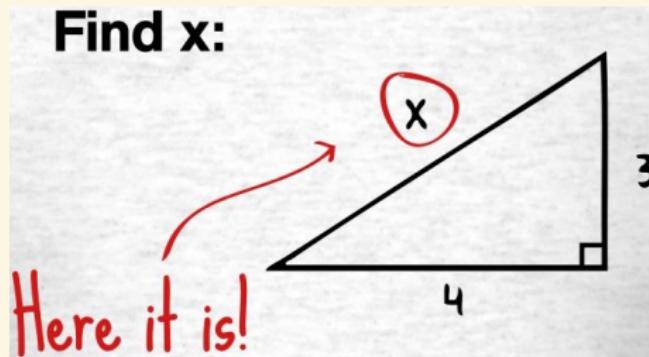
- If (A, α) is a representation of $F : \mathbf{C} \rightarrow \mathbf{Set}$, then $(A, \alpha_A(1_A))$ is a universal element of F .
- The natural transformation $\psi(a) : \text{Hom}(A, -) \rightarrow F$ induced by $a \in FA$ in Yoneda lemma is an isomorphism iff (A, a) is a universal element of F .

Remark

All the information contained in a representable functor $F : \mathbf{C} \rightarrow \mathbf{Set}$ is condensed in the representing object $A \in \mathbf{C}$ and the universal element $a \in FA$, which ‘generates’ all the other elements $b \in FB$ by applying functions of the form Ff to it.

Philosophy — Object as a Solution to a Problem

Find x s.t. $x^2 + 1 = 0$.



Problem

For a functor $F : \mathbf{C} \rightarrow \mathbf{Set}$, find an object X of the category \mathbf{C} together with $\alpha : \text{Hom}(X, -) \cong F$.

Remark: If we find two solutions $\alpha : \text{Hom}(X, -) \cong F$ and $\beta : \text{Hom}(Y, -) \cong F$, then by Yoneda's lemma, $X \cong Y$, i.e. the object is unique up to unique isomorphism.

Philosophy — Objects as tokens for Eigenbehaviors

“We identify the world in terms of how we shape it. We shape the world in response to how it changes us. Objects arise as tokens of behavior that leads to seemingly unchanging forms. Forms are seen to be unchanging through their invariance under our attempts to change, to shape them.”

— Louis H. Kauffman

Category of Elements

Definition

- ▶ The *category of elements* $\int^{\mathbf{C}} F$ of a covariant functor $F : \mathbf{C} \rightarrow \mathbf{Set}$ has
 1. as objects (A, a) , where $A \in \mathbf{C}$ and $a \in FA$, and
 2. as morphisms $(A, a) \rightarrow (B, b)$ with $f : A \rightarrow B$ in \mathbf{C} s.t. $Ff(a) = b$.
- ▶ The *category of elements* $\int_{\mathbf{C}} P$ of a contravariant functor $P : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}$ has
 1. as objects (A, a) where $A \in \mathbf{C}$ and $a \in PA$, and
 2. as morphisms $(A, a) \rightarrow (B, b)$ with $f : A \rightarrow B$ in \mathbf{C} s.t. $Pf(b) = a$.

A universal element can be viewed as an initial object in the category of elements of F .

Theorem

A covariant set-valued functor is representable iff its category of elements has an initial object. Dually, a contravariant set-valued functor is representable iff its category of elements has a terminal object.

The category of elements $\int_{\mathbf{C}} P$ has an evident projection functor:

$$\pi_P : \int_{\mathbf{C}} P \rightarrow \mathbf{C} :: (A, a) \mapsto A$$

Theorem

If $F : \mathbf{C} \rightarrow \mathbf{D}$ is a functor from a small category \mathbf{C} to a cocomplete category \mathbf{D} , the functor $R : \mathbf{D} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ given by

$$R(B) : A \mapsto \text{Hom}_{\mathbf{D}}(FA, B)$$

has a left adjoint $L : \mathbf{Set}^{\mathbf{C}^{\text{op}}} \rightarrow \mathbf{D}$ given by

$$L(P) = \varinjlim \left(\int_{\mathbf{C}} P \xrightarrow{\pi_P} \mathbf{C} \xrightarrow{F} \mathbf{D} \right)$$

In other words,

$$\text{Hom}_{\mathbf{D}}(LP, B) \cong \mathbf{Set}^{\mathbf{C}^{\text{op}}}(P, RB) \quad L \dashv R$$

Proof.

For a natural transformation $\alpha : P \rightarrow RB$,

$$\alpha_A : PA \rightarrow \mathbf{D}(FA, B)$$

$\{\alpha_A\}_{A \in \mathbf{C}}$ is natural in A .

$$\begin{array}{ccc} A & PA & \xrightarrow{\alpha_A} \mathbf{D}(FA, B) \\ \uparrow f & Pf \downarrow & \downarrow \mathbf{D}(Ff, B) \\ A' & PA' & \xrightarrow{\alpha_{A'}} \mathbf{D}(FA', B) \end{array}$$

Such an α can also be considered as $\{\alpha_A(a) : FA \rightarrow B\}_{(A, a) \in \int_{\mathbf{C}} P}$. Then

$$\begin{array}{ccc} A & FA = F\pi_P(A, a) & \\ \uparrow f & Ff \uparrow & \searrow \alpha_A(a) \\ A' & FA' = F\pi_P(A', a') & \nearrow \alpha_{A'}(a') \end{array}$$

This means that (B, α_A) constitute a cocone over $F\pi_P : \int_{\mathbf{C}} P \rightarrow \mathbf{D}$.

Each such cocone comes by composing the colimiting cocone with a unique arrow from the colimit LP to the object B . In other words,

$$\mathrm{Hom}_{\mathbf{D}}(LP, B) \cong \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}} (P, RB)$$

Corollary

Every presheaf is a colimit of representable presheaves.

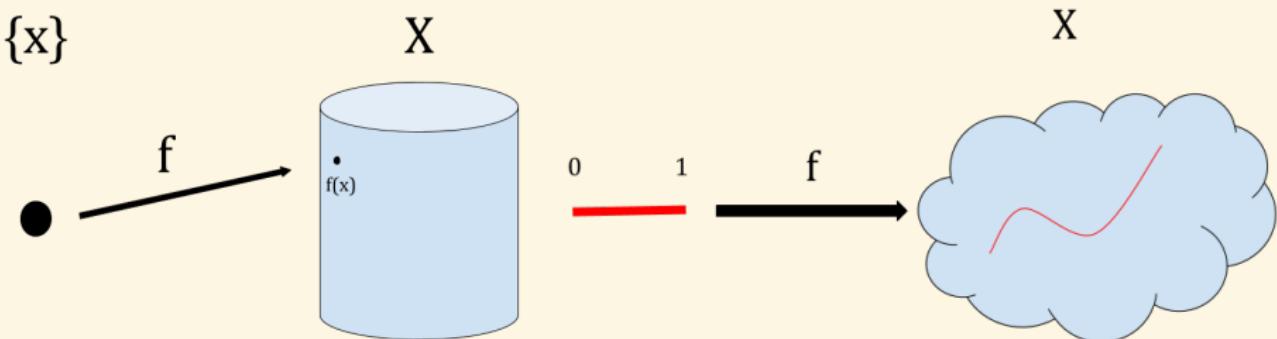
Proof.

By the Yoneda lemma,

$$R_y(B)(A) = \mathbf{Set}^{\mathbf{C}^{\text{op}}}(yA, B) \cong B(A)$$

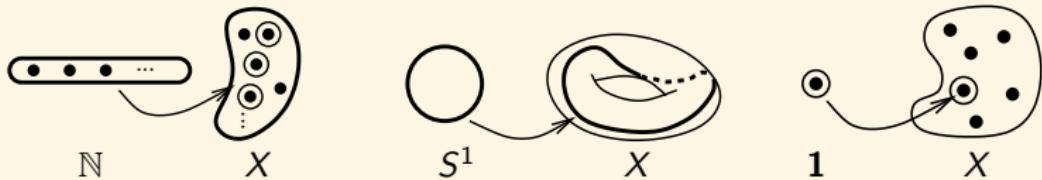
this means that R_y is isomorphic to the identity functor of $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$.
Its left adjoint L must also be isomorphic to the identity functor.

$$P \cong \varinjlim \left(\int_{\mathbf{C}} P \xrightarrow{\pi_P} \mathbf{C} \xrightarrow{y} \mathbf{Set}^{\mathbf{C}^{\text{op}}} \right)$$



Suppose X and Y are topological spaces and let \bullet denote the one-point space and I and S^1 the unit interval and the circle. Then,

- ▶ X and Y have the same cardinality iff $\text{Hom}(\bullet, X) \cong \text{Hom}(\bullet, Y)$.
 - ▶ X and Y have the same path space iff $\text{Hom}(I, X) \cong \text{Hom}(I, Y)$.
 - ▶ X and Y have the same loop space iff $\text{Hom}(S^1, X) \cong \text{Hom}(S^1, Y)$.
 - ▶ Probing X and Y with various spaces gives us more information.
 - ▶ Probing them with all spaces gives us all information.



a sequence / a loop / an element

Given any objects A, B in a locally small category \mathbf{C} , to find a morphism $h : A \rightarrow B$ it suffices to give one $\theta : yA \rightarrow yB$ in $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$, for then there is a unique h with $\theta = yh$. Why should it be easier to give $yA \rightarrow yB$ than $A \rightarrow B$? The key difference is that in general $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$ has much more structure to work with than does \mathbf{C} . The category $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$ is complete, cocomplete, cartesian closed, and more. It is like an extension of \mathbf{C} by “ideal elements” that permit calculations which cannot be done in \mathbf{C} . This is something like passing to the complex numbers to solve equations in the reals, or adding higher types to an elementary logical theory.

Digression — Mazzola's Path to Creativity

1. Exhibiting the open question = to understand the object X
2. Identifying the semiotic context = to describe the category \mathbf{C} of which X is an object
3. Finding the question's critical concept in the semiotic context = X
4. Identifying the concept's walls = the uncontrolled behaviour of the Yoneda functor $yX = \text{Hom}_{\mathbf{C}}(-, X)$
5. Opening the walls and displaying its new perspectives = finding a subcategory \mathbf{A} of \mathbf{C} such that: $y|_{\mathbf{A}} : \mathbf{C} \rightarrow \mathbf{Set}^{\mathbf{A}^{\text{op}}} :: X \mapsto \text{Hom}_{\mathbf{A}}(-, X)$ is fully faithful, and for any $X \in \mathbf{C}$ there is a diagram D in \mathbf{A} whose colimit $\varinjlim D \cong X$
6. Evaluating the extended walls = try to understand X via the isomorphism $\varinjlim D \cong X$

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Adjunction

Definition (Left/Right Adjoint)

Functors $\mathbf{C} \xrightleftharpoons[F]{G}$ \mathbf{D} are *adjoint* $F \dashv G$ iff there is an isomorphism

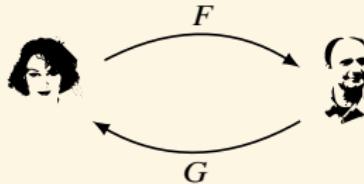
$$\theta_{A,B} : \mathbf{D}(FA, B) \xrightarrow{\cong} \mathbf{C}(A, GB)$$

that is natural in both A and B .

Naturality of θ means that for $f : A \rightarrow A'$ and $g : B \rightarrow B'$,

$$\begin{array}{ccc} \mathbf{D}(FA', B) & \xrightarrow{\theta_{A',B}} & \mathbf{C}(A', GB) \\ \mathbf{D}(Ff, B) \downarrow & & \downarrow \mathbf{C}(f, GB) \\ \mathbf{D}(FA, B) & \xrightarrow{\theta_{A,B}} & \mathbf{C}(A, GB) \end{array} \quad \begin{array}{ccc} \mathbf{D}(FA, B) & \xrightarrow{\theta_{A,B}} & \mathbf{C}(A, GB) \\ \mathbf{D}(FA, g) \downarrow & & \downarrow \mathbf{C}(A, Gg) \\ \mathbf{D}(FA, B') & \xrightarrow{\theta_{A,B'}} & \mathbf{C}(A, GB') \end{array}$$

Remark



category = country

object = citizen

morphism = speaking in country's language

functor = translation

- ▶ Equivalence: doesn't matter whether I travel to you and speak your language, or you travel to me and speak my language.
- ▶ Some things get lost in translation; adjunction is next best thing.

Theorem

Given $\mathbf{D}(FA, B) \xrightleftharpoons[\sharp]{\flat} \mathbf{C}(A, GB)$, the naturality condition of the adjunction implies that for every $f : A \rightarrow A'$, $g : B \rightarrow B'$, $h^\sharp : FA \rightarrow B$, $k^\sharp : FA' \rightarrow B'$,

$$\begin{array}{ccc} A & \xrightarrow{h^\flat} & GB \\ f \downarrow & & \downarrow Gg \\ A' & \xrightarrow{k^\flat} & GB' \end{array} \iff \begin{array}{ccc} FA & \xrightarrow{h^\sharp} & B \\ Ff \downarrow & & \downarrow g \\ FA' & \xrightarrow{k^\sharp} & B' \end{array}$$

Proof.

$$\begin{array}{ccc} \mathbf{D}(FA', B') & \xrightarrow{\flat} & \mathbf{C}(A', GB') \\ - \circ Ff \downarrow & & \downarrow - \circ f \\ \mathbf{D}(FA, B') & \xrightarrow{\flat} & \mathbf{C}(A, GB') \end{array} \quad \begin{array}{ccc} \mathbf{D}(FA, B) & \xrightarrow{\flat} & \mathbf{C}(A, GB) \\ g \circ - \downarrow & & \downarrow Gg \circ - \\ \mathbf{D}(FA, B') & \xrightarrow{\flat} & \mathbf{C}(A, GB') \end{array}$$

$$k^\flat \circ f = (k^\sharp \circ Ff)^\flat \quad Gg \circ h^\flat = (g \circ h^\sharp)^\flat$$

Left/Right Adjoint

Example

$$\frac{A \wedge B \vdash C}{A \vdash B \rightarrow C}$$

$$F_B : X \mapsto X \wedge B \quad G_B : X \mapsto B \rightarrow X \quad F_B \dashv G_B$$

Example

$$\frac{A \cap B \subset C}{A \subset B \rightarrow C} \quad \text{where } B \rightarrow C := \overline{B} \cup C$$

$$F_B : X \mapsto X \cap B \quad G_B : X \mapsto B \rightarrow X \quad F_B \dashv G_B$$

Example

$$\frac{A \setminus B \subset C}{A \subset B \cup C}$$

$$F_B : X \mapsto X \setminus B \quad G_B : X \mapsto B \cup X \quad F_B \dashv G_B$$

Left/Right Adjoint

Example **Cost** := $([0, \infty], \geq, +, 0)$

$$\frac{A + B \geq C}{A \geq B \rightarrow C}$$

where $B \rightarrow C := \max\{0, C - B\}$.

$$F_B : X \mapsto X + B \quad G_B : X \mapsto B \rightarrow X \quad F_B \dashv G_B$$

Example

Consider the inclusion map $i : \mathbb{Z} \hookrightarrow \mathbb{R}$.

This has both a left adjoint $\lceil \rceil$ and a right adjoint $\lfloor \rfloor$. For $z \in \mathbb{Z}, r \in \mathbb{R}$:

$$\frac{r \leq i(z)}{\lceil r \rceil \leq z} \quad \frac{i(z) \leq r}{z \leq \lfloor r \rfloor}$$

Left/Right Adjoint

Example

$$\text{Hom}(A \times B, C) \cong \text{Hom}(A, C^B)$$

$$F_B : X \mapsto X \times B \quad G_B : X \mapsto X^B \quad F_B \dashv G_B$$

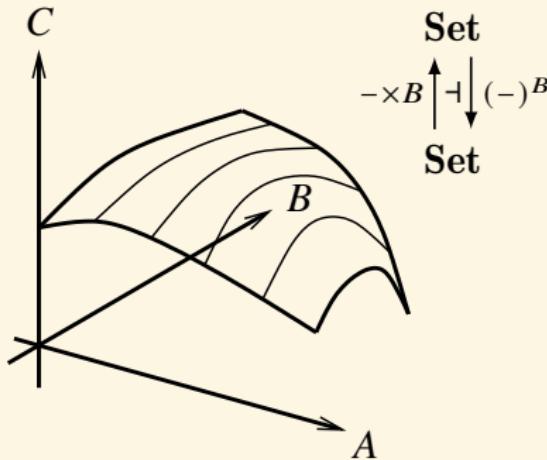


Figure: In **Set**, a map $A \times B \rightarrow C$ can be seen as a way of assigning to each element of A a map $B \rightarrow C$.

Left/Right Adjoint

Example

The forgetful functor $U : \mathbf{Grp} \rightarrow \mathbf{Set}$ has as a left adjoint $F : \mathbf{Set} \rightarrow \mathbf{Grp}$ which sends a set to the free group on that set. $F \dashv U$.

Example

- ▶ The forgetful functor $\text{ob} : \mathbf{Cat} \rightarrow \mathbf{Set}$ has a left adjoint Disc sending A to the discrete category whose objects are the members of A , with only identity morphisms.
- ▶ And $\text{ob} : \mathbf{Cat} \rightarrow \mathbf{Set}$ has a right adjoint Indisc sending A to the preorder with objects $a \in A$ and one morphism $a \rightarrow b$ for each pair $(a, b) \in A \times A$.
- ▶ The functor Disc also has a left adjoint π_0 sending \mathbf{C} to its set of connected components, i.e. the quotient of $\text{ob } \mathbf{C}$ by the equivalence $A \sim B$ whenever there exists a morphism $A \rightarrow B \in \mathbf{C}$.

$$\pi_0 \dashv \text{Disc} \dashv \text{ob} \dashv \text{Indisc}$$

Left/Right Adjoint

Example

Let X be the poset of subsets of \mathbb{R}^2 , ordered by inclusion. Let Y be the poset of convex subsets of \mathbb{R}^2 .

The *convex hull* of a subset $A \subset \mathbb{R}^2$ is defined as either

- ▶ The smallest convex subset of \mathbb{R}^2 containing A ;
- ▶ The intersection of all convex subsets of \mathbb{R}^2 containing A ;
- ▶ The set obtained by closing A under all possible convex combinations.

Let $c : X \rightarrow Y$ be the map assigning to each $S \in X$ its convex hull.

$$\frac{c(A) \subset B}{A \subset i(B)}$$

Topological interior as an adjoint

- ▶ A *topological space* $(X, \mathcal{O}(X))$ is a set X with a family $\mathcal{O}(X) \subset \mathbf{P}(X)$ of subsets of X which contains \emptyset and X , and is closed under finite intersections and arbitrary unions.
- ▶ The topological *interior* of a subset $S \subset X$ is

$$S^\circ := \bigcup \{U \in \mathcal{O}(X) : U \subset S\}$$

- ▶ For $U \in \mathcal{O}(X)$ and $S \in \mathbf{P}(X)$, topological interior is a right adjoint to the inclusion of $\mathcal{O}(X)$ into $\mathbf{P}(X)$.

$$\frac{i: U \subset S}{U \subset S^\circ}$$

$$\begin{array}{ccc} \mathcal{O}(X) & \xrightarrow{\quad i \quad} & \mathbf{P}(X) \\ & \xleftarrow[\text{()}\circ]{\perp} & \end{array}$$

$$0_C \dashv !_C \dashv 1_C$$

- The terminal object of **CAT** is the category **1** containing just one

$$\begin{array}{c} 1_{\bullet} \\ \Downarrow \\ \bullet \end{array}$$

object and one morphism \bullet .

- For any category **C**, there exists a unique functor $!_C : C \rightarrow 1$, which maps every object $A \in C$ to \bullet .
- An object $A \in C$ can be viewed as a functor $A : 1 \rightarrow C$, i.e. $A : \bullet \rightarrow A$ and $A : 1_{\bullet} \rightarrow 1_A$.
- Then the terminal object 1_C of **C** is the right adjoint of $!_C : C \rightarrow 1$, for the corresponding functor $1_C : 1 \rightarrow C$ has the property that, for every $A \in C$ we have a trivial natural bijective correspondence:

$$\frac{1_{\bullet} : !_C A \rightarrow \bullet}{!_A : A \rightarrow 1_C \bullet} \quad \text{similarly,} \quad \frac{1_{\bullet} : \bullet \rightarrow !_C A}{!_A : 0_C \bullet \rightarrow A}$$

$$1(!_C A, \bullet) \cong C(A, 1_C \bullet)$$

$$C(0_C \bullet, A) \cong 1(\bullet, !_C A)$$

$$0_C \dashv !_C \dashv 1_C$$

$$+ \dashv \Delta \dashv \times$$

Theorem

1. Δ has a right adjoint iff \mathbf{C} has binary products, and the right adjoint is $\times : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$.
2. Δ has a left adjoint iff \mathbf{C} has binary coproducts, and the left adjoint is $+ : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$.

$$\mathbf{C} \times \mathbf{C}(\Delta X, (A, B)) \cong \mathbf{C}(X, A) \times \mathbf{C}(X, B) \cong \mathbf{C}(X, A \times B)$$

$$\mathbf{C}(A + B, X) \cong \mathbf{C}(A, X) \times \mathbf{C}(B, X) \cong \mathbf{C} \times \mathbf{C}((A, B), \Delta X)$$

$$\begin{array}{ccccccc}
X & \xleftarrow{\pi_1} & X \times Y & \xrightarrow{\pi_2} & Y & X & \xleftarrow{\pi_1} X \times X & \xrightarrow{\pi_2} X & \xrightarrow{(f, g)} \Delta X \rightarrow (A, B) \\
f \downarrow & & \downarrow f \times g & & \downarrow g & f \downarrow & & \downarrow f \times g & \downarrow g & f \times g : X \rightarrow A \times B \\
A & \xleftarrow{\pi_1} & A \times B & \xrightarrow{\pi_2} & B & A & \xleftarrow{\pi_1} A \times B & \xrightarrow{\pi_2} B & \\
& & & & & & & & \\
X & \xrightarrow{\iota_1} & X + Y & \xleftarrow{\iota_2} & Y & X & \xrightarrow{\iota_1} X + X & \xleftarrow{\iota_2} X & \xrightarrow{f + g} A + B \rightarrow X \\
f \uparrow & & \uparrow f + g & & \uparrow g & f \uparrow & & \uparrow f + g & \uparrow g & (f, g) : (A, B) \rightarrow \Delta X \\
A & \xrightarrow{\iota_1} & A + B & \xleftarrow{\iota_2} & B & A & \xrightarrow{\iota_1} A + B & \xleftarrow{\iota_2} B &
\end{array}$$

Cartesian Closed Category

Theorem

A category \mathbf{C} is cartesian closed iff, the following functors have right adjoints:

$$!_{\mathbf{C}} : \mathbf{C} \rightarrow \mathbf{1}$$

$$\Delta : \mathbf{C} \rightarrow \mathbf{C} \times \mathbf{C}$$

$$(- \times A) : \mathbf{C} \rightarrow \mathbf{C}$$

Here $!_{\mathbf{C}}$ is the unique functor from \mathbf{C} to the terminal category $\mathbf{1}$ and Δ is the diagonal functor $\Delta A = \langle A, A \rangle$, and the right adjoint of $- \times A$ is exponentiation by A .

$$\vee \dashv \Delta \dashv \wedge$$

$$\vee \dashv \Delta$$

$$\frac{A \vee B \rightarrow C}{(A \rightarrow C) \wedge (B \rightarrow C)}$$

$$\mathbf{Prop}(A \vee B, C) \cong \mathbf{Prop} \times \mathbf{Prop}((A, B), \Delta C)$$

$$\Delta \dashv \wedge$$

$$\frac{(C \rightarrow A) \wedge (C \rightarrow B)}{C \rightarrow A \wedge B}$$

$$\mathbf{Prop} \times \mathbf{Prop}(\Delta C, (A, B)) \cong \mathbf{Prop}(C, A \wedge B)$$

$$\varinjlim \dashv \Delta \dashv \varprojlim$$

Consider the constant diagram functor $\Delta : \mathbf{C} \rightarrow \mathbf{C}^I$. It maps $X \in \mathbf{C}$ to the constant diagram $\Delta X : I \rightarrow \mathbf{C}$ which maps every object to X and every morphism to 1_X . The limit construction is a functor $\varprojlim : \mathbf{C}^I \rightarrow \mathbf{C}$ that maps each diagram $D \in \mathbf{C}^I$ to its limit $\varprojlim D$.

The cones over $D : I \rightarrow \mathbf{C}$ with vertex X is the hom-set $\mathbf{C}^I(\Delta X, D)$.

The cones over $D : I \rightarrow \mathbf{C}$ with vertex X correspond one-to-one with $\mathbf{C}(X, \varprojlim D)$.

If \mathbf{C} has all limits of shape I , then

$$\mathbf{C}^I(\Delta X, D) \cong \mathbf{C}(X, \varprojlim D)$$

$$\varinjlim \dashv \Delta \dashv \varprojlim$$

Uniqueness

Theorem

$$\begin{array}{ccccc} \mathbf{C} & \xrightarrow{\quad F \quad} & \mathbf{D} & \xrightarrow{\quad F' \quad} & \mathbf{E} \\ & \xleftarrow{\quad G \quad} & & \xleftarrow{\quad G' \quad} & \\ \end{array} \quad \Rightarrow \quad \begin{array}{ccccc} \mathbf{C} & \xrightarrow{\quad F'F \quad} & & & \mathbf{E} \\ & \xleftarrow{\quad G'G \quad} & & & \end{array}$$

Theorem

Adjoints are unique up to natural isomorphism. If $F \dashv G$ and $F \dashv G'$ then $G \cong G'$. If $F \dashv G$ and $F' \dashv G$ then $F \cong F'$.

Theorem

If $F \dashv G$ and $G \cong G'$ then $F \dashv G'$. If $F \dashv G$ and $F \cong F'$ then $F' \dashv G$.

Left/Right Adjoint via Unit/Counit

Theorem

Functors $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{G} \end{array} \mathbf{D}$ are adjoint iff there are two natural transformations $\eta : 1_{\mathbf{C}} \rightarrow GF$ and $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$ s.t.

$$\begin{array}{ccc} F & \xrightarrow{F\eta} & FGF \\ & \searrow 1_F & \downarrow \varepsilon F \\ & F & \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{\eta G} & GFG \\ & \searrow 1_G & \downarrow G\varepsilon \\ & G & \end{array}$$

The natural transformations η and ε are called the *unit* and *counit* of the adjunction.

Remark: The triangle identities have the virtue of being entirely “algebraic” — no quantifiers, limits, Hom-sets, infinite conditions, etc. Thus, anything defined by adjunctions such as free groups, product spaces, quantifiers, ... can be defined equationally.

$X \xrightarrow{f} Y$	Topology	Category	$C \xrightleftharpoons[G]{F} D$
$fg = 1_Y$ $gf = 1_X$ equality	homeomorphism between spaces	isomorphism $C \cong D$	$FG = 1_D$ $GF = 1_C$ equality
$fg \cong 1_Y$ $gf \cong 1_X$ homotopy	homotopy equivalence between spaces	equivalence $C \simeq D$	$FG \cong 1_D$ $GF \cong 1_C$ natural isomorphism
		adjunction $F \dashv G$	$\eta : 1_C \rightarrow GF$ $\varepsilon : FG \rightarrow 1_D$ natural transformation

Every sufficiently good analogy is yearning to become a functor.

— John Baez

Adjunctions and Equivalent Categories

- An equivalence between categories **C** and **D** is a pair of functors

$\begin{array}{ccc} \mathbf{C} & \xrightleftharpoons[F]{G} & \mathbf{D} \end{array}$ and a pair of natural *isomorphisms* $\eta : 1_{\mathbf{C}} \rightarrow GF$ and $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$.

- An adjunction between categories **C** and **D** is a pair of functors

$\begin{array}{ccc} \mathbf{C} & \xrightleftharpoons[F]{G} & \mathbf{D} \end{array}$ and a pair of natural *transformations* $\eta : 1_{\mathbf{C}} \rightarrow GF$ and $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$ s.t.

$$\begin{array}{ccc} F & \xrightarrow{F\eta} & FGF \\ & \searrow 1_F & \downarrow \varepsilon_F \\ & F & \end{array} \quad \begin{array}{ccc} G & \xrightarrow{\eta G} & GFG \\ & \searrow 1_G & \downarrow G\varepsilon \\ & G & \end{array}$$

Theorem

If there is an equivalence $\begin{array}{ccc} \mathbf{C} & \xrightleftharpoons[F]{G} & \mathbf{D} \end{array}$ and a pair of natural isomorphisms $\eta : 1_{\mathbf{C}} \rightarrow GF$ and $\gamma : FG \rightarrow 1_{\mathbf{D}}$, then there is an adjunction $F \dashv G$ with unit η and counit $\varepsilon : FG \xrightarrow{FG\gamma^{-1}} FGF \xrightarrow{F\eta^{-1}G} FG \xrightarrow{\gamma} 1_{\mathbf{D}}$.

Let $\theta : \mathbf{D}(F-, -) \rightarrow \mathbf{C}(-, G-)$ be the natural isomorphism witnessing $F \dashv G$. For any $A \in \mathbf{C}$, there is a distinguished morphism $\eta_A := \theta_{A, FA} 1_{FA} : A \rightarrow G(FA)$.

$$\frac{1_{FA} : FA \rightarrow FA}{\eta_A : A \rightarrow G(FA)}$$

In fact, we can recover θ from η as follows, for $g : FA \rightarrow B$,

$$\theta_{A, BG} = \theta_{A, B}(g \circ 1_{FA}) = Gg \circ \theta_{A, FA}(1_{FA}) = Gg \circ \eta_A$$

$$\begin{array}{ccc}
 \mathbf{D}(FA, FA) & \xrightarrow{\theta_{A, FA}} & \mathbf{C}(A, GFA) \\
 \mathbf{D}(FA, g) \downarrow & & \downarrow \mathbf{C}(A, Gg) \\
 \mathbf{D}(FA, B) & \xrightarrow{\theta_{A, B}} & \mathbf{C}(A, GB)
 \end{array}$$

Similarly, for any $B \in \mathbf{D}$, there is a distinguished morphism
 $\varepsilon_B := \theta_{GB,B}^{-1} 1_{GB} : F(GB) \rightarrow B$.

$$\frac{1_{GB} : GB \rightarrow GB}{\varepsilon_B : F(GB) \rightarrow B}$$

In fact, we can recover θ^{-1} from ε as follows, for $f : A \rightarrow GB$,

$$\theta_{A,B}^{-1} f = \theta_{A,B}^{-1} (1_{GB} \circ f) = \theta_{GB,B}^{-1} 1_{GB} \circ Ff = \varepsilon_B \circ Ff$$

$$\begin{array}{ccc}
 \mathbf{D}(FGB, B) & \xleftarrow{\theta_{GB,B}^{-1}} & \mathbf{C}(GB, GB) \\
 \downarrow & & \downarrow \\
 \mathbf{D}(Ff, B) & & \mathbf{C}(f, GB) \\
 \downarrow & & \downarrow \\
 \mathbf{D}(FA, B) & \xleftarrow{\theta_{A,B}^{-1}} & \mathbf{C}(A, GB)
 \end{array}$$

- $1_{FA} = \varepsilon_{FA} \circ F(\eta_A)$ (substitut FA for B and η_A for f)
- $1_{GB} = G(\varepsilon_B) \circ \eta_{GB}$ (substitut GB for A and ε_B for g)

$$\begin{array}{ccc}
FA & \xrightarrow{1_{FA}} & FA \\
& & A \xrightarrow{\eta_A} GFA \\
\\
FA & \xrightarrow{f} & B \\
& & A \xrightarrow{\eta_A} GFA \xrightarrow{Gf} GB \\
\\
GB & \xrightarrow{1_{GB}} & GB \\
& & FGB \xrightarrow{\varepsilon_B} B \\
\\
A & \xrightarrow{g} & GB \\
& & FA \xrightarrow{Fg} FGB \xrightarrow{\varepsilon_B} B
\end{array}$$

Theorem

- Functors $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{G} \end{array} \mathbf{D}$ are adjoint iff there is a natural transformation $\eta : 1_{\mathbf{C}} \rightarrow GF$, for which for any $f : A \rightarrow GB$ in \mathbf{C} there is a unique $g : FA \rightarrow B$ in \mathbf{D} s.t. $f = Gg \circ \eta_A$.

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(FA) \\ & \searrow f & \downarrow Gg \\ & & GB \end{array}$$

- Functors $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{G} \end{array} \mathbf{D}$ are adjoint iff there is a natural transformation $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$, for which for any $g : FA \rightarrow B$ in \mathbf{D} there is a unique $f : A \rightarrow GB$ in \mathbf{C} s.t. $g = \varepsilon_B \circ Ff$.

$$\begin{array}{ccc} B & \xleftarrow{\varepsilon_B} & F(GB) \\ & \swarrow g & \uparrow Ff \\ & & FA \end{array}$$

Lemma

Given $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\[-1ex] \perp \\[-1ex] \xleftarrow{G} \end{array} \mathbf{D}$, with counit $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$,

- ▶ G is faithful iff ε_B is an epimorphism for all B .
- ▶ G is full and faithful iff ε_B is an isomorphism for all B .

Definition

An adjunction where G is full and faithful is called a *reflection*.

Definition (Reflective Subcategory)

A full subcategory $i : \mathbf{C} \hookrightarrow \mathbf{D}$ is *reflective* if the inclusion functor i has a left adjoint $r \dashv i$:

$$\mathbf{C} \begin{array}{c} \xleftarrow{r} \\[-1ex] \perp \\[-1ex] \xrightarrow{i} \end{array} \mathbf{D}$$

Adjoint Equivalence

Definition (Adjoint Equivalence)

Functors $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \xleftarrow{G} \end{array} \mathbf{D}$ are *adjoint equivalent* iff there is an adjunction $F \dashv G$, and the unit $\eta : 1_{\mathbf{C}} \rightarrow GF$ and the counit $\varepsilon : FG \rightarrow 1_{\mathbf{D}}$ are natural isomorphisms.

Theorem

Let $(F, G, \eta, \varepsilon)$ be an adjoint equivalence. Then

1. $(F, G, \eta, \varepsilon)$ is an equivalence of categories.
 2. $(G, F, \varepsilon^{-1}, \eta^{-1})$ is also an adjoint equivalence.
 3. $F \dashv G \dashv F$
1. Adjunctions may or may not be equivalences.
e.g. $- \times B \dashv (-)^B$ is not an equivalence, as the counit $\varepsilon_A : A^B \times B \rightarrow A$ is not invertible.
 2. Equivalences may or may not be adjunctions.
 3. If $F \dashv G \dashv F$, then (F, G) may or may not be an equivalence.

Theorem

If $(F, G, \eta, \varepsilon)$ is an equivalence, then there exists a unique $\varepsilon_0 : FG \rightarrow 1_D$ such that $(F, G, \eta, \varepsilon_0)$ is an adjoint equivalence.

Proof Sketch.

η and ε may not satisfy the triangle identity. Define ε_0 to be

$$\begin{array}{ccc} FGFG & \xrightarrow{F\eta^{-1}G} & FG \\ FG\varepsilon^{-1} \uparrow & & \downarrow \varepsilon \\ FG & \xrightarrow{\varepsilon_0} & 1_D \end{array}$$

the following diagram commutes,

$$\begin{array}{ccccc} F & \xrightarrow{\varepsilon^{-1}F} & FGF & & \\ \swarrow F\eta & & \searrow F\eta GF & & \\ FGF & \xrightarrow{FG\varepsilon^{-1}F} & FGFGF & & \\ \swarrow \varepsilon_0 F & & \searrow F\eta^{-1}GF & & \\ F & \xleftarrow{\varepsilon F} & FGF & & \end{array}$$

which gives a triangle identity $\varepsilon_0 F \circ F\eta = 1_F$.

Fixpoint Equivalence of an Adjunction

Definition (Fixpoint Equivalence of an Adjunction)

Let $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\[-1ex] \perp \\[-1ex] \xleftarrow{G} \end{array} \mathbf{D}$ be a pair of adjoint functors.

- and object $A \in \mathbf{C}$ is a fixpoint of the adjunction if its adjunction unit is an isomorphism

$$\eta_A : A \xrightarrow{\cong} GFA$$

and write $\mathbf{C}_{\text{fix}} \hookrightarrow \mathbf{C}$ for the full subcategory on these fixed objects;

- and object $B \in \mathbf{D}$ is a fixpoint of the adjunction if its adjunction counit is an isomorphism

$$\varepsilon_B : FGB \xrightarrow{\cong} B$$

and write $\mathbf{D}_{\text{fix}} \hookrightarrow \mathbf{D}$ for the full subcategory on these fixed objects.

Theorem: Then the adjunction (co-)restricts to an adjoint equivalence on these full subcategories of fixed points:

$$\mathbf{C}_{\text{fix}} \begin{array}{c} \xrightarrow{F} \\[-1ex] \cong \perp \\[-1ex] \xleftarrow{G} \end{array} \mathbf{D}_{\text{fix}}$$

Fixpoint Equivalence of an Adjunction

$$\begin{array}{ccc} \mathbf{C} & \xrightleftharpoons[\quad G \quad]{\quad F \quad} & \mathbf{D} \\ \downarrow & & \downarrow \\ \mathbf{C}_{\text{fix}} & \xrightleftharpoons[\quad G \quad]{\quad F \quad \simeq \perp \quad} & \mathbf{D}_{\text{fix}} \end{array}$$

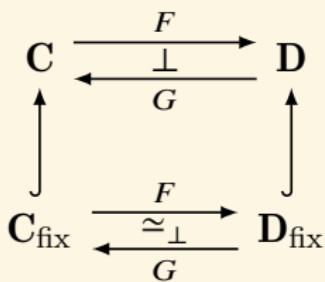
Proof.

- for $A \in \mathbf{C}_{\text{fix}} \hookrightarrow \mathbf{C}$, since η_A is an isomorphism in \mathbf{C} , ε_{FA} is an isomorphism in \mathbf{D} .
- for $B \in \mathbf{D}_{\text{fix}} \hookrightarrow \mathbf{D}$, since ε_B is an isomorphism in \mathbf{D} , η_{GB} is an isomorphism in \mathbf{C} .

$$\begin{array}{ccc} FA & \xrightarrow{F\eta_A} & FGFA \\ & \searrow 1_{FA} & \downarrow \varepsilon_{FA} \\ & FA & \end{array} \quad \begin{array}{ccc} GB & \xrightarrow{\eta_{GB}} & GFGB \\ & \searrow 1_{GB} & \downarrow G\varepsilon_B \\ & GB & \end{array}$$

Digression — Dialectical Interpretations

"All things are in flux; the flux is subject to a unifying measure or rational principle. This principle (logos, the hidden harmony behind all change) bound opposites together in a unified tension, which is like that of a lyre, where a stable harmonious sound emerges from the tension of the opposing forces that arise from the bow bound together by the string." — Heraclitus



"The technical advances forged by category theorists will be of value to dialectical philosophy. ... Of course this will require that philosophers learn mathematics and that mathematicians learn philosophy."

— Lawvere

1. We may think of (F, G) as establishing a contradiction between \mathbf{C} and \mathbf{D} . The equivalence $\mathbf{C}_{\text{fix}} \simeq \mathbf{D}_{\text{fix}}$ is then the unity of opposites.
2. We may think of F as the thesis, its right adjoint G as the antithesis, and the adjunction itself $F \dashv G$ as the synthesis.

Example

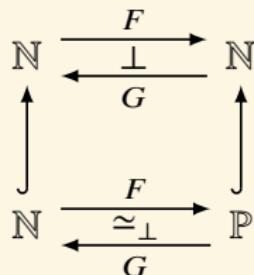
Take $\mathbf{C} = \mathbf{D} = (\mathbb{N}, \geq)$.

$$F(m) := \begin{cases} 0 & \text{if } m = 0 \\ \text{the } m\text{-th prime number} & \text{if } m > 0 \end{cases}$$

$$G(n) := \text{the number of primes } \leq n$$

$$\frac{F(m) \geq n}{m \geq G(n)}$$

- $m \geq GF(m)$ for all $m \in \mathbb{N}$.
- $FG(n) \geq n$ iff $n \in \mathbb{P}$.



Left/Right Adjoint $L \dashv T \dashv R$ ☺

- ▶ Let $L : N \rightarrow N$:: $n \mapsto 2n$ and $R : N \rightarrow N$:: $n \mapsto 2n + 1$.
- ▶ There is a third functor $T : N \rightarrow N$ satisfying $L \dashv T \dashv R$.
 1. The triple $L \dashv T \dashv R$ expresses the *unity* by the idempotency of $(R \circ T)^2 = R \circ T$ and $(L \circ T)^2 = L \circ T$.
 2. it expresses the *opposition* between L and R by an entailed adjunction $L \circ T \dashv R \circ T$.
 3. it expresses the *identity* by the entailed equivalence $T \circ L \cong T \circ R$.
- ▶ For our poset example N , when T exists it must satisfy $T \circ L = 1_N = T \circ R$, which indicates as definition for T :

$$T(n) := \begin{cases} \frac{n}{2} & n \in N_{\text{even}} \\ \frac{n-1}{2} & n \in N_{\text{odd}} \end{cases}$$

- ▶ The idempotent comonad $\text{sk} = L \circ T$ and the idempotent monad $\text{cosk} = R \circ T$:

$$\text{sk}(n) = \begin{cases} n & n \in N_{\text{even}} \\ n - 1 & n \in N_{\text{odd}} \end{cases} \quad \text{and} \quad \text{cosk}(n) = \begin{cases} n + 1 & n \in N_{\text{even}} \\ n & n \in N_{\text{odd}} \end{cases}$$

Hegel's Aufhebung

- ▶ A *localization* of a category \mathbf{A} with finite limits is a reflective subcategory $\mathbf{B} \xhookrightarrow{i_*} \mathbf{A}$ whose reflection preserves finite limits. The localization is called *essential* when the reflection i^* has furthermore a left adjoint $i_! \dashv i^* \dashv i_*$.
- ▶ When \mathbf{A} is a topos, \mathbf{B} is called an essential subtopos.
- ▶ An essential subtopos $\mathbf{A}_i \hookrightarrow \mathbf{A}$ is called a level of \mathbf{A} .
- ▶ An adjoint triple $i_! \dashv i^* \dashv i_*$ yields two adjoint modalities $\square_i \dashv \bigcirc_i$ on \mathbf{A} .
 $\square_i := i_! i^*$ and $\bigcirc_i := i^* i_*$.
- ▶ The modalities yield notions of modal types
 1. (*i*-sheaves) $X \in \mathbf{A}$ with $\bigcirc_i X \cong X$.
 2. (*i*-skeleta) $X \in \mathbf{A}$ with $\square_i X \cong X$.
- ▶ We say that the level i is lower than level j , (written $i < j$) when
 1. every i -sheaf is a j -sheaf: $\bigcirc_j \bigcirc_i = \bigcirc_i$
 2. every i -skeleton is a j -skeleton: $\square_j \square_i = \square_i$
- ▶ Let $i < j$, we say that the level j resolves the opposite of level i , (written $i \ll j$) when $\bigcirc_j \square_i = \square_i$.
- ▶ A level \bar{i} is called the **Aufhebung** of level i iff it is a minimal level which resolves the opposites of level i .

Example — Left/Right Adjoint & Unit/Counit $+ \dashv \Delta \dashv \times$

$$\mathbf{C} \times \mathbf{C}(\Delta X, (A, B)) \cong \mathbf{C}(X, A \times B)$$

$$\eta : 1_{\mathbf{C}} \rightarrow \times \circ \Delta$$

$$\varepsilon : \Delta \circ \times \rightarrow 1_{\mathbf{C} \times \mathbf{C}}$$

$$\begin{array}{ccc} & A & \\ \Delta \swarrow & \downarrow \eta & \searrow \Delta \\ (A, A) & & A \times A \\ & \searrow \times & \\ & & (A \times B, A \times B) \\ & & \downarrow (\pi_1, \pi_2) \\ & & (A, B) \\ & & \nearrow \times \\ & & A \times B \end{array}$$

$$\mathbf{C}(A + B, X) \cong \mathbf{C} \times \mathbf{C}((A, B), \Delta X)$$

$$\eta : 1_{\mathbf{C} \times \mathbf{C}} \rightarrow \Delta \circ +$$

$$\varepsilon : + \circ \Delta \rightarrow 1_{\mathbf{C}}$$

$$\begin{array}{ccc} & (A, B) & \\ + \swarrow & \downarrow (\iota_1, \iota_2) & \searrow + \\ A + B & & (A + B, A + B) \\ & \searrow \Delta & \\ & & A + A \\ & & \downarrow \varepsilon \\ & & (A, A) \\ & & \nearrow + \\ & & A \end{array}$$

Example — Left/Right Adjoint & Unit/Counit

$- \times B \dashv (-)^B$

$$\text{Hom}(A \times B, C) \cong \text{Hom}(A, C^B)$$

$$\eta_A : A \rightarrow (A \times B)^B$$

$$\varepsilon_A : A^B \times B \rightarrow A$$

$$\begin{array}{ccc} & A & \\ A \times B & \begin{array}{c} \nearrow - \times B \\ \downarrow \eta \\ \searrow (-)^B \end{array} & (A \times B)^B \\ & \varepsilon & \\ A^B \times B & \begin{array}{c} \nearrow - \times B \\ \downarrow \varepsilon \\ \searrow (-)^B \end{array} & A^B \\ & \downarrow & \\ & A & \end{array}$$

$$\frac{A \wedge B \vdash C}{A \vdash B \rightarrow C}$$

$$\begin{aligned} \eta_A : A \rightarrow B \rightarrow A \wedge B \\ \varepsilon_A : (B \rightarrow A) \wedge B \rightarrow A \end{aligned}$$

Left/Right Adjoint via Universal Property

- A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ has a right adjoint, iff, for any $B \in \mathbf{D}$, there is an object $GB \in \mathbf{C}$ and a morphism $\varepsilon_B : F(GB) \rightarrow B$ such that (GB, ε_B) is a universal morphism from F to B .

$$\begin{array}{ccc} B & \xleftarrow{\varepsilon_B} & F(GB) \\ & \swarrow g & \uparrow Ff \\ & & FA \end{array}$$

- A functor $G : \mathbf{D} \rightarrow \mathbf{C}$ has a left adjoint, iff, for any $A \in \mathbf{C}$, there is an object $FA \in \mathbf{D}$ and a morphism $\eta_A : A \rightarrow G(FA)$ such that (FA, η_A) is a universal morphism from A to G .

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(FA) \\ & \searrow f & \downarrow Gg \\ & & GB \end{array}$$

Universality \equiv Adjunctions

Example — Extension Problem

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(FA) \\ & \searrow f & \downarrow G\hat{f} \\ & & GB \end{array}$$

1. We often start with a set A .

Example: take $A := \{x, y, z\}$ to be a set with three elements.

2. The elements in A are then used as building blocks to construct a bigger mathematical object FA , which contains the original A and more.

Example: take $FA := \{ax + by + cz : a, b, c \in \mathbb{R}\}$ to be the three-dimensional real vector space with basis A .

3. As a consequence, we observe that whenever another object also “contains” A , it automatically contains FA , too.

Example: if B is any vector space and there is a mapping f from A to GB , then you automatically have a linear transformation $\hat{f} : FA \rightarrow B$. In other word, \hat{f} is the unique map that extends f linearly from the basis set A to the entire vector space FA .

Theorem (Continuity)

- ▶ Right adjoints preserve limits.
- ▶ Left adjoints preserve colimits.

Proof.

Given $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{G} \end{array} \mathbf{D}$, assume limits of shape \mathbf{I} exist in both \mathbf{C} and \mathbf{D} .

Define $F_*(D) := FD$ and $G_*(D) := GD$. Then it's easy to see that

$$\mathbf{C}^{\mathbf{I}} \begin{array}{c} \xrightarrow{F_*} \\ \perp \\ \xleftarrow{G_*} \end{array} \mathbf{D}^{\mathbf{I}}$$

Since the diagram of right adjoints of the functors in a commutative square commutes up to natural isomorphism, then

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{F} & \mathbf{D} \\ \Delta \downarrow & & \downarrow \Delta \\ \mathbf{C}^{\mathbf{I}} & \xrightarrow{F_*} & \mathbf{D}^{\mathbf{I}} \end{array} \quad \Rightarrow \quad \begin{array}{ccc} \mathbf{C} & \xleftarrow{G} & \mathbf{D} \\ \lim_{\leftarrow} \uparrow & & \uparrow \lim_{\leftarrow} \\ \mathbf{C}^{\mathbf{I}} & \xleftarrow{G_*} & \mathbf{D}^{\mathbf{I}} \end{array}$$
$$G \varprojlim D \cong \varprojlim GD$$

Example

- ▶ Right adjoints preserve limits.

$$\frac{C \rightarrow A \wedge B}{(C \rightarrow A) \wedge (C \rightarrow B)} - \wedge C \dashv C \rightarrow -$$

$$\frac{\forall x(Ax \wedge Bx)}{\forall x Ax \wedge \forall x Bx} \exists \dashv \pi^* \dashv \forall$$

- ▶ Left adjoints preserve colimits.

$$\frac{(A \vee B) \wedge C}{(A \wedge C) \vee (B \wedge C)} - \wedge C \dashv C \rightarrow -$$

$$\frac{\exists x(Ax \vee Bx)}{\exists x Ax \vee \exists x Bx} \exists \dashv \pi^* \dashv \forall$$

Theorem

Fully faithful functor reflects limits and colimits.

Proof.

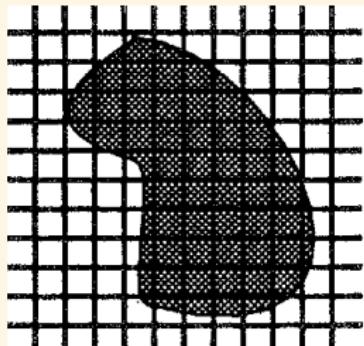
If F is fully faithful and $FL \cong \varprojlim FD$, one may sketch the proof for $L \cong \varprojlim D$ as follows:

$$\frac{\frac{\frac{\Delta C \rightarrow D}{\Delta FC \rightarrow FD} (F \text{ fully faithful})}{FC \rightarrow \varprojlim FD} (\Delta \dashv \varprojlim)}{FC \rightarrow FL \cong \varprojlim FD} (FL \cong \varprojlim FD)$$
$$C \rightarrow L \quad (F \text{ fully faithful})$$

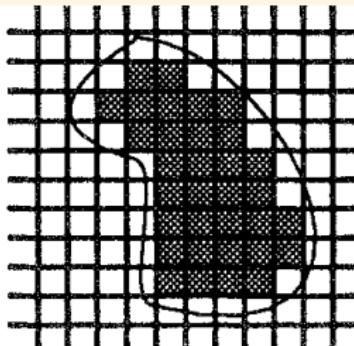
Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References

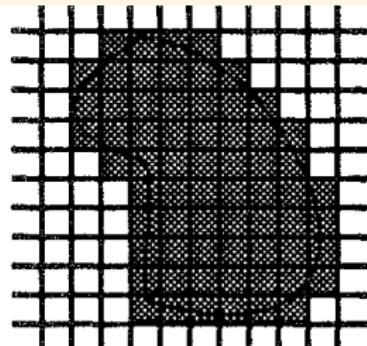
Left/Right Adjoint



A



$\square A$



$\diamond A$

$\square A$ squares that are completely covered by A .

$\diamond A$ squares that are partly or totally covered by A .

$$\frac{\diamond A \subset B}{A \subset \square B} \quad \diamond \dashv \square$$

Left/Right Adjoint

Example

Assume $R \subset X \times Y$, and let $F_R : P(X) \rightarrow P(Y) :: A \mapsto \bigcup_{x \in A} \{y : Rxy\}$.

This has a right adjoint $[R] : P(Y) \rightarrow P(X)$:

$$\frac{F_R(A) \subset B}{A \subset [R]B}$$

The definition of $[R]$ which satisfies this condition is:

$$[R]B := \{x : \forall y (Rxy \rightarrow y \in B)\}$$

If we take $X = Y = W$ and (W, R) as the Kripke frame for modal logic, then $[R]$ gives the usual Kripke semantics for \Box .

Left/Right Adjoint $\exists_f \dashv f^* \dashv \forall_f$

Example

Given a function $f : X \rightarrow Y$, consider

$$f^* : P(Y) \rightarrow P(X) :: B \mapsto \{x \in X : fx \in B\}.$$

Take the subset $B \subset Y$ as a predicate $B(y)$ over Y , and f^*B as $f^*B(x)$ over X .

$$\text{By the pullback, } f^*B(x) = B(fx) =: (Bf)(x).$$

Then f^* has both a left and a right adjoint $\exists_f, \forall_f : P(X) \rightarrow P(Y)$.

$$\begin{array}{ccc} f^*B & \longrightarrow & B \\ \downarrow & \lrcorner & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

$$\frac{A \subset f^*B}{\exists_f A \subset B} \quad \frac{f^*B \subset A}{B \subset \forall_f A} \quad \text{i.e.} \quad \frac{A \vdash_X Bf}{\exists_f A \vdash_Y B} \quad \frac{Bf \vdash_X A}{B \vdash_Y \forall_f A}$$

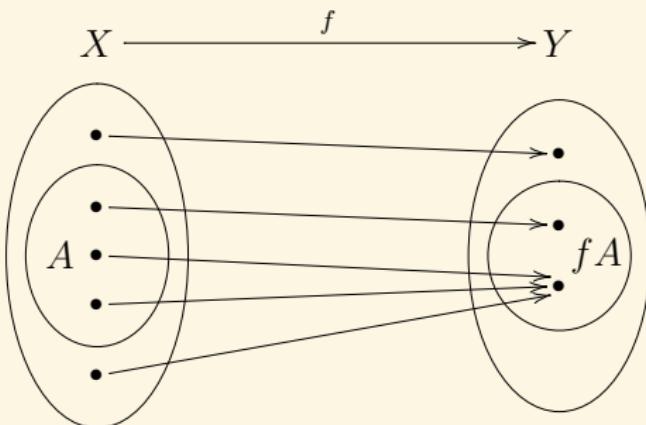
$$\boxed{\exists_f \dashv f^* \dashv \forall_f}$$

The unique functions satisfying these conditions can be defined as

$$\exists_f A := \bigcap \{B : A \subset f^*B\} = fA = \{y \in Y : \exists x (fx = y \wedge x \in A)\}$$

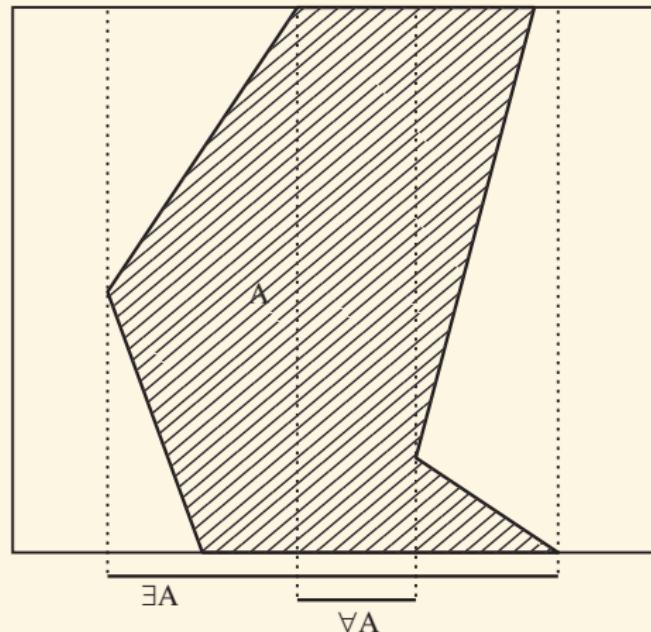
$$\forall_f A := \bigcup \{B : f^*B \subset A\} = \{y \in Y : f^*y \subset A\} = \{y \in Y : \forall x (fx = y \rightarrow x \in A)\}$$

Quantifiers are Adjoints



$$\frac{A \subset f^{-1}B}{fA \subset B}$$

$$\frac{A \vdash_X Bf}{\exists_f A \vdash_Y B}$$



$$\begin{array}{c}
 \exists_f \longrightarrow \\
 \perp \\
 P(X) \leftarrow f^* \longrightarrow P(Y) \\
 \perp \\
 \forall_f \longrightarrow
 \end{array}$$

$$\exists_{\pi} \dashv \pi^* \dashv \forall_{\pi}$$

Let f be the projection $\pi : X \times Y \rightarrow X$. Hence $\pi^* : \mathbf{P}(X) \rightarrow \mathbf{P}(X \times Y)$.

$$\begin{array}{ccc} \pi^* B & \longrightarrow & B \\ \downarrow & \lrcorner & \downarrow i \\ X \times Y & \xrightarrow{\pi} & X \end{array}$$

By the pullback, $\pi^* B(x, y) = B\pi(x, y)$.

Then π^* has both a left and a right adjoint $\exists_{\pi}, \forall_{\pi} : \mathbf{P}(X \times Y) \rightarrow \mathbf{P}(X)$.

$$\boxed{\exists_{\pi} \dashv \pi^* \dashv \forall_{\pi}}$$

We write $\exists_{\pi} A$ as $\exists y A(x, y)$, $\forall_{\pi} A$ as $\forall y A(x, y)$, and \subset as \vdash .

$$\exists y A(x, y) = \exists_{\pi} A = \{x \in X : \exists y. (x, y) \in A\}$$

$$\forall y A(x, y) = \forall_{\pi} A = \{x \in X : \forall y. (x, y) \in A\}$$

$$\frac{A \subset \pi^* B}{\exists_{\pi} A \subset B}$$

$$\frac{\pi^* B \subset A}{B \subset \forall_{\pi} A}$$

$$\frac{A(x, y) \vdash_{X \times Y} B(x)}{\exists y A(x, y) \vdash_X B(x)}$$

$$\frac{B(x) \vdash_{X \times Y} A(x, y)}{B(x) \vdash_X \forall y A(x, y)}$$

Quantifiers are Adjoints

For a list $\mathbf{x} = x_1, \dots, x_n$ of distinct variables, let $\text{Form}(\mathbf{x})$ be the set of formulas that has at most \mathbf{x} free. Then $\text{Form}(\mathbf{x})$ is a preorder under \vdash . Let y be a variable not in \mathbf{x} . We have a trivial operation

$$*: \text{Form}(\mathbf{x}) \rightarrow \text{Form}(\mathbf{x}, y)$$

The operation $*$ is trivially a functor, since

$$A(\mathbf{x}) \vdash B(\mathbf{x}) \text{ in } \text{Form}(\mathbf{x}) \implies A(\mathbf{x}, y) \vdash B(\mathbf{x}, y) \text{ in } \text{Form}(\mathbf{x}, y)$$

For any $A \in \text{Form}(\mathbf{x}, y)$, obviously $y \notin \text{Fv}(\exists y A)$ and $y \notin \text{Fv}(\forall y A)$. We have $\exists y / \forall y : \text{Form}(\mathbf{x}, y) \rightarrow \text{Form}(\mathbf{x})$.

Quantifiers are adjoints $\exists \dashv * \dashv \forall$.

Conversely, we could take $\exists \dashv * \dashv \forall$ as basic and derive the customary introduction and elimination rules from it. $\forall x A(x, y) \vdash A(x, y)$ is just the counit of $* \dashv \forall$, and $A(x, y) \vdash \exists y A(x, y)$ is the unit of $\exists \dashv *$.

$$\forall x A(x, y) \vdash A(x, y) \quad (\text{counit of } * \dashv \forall)$$

$$A(x, y) \vdash \exists y A(x, y) \quad (\text{unit of } \exists \dashv *)$$

$$\forall x A(x, y) \vdash \exists y A(x, y) \quad (\text{transitivity of } \vdash)$$

$$\exists y \forall x A(x, y) \vdash \exists y A(x, y) \quad (\exists \dashv *)$$

$$\exists y \forall x A(x, y) \vdash \forall x \exists y A(x, y) \quad (* \dashv \forall)$$

Quantifiers are Adjoints

Given a wff A . Let $\llbracket A \rrbracket := \{(\mathbf{b}, a) : \mathcal{M} \models A[\mathbf{b}, a]\}$. Take the projection $\pi : (\mathbf{b}, a) \mapsto \mathbf{b}$. It can be regarded as $\pi : v(a/x) \mapsto v$.

$$\boxed{\exists_\pi \dashv \pi^* \dashv \forall_\pi}$$

$$\frac{\llbracket A \rrbracket \subset \pi^* \llbracket B \rrbracket}{\exists_\pi \llbracket A \rrbracket \subset \llbracket B \rrbracket} \quad \frac{\pi^* \llbracket B \rrbracket \subset \llbracket A \rrbracket}{\llbracket B \rrbracket \subset \forall_\pi \llbracket A \rrbracket}$$

Explicitly,

$$\begin{aligned}\exists_\pi \llbracket A \rrbracket &= \left\{ \mathbf{b} : \exists a \left(\mathcal{M} \models A[\mathbf{b}, a] \right) \right\} = \bigcup_{a \in M} \left\{ v : \mathcal{M}, v(a/x) \models A \right\} \\ \forall_\pi \llbracket A \rrbracket &= \left\{ \mathbf{b} : \forall a \left(\mathcal{M} \models A[\mathbf{b}, a] \right) \right\} = \bigcap_{a \in M} \left\{ v : \mathcal{M}, v(a/x) \models A \right\}\end{aligned}$$

And we have

$$\llbracket \exists x A \rrbracket = \exists_\pi \llbracket A \rrbracket \quad \llbracket \forall x A \rrbracket = \forall_\pi \llbracket A \rrbracket$$

Internal Logic

Logical operator	Operation on $\text{Sub}(A)$
truth: T	top element (A itself)
falsity: \perp	bottom element (strict initial object)
conjunction: \wedge	intersection (pullback)
disjunction: \vee	union
implication: \rightarrow	Heyting implication
existential quantification: \exists	left adjoint to pullback
universal quantification: \forall	right adjoint to pullback

Lawvere Theory

Definition (Lawvere Theory)

A *Lawvere theory* is a category \mathbf{T} with finite products and with a distinguished object A such that every object of \mathbf{T} is a finite power of A :

$$\forall X \in \mathbf{T} \exists n \in \mathbb{N} : X \cong A^n$$

- ▶ A morphism $f : A^n \rightarrow A$ is called an n -ary operation (and, in particular, $1 \rightarrow A$ are called constants).
- ▶ Every $f : A^n \rightarrow A^m$ is the tupling of m operations $f_i : A^n \rightarrow A$ ($i = 1, \dots, m$).

Definition (Model)

A *model* (or algebra) of a Lawvere theory \mathbf{T} in any category \mathbf{C} with finite products is a finite-product-preserving functor

$$\mathcal{M} : \mathbf{T} \rightarrow \mathbf{C}$$

The category of \mathbf{T} -models in \mathbf{C} is written $\text{Mod}(\mathbf{T}, \mathbf{C})$.

Functorial Semantics

- ▶ Categories with finite products give multi-sorted theories
- ▶ Categories with finite limits give essentially algebraic theories
- ▶ Regular categories give logic with \exists, \wedge, \vee
- ▶ Pretoposes give full first-order logic $\exists, \forall, \neg, \wedge, \vee$
 - ▶ a theory is a category with some structure
 - ▶ a model is a functor $\mathbf{T} \rightarrow \mathbf{Set}$ that preserves the relevant structure
 - ▶ a homomorphism between models is a natural transformation between them

Diagonalization[Law69]¹⁸

Definition (Point-Surjective)

A morphism $f : X \rightarrow Y$ is *point-surjective* iff for every $y : 1 \rightarrow Y$, there is an $x : 1 \rightarrow X$ s.t. $y = f \circ x$.

$$\begin{array}{ccc} 1 & & \\ \downarrow x & \searrow y & \\ X & \xrightarrow{f} & Y \end{array}$$

Definition (Weakly Point-Surjective)

A morphism $f : X \times Y \rightarrow Z$ is *weakly point-surjective* iff for every $g : X \rightarrow Z$, there exists $y : 1 \rightarrow Y$ such that, for all $x : 1 \rightarrow X$:

$$g \circ x = f \circ \langle x, y \rangle$$

$$\begin{array}{ccc} 1 & \xrightarrow{x} & X \\ \downarrow \langle x, y \rangle & & \downarrow g \\ X \times Y & \xrightarrow{f} & Z \end{array}$$

Theorem (Lawvere's Fixpoint Theorem)

Let \mathbf{C} be a category with a terminal object and binary products. If $f : X \times X \rightarrow Y$ is weakly point-surjective, then every $\alpha : Y \rightarrow Y$ has a fixpoint $y : 1 \rightarrow Y$.

$$\begin{array}{ccc} X \times X & \xrightarrow{f} & Y \\ \Delta \uparrow & & \downarrow \alpha \\ X & \xrightarrow{g} & Y \end{array}$$

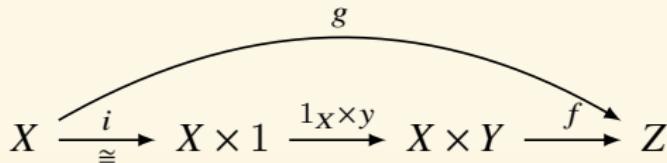
¹⁸ Lawvere: Diagonal arguments and cartesian closed categories.

Yanofsky: A universal approach to self-referential paradoxes, incompleteness and fixed points.

Definition (Representability)

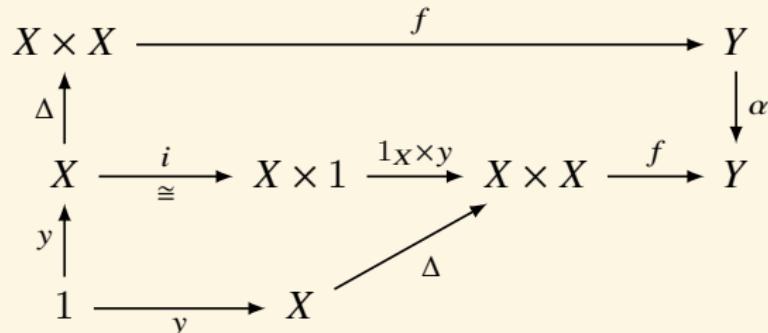
$g : X \rightarrow Z$ is representable by $f : X \times Y \rightarrow Z$ iff there exists $y : 1 \rightarrow Y$ s.t.

$$g = f \circ (1_X \times y) \circ i$$



Theorem (Another Version of Lawvere's Fixpoint Theorem)

Let \mathbf{C} be a category with a terminal object and binary products. For $f : X \times X \rightarrow Y$, $\alpha : Y \rightarrow Y$, if $\alpha \circ f \circ \Delta$ is representable by f , then $\alpha : Y \rightarrow Y$ has a fixpoint.



If $\alpha \circ f \circ \Delta$ is represented by $f(-, y)$, then

$$\alpha \circ f \circ \Delta \circ y = f \circ (1_X \times y) \circ i \circ y = f \circ \Delta \circ y$$

Observations

In the proof of Lawvere's fixpoint theorem,

- ▶ associativity of the product \times is never used
- ▶ commutativity of the product \times is never used
- ▶ unitality of the product \times with respect to 1 is never used
- ▶ projections are never used
- ▶ the universal property of \times is only used to construct the diagonals
 $\Delta : X \rightarrow X \times X$
- ▶ 1 is only used to be the domain of global elements

Another Version of Lawvere's Fixpoint Theorem

Definition (Pointed Magmoidal Category with Diagonals)

- ▶ A *magmoidal category* is a category \mathbf{C} with a functor $\otimes : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$.
- ▶ A *pointed magmoidal category* is a magmoidal category with a distinguished object T .
- ▶ A magmoidal category is said to have *diagonals* $\Delta : X \rightarrow X \otimes X$ if there is a natural transformation $\Delta : 1_{\mathbf{C}} \rightarrow \otimes \circ \Delta_{\mathbf{C}}$ from the identity functor $1_{\mathbf{C}}$ to the composite $\mathbf{C} \xrightarrow{\Delta_{\mathbf{C}}} \mathbf{C} \times \mathbf{C} \xrightarrow{\otimes} \mathbf{C}$ of \otimes with the diagonal functor $\Delta_{\mathbf{C}}$.

$$\begin{array}{ccc} X & \xrightarrow{\Delta_X} & X \otimes X \\ f \downarrow & & \downarrow f \otimes f \\ Y & \xrightarrow{\Delta_Y} & Y \otimes Y \end{array}$$

Theorem (Another Version of Lawvere's Fixpoint Theorem)

Let $(\mathbf{C}, \otimes, \Delta, T)$ be a pointed magmoidal category with diagonals. For $f : X \otimes Y \rightarrow Z$, $\alpha : Z \rightarrow Z$, $\beta : X \rightarrow Y$, if

$\forall y : T \rightarrow Y. \exists \dot{x} : T \rightarrow X. [\beta \circ \dot{x} = y]$, and if

$\exists y : T \rightarrow Y. \forall x : T \rightarrow X. [\alpha \circ f \circ (1_X \otimes \beta) \circ \Delta_X \circ x = f \circ (x \otimes y) \circ \Delta_T]$, then $\alpha \circ z = z$ for some $z : T \rightarrow Z$.

$$\begin{array}{ccccccc} X & \xrightarrow{\Delta_X} & X \otimes X & \xrightarrow{1_X \otimes \beta} & X \otimes Y & \xrightarrow{f} & Z \\ \uparrow \dot{x} & & & & & & \downarrow \alpha \\ T & \xrightarrow{\Delta_T} & T \otimes T & \xrightarrow{\dot{x} \otimes y} & X \otimes Y & \xrightarrow{f} & Z \\ \downarrow \dot{x} & & \downarrow \dot{x} \otimes \dot{x} & & & & \\ X & \xrightarrow{\Delta_X} & X \otimes X & & & & \end{array}$$

$1_X \otimes \beta$

$$\begin{aligned} \alpha \circ f \circ (1_X \otimes \beta) \circ \Delta_X \circ \dot{x} &= f \circ (\dot{x} \otimes y) \circ \Delta_T = f \circ (1_X \otimes \beta) \circ (\dot{x} \otimes \dot{x}) \circ \Delta_T \\ &= f \circ (1_X \otimes \beta) \circ \Delta_X \circ \dot{x} \end{aligned}$$

Lindenbaum Category

- ▶ Consider a first-order theory T .

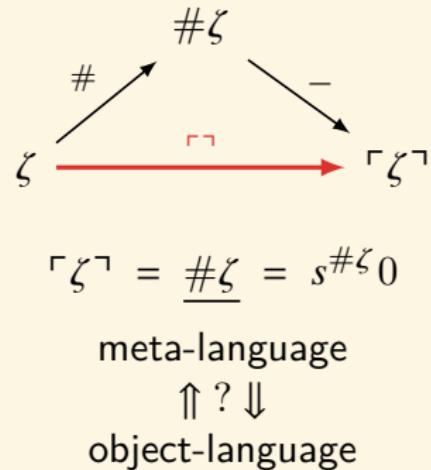
We form C_T a classifying category of T in the following way:

The C_T -objects are generated by a sort object A (more object if the theory is multi-sorted), and an object 2 , by closure under products.

C_T -morphisms	Equivalence classes of ...
$A^n \rightarrow 2$	provably equivalent wffs of n variables
$A^n \rightarrow 2 \times 2$	provably equivalent tuples of wffs of n variables
$A^n \rightarrow A$	provably equivalent terms of n variables
$1 \rightarrow 2$	sentences
$1 \rightarrow A$	constant terms
$\top : 1 \rightarrow 2$	sentences provable
$\perp : 1 \rightarrow 2$	sentences refutable
$2^n \rightarrow 2$	propositional operations e.g., $\neg : 2 \rightarrow 2$

- ▶ A theory is *consistent* iff $\text{Hom}(1, 2)$ contains at least two elements $\text{Hom}(1, 2) \supset \{\top, \perp\}$. Equivalently, there is a morphism $\neg : 2 \rightarrow 2 : \neg\varphi \neq \varphi$ for all $\varphi : 1 \rightarrow 2$.
- ▶ A theory is *complete* iff $\text{Hom}(1, 2) = \{\top, \perp\}$.

Gödel Encoding



Definition (Gödel Encoding)

Gödel encoding is a morphism $\Gamma^\dashv : \text{Hom}(A^n, 2) \rightarrow \text{Hom}(1, A)$.

Undefinability of sat

Definition (Satisfiability Predicate)

Satisfiability predicate is definable in T iff there is $\text{sat} : A \times A \rightarrow 2$ such that, for any $\varphi : A \rightarrow 2$, and for all $a : 1 \rightarrow A$: $T \vdash \text{sat}\langle a, \neg \varphi \rangle \leftrightarrow \varphi a$.

$$\begin{array}{ccc} 1 & \xrightarrow{a} & A \\ \downarrow \langle a, \neg \varphi \rangle & & \downarrow \varphi \\ A \times A & \xrightarrow[\text{sat}]{} & 2 \end{array}$$

Remark: This is exactly the condition for **weak point-surjectivity!**

Theorem (Undefinability of sat)

If T is consistent, then sat is not definable in T .

Proof.

If sat is definable in T , then \neg has a fixpoint.

$$\begin{array}{ccc} A \times A & \xrightarrow{\text{sat}} & 2 \\ \Delta \uparrow & & \downarrow \neg \\ A & \longrightarrow & 2 \end{array}$$

Truth Predicate

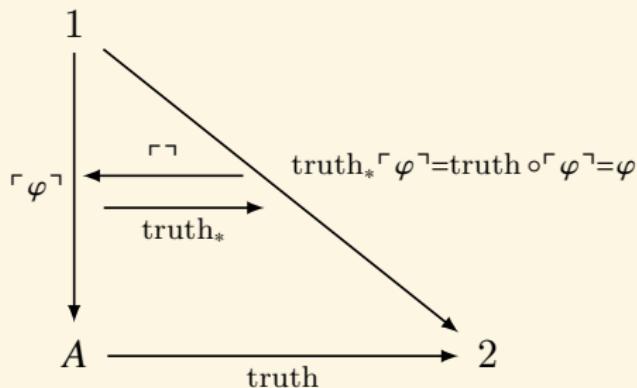
“snow is white” is true iff snow is white.

Definition (Truth Predicate)

Truth Predicate is definable in T iff there is $\text{truth} : A \rightarrow 2$ such that

$$\text{truth}_* : \text{Hom}(1, A) \rightarrow \text{Hom}(1, 2)$$

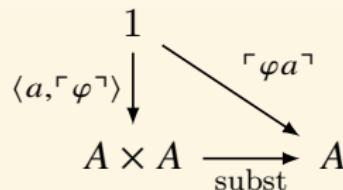
is a retraction of $\ulcorner\urcorner : \text{Hom}(1, 2) \rightarrow \text{Hom}(1, A)$, i.e., $\text{truth} \circ \ulcorner\urcorner = \varphi$.



Tarski's Undefinability of truth Theorem

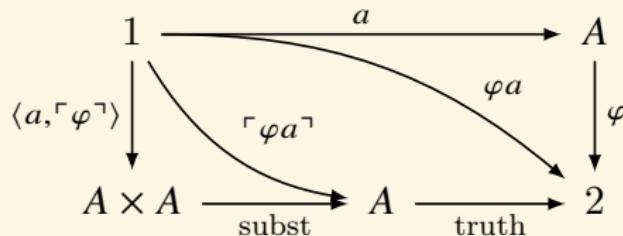
Definition (Substitution)

“*substitution*” is definable in T iff there is $\text{subst} : A \times A \rightarrow A$ such that $T \vdash \text{subst}\langle a, \ulcorner \varphi \urcorner \rangle = \ulcorner \varphi a \urcorner$.



Theorem (Tarski's Undefinability of truth Theorem)

If T is consistent and “*substitution*” is definable in T , then truth is not definable in T .



$$\text{sat} = \text{truth} \circ \text{subst}$$

Gödel's First Incompleteness Theorem

Definition (Provability Predicate)

Provability is representable in T iff there is $\text{prov} : A \rightarrow 2$ such that,

$$T \vdash \varphi \iff T \vdash \text{prov}(\ulcorner \varphi \urcorner)$$

Theorem (Gödel's First Incompleteness Theorem)

If T is consistent, and “substitution” is definable in T , and “provability” is representable, then T is not complete.

Proof.

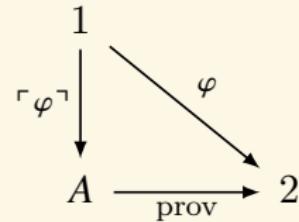
If T is complete, then $\varphi = \top$ or $\varphi = \perp$.

$\varphi = \top \implies \text{prov}(\ulcorner \varphi \urcorner) = \top$.

$\varphi = \perp \implies \text{prov}(\ulcorner \varphi \urcorner) = \perp$.

Therefore, $\text{prov} \circ \ulcorner \varphi \urcorner = \varphi$ for all $\varphi : 1 \rightarrow 2$.

Namely, truth = prov.



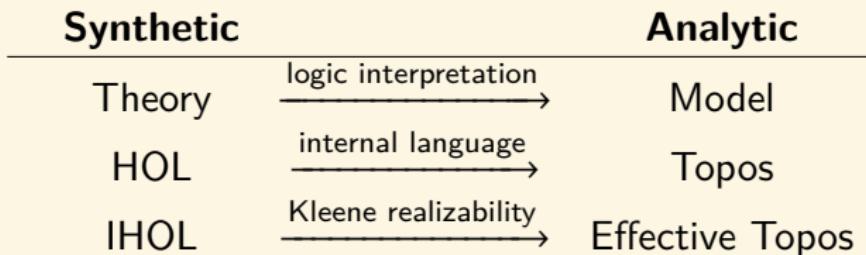
Synthetic Mathematics vs Analytic Mathematics

- ▶ Synthetic
 - ▶ Basic objects are taken as primitive.
 - ▶ Their properties & relations are axiomatized.
 - ▶ We work within the axiomatic system.
- ▶ Analytic
 - ▶ Basic objects are constructed from other objects.
 - ▶ Their properties & relations are deduced.
 - ▶ We work in a wider mathematical environment.

Example:

- ▶ Analytic geometry analyzes the plane geometry of points, lines, etc. in terms of \mathbb{R} : points are elements of \mathbb{R}^2 , lines are sets of points, etc.
- ▶ Synthetic geometry is more like the geometry of Euclid: points and lines are undefined terms, given meaning by the axioms that specify what we can do with them.
- ▶ Synthetic differential geometry: “All maps are smooth!”
- ▶ Synthetic topology: “All maps are continuous!”
- ▶ Synthetic computability: “All maps are computable!”

- ▶ Mathematics is the analysis of invariants and of the transformations that preserve them (including the analysis of non-preservations, deformations and symmetry breakings).
- ▶ We are presented with an open universe of categories, then, to which new categories are constantly added; new invariants, and new transformations. Concepts are created by being correlating with existent ones, and by deforming one into the other, thus enriching them, paying attention to the meaning of what is being done.



- ▶ In **Eff** all objects and morphisms are equipped with computability structure.
- ▶ We need not know how **Eff** is built — we just use the logic and axioms which are valid in it.

Symbol	External view of Eff	Internal view of Eff
\mathbb{N}	natural numbers	natural numbers
\mathbb{R}	computable reals	all reals
$f : \mathbb{N} \rightarrow \mathbb{N}$	computable function	any function
$e : \mathbb{N} \twoheadrightarrow A$	computable enumeration of A	any enumeration of A
$\{\perp, \top\}$	truth values	decidable truth values
Ω	truth values of Eff	truth values
$\forall x$	computably for all x	for all x
$\exists x$	there exists computable x	there exists x
$p \vee \neg p$	decision procedure for p	p or not p

Synthetic Computability

Definition (Assembly)

An assembly $\mathbf{X} = (X, \Vdash_{\mathbf{X}})$ is a set X with a realizability relation $\Vdash_{\mathbf{X}} \subset \mathbb{N} \times X$ such that

$$\forall x \in X \exists n \in \mathbb{N} : n \Vdash_{\mathbf{X}} x$$

Definition (Assembly Morphism)

An *assembly morphism* $f : \mathbf{X} \rightarrow \mathbf{Y}$ is a function $f : X \rightarrow Y$ for which

$$\exists n \in \mathbb{N} \forall x \in X \forall m \in \mathbb{N} : m \Vdash_{\mathbf{X}} x \implies \varphi_n(m) \downarrow \text{ & } \varphi_n(m) \Vdash_{\mathbf{Y}} f(x)$$

Asm is the category of assemblies.

Examples:

- ▶ Natural numbers: $\mathbf{N} = (\mathbb{N}, \Vdash_{\mathbf{N}})$ where $n \Vdash_{\mathbf{N}} m \iff n = m$.
- ▶ Partial computable functions: $\mathbf{N}^{\mathbb{N}} = (\mathcal{R}, \Vdash_{\mathbf{N}^{\mathbb{N}}})$ where \mathcal{R} is the set of partial computable functions and $n \Vdash_{\mathbf{N}^{\mathbb{N}}} f \iff \varphi_n = f$.
- ▶ Computable enumerable sets: $\mathbf{E} = (\mathbf{CE}, \Vdash_{\mathbf{E}})$ where \mathbf{CE} is the set of c.e. sets and $n \Vdash_{\mathbf{E}} A \iff A = W_n = \{m : \varphi_n(m) \downarrow\}$.

- ▶ Boolean truth values: $2 = (\{0, 1\}, \Vdash_2)$ where $n \Vdash_2 m \iff n = m$.
- ▶ Semidecidable truth values: $\Sigma = (\{\perp, \top\}, \Vdash_\Sigma)$ where
 $n \Vdash_\Sigma \top \iff \varphi_n(n) \downarrow$ and $n \Vdash_\Sigma \perp \iff \varphi_n(n) \uparrow$.
- ▶ Assembly morphisms $\mathbf{N} \rightarrow 2$ are decision procedure/sets.
- ▶ Assembly morphisms $\mathbf{N} \rightarrow \Sigma$ are semi-decision procedure/sets.
- ▶ The exponent $\Sigma^{\mathbf{N}}$ is then the collection of c.e. sets.
- ▶ We know that there is an enumeration of c.e. sets, thus a weakly point-surjective $W : N \twoheadrightarrow \Sigma^{\mathbf{N}}$.
- ▶ Hence, by Lawvere's theorem every map $\Sigma \rightarrow \Sigma$ has a fixpoint.
- ▶ It immediately follows that negation is not definable on Σ and hence c.e. sets are not closed under complements.
- ▶ Note that $W : \mathbf{N} \twoheadrightarrow \Sigma^{\mathbf{N}} \cong \Sigma^{\mathbf{N} \times \mathbf{N}} \cong \Sigma^{\mathbf{N}^{\mathbf{N}}}$, so every map $F : \Sigma^{\mathbf{N}} \rightarrow \Sigma^{\mathbf{N}}$ has a fixpoint.
- ▶ We can identify the exponent $\Sigma^{\mathbf{N}}$ with an assembly $(\mathbf{CE}, \Vdash_{\mathbf{E}})$.
- ▶ A map $F : \Sigma^{\mathbf{N}} \rightarrow \Sigma^{\mathbf{N}}$ is an enumeration operator: $F(W_e) = W_{f(e)}$ for some computable f .
- ▶ Lawvere's theorem shows that every such operator has a fixpoint:
 $W_e = W_{f(e)}$.

Scott's Reflexive Domain[SV84]¹⁹

A *reflexive domain* is a space where every object is a transformation, and every transformation corresponds uniquely to an object.



- ▶ **Po**: the category of all partially-ordered sets (posets) and monotone mappings.
- ▶ **CPo**: all posets which have a least element \perp , and such that every countable monotone chain has a supremum.
- ▶ A monotone map f is continuous iff it preserves supremums of countable chains $f(\coprod_n x_n) = \coprod_n f(x_n)$.
- ▶ By Tarski's argument, it is then clear that every continuous endomorphism $f : D \rightarrow D$ of such poset $D \in \mathbf{CPo}$ has a least fixed point, namely the supremum of the monotone sequence $\coprod_n f^n(\perp)$.
- ▶ **CCPo**: the subcategory of **CPo** obtained by restricting the morphisms to be continuous.

¹⁹J. Soto-Andrade & F. J. Varela: Self-Reference and Fixed Points: A Discussion and an Extension of Lawvere's Theorem.

Examples of CPO

- ▶ **powersets** ($P(X), \sqsubset$). Least upper bounds = unions.
- ▶ **partial functions** ($\mathbb{N} \rightarrow \mathbb{N}, \sqsubset$), where $\mathbb{N} \rightarrow \mathbb{N}$ is the set of partial functions on \mathbb{N} , and

$$f \sqsubset g := \forall xy \in \mathbb{N}. f(x) \simeq y \rightarrow g(x) \simeq y$$

- ▶ **flat nats** ($\mathbb{N}_\perp, \sqsubset$), where $\mathbb{N}_\perp := \mathbb{N} \cup \{\perp\}$, and

$$x \sqsubset y := x = \perp \vee x = y$$

- ▶ **streams** ($\Sigma^\#, \sqsubset$), where $\Sigma^\#$ is the set of finite or infinite sequences over Σ , and

$$x \sqsubset y \text{ iff } x \text{ is a prefix of } y$$

Remark:

- ▶ \sqsubset : the partial order of definedness
- ▶ \coprod : least upper bounds (lub) as limits
- ▶ $\coprod_i f_i$: functions defined by recursion as fixed points
- ▶ Continuity serves as an '*intrinsic approximation*' to computability.

Reflexive Domain

For $D \in \text{ob}(\mathbf{CPO})$, define

$$D_1 := D$$

$$D_{n+1} := [D_n, D_n]$$

$$i_n : D_n \rightarrow D_{n+1}$$

$$j_n : D_{n+1} \rightarrow D_n$$

$$i_1(x) := \text{con}(x) : D \rightarrow D, \text{ where } \text{con}(x)(y) := x$$

$$j_1(f) := f(\perp)$$

$$i_{n+1}(x_{n+1}) := i_n \circ x_{n+1} \circ j_n$$

$$j_{n+1}(x_{n+2}) := j_n \circ x_{n+2} \circ i_n$$

$$D_{n+1} \xrightarrow{i_{n+1}(x_{n+1})} D_{n+1}$$

$$j_n \downarrow$$

$$D_n \xrightarrow{x_{n+1}} D_n$$

$$D_{n+1} \xrightarrow{x_{n+2}} D_{n+1}$$

$$i_n \uparrow$$

$$D_n \xrightarrow{j_{n+1}(x_{n+2})} D_n$$

then we have

$$i_n \circ j_n \leq 1_{D_{n+1}}$$

$$j_n \circ i_n = 1_{D_n}$$

Reflexive Domain

$$D^\infty := \varprojlim(D_n, j_n)$$

$$D_\infty := \varinjlim(D_n, i_n)$$

$$D^\infty = \left\{ x \in \prod_{n=1}^{\infty} D_n : x_n \in D_n \text{ and } j_n(x_{n+1}) = x_n \text{ for all } n \right\}$$

$$D_\infty = \left\{ x \in D^\infty : x_{m+1} = i_m(x_m) \text{ for all } m \geq n, \text{ for some } n \right\}$$

$$J_n : D^\infty \rightarrow D_n :: x \mapsto x_n$$

$$I_n : D_n \rightarrow D_\infty :: x_n \mapsto (j_1 \circ \dots \circ j_{n-1}(x_n), \dots, j_{n-1}(x_n), x_n, i_n(x_n), i_{n+1} \circ i_n(x_n), \dots)$$

Then we have

$$I_n \circ J_n \leq 1_{D_\infty}$$

$$J_n \circ I_n = 1_{D_n}$$

Reflexive Domain

Define

$$F : D^\infty \rightarrow [D^\infty \rightarrow D^\infty]$$

$$G : [D^\infty \rightarrow D^\infty] \rightarrow D^\infty$$

as

$$F(x) = \coprod_{n=0}^{\infty} I_n \circ x_{n+1} \circ J_n$$

$$G(f) = \coprod_{n=0}^{\infty} I_{n+1}(J_n \circ f \circ I_n)$$

Then D^∞ is reflexive.

$$F \circ G = 1_{[D^\infty \rightarrow D^\infty]}$$

$$G \circ F = 1_{D^\infty}$$

Theorem

- In the category **CPo**, we have $D^\infty \cong [D_\infty, D^\infty]$.
- In the category **CCPo**, we have $D^\infty \cong [D^\infty, D^\infty]$.

Models of λ -Calculus

Definition (Reflexive Object)

Let \mathbf{C} be a CCC. An object D is *reflexive* iff D^D is a retract of D , i.e. there are $\text{app} : D \rightarrow D^D$ and $\text{lam} : D^D \rightarrow D$ s.t. $\text{app} \circ \text{lam} = 1_{D^D}$.

Definition $(D, \cdot, [\![\cdot]\!])$

- Let \mathbf{C} be a CCC with reflexive object D via app, lam . For $x, y : 1 \rightarrow D$,
$$x \cdot y := \text{app}(x)(y)$$

- Let $\rho : \text{Var} \rightarrow D$ be a variable assignment. Define $[\![\cdot]\!]_\rho : \Lambda \rightarrow D$ as:

$$[\![x]\!]_\rho := \rho(x)$$

$$[\![MN]\!]_\rho := [\![M]\!]_\rho \cdot [\![N]\!]_\rho$$

$$[\![\lambda x. M]\!]_\rho := \text{lam}(f) \text{ where } f : d \mapsto [\![M]\!]_{\rho(d/x)}$$

Definition: An object D has *enough points* iff for all $f, g : D \rightarrow D$:
 $f \neq g \implies \exists x : 1 \rightarrow D : fx \neq gx$.

Theorem

Any reflexive object D has enough points, iff, $(D, \cdot, [\![\cdot]\!])$ is a λ -model.

Heritability of the Fixpoint Property

Definition (Weak Retraction)

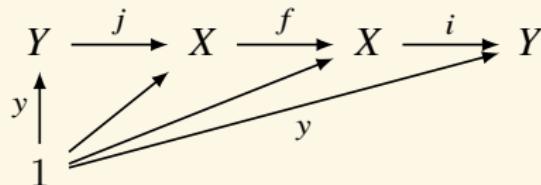
$j : Y \rightarrow X$ is a *weak retraction* of Y onto X iff there is a morphism $i : X \rightarrow Y$ s.t. for all $x : 1 \rightarrow X$,

$$(j \circ i) \circ x = x$$

Theorem

Let \mathbf{C} be a category with terminal object 1 . If X is a weak retract of Y and Y has the fixpoint property, then X has the fixpoint property.

Proof.



Let $f : X \rightarrow X$. Then $i \circ f \circ j : Y \rightarrow Y$, and there is $y : 1 \rightarrow Y$ s.t. $(i \circ f \circ j) \circ y = y$. It follows that

$$j \circ y = j \circ (i \circ f \circ j \circ y) = (j \circ i) \circ (f \circ j \circ y) = f \circ j \circ y$$

Theorem

Let \mathbf{C} be a Cartesian Closed Category. Assume we have $\{X_n, i_n, j_n\}_{n \geq 0}$ s.t.
 $i_n : X_n \rightarrow X_{n+1}$, $j_n : X_{n+1} \rightarrow X_n$, with $j_n \circ i_n = 1_{X_n}$ for all n , and
 $j_n(x_{n+1}) = x_{n+1} \circ i_{n-1}$ for all $x_{n+1} \in X_{n+1}$, where $X_{n+1} := Y^{X_n}$. Let
 $X_\infty := \varinjlim(X_n, i_n)$ and $X^\infty := \varprojlim(X_n, j_n)$ whenever such limits exist. Then

$$X^\infty \cong Y^{X_\infty}$$

Proof.

Let us abbreviate $\text{Hom}(X, Y)$ as $[X, Y]$.

$$\begin{aligned}[Z, Y^{X_\infty}] &\cong [Z \times X_\infty, Y] \\&\cong [Z \times \varinjlim X_n, Y] \\&\cong [\varinjlim(Z \times X_n), Y] \\&\cong \varprojlim[Z \times X_n, Y] \\&\cong \varprojlim[Z, Y^{X_n}] \\&\cong [Z, \varprojlim Y^{X_n}] \\&\cong [Z, X^\infty]\end{aligned}$$

Remark: If $X_\infty = X^\infty$, then Y has the fixpoint property.

Conjecture: The fixpoint property in any structure is a reflection of a higher reflexive domain of which it is a retraction.

Restriction Category

Definition (Restriction Category)

A restriction category is a category with a restriction operator $\bar{f} : A \rightarrow A$ for each morphism $f : A \rightarrow B$ satisfying

1. $f \circ \bar{f} = f$
2. $\bar{f} \circ \bar{g} = \bar{g} \circ \bar{f}$ whenever $\text{dom } f = \text{dom } g$
3. $\bar{g} \circ \bar{f} = \bar{g} \circ \bar{f}$ whenever $\text{dom } f = \text{dom } g$
4. $\bar{g} \circ f = f \circ \bar{g \circ f}$ whenever $\text{dom } g = \text{cod } f$

Example

- ▶ Every category admits the trivial restriction operator $\bar{f} = 1_{\text{dom } f}$.
- ▶ Sets and partial functions.

$$\bar{f} = \begin{cases} x & f(x) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

Definition: A total morphism $f : A \rightarrow B$ is a morphism for which $\bar{f} = 1_A$.

Turing Category

Definition: A *cartesian restriction category* is a restriction category which has a terminal object and for which each pair of objects has a product.

Definition (Turing Category)

A *Turing category* is a cartesian restriction category \mathbf{C} with a *Turing object* A such that, for each $X, Y \in \mathbf{C}$, there is a *universal application morphism* $\tau_{X,Y} : A \times X \rightarrow Y$, for any $f : Z \times X \rightarrow Y$, there exists a total morphism $h : Z \rightarrow A$ for which the following diagram is commutative:

$$\begin{array}{ccc} A \times X & \xrightarrow{\tau_{X,Y}} & Y \\ h \times 1_X \uparrow & \nearrow f & \\ Z \times X & & \end{array}$$

Remark: In the special case when h is uniquely determined we say that $\tau_{X,Y}$ is *extensional*.

In the special case when $Z = 1$ is the terminal object, we say $h : 1 \rightarrow A$ is a *code* for f .

- ▶ A reflexive object in a CCC is an object A together with embedding-retraction pairs $A^A \xrightleftharpoons[\text{app}]{\text{lam}} A$ s.t. $\text{app} \circ \text{lam} = 1_{A^A}$.
- ▶ A reflexive object is said to be **extensional** when also $\text{lam} \circ \text{app} = 1_A$.
- ▶ In a Turing category with Turing object A , the Turing morphism is defined by taking an embedding-retraction pair $(\text{lam}, \text{app}) : A^A \triangleleft A$,

$$\tau_{A,A} : A \times A \xrightarrow{\text{app} \times 1_A} A^A \times A \xrightarrow{\varepsilon} A$$

Theorem

In a Turing category \mathbf{C} with Turing object A , every object $X \in \mathbf{C}$ is a retract of A .

Proof.

$$\begin{array}{ccc} A \times 1 & \xrightarrow{\tau_{1,X}} & X \\ \text{lam} \times 1 \uparrow & & \nearrow \pi_1 \\ X \times 1 & & \end{array}$$

Let $\text{app} := \langle 1_X, ! \rangle \tau_{1,X}$. Then

$$\text{app} \circ \text{lam} = 1_X$$

Theorem

For a cartesian restriction category \mathbf{C} , the following are equivalent:

1. \mathbf{C} is a Turing category.
2. There is an object A of which every object is a retract, and for which there exists a universal self-application Turing morphism

$$A \times A \xrightarrow{\tau_{A,A}} A .$$

Proof.

“ $2 \Rightarrow 1$ ”: For arbitrary objects $X, Y \in \mathbf{C}$, by assumption we have $(\text{lam}_X, \text{app}_X) : X \triangleleft A$ and $(\text{lam}_Y, \text{app}_Y) : Y \triangleleft A$.

$$A \times X \xrightarrow{\tau_{X,Y}} Y = A \times X \xrightarrow{1_A \times \text{lam}_X} A \times A \xrightarrow{\tau_{A,A}} A \xrightarrow{\text{app}_Y} Y$$

Example of Turing Category

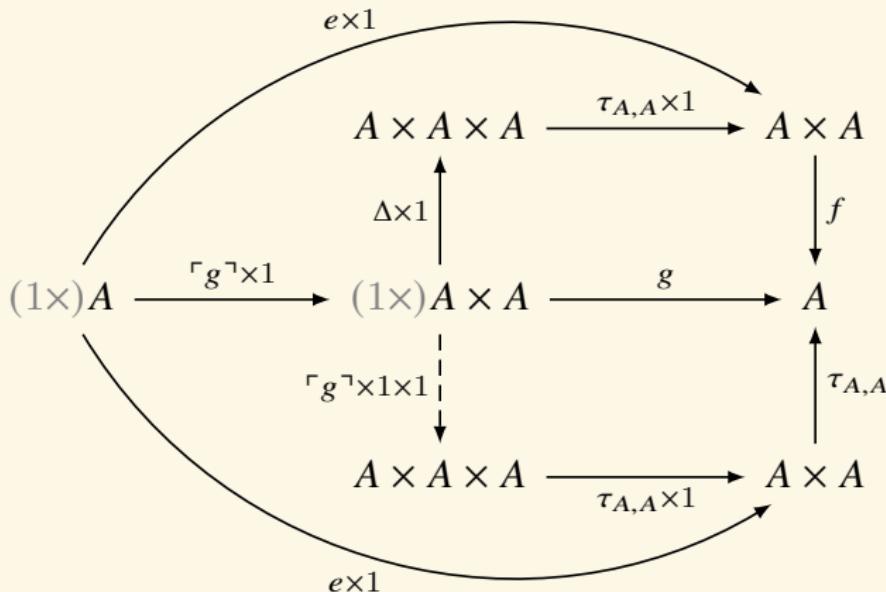
The classical category **Comp**(\mathbb{N}) of partial computable functions.

- ▶ objects: $0, 1, 2 \dots$ the natural numbers.
- ▶ morphism: $f : n \rightarrow m$ partial computable functions $f : \mathbb{N}^n \rightarrow \mathbb{N}^m$.
- ▶ Turing object: $1 (= \mathbb{N}^1)$.
- ▶ Turing morphism: $\tau : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} :: (n, m) \mapsto \varphi_n(m)$.

Theorem (Second Recursion Theorem)

In any Turing category, for any partial map $f : A \times A \rightarrow A$ on the Turing object A , there is a total point $e : 1 \rightarrow A$ such that $\tau_{A,A}(e \times 1) = f(e \times 1)$.

Proof.



$$g := f(\tau_{A,A} \times 1)(\Delta \times 1) \quad e := \tau_{A,A}(\lceil g \rceil \times \lceil g \rceil)$$

Dependent Sum

Theorem

For $f : A \rightarrow B$ a morphism in a category \mathbf{C} with pullbacks, the pullback functor $f^* : \mathbf{C}/B \rightarrow \mathbf{C}/A :: y \mapsto f^*y$ has a left adjoint $\Sigma_f \dashv f^*$.

$$\begin{array}{ccc} A \times_B Y & \longrightarrow & Y \\ f^*b \downarrow & \lrcorner & \downarrow b \\ A & \xrightarrow{f} & B \end{array}$$

Proof Sketch.

Let $\Sigma_f : \mathbf{C}/A \rightarrow \mathbf{C}/B :: a \mapsto f \circ a$.

We have to check that there is a natural isomorphism:

$$\theta : \text{Hom}_{\mathbf{C}/B}(\Sigma_f a, b) \xrightarrow{\cong} \text{Hom}_{\mathbf{C}/A}(a, f^*b).$$

Assume $g \in \text{Hom}_{\mathbf{C}/B}(\Sigma_f a, b)$.

$$\begin{array}{ccc} X & \xrightarrow{g} & Y \\ a \downarrow & & \downarrow b \\ A & \xrightarrow{f} & B \end{array}$$

By definition of f^*b , the following diagram is a pullback.

$$\begin{array}{ccccc} X & \xrightarrow{g} & & & Y \\ & \searrow u & \curvearrowleft & \nearrow p & \\ & & A \times_B Y & \xrightarrow{p} & Y \\ & \swarrow a & \downarrow f^*b & \lrcorner & \downarrow b \\ & A & \xrightarrow{f} & B & \end{array}$$

So for any $g \in \text{Hom}_{\mathbf{C}/B}(\Sigma_f a, b)$, there is a unique $u \in \text{Hom}_{\mathbf{C}/A}(a, f^*b)$ s.t. $\theta : g \mapsto u$ is a bijection.

Locally Cartesian Closed Category

Definition (Locally Cartesian Closed Category)

A category \mathbf{C} is called *locally cartesian closed* whenever, for all object $A \in \text{ob}(\mathbf{C})$, the slice category \mathbf{C}/A is cartesian closed.

Theorem

If \mathbf{C} is locally cartesian closed and has a terminal object, then \mathbf{C} is cartesian closed.

Dependent Product

Theorem

Let \mathbf{C} be a category with all pullbacks. Then \mathbf{C} is locally cartesian closed, iff, for any morphism $f : A \rightarrow B$, the pullback functor $f^* : \mathbf{C}/B \rightarrow \mathbf{C}/A$ has a right adjoint Π_f .

proof sketch of “ \Rightarrow ”.

Let $f : A \rightarrow B$ in \mathbf{C} , and $X \xrightarrow{a} A$ in \mathbf{C}/A . The pullback of $Y \xrightarrow{b} B$ along f corresponds to $f \times_B b : A \times_B Y \rightarrow B$ in \mathbf{C}/B .

$$\begin{array}{ccccc} & A \times_B Y & \longrightarrow & Y & \\ g \swarrow & f^*b \downarrow & \searrow f \times_B b & & \downarrow b \\ X & \xrightarrow{a} & A & \xrightarrow{f} & B \end{array}$$

Since \mathbf{C}/B is cartesian closed, we may exponentiate $fa : X \rightarrow B$ by $f : A \rightarrow B$ to obtain a morphism $(fa)^f : X^f \rightarrow B$ such that

$$\mathrm{Hom}_{\mathbf{C}/B}(f \times_B b, fa) \cong \mathrm{Hom}_{\mathbf{C}/B}(b, (fa)^f)$$

proof sketch of " \Rightarrow " continued.

Since $(-)^f : \mathbf{C}/B \rightarrow \mathbf{C}/B$ is a functor and we have a morphism $a : fa \rightarrow f$ in \mathbf{C}/B , so we obtain a morphism $a^f : (fa)^f \rightarrow f^f$ in \mathbf{C}/B . Moreover, $1_B \times_B f \cong f$, so by the product-exponential adjunction

$$\mathrm{Hom}_{\mathbf{C}/B}(f, f) \cong \mathrm{Hom}_{\mathbf{C}/B}(1_B, f^f)$$

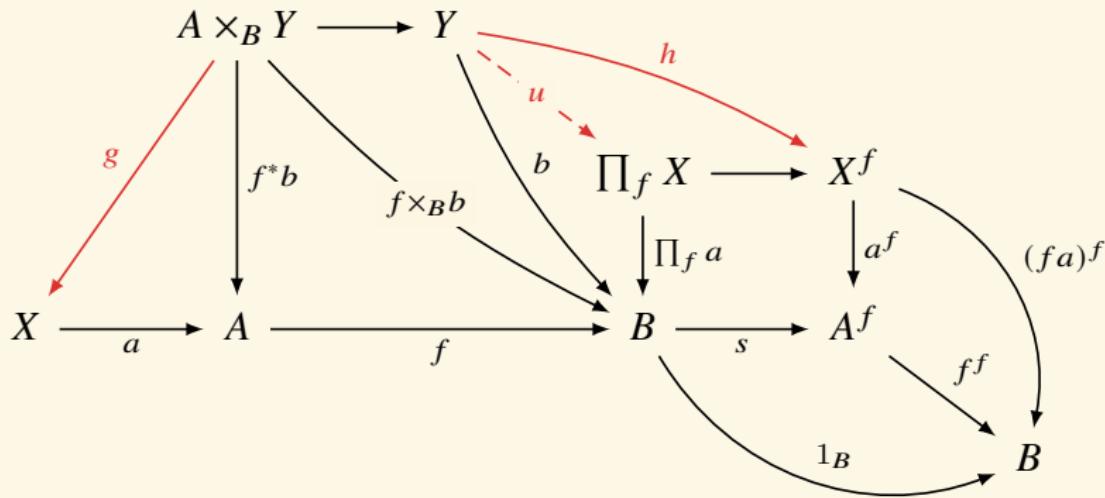
$$\begin{array}{ccc}
 \prod_f X & \longrightarrow & X^f \\
 \Pi_f a \downarrow & \lrcorner & \downarrow a^f \\
 B & \xrightarrow{s} & A^f \\
 & \searrow & \swarrow f^f \\
 & 1_B &
 \end{array}
 \quad
 \begin{array}{c}
 (fa)^f \\
 \curvearrowright \\
 \curvearrowright
 \end{array}$$

In particular, $1_f : f \rightarrow f$ is mapped to some $s : 1_B \rightarrow f^f$ (i.e. a morphism $s : B \rightarrow A^f$ in \mathbf{C} such that $f^f \circ s = 1_B$). Now, take the pullback (in \mathbf{C}) of a^f along s to obtain $\prod_f a := s^* a^f : \prod_f X \rightarrow B$.

proof sketch of " \Rightarrow " continued.

Now we prove there is a bijection $\text{Hom}_{\mathbf{C}/A}(f^*b, a) \cong \text{Hom}_{\mathbf{C}/B}(b, \prod_f a)$, which is natural in $X \xrightarrow{a} A$ and $Y \xrightarrow{b} B$.

The left hand side can be identified with morphisms $g : f \times_B b \rightarrow fa$ in \mathbf{C}/B satisfying $a \circ g = f^*b$, where $f^*b : f \times_B b \rightarrow f$ is the projection. The right hand side can be identified with morphisms $h : b \rightarrow (fa)^f$ such that $a^f \circ h = s \circ b$. Then $\mathrm{Hom}_{\mathbf{C}/B}(f \times_B b, fa) \cong \mathrm{Hom}_{\mathbf{C}/B}(b, (fa)^f)$ restricts to a bijection $g \mapsto u$.



proof sketch of “ \Leftarrow ”.

The terminal object in \mathbf{C}/B is 1_B .

The pullback of f and b in \mathbf{C} corresponds to a product in \mathbf{C}/B .

$$\begin{array}{ccc} P & \longrightarrow & X \\ f^*b \downarrow & \searrow f \times_B b & \downarrow b \\ A & \xrightarrow{f} & B \end{array}$$

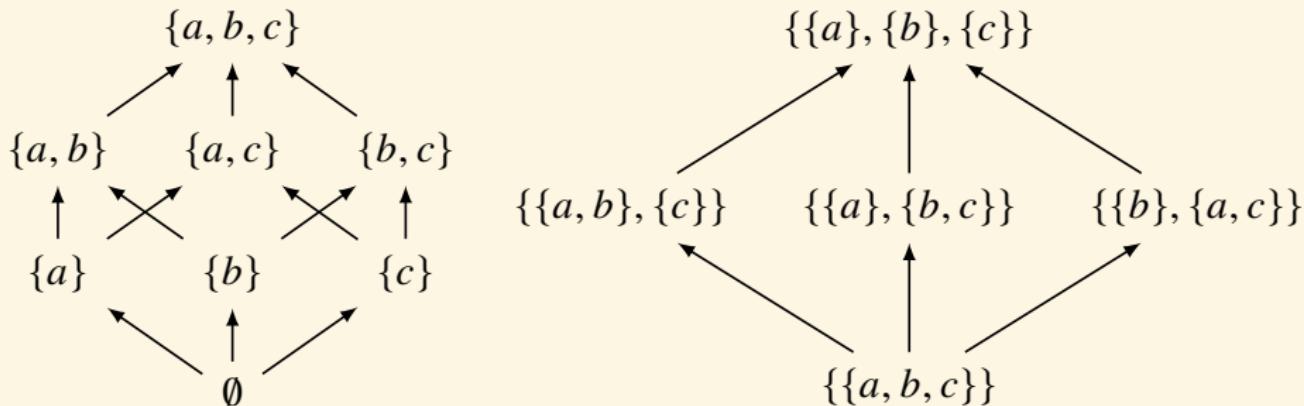
$$f \times_B b = f \circ f^*b = \sum_f f^*b$$

We deduce the following equivalence

$$\begin{aligned} \text{Hom}_{\mathbf{C}/B}(f \times_B b, u) &= \text{Hom}_{\mathbf{C}/B}(\sum_f (f^*b), u) \\ &\cong \text{Hom}_{\mathbf{C}/A}(f^*b, f^*u) \\ &\cong \text{Hom}_{\mathbf{C}/B}(b, \prod_f (f^*(u))) \end{aligned}$$

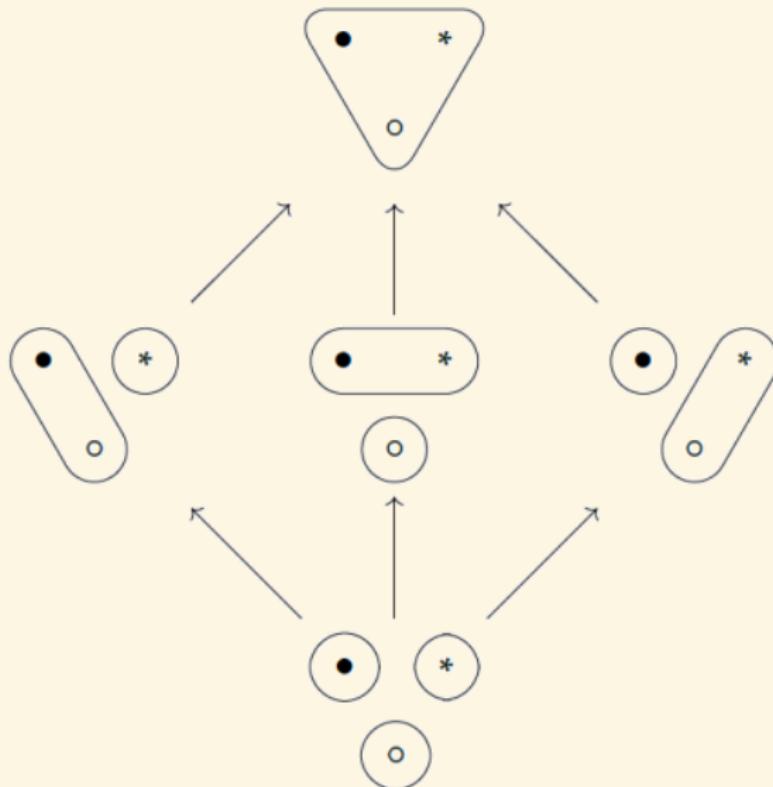
Then $u^f = \prod_f (f^*(u))$.

Classical Logic vs Partition Logic



- ▶ Creating Elements vs Creating Distinctions
- ▶ Classical logic is closely connected to the logic of subsets. For a set X of “states” of the world, we get a poset $P(X)$, with the partial order being \subseteq . Elements of $P(X)$ are “propositions” about the world.
- ▶ In classical logic, propositions correspond to subsets of X . In partition logic, propositions correspond to partitions of X .
- ▶ In both approaches we get a poset of propositions where the partial order is “implication” \rightarrow .

The Poset of Partitions



Partition Logic

- ▶ A set X has a poset of partitions. Let $\mathcal{E}(X)$ be the set of partitions of X . Each partition P corresponds to an equivalence relation \sim_P . We say a partition P is finer than Q ($P \leq Q$) iff $\forall xy : x \sim_P y \implies x \sim_Q y$.
- ▶ The meet $P \wedge Q$ is the coarsest partition that is finer than P and Q .

$$\sim_{P \wedge Q} := \sim_P \cap \sim_Q$$

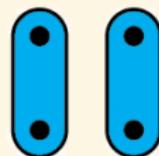
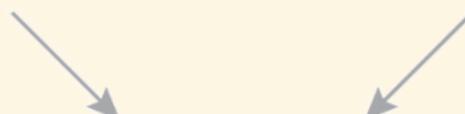
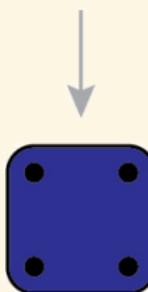
- ▶ The join $P \vee Q$ is the finest partition that is coarser than P and Q .

$$\sim_{P \vee Q} := (\sim_P \cup \sim_Q)^*$$

where $()^*$ is the transitive closure operator.

- ▶ Given a function $f : X \rightarrow Y$ and a partition P of Y , the pullback of P along f is the partition of X : $f^*(P) := \{f^*(S) : S \in P \ \& \ f^*(S) \neq \emptyset\}$.
- ▶ We always have $f^*(P \wedge Q) = f^*(P) \wedge f^*(Q)$.
- ▶ But sometimes we have $f^*(P \vee Q) \neq f^*(P) \vee f^*(Q)$.

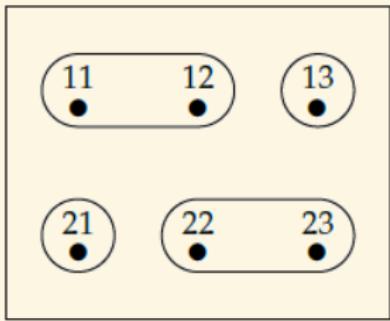
Remark: $f(a) \vee f(b) \not\equiv f(a \vee b)$ implies that we see something when we observe the combined system that we could not expect by merely combining our observations of the subsystems.

 P  Q  $x \sim_{P \vee Q} y$  $x \sim_P z_1$ $z_2 \sim_P y$ $z_1 \sim_Q z_2$  $P \vee Q$

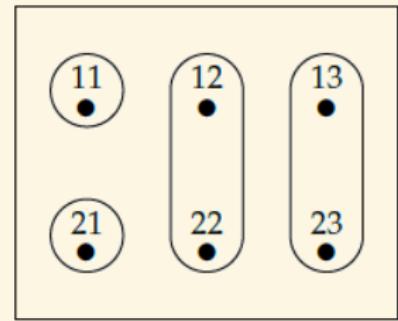
Proof of $f^*(P \vee Q) \neq f^*(P) \vee f^*(Q)$

Take $X = \{11, 22\}$, $Y = \{11, 12, 13, 21, 22, 23\}$, and let $i : X \hookrightarrow Y$.

$P =$



$Q =$



Then

$$i^*(P) = \{\{11\}, \{22\}\} = i^*(Q)$$

$$i^*(P) \vee i^*(Q) = \{\{11\}, \{22\}\}$$

$$P \vee Q = \{\{11, 12, 13, 22, 23\}, \{21\}\}$$

$$i^*(P \vee Q) = \{\{11, 22\}\}$$

$$i^*(P \vee Q) \neq i^*(P) \vee i^*(Q)$$

Galois Correspondence

Definition (Galois Correspondence)

The function $X \mapsto X^*$ from $P(A)$ to $P(B)$ and the function $Y \mapsto Y^\dagger$ from $P(B)$ to $P(A)$ constitute a *Galois correspondence* iff

1. $X_1 \subset X_2 \implies X_2^* \subset X_1^*$
2. $Y_1 \subset Y_2 \implies Y_2^\dagger \subset Y_1^\dagger$
3. $X \subset (X^*)^\dagger$
4. $Y \subset (Y^\dagger)^*$

Definition (Polarity)

Given $R \subset A \times B$, $X \subset A$, $Y \subset B$. Let

$$X^* := \bigcap_{x \in X} \{y \in B : Rxy\} \quad Y^\dagger := \bigcap_{y \in Y} \{x \in A : Rxy\}$$

We refer to the functions $X \mapsto X^*$ and $Y \mapsto Y^\dagger$ as *polarities*.

- ▶ The polarities induced by a relation constitute a Galois correspondence.
- ▶ Every Galois correspondence arises from polarities induced by a relation.

Galois Connection

Definition (Galois Connection)

- Let (A, \leq_A) and (B, \leq_B) be two partially ordered sets. A monotone Galois connection between these posets consists of two monotone functions: $f : A \rightarrow B, g : B \rightarrow A$ s.t.

$$\forall a \in A \forall b \in B : f(a) \leq_B b \iff a \leq_A g(b)$$

- An antitone Galois connection between these posets consists of two order-reversing functions: $f : A \rightarrow B, g : B \rightarrow A$ s.t.

$$\forall a \in A \forall b \in B : b \leq_B f(a) \iff a \leq_A g(b)$$

Example: $B \rightarrow \neg A \iff A \rightarrow \neg B, f = g = \neg$

- A Galois correspondence is an antitone Galois connection.
- An antitone Galois connection between **C** and **D** is just a monotone Galois connection between **C** and the order dual **D**^{OP}.
- A Galois connection is a pair of adjoint functors between two categories that arise from partially ordered sets.

- ▶ Suppose we have two preorders (A, \leq_A) and (B, \leq_B) .
If f has a right adjoint $g : B \rightarrow A$, then g is unique and

$$g(b) = \bigvee \{a \in A : f(a) \leq_B b\}$$

If $g : B \rightarrow A$ has a left adjoint $f : A \rightarrow B$, then f is unique and

$$f(a) = \bigwedge \{b \in B : a \leq_A g(b)\}$$

- ▶ The function $g : B \rightarrow A$ is the inverse of $f : A \rightarrow B$ iff

$$\forall a, b : f(a) = b \iff a = g(b)$$

- ▶ The right adjoint g is the “best approximation from below” to the “nonexistent” inverse of f .
- ▶ The left adjoint f is the “best approximation from above” to the “nonexistent” inverse of g .

Fundamental Theorem of Galois Theory

Theorem (Fundamental Theorem of Galois Theory)

Let $K \rightarrow L$ be a finite separable normal field extension with Galois group $G := \text{Aut}(L/K)$. For any subfield F of L containing K , any subgroup $H < G$, let

$$F^* := \text{Aut}(L/F) := \{\sigma \in \text{Aut}(L) : \forall x \in F (\sigma(x) = x)\}$$

$$H^\dagger := \{x \in L : \forall \sigma \in H (\sigma(x) = x)\}$$

Then

1. $[L : K] = |G|$, where $[L : K]$ is the dimension of L as a vector space over K .
2. $F = (F^*)^\dagger$, $H = (H^\dagger)^*$, $[L : F] = |F^*|$, $[F : K] = |G|/|F^*|$.
3. F is a normal extension of K iff $F^* \triangleleft G$.
4. $F^* \triangleleft G \implies \text{Aut}(F/K) \cong G/F^*$.

Example: Formal Concept Analysis

- ▶ A **formal context** is a triple (X, Y, \sqsubseteq) , where X is a set of objects, Y is a set of attributes, and $\sqsubseteq \subset X \times Y$.
- ▶ A morphism from (X, Y, \sqsubseteq) to (X', Y', \sqsubseteq') is a pair of functions (f, g) with $f : X \rightarrow X'$ and $g : Y' \rightarrow Y$ s.t.

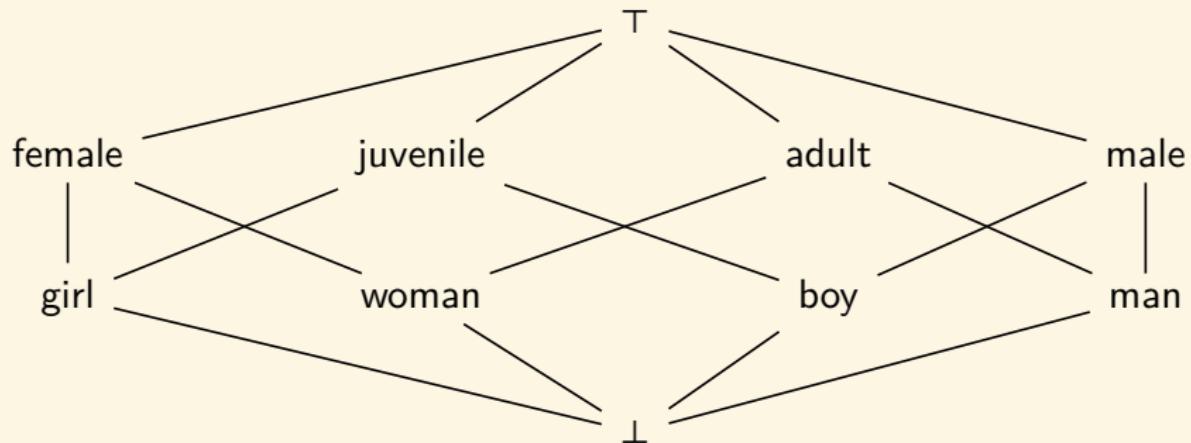
$$\forall x \in X \forall y \in Y' : f(x) \sqsubseteq' y \iff x \sqsubseteq g(y)$$

- ▶ For $A \subset X$, let $A^\uparrow := \{y \in Y : \forall x \in A : x \sqsubseteq y\}$, i.e., a set of attributes shared by all objects from A .
- ▶ For $B \subset Y$, let $B^\downarrow := \{x \in X : \forall y \in B : x \sqsubseteq y\}$, i.e., a set of objects sharing all attributes from B .
- ▶ Then we have the Galois connection.

$$A^\uparrow \supset B \iff A \subset B^\downarrow$$

Remark: both sides mean “every object in A has every attribute in B ”.

\Vdash	male	female	juvenile	adult
boy	1		1	
girl		1	1	
man	1			1
woman		1		1



- A pair (A, B) is a **formal concept** of a context (X, Y, \sqsubseteq) iff

$$A^\uparrow = B \quad \& \quad B^\downarrow = A$$

The novel idea of FCA is the clustering of attributes based on Galois connection. The clustering determines which collection of attributes forms a coherent entity called a concept, by the philosophical criteria of unity between extension and intension.

$$\text{concept} = \text{extent } A + \text{intent } B$$

- The set of formal concepts of (X, Y, \sqsubseteq) is

$$\mathbf{B}(X, Y, \sqsubseteq) := \{(A, B) \in 2^X \times 2^Y : A^\uparrow = B \quad \& \quad B^\downarrow = A\}$$

- formal concept = fixpoint of $\uparrow\downarrow$

$$\mathbf{B}(X, Y, \sqsubseteq) \cong \text{Fix}(\uparrow\downarrow) \cong \text{Fix}(\downarrow\uparrow)$$

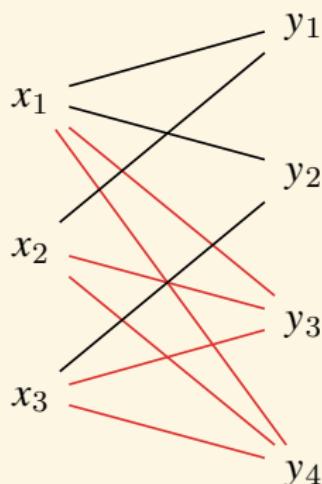
where $\text{Fix}(f) = \{x : f(x) = x\}$.

formal concepts = maximal rectangles = complete bipartite subgraph

\models	y_1	y_2	y_3	y_4
x_1	1	1	1	1
x_2	1		1	1
x_3		1	1	1

\models	y_1	y_2	y_3	y_4
x_1	1	1	1	1
x_2	1		1	1
x_3		1	1	1

\models	y_1	y_2	y_3	y_4
x_1	1	1	1	1
x_2	1		1	1
x_3		1	1	1



$$(A_1, B_1) = (\{x_1, x_2, x_3\}, \{y_3, y_4\})$$

$$(A_2, B_2) = (\{x_1, x_3\}, \{y_2, y_3, y_4\})$$

$$(A_3, B_3) = (\{x_1, x_2\}, \{y_1, y_3, y_4\})$$

- The formal context is said to be *extensional* if $\downarrow: 2^Y \rightarrow 2^X$ is injective and is said to be *separable* if $\uparrow: 2^X \rightarrow 2^Y$ is injective.
- Subconcept $(A, B) \leq (A', B')$ if $A \subset A'$, or equivalently if $B \supset B'$.
- The set of concepts $\mathbf{B}(X, Y, \sqsubseteq)$ is a complete lattice.

$$(A, B) \wedge (A', B') = (A \cap A', (B \cup B')^{\uparrow\downarrow})$$

$$(A, B) \vee (A', B') = ((A \cup A')^{\uparrow\downarrow}, B \cap B')$$

$$\bigwedge_{i \in I} (A_i, B_i) = \left(\bigcap_{i \in I} A_i, \left(\bigcup_{i \in I} B_i \right)^{\uparrow\downarrow} \right)$$

$$\bigvee_{i \in I} (A_i, B_i) = \left(\left(\bigcup_{i \in I} A_i \right)^{\uparrow\downarrow}, \bigcap_{i \in I} B_i \right)$$

- Attribute Implication $B \rightarrow B' := B^\downarrow \subset B'^\downarrow$ for $B, B' \subset Y$.
- Armstrong rules for attribute implication.

$$\frac{}{A \rightarrow A} \quad \frac{A \rightarrow B}{A \cup C \rightarrow B} \quad \frac{A \rightarrow B, \quad B \cup C \rightarrow D}{A \cup C \rightarrow D}$$

Adjoint Functor Theorem for Posets

Theorem (Adjoint Functor Theorem for Posets)

Let (X, \leq) and (Y, \leq) be posets. Suppose that Y has all meets, and let $g : Y \rightarrow X$ be a monotone function preserving all meets. Then g has a left adjoint $f : X \rightarrow Y$, given by

$$f(x) := \bigwedge \{y \in Y : x \leq g(y)\}$$

In particular, a monotone map $g : Y \rightarrow X$ is the right adjoint of a Galois connection iff it preserves all meets.

Corollary

Suppose that X has all joins. A monotone map $f : X \rightarrow Y$ has a right adjoint iff it preserves all joins.

Proof.

$$g(f(x)) = g\left(\bigwedge \{y \in Y : x \leq g(y)\}\right) = \bigwedge \{g(y) : y \in Y \& x \leq g(y)\}$$

$$x \leq \bigwedge \{g(y) : y \in Y \& x \leq g(y)\} = g(f(x))$$

This inequality is the unit of the adjunction.

For the counit, let $z \in Y$. Then

$$f(g(z)) = \bigwedge \{y \in Y : g(z) \leq g(y)\}$$

Since $g(z) \leq g(z)$, we have

$$z \geq \bigwedge \{y \in Y : g(z) \leq g(y)\} = f(g(z))$$

General Adjoint Functor Theorem

Lemma

A functor $G : \mathbf{D} \rightarrow \mathbf{C}$ has a left adjoint iff for every $A \in \mathbf{C}$ the comma category $A \downarrow G$ has an initial object.

Lemma

Suppose \mathbf{D} is locally small and complete. Then \mathbf{D} has an initial object iff \mathbf{D} has a **weakly initial set**: there is a set of objects $(B_i)_{i \in I}$ in \mathbf{D} s.t. for any $B \in \mathbf{D}$ there exists some $i \in I$ and a morphism $g_i : B_i \rightarrow B$.

Theorem (General Adjoint Functor Theorem)

Suppose \mathbf{D} is locally small and complete. Then $G : \mathbf{D} \rightarrow \mathbf{C}$ has a left adjoint iff G is continuous and for each $A \in \mathbf{C}$, the comma category $A \downarrow G$ has a **weakly initial set**: there is a set of objects $(B_i, f_i : A \rightarrow GB_i)_{i \in I}$ in $A \downarrow G$ s.t. for any $(B, f : A \rightarrow GB)$ there exists some $i \in I$ and $g_i : B_i \rightarrow B$ with $f = Gg_i \circ f_i$.

$$\begin{array}{ccc} A & \xrightarrow{f_i} & GB_i \\ & \searrow f & \downarrow Gg_i \\ & & GB \end{array}$$

Special Adjoint Functor Theorem

Definition (Coseparating Family)

A *coseparating family* for a category \mathbf{C} is a family of objects $(G_i)_{i \in I}$ such that for any pair $A \xrightarrow{\begin{smallmatrix} f \\ g \end{smallmatrix}} B$ with $f \neq g$, there is an $i \in I$ and an $h : B \rightarrow G_i$ such that $hf \neq hg$.

Theorem (Special Adjoint Functor Theorem)

Suppose both \mathbf{C} and \mathbf{D} are locally small, and that \mathbf{D} is complete and well-powered and has a coseparating set. Then a functor $G : \mathbf{D} \rightarrow \mathbf{C}$ has a left adjoint iff G preserves small limits.

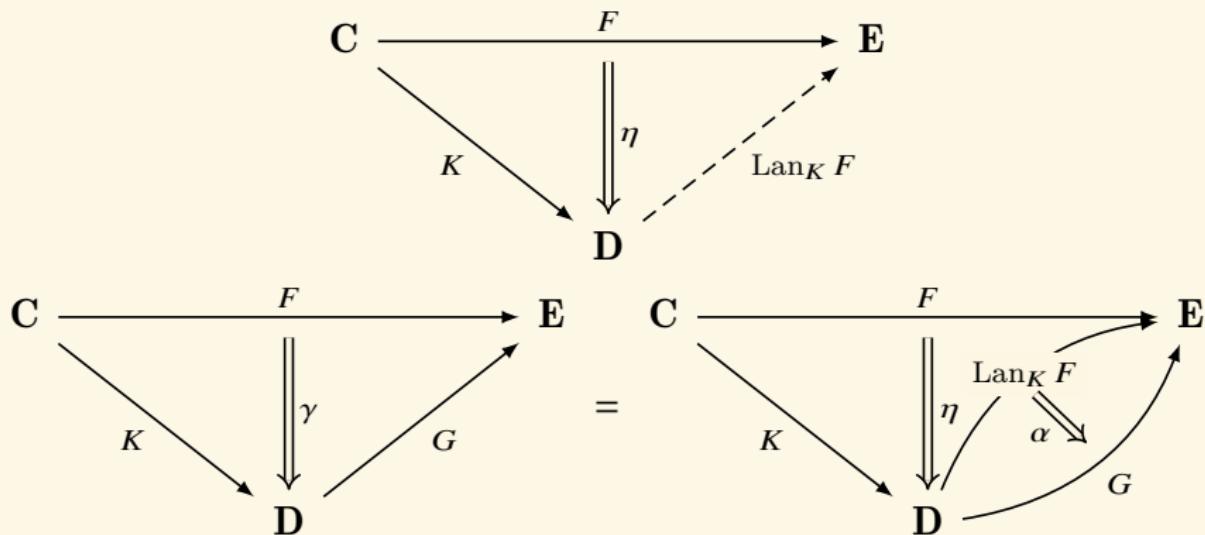
Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Kan Extension

Definition (Left Kan Extension)

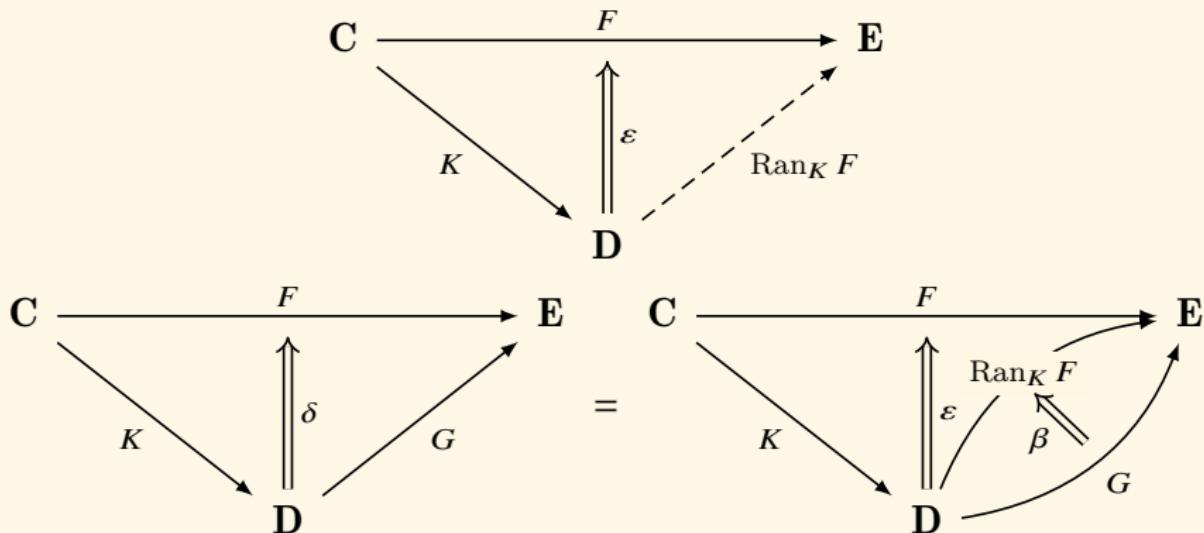
Given functors $F : \mathbf{C} \rightarrow \mathbf{E}$ and $K : \mathbf{C} \rightarrow \mathbf{D}$, a *left Kan extension* of F along K is a functor $\text{Lan}_K F : \mathbf{D} \rightarrow \mathbf{E}$ with a natural transformation $\eta : F \rightarrow \text{Lan}_K F \circ K$ s.t. for any such pair $(G : \mathbf{D} \rightarrow \mathbf{E}, \gamma : F \rightarrow GK)$, there exists a unique natural transformation $\alpha : \text{Lan}_K F \rightarrow G$ with $\gamma = \alpha K \circ \eta$.



Kan Extension

Definition (Right Kan Extension)

Given functors $F : \mathbf{C} \rightarrow \mathbf{E}$ and $K : \mathbf{C} \rightarrow \mathbf{D}$, a *right Kan extension* of F along K is a functor $\text{Ran}_K F : \mathbf{D} \rightarrow \mathbf{E}$ with a natural transformation $\varepsilon : \text{Ran}_K F \circ K \rightarrow F$ s.t. for any such pair $(G : \mathbf{D} \rightarrow \mathbf{E}, \delta : GK \rightarrow F)$, there exists a unique natural transformation $\beta : G \rightarrow \text{Ran}_K F$ with $\delta = \varepsilon \circ \beta K$.



Example

For any object $A \in \mathbf{C}$ and any $F : \mathbf{C} \rightarrow \mathbf{Set}$, there is a bijection between elements $x \in FA$ and natural transformations with boundary as displayed

$$\begin{array}{ccc} 1 & \xrightarrow{*} & \mathbf{Set} \\ & \searrow A & \downarrow \begin{matrix} \parallel \\ x \end{matrix} \\ & C & \nearrow F \end{array}$$

By the Yoneda lemma, the representable functor $\text{Hom}(A, -)$ and the identity $1_A : A \rightarrow A$ define the left Kan extension of $* : 1 \rightarrow \mathbf{Set}$ along $A : 1 \rightarrow \mathbf{C}$.

$$\begin{array}{ccc} 1 & \xrightarrow{*} & \mathbf{Set} \\ & \searrow A & \downarrow \begin{matrix} \parallel \\ 1_A \end{matrix} \\ & C & \nearrow \text{Hom}(A, -) \end{array}$$

$$\begin{array}{ccc} 1 & \xrightarrow{*} & \mathbf{Set} \\ & \searrow A & \downarrow \begin{matrix} \parallel \\ 1_A \\ \psi(x) \end{matrix} \\ & C & \nearrow \begin{matrix} \text{Hom}(A, -) \\ \Downarrow \psi(x) \\ F \end{matrix} \end{array}$$

The required unique factorization is the natural transformation $\psi(x) : \text{Hom}(A, -) \rightarrow F$ with $\psi(x)_A(1_A) = x$.

$$\text{Lan}_K \dashv K^* \dashv \text{Ran}_K$$

Theorem

If the Kan extensions exist for all F , then $\text{Lan}_K \dashv K^* \dashv \text{Ran}_K$, where $K^* := - \circ K$.

$$\begin{array}{ccc} & \text{Lan}_K & \\ E^C & \xleftarrow{\perp} & E^D \\ & K^* & \\ & \perp & \\ & \text{Ran}_K & \end{array}$$

Proof.

By the Yoneda Lemma, any pair (G, γ) , as in the definition for the left Kan extension, yields a natural transformation by $\gamma_H^*(\alpha) := \alpha K \circ \gamma$.

$$\gamma^* : E^D(G, -) \rightarrow E^C(F, - \circ K)$$

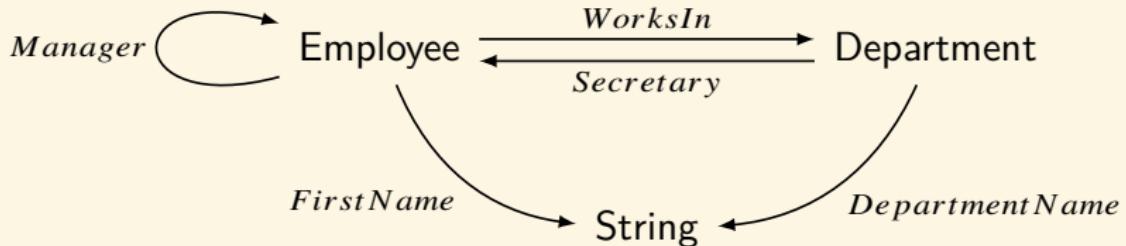
The universal property of the left Kan extension says that (Lan_K, η) yields a natural isomorphism.

$$E^D(\text{Lan}_K F, -) \cong E^C(F, - \circ K)$$

Example: Databases

- ▶ A “database schema” is a category **C**.
- ▶ An database built using this schema is a functor

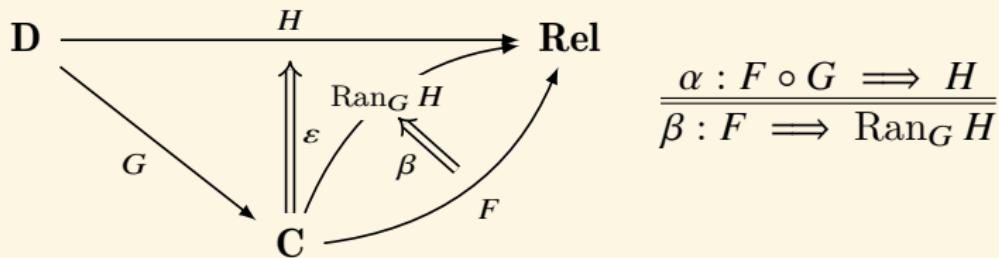
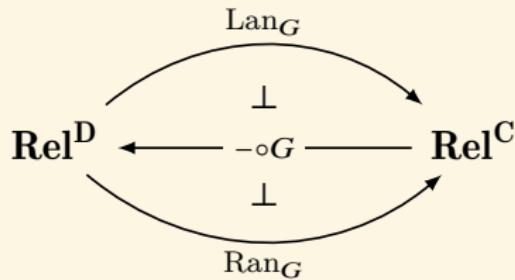
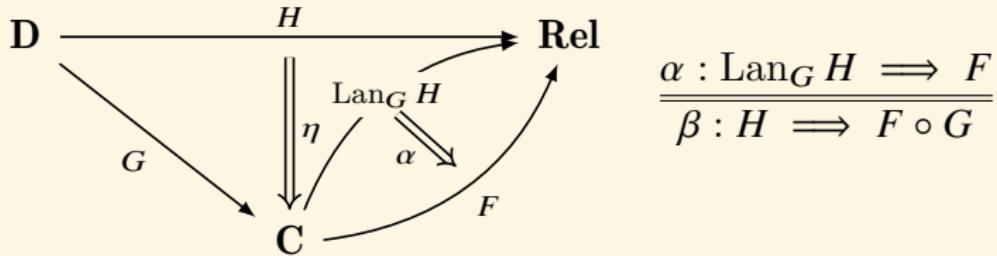
$$F : \mathbf{C} \rightarrow \mathbf{Rel}$$



- ▶ How can we transform our database into a different database built using a different schema **D**?

$$F \circ G : \mathbf{D} \xrightarrow{G} \mathbf{C} \xrightarrow{F} \mathbf{Rel}$$

- ▶ How can we turn databases built using **D** into databases built using **C**?
- ▶ The functor $- \circ G : \mathbf{Rel}^{\mathbf{C}} \rightarrow \mathbf{Rel}^{\mathbf{D}}$ has both a left adjoint $\text{Lan}_G : \mathbf{Rel}^{\mathbf{D}} \rightarrow \mathbf{Rel}^{\mathbf{C}}$ and a right adjoint $\text{Ran}_G : \mathbf{Rel}^{\mathbf{D}} \rightarrow \mathbf{Rel}^{\mathbf{C}}$.



Example: Databases

$\mathbf{C} := \text{Germans} \xrightarrow{\textit{Friend}} \text{Italians}$

$\mathbf{D} := \text{Germans}$

$G : \mathbf{D} \hookrightarrow \mathbf{C}$

Germans	Friend	Italians	Germans
Ilsa	Giulia	Bianca	Ilsa
Klaus	Gian-Carlo	Giulia	Klaus
Jörg	Martina	Gian-Carlo	Jörg
Sabine	Alessandro	Alessandro	Sabine
Heinrich	Martina	Martina	Heinrich

Table: $F : \mathbf{C} \rightarrow \mathbf{Rel}$

Table: $F \circ G : \mathbf{D} \rightarrow \mathbf{Rel}$

Example: Databases — Left Kan Extension

Germans
Ilsa
Klaus
Jörg
Sabline

Table: $H : \mathbf{D} \rightarrow \mathbf{Rel}$

Germans	Friend	Italians
Ilsa	Italian1	Italian1
Klaus	Italian2	Italian2
Jörg	Italian3	Italian3
Sabine	Italian4	Italian4

Table: $\text{Lan}_G H : \mathbf{C} \rightarrow \mathbf{Rel}$

Remark: the left Kan extension is a left adjoint, it does this in a “liberal” way. It freely makes up the entries obeying only the equations that are needed to get a valid database.

Example: Databases — Right Kan Extension

Germans
Ilsa
Klaus
Jörg
Sabline

Table: $H : \mathbf{D} \rightarrow \mathbf{Rel}$

Germans	Friend	
Ilsa	Italian1	
Klaus	Italian1	
Jörg	Italian1	
Sabine	Italian1	

Table: $\text{Ran}_G H : \mathbf{C} \rightarrow \mathbf{Rel}$

Remark: the right Kan extension is a right adjoint, it does this in a “conservative” way. It imposes all the equations that are possible in a valid database.

(Co)Limits are Kan Extensions

Theorem ((Co)Limits are Kan Extensions)

1. The left Kan extension $\text{Lan}_! D$ of $D : \mathbf{I} \rightarrow \mathbf{C}$ along $! : \mathbf{I} \rightarrow \mathbf{1}$ defines the colimit $\lim_{\rightarrow} D$.

$$\begin{array}{ccc} \mathbf{I} & \xrightarrow{D} & \mathbf{C} \\ \searrow ! & \Downarrow \eta & \swarrow C \\ \mathbf{1} & & \end{array} = \begin{array}{ccc} \mathbf{I} & \xrightarrow{D} & \mathbf{C} \\ & \Downarrow \eta & \\ & \Delta C & \end{array}$$

2. Dually, the right Kan extension $\text{Ran}_! D$ defines the limit $\lim_{\leftarrow} D$.

$$\begin{array}{ccc} \mathbf{I} & \xrightarrow{D} & \mathbf{C} \\ \searrow ! & \Uparrow \varepsilon & \swarrow C \\ \mathbf{1} & & \end{array} = \begin{array}{ccc} \mathbf{I} & \xrightarrow{D} & \mathbf{C} \\ & \Uparrow \varepsilon & \\ & \Delta C & \end{array}$$

Adjunctions are Kan Extensions

Theorem (Adjunctions are Kan Extensions)

1. If $F \dashv G$ is an adjunction with unit $\eta : 1_C \rightarrow GF$ and counit $\varepsilon : FG \rightarrow 1_D$, then (G, η) is a left Kan extension of the identity functor 1_C along F and (F, ε) is a right Kan extension of the identity functor 1_D along G .

$$\begin{array}{ccc} C & \xrightarrow{1_C} & C \\ F \searrow & \Downarrow \eta & \nearrow G \cong \text{Lan}_F 1_C \\ D & & \end{array} \quad \begin{array}{ccc} D & \xrightarrow{1_D} & D \\ G \searrow & \Updownarrow \varepsilon & \nearrow F \cong \text{Ran}_G 1_D \\ C & & \end{array}$$

Moreover, both Kan extensions are absolute (preserved by all functors).

2. Conversely, if $(G, \eta : 1_C \rightarrow GF)$ is a left Kan extension of the identity functor 1_C along F and if F preserves this Kan extension, then $F \dashv G$ with unit η .

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Monoidal Category

Definition (Monoidal Category)

A *monoidal category* is a category \mathbf{C} equipped with a monoidal structure.

A monoidal structure consists of:

- ▶ a bifunctor $\otimes : \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ called the *tensor product* or *monoidal product*.
- ▶ an object I called the *unit*.

such that,

- ▶ \otimes is **associative**: there is a natural (in each of three arguments A, B, C) isomorphism α , called *associator*, with components $\alpha_{A,B,C} : A \otimes (B \otimes C) \cong (A \otimes B) \otimes C$,
- ▶ I acts as **left and right unit**: there are two natural isomorphisms λ and ρ , respectively called left and right *unitor*, with components $\lambda_A : I \otimes A \cong A$ and $\rho_A : A \otimes I \cong A$.

A *strict monoidal category* is one for which the natural isomorphisms α, λ and ρ are identities.

Monoidal Category

$$\begin{array}{ccccc} A \otimes (B \otimes (C \otimes D)) & \xrightarrow{\alpha_{A,B,C \otimes D}} & (A \otimes B) \otimes (C \otimes D) & \xrightarrow{\alpha_{A \otimes B,C,D}} & ((A \otimes B) \otimes C) \otimes D \\ \downarrow 1_A \otimes \alpha_{B,C,D} & & & & \uparrow \alpha_{A,B,C} \otimes 1_D \\ A \otimes ((B \otimes C) \otimes D) & \xrightarrow{\alpha_{A,B \otimes C,D}} & (A \otimes (B \otimes C)) \otimes D & & \\ \\ A \otimes (I \otimes B) & \xrightarrow{\alpha_{A,I,B}} & (A \otimes I) \otimes B & & \\ & \searrow 1_A \otimes \lambda_B & & \swarrow \rho_A \otimes 1_B & \\ & & A \otimes B & & \end{array}$$

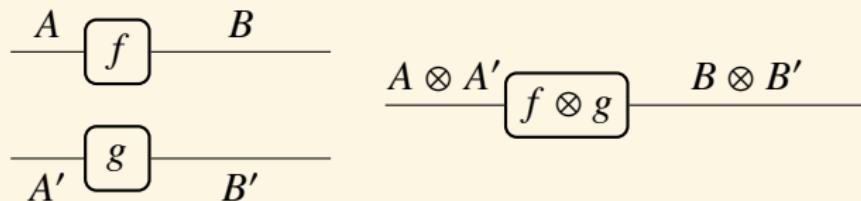
- composition of $f : A \rightarrow B$ and $g : B \rightarrow C$

$$g \circ f : A \rightarrow C$$



- tensor product of $f : A \rightarrow B$ and $g : A' \rightarrow B'$

$$f \otimes g : A \otimes A' \rightarrow B \otimes B'$$



- composition and tensor product must obey

$$(g \circ f) \otimes (g' \circ f') = (g \otimes g') \circ (f \otimes f')$$

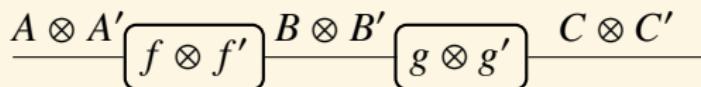
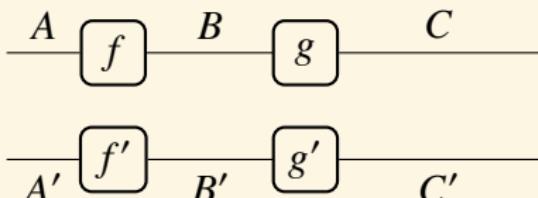
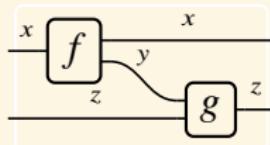
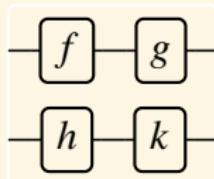


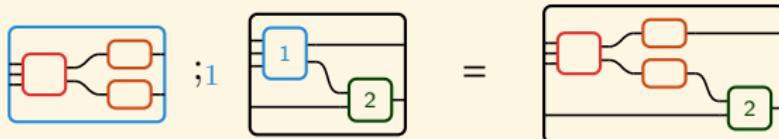
Diagram Representation



$$(f \otimes 1_z); (1_x \otimes g)$$



$$(f; g) \otimes (h; k) = (f \otimes h); (g \otimes k)$$



Example

Definition

The monoidal structure on the category **Rel** is defined as follows:

- ▶ the tensor product is Cartesian product of sets, $A \times A' \xrightarrow{R \times R'} B \times B'$
for $A \xrightarrow{R} B$ & $A' \xrightarrow{R'} B'$, where

$$R \times R'((a, a'), (b, b')) := Rab \wedge R'a'b'$$

- ▶ the unit object is a chosen singleton set $I := \{\bullet\}$.
- ▶ associators $A \times (B \times C) \xrightarrow{\alpha_{A,B,C}} (A \times B) \times C$ are the relations defined by $(a, (b, c)) \sim ((a, b), c)$.
- ▶ left unitors $I \times A \xrightarrow{\lambda_A} A$ are the relations defined by $(\bullet, a) \sim a$.
- ▶ right unitors $A \times I \xrightarrow{\rho_A} A$ are the relations defined by $(a, \bullet) \sim a$.

Examples

1. Any monoid can be thought of as a monoidal category. The elements of the monoid form a discrete category.
2. $(\mathbb{N}, \leq, +, 0)$ is a monoidal preorder.
3. Any category with finite products can be regarded as monoidal with the product as the tensor product and the terminal object as the unit. Such a category is sometimes called a cartesian monoidal category.
For example: **Set** and **Cat**.
4. The category of all endofunctors on a category **C** is a strict monoidal category with the composition of functors as the product and the identity functor as the unit.
5. Bounded-above meet semilattices are strict symmetric monoidal categories: the product is meet and the identity is the top element.
6. **R-Mod**, the category of modules over a commutative ring R , is a monoidal category with the tensor product of modules \otimes_R serving as the monoidal product and the ring R (thought of as a module over itself) serving as the unit.

Braided Monoidal Category

Definition (Braided Monoidal Category)

A *braided monoidal category* \mathbf{C} is a monoidal category equipped with a natural isomorphism σ called the *braiding* that assigns to every pair of objects $A, B \in \mathbf{C}$ an isomorphism $\sigma_{A,B} : A \otimes B \rightarrow B \otimes A$ such that,

$$\begin{array}{ccccc} A \otimes (B \otimes C) & \xrightarrow{\alpha_{A,B,C}} & (A \otimes B) \otimes C & \xrightarrow{\sigma_{A,B} \otimes 1_C} & (B \otimes A) \otimes C \\ \downarrow \sigma_{A,B \otimes C} & & & & \downarrow \alpha_{B,A,C}^{-1} \\ (B \otimes C) \otimes A & \xleftarrow{\alpha_{B,C,A}} & B \otimes (C \otimes A) & \xleftarrow[1_B \otimes \sigma_{A,C}]{} & B \otimes (A \otimes C) \end{array}$$

$$\begin{array}{ccccc} (A \otimes B) \otimes C & \xrightarrow{\alpha_{A,B,C}^{-1}} & A \otimes (B \otimes C) & \xrightarrow{1_A \otimes \sigma_{B,C}} & A \otimes (C \otimes B) \\ \downarrow \sigma_{A \otimes B,C} & & & & \downarrow \alpha_{A,C,B} \\ C \otimes (A \otimes B) & \xleftarrow{\alpha_{C,A,B}^{-1}} & (C \otimes A) \otimes B & \xleftarrow[\sigma_{A,C \otimes B} \otimes 1_B]{} & (A \otimes C) \otimes B \end{array}$$

Symmetric Monoidal Category

Definition (Symmetric Monoidal Category)

A *symmetric monoidal category* is a braided monoidal category where the braiding satisfies $\sigma_{B,A} \circ \sigma_{A,B} = 1_{A \otimes B}$.

Remark: In a symmetric monoidal category, the braiding $\sigma_{A,B} = \sigma_{B,A}^{-1}$.

$$\begin{array}{c} A \quad B \\ \diagdown \quad \diagup \\ B \quad A \end{array} = \begin{array}{c} A \quad B \\ \diagup \quad \diagdown \\ B \quad A \end{array}$$

- A **strict monoidal monotone** from a monoidal preorder $(X, \leq_X, \otimes_X, I_X)$ to a monoidal preorder $(Y, \leq_Y, \otimes_Y, I_Y)$ is a map $f : X \rightarrow Y$ s.t.

$$x \leq_X x \implies f(x) \leq_Y f(y)$$

$$f(x \otimes_X x') = f(x) \otimes_Y f(x')$$

$$f(I_X) = I_Y$$

- A **lax monoidal monotone** from a monoidal preorder $(X, \leq_X, \otimes_X, I_X)$ to a monoidal preorder $(Y, \leq_Y, \otimes_Y, I_Y)$ is a map $f : X \rightarrow Y$ s.t.

$$x \leq_X x \implies f(x) \leq_Y f(y)$$

$$f(x \otimes_X x') \geq_Y f(x) \otimes_Y f(x')$$

$$f(I_X) \geq_Y I_Y$$

- A **oplax monoidal monotone** from a monoidal preorder $(X, \leq_X, \otimes_X, I_X)$ to a monoidal preorder $(Y, \leq_Y, \otimes_Y, I_Y)$ is a map $f : X \rightarrow Y$ s.t.

$$x \leq_X x \implies f(x) \leq_Y f(y)$$

$$f(x \otimes_X x') \leq_Y f(x) \otimes_Y f(x')$$

$$f(I_X) \leq_Y I_Y$$

- **Example:** $[x] + [x'] \leq [x + x']$ and $[x] + [x'] \geq [x + x']$

Theorem

Suppose the monotone function $f : X \rightarrow Y$ is a left adjoint to the monotone function $g : Y \rightarrow X$. Then f is an oplax monoidal iff g is a lax monoidal.

Corollary

- ▶ *Suppose $f : X \rightarrow Y$ is a strict monoidal monotone and $g : Y \rightarrow X$ is a right adjoint of f . Then g is a lax monoidal monotone.*
- ▶ *Suppose $g : Y \rightarrow X$ is a strict monoidal monotone and $f : X \rightarrow Y$ is a left adjoint of g . Then f is an oplax monoidal monotone.*

Left/Right Closed Monoidal Category

Definition (Left/Right Closed Monoidal Category)

A monoidal category \mathbf{C} is *left closed* if there is an *internal hom* functor

$$\multimap : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{C}$$

together with a natural isomorphism c called *currying* that assigns to any objects $A, B, C \in \mathbf{C}$ a bijection

$$c_{A,B,C} : \text{Hom}(A \otimes B, C) \xrightarrow{\cong} \text{Hom}(A, B \multimap C)$$

It is *right closed* if there is an internal hom functor as above and a natural isomorphism

$$c_{A,B,C} : \text{Hom}(A \otimes B, C) \xrightarrow{\cong} \text{Hom}(B, A \multimap C)$$

Remark: there is no difference between left and right closed for a braided monoidal category, as the braiding gives an isomorphism $A \otimes B \cong B \otimes A$.

$*$ -autonomous Category

Definition ($*$ -autonomous Category)

A $*$ -autonomous category $(\mathbf{C}, \otimes, I, \multimap, \perp)$ is an symmetric monoidal closed category \mathbf{C} with a *dualizing* object \perp , such that if we set $A^* := A \multimap \perp$, the canonical morphism $A \rightarrow A^{**}$ is an isomorphism.

Remark: The operation $(-)^*$ induces a contravariant dualizing functor

$$*: \mathbf{C} \rightarrow \mathbf{C}^{\text{op}}$$

such that

- ▶ $\text{Hom}(A, B) \cong \text{Hom}(B^*, A^*)$
- ▶ $\text{Hom}(A \otimes B, C^*) \cong \text{Hom}(A, (B \otimes C)^*)$
- ▶ $(A \multimap B)^* \cong A \otimes B^*$
- ▶ $I \cong \perp^*$
- ▶ $A \multimap B \cong B^* \multimap A^*$

A *compact closed category* is a $*$ -autonomous category with natural isomorphisms $(A \otimes B)^* \cong A^* \otimes B^*$ and $I^* \cong I$.

It follows that $A \multimap B \cong A^* \otimes B$.

Linear Logic²⁰[Gir11]

$$A ::= p \mid 0 \mid 1 \mid \perp \mid \top \mid A^\perp \mid A \oplus A \mid A \& A \mid A \otimes A \mid A \wp A \mid A \multimap A \mid !A \mid ?A$$

\oplus	plus	+	additives	Positive	Negative					
0	the unit of \oplus									
$\&$	with	-								
\top	the unit of $\&$									
\otimes	tensor product	+	multiplicatives							
1	the unit of \otimes									
\wp	parallel product	-								
\perp	the unit of \wp									
!	of course	+	exponential	Action	Reaction					
?	why not	-	modalities	Answer	Question					

²⁰Philip Wadler: A Taste of Linear Logic.

Negation

$(p)^\perp = p^\perp$	$(p^\perp)^\perp = p$
$(A \otimes B)^\perp = A^\perp \wp B^\perp$	$(A \wp B)^\perp = A^\perp \otimes B^\perp$
$(A \oplus B)^\perp = A^\perp \& B^\perp$	$(A \& B)^\perp = A^\perp \oplus B^\perp$
$(1)^\perp = \perp$	$(\perp)^\perp = 1$
$(0)^\perp = \top$	$(\top)^\perp = 0$
$(!A)^\perp = ?(A^\perp)$	$(?A)^\perp = !(A^\perp)$

Linear Logic: A logic of resources

- ▶ $A \multimap B := A^\perp \wp B$: consume A to produce B .
- ▶ $A \wp B$: you have both A and B , but you can't use them together.
- ▶ $A \otimes B$: you can have both A and B simultaneously.
- ▶ $A \& B$: you can choose from A and B , but not both simultaneously.
- ▶ $A \oplus B$: you may have A or B , but you have no choice.
- ▶ $!A$: you can produce as many copies of A as you want, including zero copies.
- ▶ $?A$: you can consume as many copies of A as you want, including zero copies.
- ▶ 1 : the trivial resource that can be produced from nothing. $A \otimes 1 \equiv A$.
- ▶ \top : it consumes all resources. $A \& \top \equiv A$.
- ▶ 0 : the impossible resource, or something that will produce any resource. $A \oplus 0 \equiv A$.
- ▶ \perp : the resource that can be consumed by nothing. $A \wp \perp \equiv A$.
- ▶ A^\perp : the demand for an A . Negation of a consumer gives rise to a producer, and vice versa. $A^{\perp\perp} \equiv A$.

Example

- $P \otimes C \vdash H$: I will be happy given both a pizza and a cake.
- $P \& C \vdash H$: I will be happy given my choice from a pizza and a cake.
- $P \oplus C \vdash H$: I will be happy given either a pizza or a cake, I don't care which.

Menu: \$5	$(\$1 \otimes \$1 \otimes \$1 \otimes \$1 \otimes \$1)$
Fish	\multimap Fish
Chips	\otimes Chips
Soup or Salad	\otimes Soup & Salad
Fruit or Cheese (depending on availability)	\oplus Fruit \oplus Cheese
Coffee (free refills)	\otimes Coffee \otimes !Coffee

	classical	linear	
re-use	$A, A \rightarrow B \vdash A \wedge B$	$A, A \multimap B \nvDash A \otimes B$	$!A \vdash A \otimes !A$
discard	$A \wedge B \vdash A$	$A \otimes B \nvDash A$	$!A \otimes B \vdash B$

- $A \& B \vdash A \oplus B$
- $A \oplus B \nvDash A \& B$
- $A \otimes B \nvDash A \& B$
- $A \& B \nvDash A \otimes B$
- $A \nvDash A \otimes A$
- $A \otimes A \nvDash A$
- $A \multimap B \& C \vdash A \otimes A \multimap B \otimes C$

Translation

1. You can spend 1 dollar to buy a bottle of water or a bag of chips.

$$D \multimap W \& C$$

2. You can exchange a ten-dollar bill for two five-dollar bills.

$$T \multimap F \otimes F$$

3. If you has a water bottle, you can refill it with water as many times as you want.

$$B \multimap !W$$

4. If you give a man a fish, he'll eat for a day. If you teach a man to fish, he'll eat for the rest of his life.

$$(F \multimap E) \otimes (T \multimap !E)$$

5. If you flip a coin, it will come up heads or tails.

$$F \multimap H \oplus T$$

6. If you have a headache, taking ibuprofen will cure your pain.

$$H \otimes I \multimap H^\perp$$

Classical Linear Logic

$$\frac{}{A \vdash A} \text{Id}$$

$$\frac{\Gamma, \Sigma \vdash \Delta, \Theta}{\Sigma, \Gamma \vdash \Theta, \Delta} \text{ Exch} \quad \frac{\Gamma \vdash \Delta, A \quad \Sigma, A \vdash \Theta}{\Gamma, \Sigma \vdash \Delta, \Theta} \text{ Cut}$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \text{ & L}$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \text{ & L} \quad \frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \& B} \text{ & R}$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta} \text{ \oplus L}$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \oplus B} \text{ \oplus R}$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \oplus B} \text{ \oplus R}$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta} \text{ \otimes L}$$

$$\frac{\Gamma \vdash \Delta, A \quad \Sigma \vdash \Theta, B}{\Gamma, \Sigma \vdash \Delta, \Theta, A \otimes B} \text{ \otimes R}$$

$$\frac{\Gamma, A \vdash \Delta \quad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \wp B \vdash \Delta, \Theta} \text{ \wp L}$$

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \wp B} \text{ \wp R}$$

$$\frac{\Gamma \vdash \Delta, A \quad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \multimap B \vdash \Delta, \Theta} \text{ \multimap L}$$

$$\frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \multimap B} \text{ \multimap R}$$

$$\text{no } \top L \text{ rule} \qquad \overline{\Gamma \vdash \Delta, \top} \top R$$

$$\overline{\Gamma, 0 \vdash \Delta} \ 0L \qquad \text{no } 0R \text{ rule}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, 1 \vdash \Delta} \ 1L \qquad \overline{\vdash 1} \ 1R$$

$$\overline{\vdash \perp} \perp L \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \perp} \perp R$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma, A^\perp \vdash \Delta} \perp L \quad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, A^\perp} \perp R$$

$$\frac{\Gamma, !A, !A \vdash \Delta}{\Gamma, !A \vdash \Delta} !C \quad \frac{\Gamma \vdash \Delta}{\Gamma, !A \vdash \Delta} !W \quad \frac{\Gamma, A \vdash \Delta}{\Gamma, !A \vdash \Delta} !D \quad \frac{! \Gamma \vdash ?\Delta, A}{! \Gamma \vdash ?\Delta, !A} !P$$

$$\frac{\Gamma \vdash \Delta, ?A, ?A}{\Gamma \vdash \Delta, ?A} ?C \quad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, ?A} ?W \quad \frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, ?A} ?D \quad \frac{! \Gamma, A \vdash ?\Delta}{! \Gamma, ?A \vdash ?\Delta} ?P$$

Valid Formulas in Linear Logic

$$A \equiv B := (A \multimap B) \& (B \multimap A)$$

- $A \otimes (B \oplus C) \equiv (A \otimes B) \oplus (A \otimes C)$
- $(A \oplus B) \otimes C \equiv (A \otimes C) \oplus (B \otimes C)$
- $A \wp (B \& C) \equiv (A \wp B) \& (A \wp C)$
- $(A \& B) \wp C \equiv (A \wp C) \& (B \wp C)$
- $A \multimap (B \& C) \equiv (A \multimap B) \& (A \multimap C)$
- $(A \oplus B) \multimap C \equiv (A \multimap C) \& (B \multimap C)$
- $A \otimes 0 \equiv 0$
- $A \wp \top \equiv \top$
- $!(A \& B) \equiv !A \otimes !B$
- $?(A \oplus B) \equiv ?A \wp ?B$
- $!\top \equiv 1$
- $?0 \equiv \perp$

- $(A \otimes (B \wp C)) \multimap ((A \otimes B) \wp C)$
- $!A \otimes !B \multimap !(A \otimes B)$
- $!A \oplus !B \multimap !(A \oplus B)$
- $? (A \wp B) \multimap ?A \wp ?B$
- $? (A \& B) \multimap ?A \& ?B$
- $(A \& B) \otimes C \multimap (A \otimes C) \& (B \otimes C)$
- $(A \& B) \oplus C \multimap (A \oplus C) \& (B \oplus C)$
- $(A \wp C) \oplus (B \wp C) \multimap (A \oplus B) \wp C$
- $(A \& C) \oplus (B \& C) \multimap (A \oplus B) \& C$

$$\Gamma \vdash \Delta \iff \otimes \Gamma \vdash \wp \Delta$$

$$A \vdash B \iff \vdash A \multimap B$$

Embedding intuitionistic logic into linear logic

$$A \rightarrow B = !A \multimap B$$

$$A \wedge B = A \& B$$

$$A \vee B = !A \oplus !B$$

$$\top = \top$$

$$\perp = 0$$

$$\neg A = !A \multimap 0$$

$$\Gamma \vdash A = !\Gamma \vdash A$$

Remark: an alternative embedding:

$$A \wedge B = !A \otimes !B$$

$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C}$	$f : \Gamma \otimes A \otimes B \otimes \Delta \longrightarrow C$ $f \circ (1_\Gamma \otimes \sigma_{B,A} \otimes 1_\Delta) : \Gamma \otimes B \otimes A \otimes \Delta \longrightarrow C$
$\overline{A \vdash A}$	$\overline{1_A : A \longrightarrow A}$
$\frac{\Gamma \vdash A \quad A, \Delta \vdash B}{\Gamma, \Delta \vdash B}$	$\frac{f : \Gamma \longrightarrow A \quad g : A \otimes \Delta \longrightarrow B}{g \circ (f \otimes 1_\Delta) : \Gamma \otimes \Delta \longrightarrow B}$
$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}$	$\frac{f : \Gamma \longrightarrow A \quad g : \Delta \longrightarrow B}{f \otimes g : \Gamma \otimes \Delta \longrightarrow A \otimes B}$
$\frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C}$	$\frac{f : (\Gamma \otimes A) \otimes B \longrightarrow C}{f \circ \alpha_{\Gamma, A, B} : \Gamma \otimes (A \otimes B) \longrightarrow C}$
$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}$	$\frac{f : \Gamma \otimes A \longrightarrow B}{\Gamma \vdash f : \Gamma \longrightarrow (A \multimap B)}$
$\frac{\Gamma \vdash A \multimap B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B}$	$\frac{f : \Gamma \longrightarrow (A \multimap B) \quad g : \Delta \longrightarrow A}{\varepsilon_{A,B} \circ (f \otimes g) : \Gamma \otimes \Delta \longrightarrow B}$

Dagger Category

Besides the duals for objects

$$*: \mathbf{C} \rightarrow \mathbf{C}^{\text{op}}$$

we have duals for morphisms:

$$\dagger : \mathbf{C} \rightarrow \mathbf{C}^{\text{op}}$$

Definition (Dagger Category)

A *dagger category* is a category \mathbf{C} such that for any morphism $f : A \rightarrow B$ in \mathbf{C} there is a specified morphism $f^\dagger : B \rightarrow A$ such that for all $f : A \rightarrow B$ and $g : B \rightarrow C$,

- ▶ $1_A^\dagger = 1_A$
- ▶ $(gf)^\dagger = f^\dagger g^\dagger$
- ▶ $(f^\dagger)^\dagger = f$

Example — Bayes

Definition: The dagger category **Bayes** is defined as follows.

- ▶ objects (X, p) are finite sets X equipped with prior probability distributions, functions $p : X \rightarrow \mathbb{R}^+$ s.t. $\sum_{x \in X} p(x) = 1$.
- ▶ morphisms $(X, p) \rightarrow (Y, q)$ are conditional probability distributions, functions $f : X \times Y \rightarrow \mathbb{R}^{\geq 0}$ s.t.

$$\forall x : \sum_{y \in Y} f(y | x) = 1 \quad \text{and} \quad \forall y : \sum_{x \in X} p(x)f(y | x) = q(y)$$

- ▶ composition is composition of probability distributions as matrices.

$$(g \circ f)(z | x) := \sum_{y \in Y} g(z | y)f(y | x)$$

- ▶ the dagger functor is the *Bayesian converse*, acting on $f : X \times Y \rightarrow \mathbb{R}^{\geq 0}$ to give $f^\dagger : Y \times X \rightarrow \mathbb{R}^{\geq 0}$, defined by

$$f^\dagger(x | y) := \frac{p(x)f(y | x)}{q(y)}$$

The monoidal structure implements stochastic independence
 $(f \otimes g)(xy | ab) = f(x | a)g(y | b)$.

Definition

A morphism $f : A \rightarrow B$ in a dagger category is:

- ▶ the *adjoint* of $g : B \rightarrow A$ iff $g = f^\dagger$;
- ▶ *self-adjoint* iff $f = f^\dagger$ (and $A = B$);
- ▶ *idempotent* iff $ff = f$ (and $A = B$);
- ▶ a *projection* iff it is idempotent and self-adjoint;
- ▶ *unitary* iff both $f^\dagger f = 1_A$ and $ff^\dagger = 1_B$;
- ▶ an *isometry* iff $f^\dagger f = 1_A$;
- ▶ a *partial isometry* iff $f^\dagger f$ is a projection;
- ▶ *positive* iff $f = g^\dagger g$ for some morphism $g : A \rightarrow B$ (and $A = B$).

Dagger Symmetric Monoidal Category

Definition (Dagger Symmetric Monoidal Category)

A *dagger symmetric monoidal category* is a symmetric monoidal category that is a dagger category, such that the dagger structure is compatible with the monoidal structure in the following sense:

- ▶ $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$
- ▶ the canonical isomorphisms of the symmetric monoidal structure $\alpha, \lambda, \rho, \sigma$ are unitary.

Compact Closed Category

Definition (Compact Closed Category)

A *compact closed category* is a symmetric monoidal category where each object A has a dual object A^* , a unit $\eta_A : I \rightarrow A^* \otimes A$, and a counit $\varepsilon_A : A \otimes A^* \rightarrow I$ such that

$$\begin{array}{ccccc} A & \xrightarrow{\rho_A^{-1}} & A \otimes I & \xrightarrow{1_A \otimes \eta_A} & A \otimes (A^* \otimes A) \\ 1_A \downarrow & & & & \downarrow \alpha_{A,A^*,A} \\ A & \xleftarrow{\lambda_A} & I \otimes A & \xleftarrow{\varepsilon_A \otimes 1_A} & (A \otimes A^*) \otimes A \end{array}$$

$$\begin{array}{ccccc} A^* & \xrightarrow{\lambda_{A^*}^{-1}} & I \otimes A^* & \xrightarrow{\eta_A \otimes 1_{A^*}} & (A^* \otimes A) \otimes A^* \\ 1_{A^*} \downarrow & & & & \downarrow \alpha_{A^*,A,A^*}^{-1} \\ A^* & \xleftarrow{\rho_{A^*}} & A^* \otimes I & \xleftarrow{1_{A^*} \otimes \varepsilon_A} & A^* \otimes (A \otimes A^*) \end{array}$$

Example

- The category $(\mathbf{FdVect}_{\mathbb{K}}, \otimes)$ is compact. The unit and counit are

$$\eta_V : \mathbb{K} \rightarrow V^* \otimes V :: 1 \mapsto \sum_{i=1}^n \bar{e}_i \otimes e_i$$

$$\varepsilon_V : V \otimes V^* \rightarrow \mathbb{K} :: e_i \otimes \bar{e}_j \mapsto \bar{e}_j(e_i)$$

where n is the dimension of V , $\{e_i\}_{i=1}^n$ is a basis of V , and \bar{e} is the linear functional in V^* s.t. $\bar{e}_j(e_i) = \delta_{ij}$.

- The linear maps η_V and ε_V do not depend on the choice of the basis $\{e_i\}_{i=1}^n$. Since there is a canonical isomorphism

$$\mathbf{FdVect}_{\mathbb{K}}(V, V) \xrightarrow{\cong} \mathbf{FdVect}_{\mathbb{K}}(\mathbb{K}, V^* \otimes V)$$

The unit η_V is the image of 1_V under this isomorphism and 1_V is independent of the choice of basis.

Name & Coname

Definition (Name & Coname)

The name $\lceil f \rceil$ and the coname $\lfloor f \rfloor$ of a morphism $f : A \rightarrow B$ in a compact closed category are

$$\begin{array}{ccc} A^* \otimes A & \xrightarrow{1_{A^*} \otimes f} & A^* \otimes B \\ \eta_A \uparrow & \nearrow \lceil f \rceil & \\ I & & \end{array} \quad \begin{array}{ccc} & & I \\ & \nearrow \lfloor f \rfloor & \uparrow \varepsilon_B \\ A \otimes B^* & \xrightarrow{f \otimes 1_{B^*}} & B \otimes B^* \end{array}$$

Example: For $R \in \text{Rel}(X, Y)$,

$$\lceil R \rceil = \{(*, (x, y)) : Rxy\}$$

$$\lfloor R \rfloor = \{((x, y), *) : Rxy\}$$

For $f \in \mathbf{FdVect}_{\mathbb{K}}(V, W)$ with (m_{ij}) the matrix of f in bases $\{e_i^V\}_{i=1}^n$ and $\{e_j^W\}_{j=1}^m$:

$$\lceil f \rceil : \mathbb{K} \rightarrow V^* \otimes W :: 1 \mapsto \sum_{ij} m_{ij} \cdot \bar{e}_i^V \otimes e_j^W$$

$$\lfloor f \rfloor : V \otimes W^* \rightarrow \mathbb{K} :: e_i^V \otimes \bar{e}_j^W \mapsto m_{ij}$$

Dagger Compact Closed Category

Definition (Dagger Compact Closed Category)

A *dagger compact closed category* is a dagger symmetric monoidal category that is also compact closed, and such that:

$$\begin{array}{ccc} I & \xrightarrow{\varepsilon_A^\dagger} & A \otimes A^* \\ & \searrow \eta_A & \downarrow \sigma_{A,A^*} \\ & & A^* \otimes A \end{array}$$

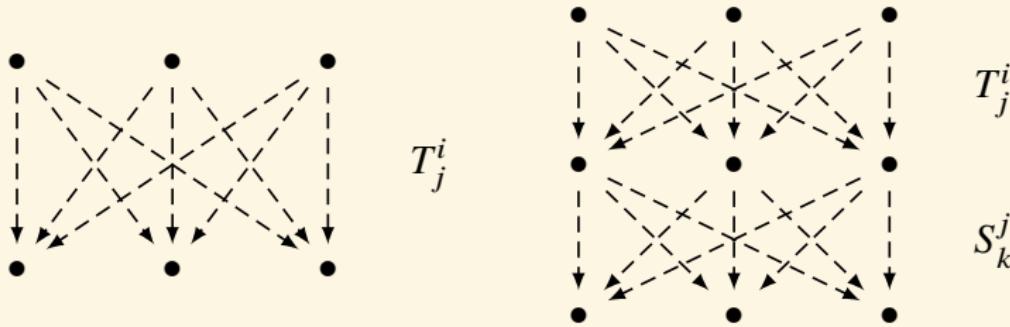
Examples

- ▶ The category **Rel** of Sets and relations. The product is the Cartesian product. The dagger is the relational converse.
- ▶ The category **FdHilb** of finite dimensional Hilbert spaces and linear maps. The morphisms are linear operators between Hilbert spaces. The product is the tensor product, and the dagger is the Hermitian conjugate.

Infinite-dimensional Hilbert spaces are dagger symmetric monoidal categories, but are not dagger compact closed categories.

Remark

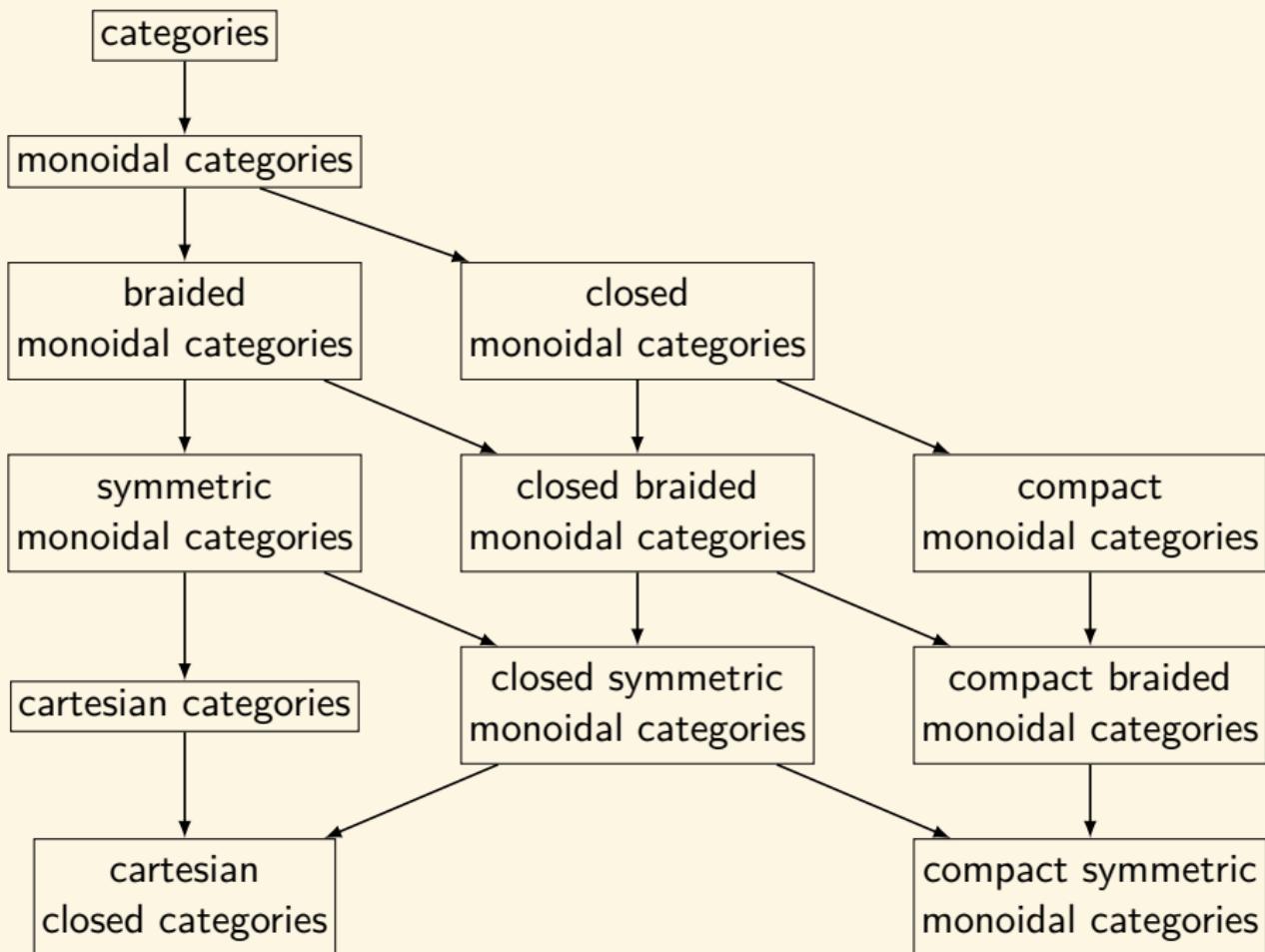
- ▶ Duality for objects $*$ and morphisms \dagger fit together in the dagger compact closed category.
- ▶ Dagger compact closed category are deeply related to ‘matrix mechanics’.

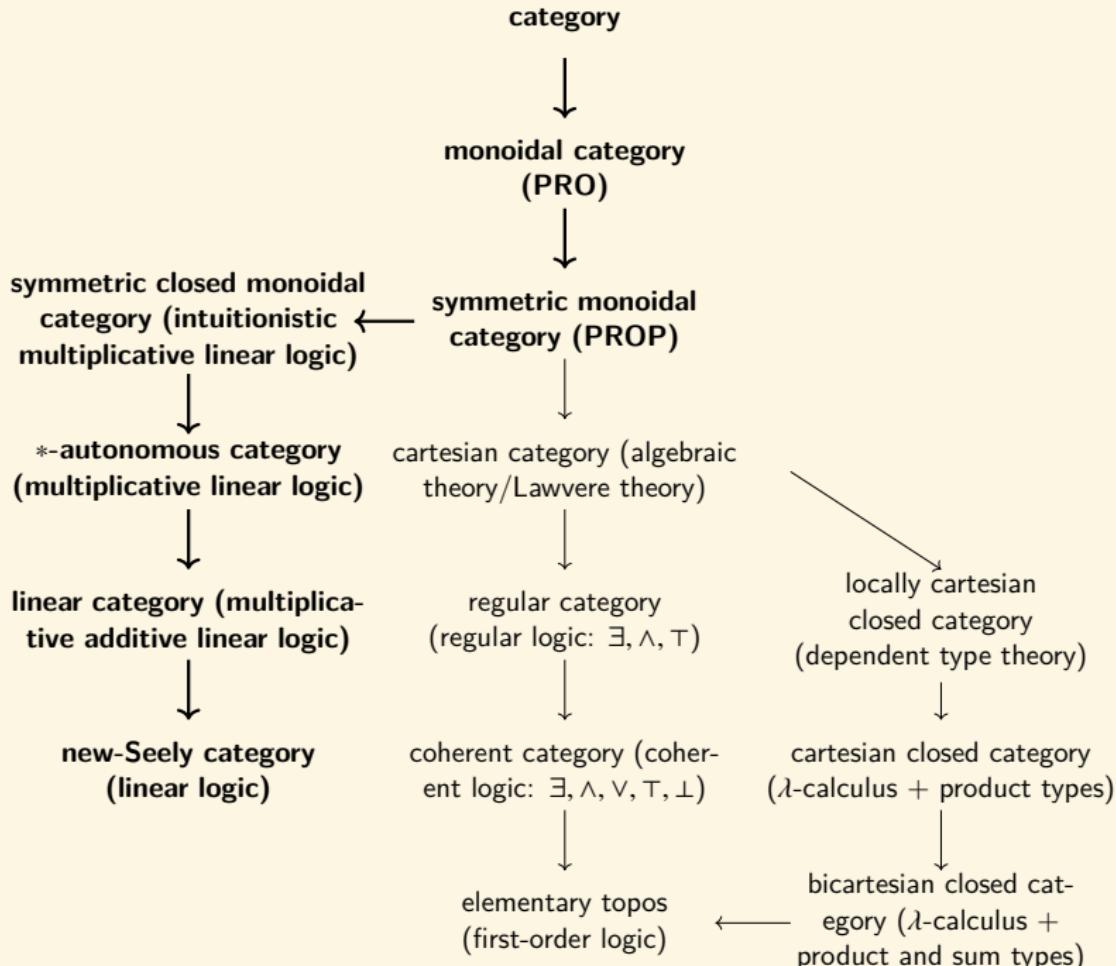


- ▶ For each input state i and output state j , the process T gives a complex number $T_j^i \in \mathbb{C}$, the amplitude to go from i to j .
- ▶ To compose processes S and T , we sum over paths:

$$(ST)_k^i = \sum_j S_k^j \times T_j^i$$

In the continuum limit, such sums become path integrals.





Definition (Monoidal Functor)

A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ between monoidal categories is *monoidal* if it is equipped with:

- ▶ a morphism $\phi : I_{\mathbf{D}} \rightarrow FI_{\mathbf{C}}$
- ▶ a natural transformation $\phi_{A,B} : FA \otimes_{\mathbf{D}} FB \rightarrow F(A \otimes_{\mathbf{C}} B)$

satisfying the following conditions:

$$\begin{array}{ccc} (FA \otimes_{\mathbf{D}} FB) \otimes_{\mathbf{D}} FC & \xrightarrow{\alpha_{FA,FB,FC}} & FA \otimes_{\mathbf{D}} (FB \otimes_{\mathbf{D}} FC) \\ \phi_{A,B} \otimes 1_{FC} \downarrow & & \downarrow 1_{FA} \otimes \phi_{B,C} \\ F(A \otimes_{\mathbf{C}} B) \otimes_{\mathbf{D}} FC & & FA \otimes_{\mathbf{D}} F(B \otimes_{\mathbf{C}} C) \\ \phi_{A \otimes_{\mathbf{C}} B, C} \downarrow & & \downarrow \phi_{A, B \otimes_{\mathbf{C}} C} \\ F((A \otimes_{\mathbf{C}} B) \otimes_{\mathbf{C}} C) & \xrightarrow{F\alpha_{A,B,C}} & F(A \otimes_{\mathbf{C}} (B \otimes_{\mathbf{C}} C)) \\ \hline I_{\mathbf{D}} \otimes_{\mathbf{D}} FA & \xrightarrow{\phi \otimes 1_{FA}} & FI_{\mathbf{C}} \otimes_{\mathbf{D}} FA & FA \otimes_{\mathbf{D}} I_{\mathbf{D}} & \xrightarrow{1_{FA} \otimes \phi} & FA \otimes_{\mathbf{D}} FI_{\mathbf{C}} \\ \lambda_{FA} \downarrow & & \downarrow \phi_{I_{\mathbf{C}}, A} & \rho_{FA} \downarrow & & \downarrow \phi_{A, I_{\mathbf{C}}} \\ FA & \xleftarrow{F\lambda_A} & F(I_{\mathbf{C}} \otimes_{\mathbf{C}} A) & FA & \xleftarrow{F\rho_A} & F(A \otimes_{\mathbf{C}} I_{\mathbf{C}}) \end{array}$$

Monoidal Functors

- If ϕ and all $\phi_{A,B}$ are isomorphisms, then F is called a *strong monoidal functor*.
- If they are identities, then F is called a *strict monoidal functor*.

Definition (Braided Monoidal Functor)

A functor $F : \mathbf{C} \rightarrow \mathbf{D}$ between braided monoidal categories is *braided monoidal* if it is monoidal and

$$\begin{array}{ccc} FA \otimes_{\mathbf{D}} FB & \xrightarrow{\sigma_{FA,FB}} & FB \otimes_{\mathbf{D}} FA \\ \phi_{A,B} \downarrow & & \downarrow \phi_{B,A} \\ F(A \otimes_{\mathbf{C}} B) & \xrightarrow{F\sigma_{A,B}} & F(B \otimes_{\mathbf{C}} A) \end{array}$$

- A *symmetric monoidal functor* is simply a braided monoidal functor that happens to go between symmetric monoidal categories!

Monoidal, Braided Monoidal, and Symmetric Monoidal Natural Transformation

Definition (Monoidal, Braided Monoidal, and Symmetric Monoidal Natural Transformation)

Suppose that (F, ϕ) and (G, ψ) are monoidal functors from the monoidal category **C** to the monoidal category **D**. Then a natural transformation $\eta : F \rightarrow G$ is *monoidal* if

$$\begin{array}{ccc} FA \otimes_D FB & \xrightarrow{\eta_A \otimes_D \eta_B} & GA \otimes_D GB \\ \phi_{A,B} \downarrow & & \downarrow \psi_{A,B} \\ F(A \otimes_C B) & \xrightarrow{\eta_{A \otimes_C B}} & G(A \otimes_C B) \end{array} \quad \begin{array}{ccc} I_D & \xrightarrow{\psi} & GI_C \\ \phi \downarrow & & \searrow \psi \\ FI_C & \xrightarrow{\eta_{I_C}} & GI_C \end{array}$$

Definition (Monoidal Equivalence)

If \mathbf{C} and \mathbf{D} are (braided / symmetric) monoidal categories, a (braided / symmetric) monoidal functor $F : \mathbf{C} \rightarrow \mathbf{D}$ is an (*braided / symmetric*) *monoidal equivalence* if there is a (braided / symmetric) monoidal functor $G : \mathbf{D} \rightarrow \mathbf{C}$ such that there exist (braided / symmetric) monoidal natural isomorphisms $GF \cong 1_{\mathbf{C}}$ and $FG \cong 1_{\mathbf{D}}$.

Theorem (Mac Lane's Strictification Theorem)

Every (braided / symmetric) monoidal category is monoidally equivalent to a strict (braided / symmetric) monoidal category.

Remark: Just like there is a 2-category **Cat** consisting of categories, functors and natural transformations, there is a 2-category **MonCat** consisting of monoidal categories, monoidal functors and monoidal transformations. Likewise, there are 2-categories **BrMonCat** and **SymmMonCat**.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
	Categorical Logic
	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
Categories	Answers to the Exercises
Cartesian Closed Categories	References 1436

Category vs Enriched Category

Definition (Category)

A category \mathbf{C} consists of

- ▶ a class $\text{ob}(\mathbf{C})$ of objects
- ▶ a set $\text{Hom}(A, B)$ for $A, B \in \text{ob}(\mathbf{C})$
- ▶ $1_a : \{\bullet\} \rightarrow \text{Hom}(A, A)$ for $A \in \text{ob}(\mathbf{C})$
- ▶ $\circ_{ABC} : \text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$ for $A, B, C \in \text{ob}(\mathbf{C})$

all subject to associativity and identity axioms.

Definition (Enrichment in a Monoidal Category)

For a monoidal category $(V, \otimes, I, \alpha, \lambda, \rho)$, a V -category \mathbf{C} consists of

- ▶ a class $\text{ob}(\mathbf{C})$ of objects
- ▶ an object $\text{Hom}(A, B)$ in V for $A, B \in \text{ob}(\mathbf{C})$
- ▶ $\text{id}_A : I \rightarrow \text{Hom}(A, A)$ in V for $A \in \text{ob}(\mathbf{C})$
- ▶ $\circ_{ABC} : \text{Hom}(A, B) \otimes \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$ in V for $A, B, C \in \text{ob}(\mathbf{C})$

all subject to associativity and identity axioms.

Enriched Category

Definition (Enrichment in a Monoidal Category)

For a monoidal category $(V, \otimes, I, \alpha, \lambda, \rho)$, a V -category \mathbf{C} consists of

- ▶ a class $\text{ob}(\mathbf{C})$ of objects.
- ▶ a hom-object $\mathbf{C}(A, B) \in V$ for $A, B \in \text{ob}(\mathbf{C})$.
- ▶ an arrow $\text{id}_A : I \rightarrow \mathbf{C}(A, A)$ in V for $A \in \text{ob}(\mathbf{C})$.
- ▶ an arrow $\circ_{ABC} : \mathbf{C}(A, B) \otimes \mathbf{C}(B, C) \rightarrow \mathbf{C}(A, C)$ in V for $A, B, C \in \text{ob}(\mathbf{C})$ such that

$$\begin{array}{ccccc} \mathbf{C}(A, B) \otimes (\mathbf{C}(B, C) \otimes \mathbf{C}(C, D)) & \xrightarrow{\alpha} & (\mathbf{C}(A, B) \otimes \mathbf{C}(B, C)) \otimes \mathbf{C}(C, D) & & \\ 1 \otimes \circ_{BCD} \downarrow & & & & \downarrow \circ_{ABC} \otimes 1 \\ \mathbf{C}(A, B) \otimes \mathbf{C}(B, D) & \xrightarrow{\circ_{ABD}} & \mathbf{C}(A, D) & \xleftarrow{\circ_{ACD}} & \mathbf{C}(A, C) \otimes \mathbf{C}(C, D) \\ \\ \mathbf{C}(A, B) \otimes \mathbf{C}(B, B) & \xrightarrow{\circ_{ABB}} & \mathbf{C}(A, B) & \xleftarrow{\circ_{AAB}} & \mathbf{C}(A, A) \otimes \mathbf{C}(A, B) \\ 1 \otimes \text{id}_B \uparrow & \nearrow \rho & & \swarrow \lambda & \uparrow \text{id}_A \otimes 1 \\ \mathbf{C}(A, B) \otimes I & & & & I \otimes \mathbf{C}(A, B) \end{array}$$

Definition (Enriched Functor)

Given two \mathbf{V} -categories \mathbf{C}, \mathbf{D} , an *enriched functor* $F : \mathbf{C} \rightarrow \mathbf{D}$ assigns to each object of \mathbf{C} an object of \mathbf{D} and for each pair of objects A and B in \mathbf{C} a morphism $F_{A,B}$ in \mathbf{V}

$$F_{A,B} : \mathbf{C}(A, B) \rightarrow \mathbf{D}(FA, FB)$$

such that

$$\begin{array}{ccc} \mathbf{C}(A, B) \otimes \mathbf{C}(B, C) & \xrightarrow{\circ_{A,B,C}} & \mathbf{C}(A, C) \\ F_{A,B} \otimes F_{B,C} \downarrow & & \downarrow F_{A,C} \\ D(FA, FB) \otimes D(FB, FC) & \xrightarrow{\circ_{FA,FB,FC}} & D(FA, FC) \end{array}$$

$$\begin{array}{ccc} & I & \\ id_A \swarrow & & \searrow id_{FA} \\ \mathbf{C}(A, A) & \xrightarrow{F_{A,A}} & \mathbf{D}(FA, FA) \end{array}$$

Examples

- ▶ A **Set**-category is a locally small category.
- ▶ A **Vect**-category is a linear category: hom-sets are vector spaces and multiplication is bilinear.
- ▶ A **Bool**-category is a preorder.

$$x \leq y \iff \text{Hom}(x, y) = \top$$

- ▶ Any preorder gives a **Bool**-category.

Hom Functors

- ▶ Hom Functor

$$\text{Hom}(-, -) : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{Set}$$

- ▶ \mathbf{V} -enriched Hom functor

$$\text{Hom}(-, -) : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{V}$$

- ▶ internal Hom functor \multimap

$$[-, -] : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{C}$$

Internalization

- ▶ Every category has a set $\text{Hom}(X, Y)$ of morphisms from one object X to another object Y .
- ▶ A cartesian closed category also has an object Y^X of morphisms from X to Y .
- ▶ Given $f : X \rightarrow Y$ in $\text{Hom}(X, Y)$ we can convert it into its *name* $\lceil f \rceil : 1 \rightarrow Y^X$ in $\text{Hom}(1, Y^X)$.
- ▶ In functional programming, objects are data types, morphisms are programs and any program $f : X \rightarrow Y$ have a name $\lceil f \rceil \in \text{Hom}(1, Y^X)$.
- ▶ *Internalization* is the process of taking math that lives in **Set** and moving it into some category **C**.

Lawvere Metric Space

Definition (Lawvere Metric Space)

A Lawvere metric space is a set X with a function $d : X \times X \rightarrow [0, \infty]$ s.t.

1. $d(x, x) = 0$
2. $d(x, z) \leq d(x, y) + d(y, z)$

- If we define $x \leq_X y := d(x, y) = 0$, then \leq_X is a partial order.
- A Lawvere metric space can be viewed as a category enriched in the monoidal poset **Cost** := $([0, \infty], \geq, +, 0)$, where the tensor product is $\otimes = +$, and the identity is $I = 0$.

$$\text{Hom}(x, y) := d(x, y) \in \text{ob}(\mathbf{Cost})$$

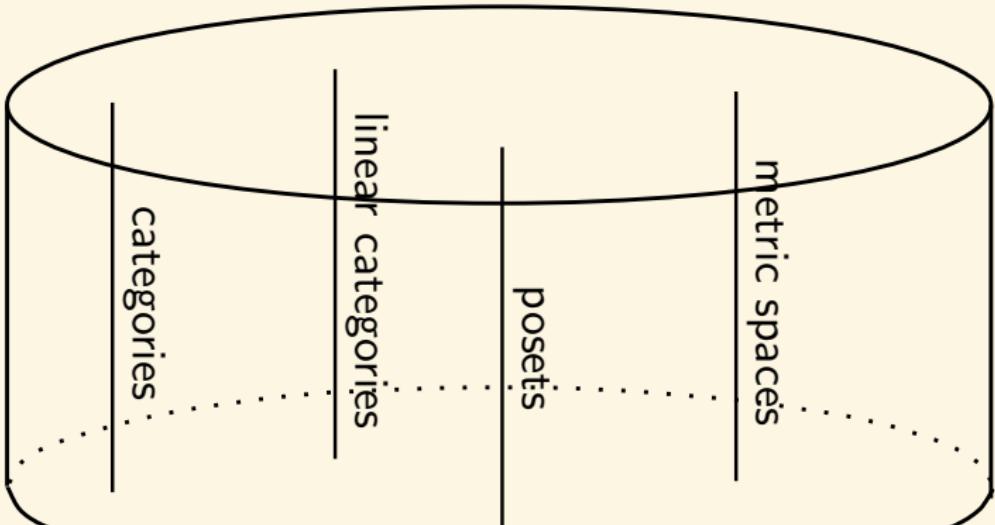
Example (I will put you in an arbitrary place of A and you have to get anywhere in B ; what is the distance in the worst-case scenario?)

$$d'(A, B) := \sup_{a \in A} \inf_{b \in B} d(a, b) \text{ for } A, B \subset X$$

then $(P(X), d')$ is a Lawvere metric space.

Enriched Categories

enriched categories



monoidal categories

• Set

• Vect

• $(0 \rightarrow 1)$

• $([0, \infty], \geq)$

Remark

Earlier	Now
$X \xrightarrow{\quad} Y$	$X \longrightarrow Y$
Hom(X, Y) is an object in Vect or Top or AbGrp ...	Hom(X, Y) is an “object” in $\{0, 1\}$ or $[0, 1]$ or $[0, \infty]$...

PROP

Definition (prop)

A *prop* is a symmetric strict monoidal category $(\mathbf{C}, 0, +)$ for which $\text{ob}(\mathbf{C}) = \mathbb{N}$, the monoidal unit is $0 \in \mathbb{N}$, and the monoidal product of objects is given by addition.

- ▶ We define a morphism of props to be a strict symmetric monoidal functor that is the identity on objects.
- ▶ Let **PROP** be the category of props.

Definition

If \mathbf{T} is a prop and \mathbf{C} is a strict symmetric monoidal category, an *algebra of \mathbf{T} in \mathbf{C}* is a strict symmetric monoidal functor $F : \mathbf{T} \rightarrow \mathbf{C}$.

The category of algebras of \mathbf{T} in \mathbf{C} , say $\text{Alg}(\mathbf{T}, \mathbf{C})$, has

- ▶ symmetric monoidal functors $F : \mathbf{T} \rightarrow \mathbf{C}$ as objects,
- ▶ symmetric monoidal natural transformations as morphisms.

Example

Example

FinSet is a prop where the morphisms $f : m \rightarrow n$ are functions from $\{1, \dots, m\}$ to $\{1, \dots, n\}$. The monoidal product on functions is given by the disjoint union of functions: that is, given $f : m \rightarrow m'$ and $g : n \rightarrow n'$, we define $f + g : m + n \rightarrow m' + n'$ by

$$i \mapsto \begin{cases} f(i) & \text{if } 1 \leq i \leq m \\ m' + g(i) & \text{if } m + 1 \leq i \leq m + n \end{cases}$$

Theorem

A symmetric monoidal category \mathbf{C} is equivalent to a prop iff there is an object $x \in \mathbf{C}$ such that every object of \mathbf{C} is isomorphic to $x^{\otimes n} = x \otimes (x \otimes (\cdots))$ for some $n \in \mathbb{N}$.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Wedge

Definition (Wedge)

Let $F : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{X}$ be a functor. A *wedge* $\alpha : x \rightarrow F$ is an object $x \in \mathbf{X}$ with maps $\alpha_A : x \rightarrow F(A, A)$ for each $A \in \mathbf{C}$, such that given any morphism $f : A \rightarrow B$ in \mathbf{C} , the following diagram commutes:

$$\begin{array}{ccc} & x & \\ \alpha_A \swarrow & & \searrow \alpha_B \\ F(A, A) & & F(B, B) \\ & \searrow F(1_A, f) & \swarrow F(f, 1_B) \\ & F(A, B) & \end{array}$$

End

Definition (End)

Let $F : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{X}$ be a functor. An end of F is a universal wedge, ie. a wedge $\pi : \text{end} \rightarrow F$ such that, for every other wedge $\alpha : x \rightarrow F$ there is a unique $u : x \rightarrow \text{end}$ such that for every $A \in \mathbf{C} : \alpha_A = \pi_A \circ u$.

$$\begin{array}{ccc} & & x \\ & \swarrow \alpha_A & \downarrow u \\ F(A, A) & \xleftarrow[\pi_A]{} & \text{end} \end{array}$$

We usually use following integral notation for ends

$$\text{end}(F) = \int_{A \in \mathbf{C}} F(A, A) \quad \text{or just} \quad \int_{\mathbf{C}} F$$

Example: the set of natural transformations between $F, G : \mathbf{C} \rightarrow \mathbf{D}$:

$$\text{Nat}(F, G) = \int_{A \in \mathbf{C}} \text{Hom}_{\mathbf{D}}(FA, GA)$$

Definition (Cowedge)

Let $F : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{X}$ be a functor. A *cowedge* $\alpha : F \rightarrow x$ is an object $x \in \mathbf{X}$ with maps $\alpha_A : F(A, A) \rightarrow x$ for each $A \in \mathbf{C}$, such that given any morphism $f : B \rightarrow A$ in \mathbf{C} , the following diagram commutes:

$$\begin{array}{ccc} & F(A, B) & \\ F(1_A, f) \swarrow & & \searrow F(f, 1_B) \\ F(A, A) & & F(B, B) \\ & \searrow \alpha_A & \swarrow \alpha_B \\ & x & \end{array}$$

Definition (Coend)

Let $F : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{X}$ be a functor. A coend of F is a universal cowedge, ie. a cowedge $\iota : F \rightarrow \text{coend}$ such that, for every other cowedge $\alpha : F \rightarrow x$ there is a unique $u : \text{end} \rightarrow x$ such that for every $A \in \mathbf{C} : \alpha_A = u \circ \iota_A$.

$$\begin{array}{ccc} F(A, A) & \xrightarrow{\iota_A} & \text{coend} \\ & \searrow \alpha_A & \downarrow u \\ & & x \end{array}$$

We usually write $\text{coend}(F) = \int^{A \in \mathbf{C}} F(A, A)$ or just $\int^{\mathbf{C}} F$

Theorem

For functors $F : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{D}$ and $B \in \mathbf{D}$,

$$\text{Hom}_{\mathbf{D}} \left(\int^{A \in \mathbf{C}} F(A, A), B \right) \cong \int_{A \in \mathbf{C}} \text{Hom}_{\mathbf{D}}(F(A, A), B)$$

$$\text{Hom}_{\mathbf{D}} \left(B, \int_{A \in \mathbf{C}} F(A, A) \right) \cong \int_{A \in \mathbf{C}} \text{Hom}_{\mathbf{D}}(B, F(A, A))$$

Profunctor

Definition (Profunctor)

A *profunctor* $F : \mathbf{C} \nrightarrow \mathbf{D}$ is a functor $F : \mathbf{C}^{\text{op}} \times \mathbf{D} \rightarrow \mathbf{Set}$.

A \mathbf{V} -enriched profunctor $F : \mathbf{C} \nrightarrow \mathbf{D}$ is a functor $F : \mathbf{C}^{\text{op}} \times \mathbf{D} \rightarrow \mathbf{V}$.

Remark

- ▶ Profunctors $F : \mathbf{C} \nrightarrow \mathbf{D}$ correspond to functors $\hat{F} : \mathbf{D} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$.
- ▶ Given $\mathbf{D} \xrightarrow{F} \mathbf{C}$, the composite $\mathbf{D} \xrightarrow{F} \mathbf{C} \xrightarrow{\text{Yoneda}} \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ induces a profunctor $\overline{F} : \mathbf{C} \nrightarrow \mathbf{D}$.
- ▶ The Hom-functor $\text{Hom} : \mathbf{C}^{\text{op}} \times \mathbf{C} \rightarrow \mathbf{Set}$ is a profunctor $\mathbf{C} \nrightarrow \mathbf{C}$.
- ▶ Profunctors are generalised relations.
A relation is a $\mathbf{V} := \{0 < 1\}$ -enriched profunctor.

The Bicategory of Profunctors

Definition (The Bicategory of Profunctors)

There exists a bicategory of profunctors **Prof** in which

- ▶ objects are categories,
- ▶ morphisms are profunctors with the composition

$$(G \circ F)(A, C) = \int^{B \in \mathbf{B}} F(A, B) \times G(B, C)$$

for $F : \mathbf{A} \rightarrow \mathbf{B}$ and $G : \mathbf{B} \rightarrow \mathbf{C}$.

- ▶ 2-morphisms are natural transformations between the profunctors.

Remark

$$(G \circ F)(A, C) = \int^{B \in \mathbf{B}} F(A, B) \times G(B, C) \quad \text{in } \mathbf{Prof}$$

$$(S \circ R)(a, c) = \exists b \in B : R(a, b) \wedge S(b, c) \quad \text{in } \mathbf{Rel}$$

Theorem

Let $F : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}$. Then

$$FA \cong \int^{X \in \mathbf{C}} \text{Hom}(X, A) \times FX$$

Proof.

For any Y , we have

$$\begin{aligned} & \text{Hom}_{\mathbf{Set}} \left(\int^{X \in \mathbf{C}} \text{Hom}(X, A) \times FX, Y \right) \\ & \cong \int_{X \in \mathbf{C}} \text{Hom}_{\mathbf{Set}}(\text{Hom}(X, A) \times FX, Y) \\ & \cong \int_{X \in \mathbf{C}} \text{Hom}_{\mathbf{Set}}(\text{Hom}(X, A), \text{Hom}_{\mathbf{Set}}(FX, Y)) \\ & \cong \text{Nat}(\text{Hom}(-, A), \text{Hom}_{\mathbf{Set}}(F-, Y)) \\ & \cong \text{Hom}_{\mathbf{Set}}(FA, Y) \end{aligned} \quad (\text{Yoneda Lemma})$$

The Hom-functor is the identity of profunctor composition.

$$(F \circ \text{Hom}(-, -))(A, B) \cong \int^{X \in \mathbf{C}} F(A, X) \times \text{Hom}(X, B) \cong F(A, B)$$

$$\text{Hom}(A, B) \cong \int^{X \in \mathbf{C}} \text{Hom}(A, X) \times \text{Hom}(X, B)$$

Analogy:

$$\int_{x \in \mathbb{R}} f(x) \delta(x - a) \, dx = f(a)$$
$$\int^{X \in \mathbf{C}} FX \times \text{Hom}(X, A) \cong FA$$

Theorem (Fubini Theorem for Ends/Coends)

Let \mathbf{V} be a symmetric monoidal category. Let \mathbf{A} and \mathbf{B} be small \mathbf{V} -enriched categories. Let

$$F : (\mathbf{A} \otimes \mathbf{B})^{\text{op}} \otimes (\mathbf{A} \otimes \mathbf{B}) \rightarrow \mathbf{V}$$

be a \mathbf{V} -enriched functor. Then: If for all object $B, B' \in \mathbf{B}$ the end $\int_{A \in \mathbf{A}} F(A, B, A, B')$ exists, then

$$\int_{(A,B) \in \mathbf{A} \otimes \mathbf{B}} F(A, B, A, B) \cong \int_{A \in \mathbf{A}} \int_{B \in \mathbf{B}} F(A, B, A, B)$$

if either side exists. In particular, since $A \otimes B \cong B \otimes A$ this implies that

$$\int_{A \in \mathbf{A}} \int_{B \in \mathbf{B}} F(A, B, A, B) \cong \int_{B \in \mathbf{B}} \int_{A \in \mathbf{A}} F(A, B, A, B)$$

Dually,

$$\int^{(A,B) \in \mathbf{A} \otimes \mathbf{B}} F(A, B, A, B) \cong \int^{A \in \mathbf{A}} \int^{B \in \mathbf{B}} F(A, B, A, B) \cong \int^{B \in \mathbf{B}} \int^{A \in \mathbf{A}} F(A, B, A, B)$$

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References 1436

Monad

Definition (Monad)

A *monad* (T, η, μ) on a category \mathbf{C} consists of

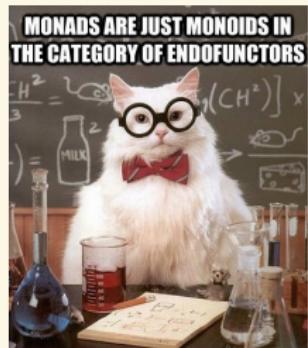
- ▶ an endofunctor $T : \mathbf{C} \rightarrow \mathbf{C}$,
- ▶ a unit natural transformation $\eta : 1_{\mathbf{C}} \rightarrow T$,
- ▶ a multiplication natural transformation $\mu : T^2 \rightarrow T$

such that:

- ▶ $\mu \circ T\mu = \mu \circ \mu T$ (as natural transformations $T^3 \rightarrow T$);
- ▶ $\mu \circ T\eta = \mu \circ \eta T = 1_T$ (as natural transformations $T \rightarrow T$).

$$\begin{array}{ccc} T^3 & \xrightarrow{\mu T} & T^2 \\ T\mu \downarrow & & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{\eta T} & T^2 \\ T\eta \downarrow & \searrow & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$



Monad

The first axiom is akin to the associativity in monoids if we think of μ as the monoid's binary operation, and the second axiom is akin to the existence of an identity element. Indeed, a monad on \mathbf{C} can be regarded as a monoid in the category $\mathbf{End}_{\mathbf{C}}$ whose objects are the endofunctors of \mathbf{C} and whose morphisms are the natural transformations between them, with the monoidal structure induced by the composition of endofunctors.

$$\begin{array}{ccc} T^3 & \xrightarrow{\mu T} & T^2 \\ T\mu \downarrow & & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{\eta T} & T^2 \\ T\eta \downarrow & \searrow & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$

$$\begin{array}{ccc} TTX & \xrightarrow{\mu_{TX}} & TTX \\ T\mu_X \downarrow & & \downarrow \mu_X \\ TTX & \xrightarrow{\mu_X} & TX \end{array}$$

$$\begin{array}{ccc} TX & \xrightarrow{\eta_{TX}} & TTX \\ T\eta_X \downarrow & \searrow & \downarrow \mu_X \\ TTX & \xrightarrow{\mu_X} & TX \end{array}$$

A *comonad* for a category \mathbf{C} is a monad for the opposite category \mathbf{C}^{op} .

Comonad

Definition (Comonad)

A *comonad* (W, ε, δ) on a category \mathbf{C} consists of

- ▶ an endofunctor $W : \mathbf{C} \rightarrow \mathbf{C}$,
- ▶ a counit natural transformation $\varepsilon : W \rightarrow 1_{\mathbf{C}}$,
- ▶ a multiplication natural transformation $\delta : W \rightarrow W^2$

such that:

- ▶ $W\delta \circ \delta = \delta W \circ \delta$ (as natural transformations $W \rightarrow W^3$);
- ▶ $W\varepsilon \circ \delta = \varepsilon W \circ \delta = 1_W$ (as natural transformations $W \rightarrow W$).

$$\begin{array}{ccc} W & \xrightarrow{\delta} & W^2 \\ \delta \downarrow & & \downarrow \delta W \\ W^2 & \xrightarrow{W\delta} & W^3 \end{array}$$

$$\begin{array}{ccc} W & \xrightarrow{\delta} & W^2 \\ \delta \downarrow & \searrow & \downarrow \varepsilon W \\ W^2 & \xrightarrow{W\varepsilon} & W \end{array}$$

Remarks

- ▶ A monad is a consistent way of extending spaces to include generalized elements and generalized functions of a specific kind.
- ▶ A comonad is a consistent way to equip spaces with extra information of a specific kind, and let some morphisms access that information.
- ▶ A monad is a consistent choice of formal expressions of a specific kind, together with ways to evaluate them.
- ▶ A comonad is a consistent way to construct, from spaces, processes of a specified structure, and give selected strategies or trajectories.

Examples

- ▶ Consider **Set**.
 - ▶ $T : A \mapsto P(A)$, and $T(f) : A \mapsto f(A)$ for object A and morphism f .
 - ▶ $\eta_A : A \rightarrow P(A)$ given by $\eta_A(a) := \{a\}$.
 - ▶ $\mu_A : P(P(A)) \rightarrow P(A)$ given by $\mu_A(B) := \bigcup B$.
- ▶ Consider **Set** and a monoid (M, e, \cdot) , the functor $M \times - : \mathbf{Set} \rightarrow \mathbf{Set}$ has a monad structure with
 - ▶ $T : A \mapsto M \times A$, and $T(f) : (m, a) \mapsto (m, f(a))$.
 - ▶ $\eta_A : A \rightarrow M \times A :: a \mapsto (e, a)$.
 - ▶ $\mu_A : M \times M \times A \rightarrow M \times A :: (m, (n, a)) \mapsto (mn, a)$.
- ▶ A preorder (P, \leq) yields a category where endofunctors are monotone functions. Given a monad (T, η, μ) , the natural transformations η and μ give that, for $a \in P$, $a \leq Ta$ and $TTa \leq Ta$, since $\eta_a : a \rightarrow Ta$, and $\mu_a : TTa \rightarrow Ta$. Then $Ta \leq TTa \leq Ta \implies TTa = Ta$. Monads on (P, \leq) are closure operators²¹.

²¹A *closure operator* on a poset (P, \leq) is $T : P \rightarrow P$ s.t. for $x, y \in P$,

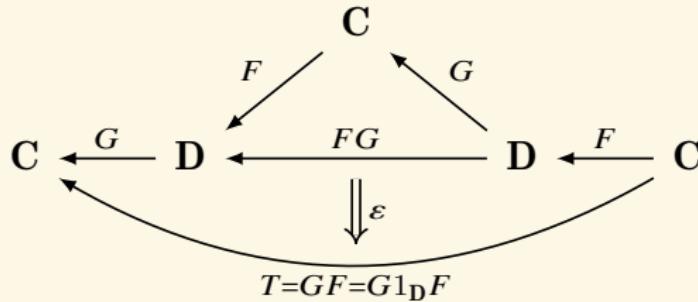
- ▶ $x \leq T(x)$
- ▶ $x \leq y \rightarrow T(x) \leq T(y)$
- ▶ $T(T(x)) = T(x)$

Monads from Adjunctions

Monads from Adjunctions

Any adjunction $C \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{G} \end{array} D$ gives rise to a monad on C , with

- ▶ the endofunctor $T := GF$,
- ▶ the unit natural transformation $\eta : 1_C \rightarrow GF$,
- ▶ the multiplication natural transformation $\mu := G\varepsilon F : GFGF \rightarrow GF$.



- ▶ $(GF, \eta, G\varepsilon F)$ is a monad.
- ▶ $(FG, \varepsilon, F\eta G)$ is a comonad.

T-Algebra

Definition

Let $T = (T, \eta, \mu)$ be a monad on \mathbf{C} . A T-algebra is a pair (A, α) where $A \in \mathbf{C}$ and $\alpha : TA \rightarrow A$ s.t.

$$\begin{array}{ccc} TTA & \xrightarrow{T\alpha} & TA \\ \mu A \downarrow & & \downarrow \alpha \\ TA & \xrightarrow{\alpha} & A \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\eta A} & TA \\ & \searrow 1_A & \downarrow \alpha \\ & & A \end{array}$$

A homomorphism of T-algebras $f : (A, \alpha) \rightarrow (B, \beta)$ is $f : A \rightarrow B$ s.t.

$$\begin{array}{ccc} TA & \xrightarrow{Tf} & TB \\ \alpha \downarrow & & \downarrow \beta \\ A & \xrightarrow{f} & B \end{array}$$

The category of T-algebras and T-algebra homomorphisms is denoted \mathbf{C}^T . This is called the Eilenberg-Moore category.

NNO — Initial T-Algebra

- ▶ An initial T-algebra is an T-algebra (I, ι) such that given any other T-algebra (A, α) there exists a unique T-algebra homomorphism $f : (I, \iota) \rightarrow (A, \alpha)$.
- ▶ A natural numbers object NNO is an initial T-algebra for the endofunctor $TA = 1 + A$.

$$\begin{array}{ccc} 1 + N & \xrightarrow{Tf} & 1 + A \\ \downarrow \iota & & \downarrow \alpha \\ N & \xrightarrow{f} & A \end{array}$$

$$\iota = \begin{bmatrix} 0 \\ s \end{bmatrix} : 1 + N \rightarrow N.$$

Theorem

Every monad $T = (T, \eta, \mu)$ arises from an adjunction $\mathbf{C} \begin{array}{c} \xrightarrow{F} \\ \perp \\ \xleftarrow{U} \end{array} \mathbf{C}^T$.

More precisely, there are natural transformations $(\dot{\eta}, \dot{\varepsilon}) : F \dashv U$ and $T = UF, \eta = \dot{\eta}, \mu = U\dot{\varepsilon}F$.

Proof.

Let the forgetful functor $U(A, \alpha) = A$, and define $FA = (TA, \mu_A)$, and $F(A \xrightarrow{f} B) = Tf$.

It is easy to check that (A, μ_A) is a T -algebra.

Clearly $UF(A) = U(TA, \mu_A) = T(A)$, and we have a natural transformation $\dot{\eta} = \eta : 1_{\mathbf{C}} \rightarrow UF$.

Define $\dot{\varepsilon} : FU \rightarrow 1_{\mathbf{C}^T}$ by $\dot{\varepsilon}_{(A, \alpha)} = \alpha : TA \rightarrow A$.

It is easy to check that $(\dot{\eta}, \dot{\varepsilon}) : F \dashv U$.

For $A \in \mathbf{C}$, $U\dot{\varepsilon}F(A) = U\dot{\varepsilon}_{FA} = U\dot{\varepsilon}_{(TA, \mu_A)} = U\mu_A = \mu_A$.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References
	1436

Sheaf

- ▶ The topology $O(X)$ of X , i.e. the poset of open subsets of X , ordered by inclusion, can be considered to be a category.
- ▶ A presheaf $F : O(X)^{\text{op}} \rightarrow \text{Set}$ is a *sheaf* iff it satisfies:
 1. (Locality) For any open cover $(U_i)_{i \in I}$ of U , and for $s, t \in F(U)$, and $\forall i : s|_{U_i} = t|_{U_i}$, then $s = t$.
 2. (Gluing) For any open cover $(U_i)_{i \in I}$ of U , and for $(s_i \in F(U_i))_{i \in I}$ such that $\forall i, j : s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$, then there exists some $s \in F(U)$ such that $\forall i : s|_{U_i} = s_i$.
- ▶ It “says” roughly that there is a unique way to “glue” together functions that are defined locally. In other words, for sheaves, one can systematically move from the local to the global.
- ▶ The category $\mathbf{Sh}(X)$ is the category of sheaves and morphisms are natural transformations between them.

Sheaf — Categorical Reformulations

- A presheaf $F : \mathcal{O}(X)^{\text{op}} \rightarrow \mathbf{Set}$ is a *sheaf* iff for any open cover $(U_i)_{i \in I}$ of U , the following diagram is an equalizer:

$$F(U) \xrightleftharpoons[e]{\quad} \prod_i F(U_i) \xrightleftharpoons[g]{\quad} \prod_{i,j} F(U_i \cap U_j)$$

Where e, f, g are given by the restriction maps:

$$e : s \mapsto (s|_{U_i})$$

$$f : (s_i) \mapsto (s_i|_{U_i \cap U_j})$$

$$g : (s_i) \mapsto (s_j|_{U_i \cap U_j})$$

$$\begin{array}{ccccc} & & F(U_i) & \xrightarrow[F(U_i \cap U_j \hookrightarrow U_i)]{} & F(U_i \cap U_j) \\ & \nearrow F(U_i \hookrightarrow U) & \uparrow \pi_i & & \uparrow \pi_{ij} \\ F(U) & \xrightleftharpoons[e]{\quad} & \prod_i F(U_i) & \xrightleftharpoons[g]{\quad} & \prod_{i,j} F(U_i \cap U_j) \\ & \searrow F(U_j \hookrightarrow U) & \downarrow \pi_j & & \downarrow \pi_{ij} \\ & & F(U_j) & \xrightarrow[F(U_i \cap U_j \hookrightarrow U_j)]{} & F(U_i \cap U_j) \end{array}$$

Sheaf — Categorical Reformulations

- Let \mathbf{I} be a category with $\text{ob}(\mathbf{I}) := \{U_i : i \in I\} \cup \{U_i \cap U_j : i, j \in I\}$, and the morphisms are the inclusions of $U_i \cap U_j$ in U_i and U_j .

$$U_i \longleftrightarrow U_i \cap U_j \longleftrightarrow U_j$$

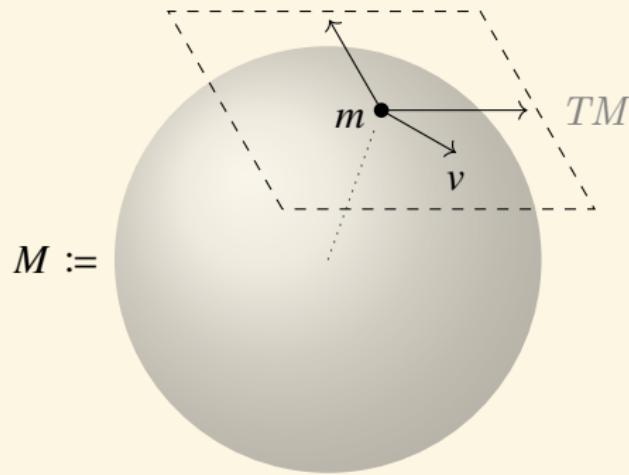
Then U can be taken as a colimit of \mathbf{I} .

$$\begin{array}{ccccc} F(U_i) & \longrightarrow & F(U_i \cap U_j) & \longleftarrow & F(U_j) \\ & \searrow & \uparrow & \nearrow & \\ & & F(U) & & \end{array}$$

A presheaf $F : \mathcal{O}(X)^{\text{op}} \rightarrow \mathbf{Set}$ is a *sheaf* iff $\varprojlim_{\mathbf{I}} F \cong F(U)$.

Sheaf — Example

A manifold M has a tangent bundle TM , whose points are pairs (m, v) , where $m \in M$ and v is a tangent vector emanating from it.



TM comes with a continuous map $f : TM \rightarrow M :: (m, v) \mapsto m$.
 $\Gamma_f : U \mapsto \{s : U \rightarrow TM : s \text{ is continuous and } f \circ s = i : U \hookrightarrow M\}$ is a sheaf. Given an open subset $U \subset M$, an element $v \in \Gamma_f(U)$ is a vector field which continuously assigns a tangent vector $v(m)$ to each point $m \in U$.

Stalk

- The *stalk* F_x of a presheaf $F : \mathcal{O}(X)^{\text{op}} \rightarrow \mathbf{Set}$ at $x \in U$ is the set of germs of F at x . Precisely,

$$F_x := \{ \text{germ}_x s : x \in U, s \in FU \}$$

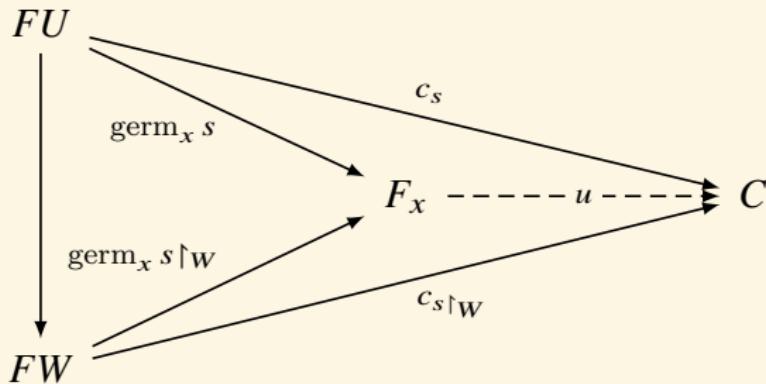
where

$$\text{germ}_x s := [s]_x$$

and $s \sim_x t$ iff there is an open set $x \in W \subset U \cap V$ with $s|_W = t|_W$ where $s \in FU, t \in FV$.

- Equivalently, $F_x := \varinjlim_{U \ni x} FU$.

The function $\text{germ}_x : FU \rightarrow F_x$ form a cocone over $F|_{\{U \in \mathcal{O}(X) : x \in U\}}$.



Etale Bundle

- ▶ Consider the slice category \mathbf{Top}/X . An *étale bundle* over X is $(Y, f : Y \rightarrow X)$ in \mathbf{Top}/X such that f is a local homeomorphism: that is, for every $y \in Y$, there is an open set $U \ni y$ such that $f(U)$ is open in X and $f|_U : U \rightarrow f(U)$ is a homeomorphism.
- ▶ The category $\mathbf{Et}(X)$ is the category of étale bundles over X and morphisms are the continuous functions between them.

$$\begin{array}{ccc} \widehat{\mathcal{O}(X)} & \xrightarrow{\Lambda} & \mathbf{Top}/X \\ & \xleftarrow{\Gamma} & \end{array}$$

where $\Gamma : Y \xrightarrow{f} X \mapsto \{s : U \rightarrow Y : f \circ s = i : U \hookrightarrow X\}$, while
 $\Lambda : F \mapsto \coprod_{x \in X} F_x = \{ \text{germ}_x s : x \in X, s \in FU \}$.

There are natural transformations

$$\eta_F : F \rightarrow \Gamma\Lambda F, \quad \varepsilon_Y : \Lambda\Gamma Y \rightarrow Y$$

for F a presheaf and Y a bundle which are unit and counit.

- ▶ If F is a sheaf, η_F is an isomorphism, while if Y is étale, ε_Y is an isomorphism. $\mathbf{Sh}(X) \xrightleftharpoons{\cong} \mathbf{Et}(X)$

Proof Sketch.

For $U \in O(X)$,

$$\eta_{FU} : FU \rightarrow \Gamma \Lambda FU :: s \mapsto \dot{s}$$

where

$$\dot{s} : U \rightarrow \Lambda F :: x \mapsto \text{germ}_x s$$

Given a bundle $Y \rightarrow X$, each point of the corresponding étale bundle $\Lambda \Gamma Y$ has the form $\dot{s}x$ for some point $x \in X$ and some actual cross-section $s : U \rightarrow Y$ of the given bundle.

$$\varepsilon_Y : \Lambda \Gamma Y \rightarrow Y :: \dot{s}x \mapsto sx$$

$$\begin{array}{ccc} \Lambda & \xrightarrow{\Lambda\eta} & \Lambda\Gamma\Lambda \\ & \searrow 1_\Lambda & \downarrow \varepsilon_\Lambda \\ & \Lambda & \end{array}$$

$$\text{germ}_x s \mapsto \text{germ}_x \dot{s} \mapsto \text{germ}_x s$$

$$\begin{array}{ccc} \Gamma & \xrightarrow{\eta\Gamma} & \Gamma\Lambda\Gamma \\ & \searrow 1_\Gamma & \downarrow \Gamma\varepsilon \\ & \Gamma & \end{array}$$

$$s \mapsto \dot{s} \mapsto s$$

Sheafification

- ▶ The inclusion functor

$$i : \mathbf{Sh}(X) \rightarrowtail \widehat{\mathcal{O}(X)}$$

has a left adjoint.

- ▶ The left adjoint functor

$$\Gamma\Lambda : \widehat{\mathcal{O}(X)} \rightarrow \mathbf{Sh}(X)$$

is known as the associated sheaf functor, or the sheafification functor. It carries each presheaf F on X to the “best approximation” $\Gamma\Lambda F$ of F by a sheaf.

Sieve

Definition (Sieve)

Given $X \in \text{ob } \mathbf{C}$, a *sieve* on X is a set S of morphisms of \mathbf{C} with codomain X which is closed under pre-composition, i.e. if $f \in S$ and $f \circ g$ is defined, then $f \circ g \in S$.

$$\begin{array}{ccc} Z & & \\ \downarrow g & \searrow f \circ g & \\ Y & \xrightarrow{f} & X \end{array}$$

Given a sieve S on X and a morphism $f : Y \rightarrow X$, then the pullback of S along f , $f^*S = \{g : \text{cod } g = Y, f \circ g \in S\}$ is a sieve on Y .

Grothendieck Topology

Definition (Grothendieck Topology)

A *Grothendieck topology* on a small category \mathbf{C} is a function J which assigns to each object $X \in \text{ob } \mathbf{C}$ a set $J(X)$ of sieves on X such that:

- ▶ (maximality) the maximal sieve $\text{Hom}(-, X) \in J(X)$.
- ▶ (stability) If $S \in J(X)$ and $f : Y \rightarrow X$, then $f^*S \in J(Y)$.
- ▶ (local character) If $S \in J(X)$ and T is any sieve on X such that, for all $f : Y \rightarrow X$ in S , $f^*T \in J(Y)$, then $T \in J(X)$.

Definition (Site)

A *site* is a pair (\mathbf{C}, J) where \mathbf{C} is a small category and J is a Grothendieck topology on \mathbf{C} .

If $X \in \text{ob } \mathbf{C}$ then we call a sieve $S \in J(X)$ a covering sieve on X .

Grothendieck Topos

- Given a site (\mathbf{C}, J) , a presheaf $P : \mathbf{C}^{\text{op}} \rightarrow \mathbf{Set}$, and a covering sieve S on $X \in \text{ob } \mathbf{C}$, a *matching family* for S of elements in P is a function which assigns to each $f : Y \rightarrow X$ in S an element $x_f \in P(Y)$ such that $P(g)(x_f) = x_{f \circ g}$ for all $g : Z \rightarrow Y$.
- If we view the sieve S as a subobject of the representable $\text{Hom}(-, X)$, then a matching family $(x_f)_{f \in S}$ is precisely a natural transformation $x : S \rightarrow P :: f \mapsto x_f$.
- An *amalgamation* of the matching family $(x_f)_{f \in S}$ is an element $x \in P(X)$ such that $P(f)(x) = x_f$ for all $f \in S$.
- Given a site (\mathbf{C}, J) , a presheaf P on \mathbf{C} is a *J-sheaf* if every matching family for any J -covering sieve on any object of \mathbf{C} has a unique amalgamation. Equivalently, P is a sheaf iff

$$\begin{array}{ccc} S & \xrightarrow{i_S} & \text{Hom}(-, X) \\ i_S : \text{Hom}(S, P) \cong \text{Hom}(\text{Hom}(-, X), P) & \downarrow x & \swarrow \\ & P & \end{array}$$

- The category $\text{Sh}(\mathbf{C}, J)$ of sheaves on the site (\mathbf{C}, J) is the full subcategory of $\widehat{\mathbf{C}}$ on the presheaves which are J -sheaves.

Grothendieck Topos

Definition (Grothendieck Topos)

A *Grothendieck topos* is any category equivalent to the category $\text{Sh}(\mathbf{C}, J)$ of sheaves on a site (\mathbf{C}, J) .

Theorem

A category \mathbf{E} is a Grothendieck topos iff there is a small category \mathbf{C} and

$$\mathbf{E} \begin{array}{c} \xleftarrow{j^*} \\[-1ex] \perp \\[-1ex] \xrightarrow{j_*} \end{array} \widehat{\mathbf{C}}$$

such that

- ▶ $j^* \dashv j_*$
- ▶ j_* is fully faithful
- ▶ j^* preserves finite limits

Grothendieck Topos

"It is the topos theme which is this 'bed' or 'deep river' where come to be married geometry and algebra, topology and arithmetic, mathematical logic and category theory, the world of the 'continuous' and that of 'discontinuous' or discrete structures. It is what I have conceived of most broad to perceive with finesse, by the same language rich of geometric resonances, an 'essence' which is common to situations most distant from each other coming from one region or another of the vast universe of mathematical things."

— Grothendieck

Lawvere-Tierney Topology

Definition (Lawvere-Tierney Topology)

A *Lawvere-Tierney topology* on a topos \mathbf{E} is a morphism $j : \Omega \rightarrow \Omega$ such that

1. j preserves truth: $j \circ \text{true} = \text{true}$.
2. j preserves intersections: $j \circ \wedge = \wedge \circ (j \times j)$.
3. j is idempotent: $j \circ j = j$.

$$\begin{array}{ccc} 1 & \xrightarrow{\text{true}} & \Omega \\ & \searrow \text{true} & \downarrow j \\ & & \Omega \end{array} \quad \begin{array}{ccc} \Omega & \xrightarrow{j} & \Omega \\ & \searrow j & \downarrow j \\ & & \Omega \end{array} \quad \begin{array}{ccc} \Omega \times \Omega & \xrightarrow{\wedge} & \Omega \\ & j \times j \downarrow & \downarrow j \\ \Omega \times \Omega & \xrightarrow{\wedge} & \Omega \end{array}$$

Universal Closure Operator

Definition (Universal Closure Operator)

A *universal closure operator* on a topos \mathbf{E} is given by, for each object X , a morphism $(\bar{\cdot}) : \text{Sub}(X) \rightarrow \text{Sub}(X)$ such that

1. $A \leq \bar{A}$
2. $\bar{\bar{A}} = \bar{A}$
3. $A \leq B \implies \bar{A} \leq \bar{B}$
4. for $f : Y \rightarrow X$ and $A \in \text{Sub}(X)$, $f^*(\bar{A}) = \overline{f^*(A)}$

Theorem

The following are equivalent:

1. A Grothendieck topology on \mathbf{C} .
2. A Lawvere-Tierney topology on $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$.
3. A universal closure operator on $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$.
4. A full subcategory \mathbf{E} of $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$ such that the inclusion $\mathbf{E} \rightarrow \mathbf{Set}^{\mathbf{C}^{\text{op}}}$ has a left adjoint which preserves finite limits.

Definition

Given a Lawvere-Tierney topology j with associated closure operator on $\mathbf{Set}^{\mathbf{C}^{\text{op}}}$, a subobject $M \in \text{Sub}(X)$ is called

- ▶ *dense* if $\overline{M} = X$.
- ▶ *colosed* if $\overline{M} = M$.

A presheaf F is a *j -sheaf* iff for every dense $M \rightarrowtail X$ the induced morphism

$$\text{Hom}(X, F) \rightarrow \text{Hom}(M, F)$$

is an isomorphism.

$$\begin{array}{ccc} M & \xleftrightarrow{\text{dense}} & X \\ \downarrow & \nearrow ! & \\ F & & \end{array}$$

F is called *j -separated* if for every dense $M \rightarrowtail X$ the induced morphism

$$\text{Hom}(X, F) \rightarrow \text{Hom}(M, F)$$

is a monomorphism.

Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

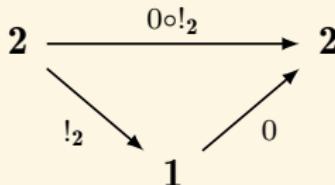
Category of Categories as Foundations CCAF

Lawvere's aim is to provide an axiomatization of category of categories as a foundation for mathematics in first-order language such that:

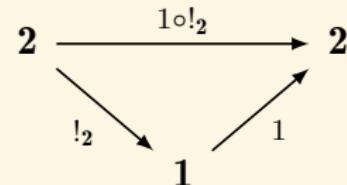
1. A model of the axioms should be a category.
2. The objects of the model should themselves be categories.
3. The basic properties of category theory can be proved, e.g. functor categories and adjoint functors should be definable, Yoneda's lemma and the adjoint functor theorem should be provable, etc.
4. Sets (all usual mathematical objects) should be definable, and all their usual properties provable.
5. It should be possible to make a distinction between small and large categories, and Grothendieck universes should be models of the theory.

CCAF

- ▶ There is a terminal category **1**.
- ▶ There is a category **2** that has exactly two functors $0 \neq 1 : 1 \rightarrow 2$ and three functors $2 \rightarrow 2$.



$$2 \xrightarrow{1_2} 2$$



- ▶ **2** is a universal generator: $\forall F \neq G : A \rightarrow B \exists f : 2 \rightarrow A [Ff \neq Gf]$

$$2 \xrightarrow{f} A \begin{array}{c} \xrightarrow{F} \\ \xleftarrow{G} \end{array} B$$

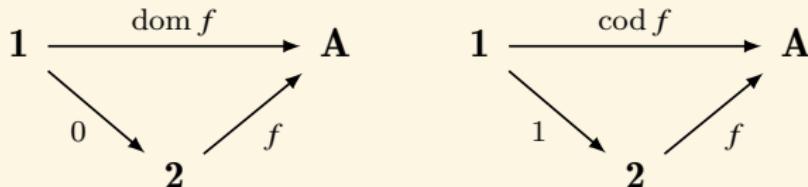
if **C** has the same property, then $\exists g : 2 \rightarrow C \exists h : C \rightarrow 2 : hg = 1_2$.

$$2 \begin{array}{c} \xrightarrow{g} \\ \xleftarrow{h} \end{array} C$$

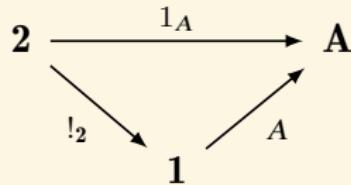
CCAF

Definition:

- an object A of \mathbf{A} means $A : \mathbf{1} \rightarrow \mathbf{A}$.
- a morphism f of \mathbf{A} means $f : \mathbf{2} \rightarrow \mathbf{A}$.
- The domain $\text{dom } f$ and codomain $\text{cod } f$ of f in \mathbf{A} are defined to be the composites of f with $0 : \mathbf{1} \rightarrow \mathbf{2}$ and $1 : \mathbf{1} \rightarrow \mathbf{2}$.



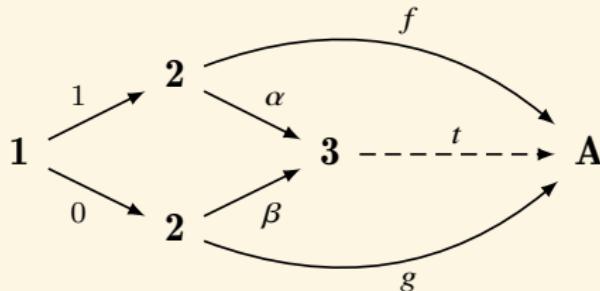
- The identity morphism 1_A on A is defined to be the composite $A \circ !_2$



- A discrete category is defined as a category \mathbf{C} such that each morphism $\mathbf{2} \rightarrow \mathbf{C}$ is the identity morphism 1_A for some object $A : \mathbf{1} \rightarrow \mathbf{C}$.

CCAF

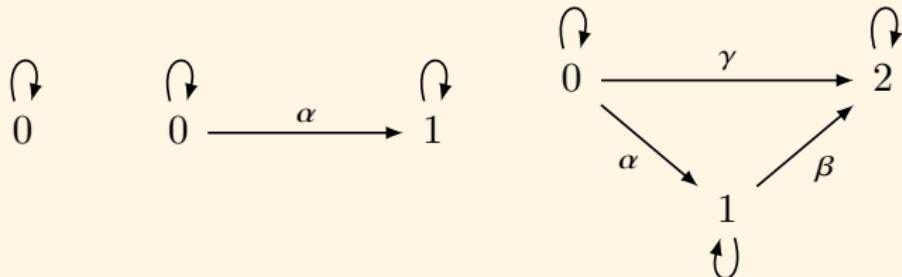
- There is a category **3** that is a pushout, and there is a functor $\gamma : \mathbf{2} \rightarrow \mathbf{3}$ with $\text{dom } \gamma = \text{dom } \alpha$ and $\text{cod } \gamma = \text{cod } \beta$.



Definition:

- given any $f : \mathbf{2} \rightarrow \mathbf{A}$ and $g : \mathbf{2} \rightarrow \mathbf{A}$ with $\text{cod } f = \text{dom } g$, the composition gf in \mathbf{A} is $t\gamma$.

Remark: **1, 2, 3** naively look like this:



CCAF

- ▶ There is an initial category **0**.
- ▶ Every pair of categories **A** and **B** has a product $\mathbf{A} \times \mathbf{B}$ and a coproduct $\mathbf{A} + \mathbf{B}$.

The left diagram shows the construction of the product $\mathbf{A} \times \mathbf{B}$. Category **C** contains objects $\mathbf{A} \times \mathbf{B}$, **A**, and **B**. There is a dashed arrow $\langle F, G \rangle$ from **C** to $\mathbf{A} \times \mathbf{B}$. From $\mathbf{A} \times \mathbf{B}$, two arrows π_1 and π_2 point to **A** and **B** respectively. There is also a curved arrow F from **C** to **A**.

The right diagram shows the construction of the coproduct $\mathbf{A} + \mathbf{B}$. Category **C** contains objects $\mathbf{A} + \mathbf{B}$, **A**, **B**, and **C**. There is a dashed arrow $\begin{bmatrix} F \\ G \end{bmatrix}$ from **C** to $\mathbf{A} + \mathbf{B}$. From $\mathbf{A} + \mathbf{B}$, two arrows ι_1 and ι_2 point to **A** and **B** respectively. There is also a curved arrow F from **A** to **C** and a curved arrow G from **B** to **C**.

- ▶ Every parallel pair of functors $F, G : \mathbf{A} \rightarrow \mathbf{B}$ has an equilizer and a coequalizer.

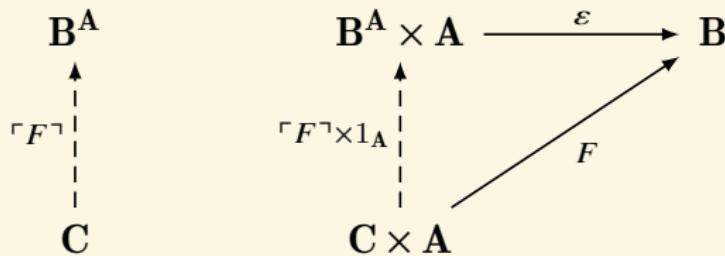
Category **C** contains objects **E**, **A**, and **B**. There is a vertical dashed arrow u from **C** to **E**. From **E**, there is a horizontal arrow e to **A**. From **A**, there are two parallel horizontal arrows F and G to **B**. There is also a diagonal arrow H from **E** to **B**.

Category **C** contains objects **A**, **B**, **Q**, and **C**. There is a horizontal arrow F from **A** to **B**. There is also a horizontal arrow G from **A** to **B**. From **B**, there is a horizontal arrow q to **Q**. From **B**, there is a diagonal arrow H to **C**. There is also a vertical dashed arrow u from **Q** to **C**.

CCAF

- There is a functor category $\mathbf{B}^{\mathbf{A}}$ from any category \mathbf{A} to any category \mathbf{B} .

$$\forall \mathbf{C} \forall F : \mathbf{C} \times \mathbf{A} \rightarrow \mathbf{B} \exists! \lceil F \rceil : \mathbf{C} \rightarrow \mathbf{B}^{\mathbf{A}} \left[\varepsilon \circ (\lceil F \rceil \times 1_{\mathbf{A}}) = F \right]$$



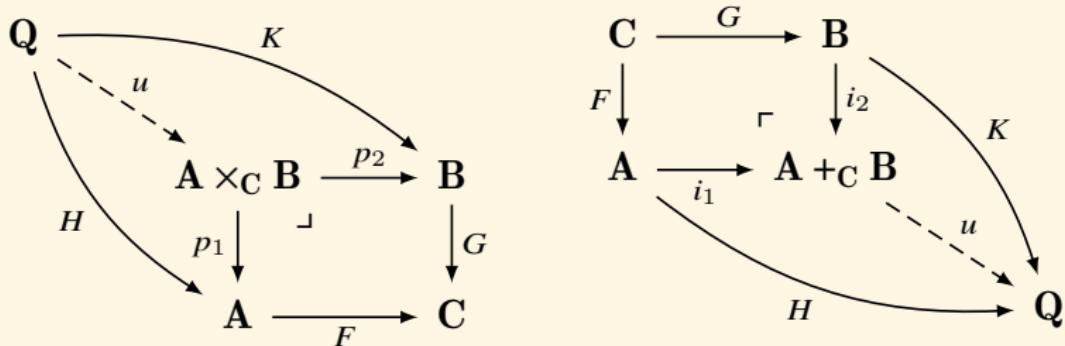
CCAF

- ▶ Every two functors $F : \mathbf{A} \rightarrow \mathbf{C}, G : \mathbf{B} \rightarrow \mathbf{C}$ have a pullback.

$$\forall H : \mathbf{Q} \rightarrow \mathbf{A}, K : \mathbf{Q} \rightarrow \mathbf{B} [FH = GK \rightarrow \exists! u (p_1 u = H \& p_2 u = K)]$$

- ▶ Every two functors $F : \mathbf{C} \rightarrow \mathbf{A}, G : \mathbf{C} \rightarrow \mathbf{B}$ have a pushout.

$$\forall H : \mathbf{A} \rightarrow \mathbf{Q}, K : \mathbf{B} \rightarrow \mathbf{Q} [HF = KG \rightarrow \exists! u (ui_1 = H \& ui_2 = K)]$$



CCAF

- There is a natural numbers object NNO category.

$$\begin{array}{ccccc} \mathbf{1} & \xrightarrow{0} & \mathbf{N} & \xrightarrow{S} & \mathbf{N} \\ & \searrow x & \downarrow F & & \downarrow F \\ & & \mathbf{X} & \xrightarrow{T} & \mathbf{X} \end{array}$$

- Choice. For $F : \mathbf{A} \rightarrow \mathbf{B}$ such that $\mathbf{A} \not\cong \mathbf{0}$ and \mathbf{B} is discrete, there exists $G : \mathbf{B} \rightarrow \mathbf{A}$ such that $FG = 1_{\mathbf{B}}$.

CCAF axioms on **Set**

- ▶ There is a category **Set** whose objects and morphisms satisfy the ETCS axioms.

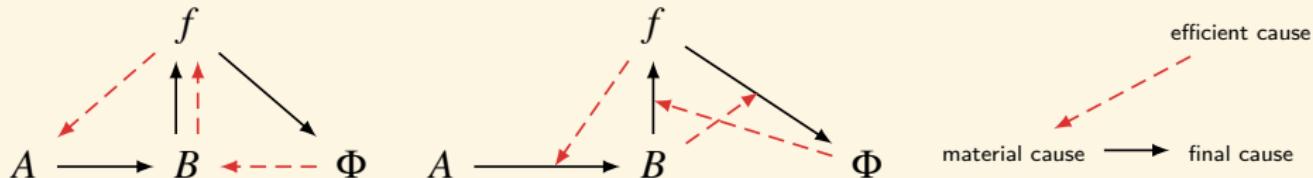
Contents

Introduction	Functors
Term Logic	Natural Transformations
Propositional Logic	Equivalence of Categories
Predicate Logic	Product and Functor Category
Modal Logic	Limits and Colimits
Set Theory	Construct New from Old
Recursion Theory	Topos
Equational Logic	ETCS
Homotopy Type Theory	Yoneda Lemma
Category Theory	Adjunctions
Categories	Categorical Logic
Cartesian Closed Categories	Kan Extensions
	Monoidal Categories
	Enriched Categories
	End/Coend
	Monads
	Sheaves
	CCAF
	Rosen's (M, R) -System
	Quantum Computing
	Answers to the Exercises
	References1436

Rosen's Metabolism-Repair (M, R)-System²²

$$A \xrightarrow{f} B \xrightarrow{\Phi} \text{Hom}(A, B) \xrightarrow{\beta} \text{Hom}(B, \text{Hom}(A, B))$$

- ▶ f : metabolism $f(a) = b$
- ▶ Φ : repair $\Phi(b) = f$
- ▶ β : organizational invariance $\beta(f) = \Phi$



Remark: β can be constructed in the following way:

If $\varepsilon_b : \text{Hom}(B, \text{Hom}(A, B)) \rightarrow \text{Hom}(A, B)$:: $\varepsilon_b(\phi) = \phi(b)$ has an inverse, $\varepsilon_b(\phi) = \varepsilon_b(\phi') \implies \phi = \phi'$, then $\varepsilon_b^{-1}(f) = \Phi$. Thus, we can set $\beta = \varepsilon_b^{-1}$. Namely, β is determined by b .

²²Letelier et al: Organizational invariance and metabolic closure: analysis in terms of (M,R) systems. 2006.

Rosen's (M, R) -System in terms of λ -calculus

If we take $\beta = B$, then

$$(fA) = B$$

$$(\Phi B) = f$$

$$(Bf) = \Phi$$

By substitution, we get

$$((fA)f)(fA) = f$$

Let

$$G := \lambda x.((xA)x)(xA)$$

we have $\mathbf{Y}G = G(\mathbf{Y}G)$ with the \mathbf{Y} combinator.

f, B, Φ are fully determined by A .

$$f = \mathbf{Y}G$$

$$B = \mathbf{Y}GA$$

$$\Phi = (\mathbf{Y}GA)(\mathbf{Y}G)$$

Ouroboros Equation $f(f) = f$

$$A \xrightarrow{f} B \xrightarrow{\Phi} \text{Hom}(A, B) \xrightarrow{\beta} \text{Hom}(B, \text{Hom}(A, B))$$

$f(a) = b$ with $f \in \text{Hom}(A, B)$

$\Phi(b) = f$ with $\Phi \in \text{Hom}(B, \text{Hom}(A, B))$

$\beta(f) = \Phi$ with $\beta \in \text{Hom}(\text{Hom}(A, B), \text{Hom}(B, \text{Hom}(A, B)))$

$$\begin{array}{lll} C_0 := A & c_0 := a \\ C_1 := B & f_0 := f & c_1 := b = f_0(c_0) \\ C_2 := \text{Hom}(C_0, C_1) & f_1 := \Phi & c_2 := f = f_1(c_1) = f_0 \\ C_n := \text{Hom}(C_{n-2}, C_{n-1}) & f_2 := \beta & c_3 := \Phi = f_2(c_2) = f_1 \\ & & c_{n+1} := f_n(c_n) = f_{n-1} \end{array}$$

$$C_0 \xrightarrow{f_0} C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} C_n \xrightarrow{f_n} \textcolor{red}{C_{n+1}} = \text{Hom}(C_{n-1}, C_n)$$

$$c_0 \longmapsto c_1 \longmapsto c_2 \longmapsto \dots \longmapsto c_n \longmapsto \textcolor{red}{c_{n+1}} = f_{n-1} = f_n(f_{n-2})$$

Ouroboros Equation $f(f) = f$

$$C_0 \xrightarrow{f_0} C_1 \xrightarrow{f_1} C_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} C_n \xrightarrow{f_n} C_{n+1} = \text{Hom}(C_{n-1}, C_n)$$

$$c_0 \longmapsto c_1 \longmapsto c_2 \longmapsto \dots \longmapsto c_n \longmapsto c_{n+1} = f_{n-1} = f_n(f_{n-2})$$

$$C_\infty := \lim_{n \rightarrow \infty} C_n = \text{Hom}(C_\infty, C_\infty)$$

$$f_\infty := \lim_{n \rightarrow \infty} f_n \implies f_\infty(f_\infty) = f_\infty$$

$$f_\infty \in \text{Hom}(C_\infty, C_\infty) = C_\infty$$

$$f_n(c_n) = f_{n-1} \implies \varepsilon_{c_n}(f_n) = f_{n-1}$$

$$p_n := \varepsilon_{c_{n-1}} : C_n \leftarrow C_{n+1} :: p_{n+1}(f_n) = f_{n-1}$$

$$C_1 \xleftarrow{p_1} C_2 \xleftarrow{p_2} \dots \xleftarrow{p_{n-1}} C_n \xleftarrow{p_n} C_{n+1} \xleftarrow{p_{n+1}} C_{n+2} \xleftarrow{p_{n+2}} \dots$$

$$c_1 \xleftarrow{p_1} f_0 \xleftarrow{p_2} \dots \xleftarrow{p_{n-1}} f_{n-2} \xleftarrow{p_n} f_{n-1} \xleftarrow{p_{n+1}} f_n \xleftarrow{p_{n+2}} \dots$$

$$C^\infty := \varprojlim(C_n, p_n) = \{(c_1, c_2, \dots) : c_n \in C_n \text{ and } p_n(c_{n+1}) = c_n \text{ for all } n\}$$

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Metric Space & Topological Space

Definition (Metric Space)

A *metric space* (X, d) is a set X with a metric $d : X \times X \rightarrow \mathbb{R}$ s.t. for all $x, y, z \in X$:

1. $d(x, y) = 0 \leftrightarrow x = y$
2. $d(x, y) = d(y, x)$
3. $d(x, z) \leq d(x, y) + d(y, z)$

Definition (Topological Space)

A *topological space* $(X, \mathcal{O}(X))$ is a set X with a family $\mathcal{O}(X) \subset \mathcal{P}(X)$ of subsets of X which contains \emptyset and X , and is closed under finite intersections and arbitrary unions.

Definition (Manifold)

An *m-manifold* is a Hausdorff space with a countable basis such that every point has an open neighborhood homeomorphic to an open neighborhood in Euclidean space \mathbb{R}^m .

Vector Space

Definition (Vector Space)

A vector space over a field \mathbb{K} is a set V with an element $0 \in V$, addition $+ : V \times V \rightarrow V$, and scalar multiplication $\cdot : \mathbb{K} \times V \rightarrow V$ s.t. for all $a, b \in \mathbb{K}$ and $u, v, w \in V$:

1. $(u + v) + w = u + (v + w)$
2. $u + v = v + u$
3. $v + 0 = v$
4. there exists a $-v \in V$ s.t $v + (-v) = 0$
5. $(ab)v = a(bv)$
6. $1v = v$
7. $a(u + v) = au + av$
8. $(a + b)v = av + bv$

Normed Vector Space

Definition (Normed Vector Space)

A *normed vector space* $(V, \|\cdot\|)$ is a vector space over a field \mathbb{K} with a *norm* $\|\cdot\| : V \rightarrow [0, \infty)$ s.t. for all $a \in \mathbb{K}$, and $u, v \in V$:

1. $\|av\| = |a|\|v\|$
2. $\|u + v\| \leq \|u\| + \|v\|$
3. $\|v\| = 0 \rightarrow v = 0$

- If $\|\cdot\|$ is a norm on V , then $d(u, v) = \|u - v\|$ defines a metric on V .
- A metric space is *complete* iff for every Cauchy sequence $\{x_n\}$,
$$\lim_{n \rightarrow \infty} \|x - x_n\| = 0.$$
- A *Banach space* is a complete normed vector space.

Inner Product Space

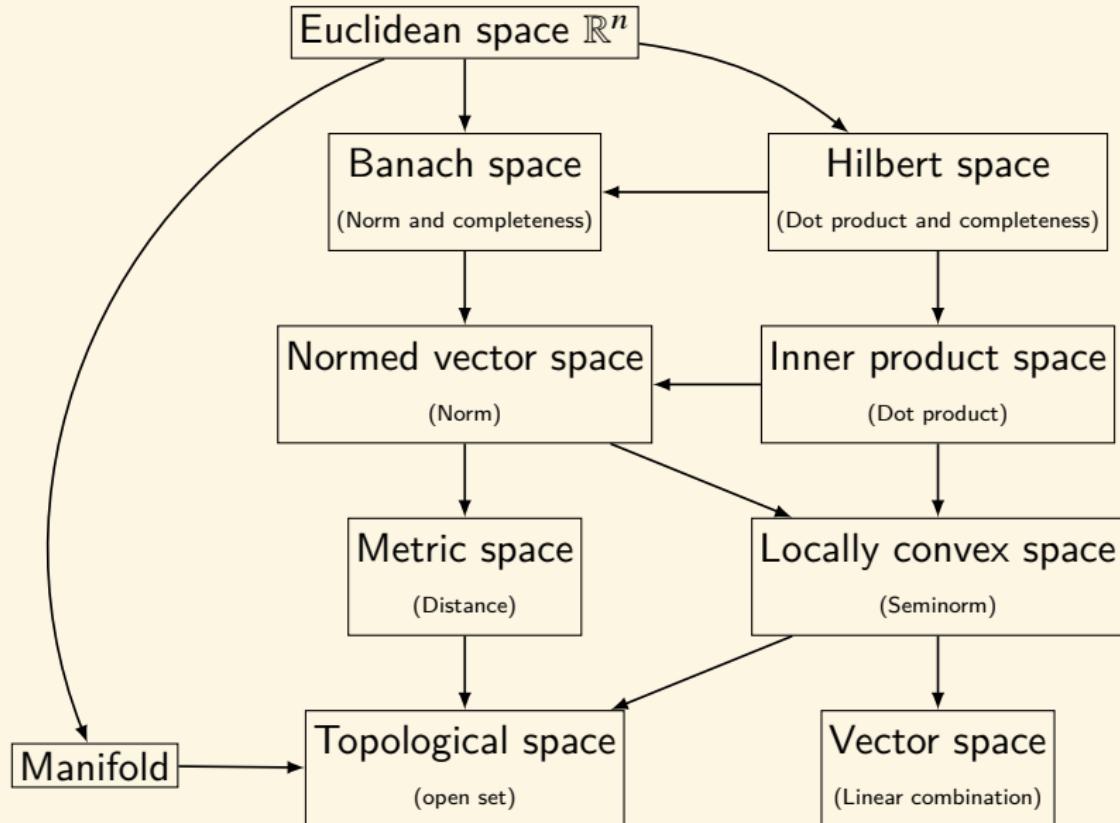
Definition (Inner Product Space)

An *inner product space* $(V, \langle \cdot | \cdot \rangle)$ is a vector space over a field \mathbb{K} with an *inner product* $\langle \cdot | \cdot \rangle : V \times V \rightarrow \mathbb{K}$ s.t. for all $a, b \in \mathbb{K}$ and $u, v, w \in V$:

1. $\langle u | av + bw \rangle = a\langle u | v \rangle + b\langle u | w \rangle$
2. $\langle u | v \rangle = \overline{\langle v | u \rangle}$
3. $\langle v | v \rangle \geq 0$
4. $\langle v | v \rangle = 0 \rightarrow v = 0$

- ▶ The vectors u, v are called *orthogonal* iff $\langle u | v \rangle = 0$.
- ▶ A basis $\{e_1, \dots, e_n\}$ is called *orthogonal* iff $\langle e_i | e_j \rangle = 0$ for all $i \neq j$. It is called *orthonormal* iff in addition $\langle e_i | e_i \rangle = 1$ for all i .
- ▶ A *Hilbert space* is a real or complex inner product space that is complete in the norm $\|v\| = \sqrt{\langle v | v \rangle}$.

Spaces



Linear Operator

Definition

A linear operator A is

- ▶ *normal* iff $AA^\dagger = A^\dagger A$.
- ▶ *unitary* iff $AA^\dagger = A^\dagger A = I$.
- ▶ *self-adjoint* iff $A = A^\dagger$.
- ▶ a *projection* iff $A = A^\dagger$ and $AA = A$.
- ▶ *bounded* iff $\exists a \geq 0 \forall v : \|Av\| \leq a\|v\|$.

The adjoint of a linear operator A is the function A^\dagger s.t. for every u, v :

$$\langle Au | v \rangle = \langle u | A^\dagger v \rangle$$

In terms of matrices, $A^\dagger = \overline{A^T}$.

Definition (Tensor Product)

Suppose U and V are vector spaces over a field \mathbb{K} . Then a tensor product of U and V is a vector space $U \otimes V$ over \mathbb{K} with a bilinear map $\varphi : U \times V \rightarrow U \otimes V :: (u, v) \mapsto u \otimes v$ having the “universal property”:

$$\begin{array}{ccc} U \times V & \xrightarrow{\varphi} & U \otimes V \\ & \searrow f & \downarrow \exists! \bar{f} \\ & & W \end{array}$$

Given two linear maps $A : U \rightarrow X$ and $B : V \rightarrow Y$ between vector spaces, the tensor product of the two linear maps A and B is a linear map $A \otimes B : U \otimes V \rightarrow X \otimes Y$ defined by

$$(A \otimes B)(u \otimes v) = Au \otimes Bv$$

$$W = X \otimes Y \quad f : (u, v) \mapsto Au \otimes Bv \quad \bar{f} = A \otimes B$$

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{m1}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

The Postulates of Quantum Mechanics[NC10]

- I. A pure state of a system in quantum mechanics is represented in terms of a normalized vector $|\psi\rangle$ in a separable complex Hilbert space.
- II. The time evolution of the state of a closed quantum system from t_0 to t_1 is described by a unitary transformation: $|\psi_{t_1}\rangle = U|\psi_{t_0}\rangle$.
- III. A quantum measurement is described by an observable, A , a self-adjoint linear operator acting on the Hilbert space. The possible outcomes of the measurement correspond to the eigenvalues a of the observable. The observable has a spectral decomposition $A = \sum_a aP_a$, where $P_a = \sum_i |e_i\rangle\langle e_i| \delta_{a_i a}$ is the projector onto the subspace spanned by all the eigenvectors that produce the same eigenvalue a . If the system is in a pure state $|\psi\rangle$ immediately before the measurement then the probability of obtaining an eigenvalue a of an observable A is $p(a) = \langle\psi|P_a|\psi\rangle$, and the state of the system after the measurement is $\frac{P_a|\psi\rangle}{\sqrt{\langle\psi|P_a|\psi\rangle}}$.
- IV. The Hilbert space of a composite system is the tensor product of the state spaces of the component systems.

The No-cloning Theorem

Theorem (The No-cloning Theorem)

If there is a unitary operator U and two quantum states $|\phi\rangle$ and $|\psi\rangle$, and U takes $|\phi\rangle \otimes |0\rangle$ to $|\phi\rangle \otimes |\phi\rangle$ and $|\psi\rangle \otimes |0\rangle$ to $|\psi\rangle \otimes |\psi\rangle$, then either $\phi = \psi$ or $\phi \perp \psi$.

Proof.

$$\begin{aligned}\langle\phi|\psi\rangle &= \langle\phi|\psi\rangle\langle 0|0\rangle \\ &= (\langle\phi|\langle 0|)(|\psi\rangle|0\rangle) \\ &= (\langle\phi|\langle 0|)U^\dagger U(|\psi\rangle|0\rangle) \\ &= (\langle\phi|\langle\phi|)(|\psi\rangle\psi\rangle) \\ &= \langle\phi|\psi\rangle\langle\phi|\psi\rangle \\ &= \langle\phi|\psi\rangle^2\end{aligned}$$

Remark: Quantum states cannot be cloned. It's impossible to measure a qubit in two different ways (even, indirectly, by using a copy trick).

Physical Concept	Mathematical Representation	
	Classical mechanics	Quantum mechanics
state	point	vector
state space	set of points (phase space)	vector space
property	function on points	operator on vectors

Quantum Computing

- ▶ the standard basis states: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- ▶ the vector representation of a 1-qubit: $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$
where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.
- ▶ n -qubit: $|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle$ with $\sum_{x \in \{0,1\}^n} |a_x|^2 = 1$.
- ▶ for $|\phi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$, $|\psi\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$, the tensor product of two qubits is

$$|\phi\rangle \otimes |\psi\rangle = |\phi\rangle |\psi\rangle = |\phi\psi\rangle = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

- ▶ the conjugate transpose of $|\phi\rangle$ is $\langle\phi| = |\phi\rangle^\dagger = [\overline{a_0} \quad \overline{a_1}]$
- ▶ the inner product: $\langle\phi||\psi\rangle = \langle\phi|\psi\rangle = \sum_i \overline{a_i} b_i = \overline{a_0} b_0 + \overline{a_1} b_1$
- ▶ the outer product: $|\phi\rangle\langle\psi| = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} [\overline{b_0} \quad \overline{b_1}] = \begin{bmatrix} a_0 \overline{b_0} & a_0 \overline{b_1} \\ a_1 \overline{b_0} & a_1 \overline{b_1} \end{bmatrix}$

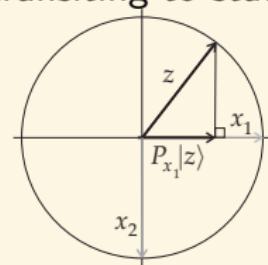
Projector

The projector P_{x_i} projects any point $|z\rangle$ in Hilbert space into the subspace L_{x_i} . It is constructed from the outer product $|x_i\rangle\langle x_i|$, i.e. for all z ,

$$P_{x_i}|z\rangle = (|x_i\rangle\langle x_i|)|z\rangle = |x_i\rangle\langle x_i|z\rangle = \langle x_i|z\rangle|x_i\rangle$$

The inner product $\langle x_i|z\rangle$ can be interpreted as the probability amplitude of transiting to state $|x_i\rangle$ from state $|z\rangle$. The probability of transiting to state $|x_i\rangle$ from state $|z\rangle$ is

$$p(x_i) = \|P_{x_i}|z\rangle\|^2 = \langle z|P_{x_i}|z\rangle = |\langle x_i|z\rangle|^2$$



The state vector $|z\rangle$ can be expressed in terms of the basis states as $|z\rangle = \sum_i \langle x_i|z\rangle|x_i\rangle$.

The measurement of an n qubit quantum state:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x|x\rangle \xrightarrow{\text{measurement}} |x\rangle \text{ with probability } |a_x|^2 = \overline{a_x}a_x.$$

Quantum Gates

- ▶ A quantum gate: Unitary operation on a number of qubits.
- ▶ A set of gates is *universal* iff for any unitary matrix U and any $\varepsilon > 0$, there is some circuit \tilde{U} built out of the set of gates such that

$$\|U - \tilde{U}\| < \varepsilon$$

In other words,

$$\sup_{\|\psi\|=1} \|U|\psi\rangle - \tilde{U}|\psi\rangle\| < \varepsilon$$

NOT Gate & $\sqrt{\text{NOT}}$ Gate

► NOT Gate

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\text{NOT } |0\rangle = |1\rangle$$

$$\text{NOT } |1\rangle = |0\rangle$$

► $\sqrt{\text{NOT}}$ Gate

$$\sqrt{\text{NOT}} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$

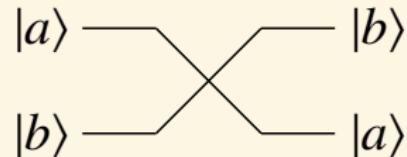
$$\sqrt{\text{NOT}} \cdot \sqrt{\text{NOT}} = \text{NOT}$$

$$\sqrt{\text{NOT}} \cdot \sqrt{\text{NOT}}^\dagger = I$$

SWAP Gate & Hadamard Gate

► SWAP Gate

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



► Hadamard Gate

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|\psi\rangle = a|0\rangle + b|1\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$$

Pauli Gates

Pauli Gates

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Phase Shift Gate

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

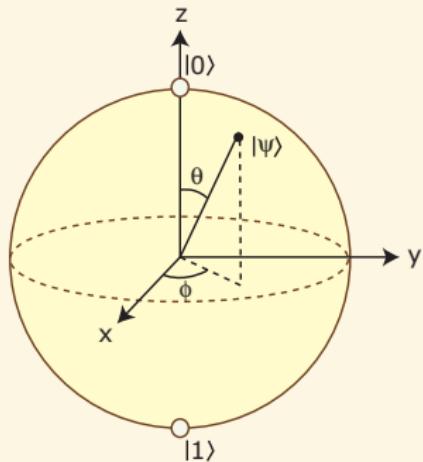
- $H = \frac{X+Z}{\sqrt{2}}$
- $H^2 = HH^\dagger = X^2 = Y^2 = Z^2 = -iXYZ = I$
- For $x \in \{0,1\}^n$,

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

where $x \cdot y := \sum_{i=1}^n x_i y_i \bmod 2$.

Bloch Sphere

$$|\psi\rangle = a|0\rangle + b|1\rangle = \cos \frac{\theta}{2}|0\rangle + e^{i\phi} \sin \frac{\theta}{2}|1\rangle = \cos \frac{\theta}{2}|0\rangle + (\cos \phi + i \sin \phi) \sin \frac{\theta}{2}|1\rangle$$



The density matrix of $|\psi\rangle$ is

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \cos^2 \frac{\theta}{2} & e^{-i\phi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} \\ e^{i\phi} \sin \frac{\theta}{2} \cos \frac{\theta}{2} & \sin^2 \frac{\theta}{2} \end{bmatrix}$$

$$\begin{aligned} &= \frac{1}{2} \begin{bmatrix} 1 + \cos \theta & e^{-i\phi} \sin \theta \\ e^{i\phi} \sin \theta & 1 - \cos \theta \end{bmatrix} \\ &= \frac{1}{2} (I + xX + yY + zZ) \end{aligned}$$

$$x = \sin \theta \cos \phi$$

$$y = \sin \theta \sin \phi$$

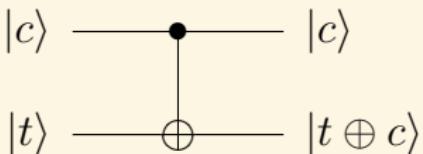
$$z = \cos \theta$$

Starting from $|0\rangle$, any state can be reached by first rotating about y by angle θ and then about z by angle ϕ .

CNOT Gate

Definition

A quantum state $\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a *product state* iff it can be expressed as a tensor product $\psi_1\rangle \otimes \cdots \otimes \psi_n\rangle$ of n 1-qubit states. Otherwise, it is *entangled*.

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$


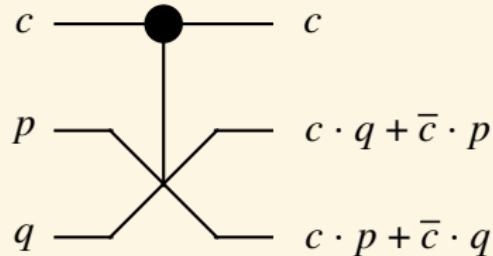
In general, one can define controlled versions of any unitary gate U as

$$CU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

$\text{CNOT}(|+\rangle \otimes |0\rangle) = \left[\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}} \right]^T = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is an entangled state which can't be separated as tensor product.

Fredkin Gate: CSWAP

c	p	q	x	y	z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1



transmit the first bit unchanged and
swap the last two bits iff the first bit is 1.
 $f : (c, p, q) \mapsto (c, c \cdot q + \bar{c} \cdot p, c \cdot p + \bar{c} \cdot q)$

$$\text{CSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- ¬ $p = 0 \ \& \ q = 1 \implies z = \bar{c}$
- Λ $q = 0 \implies z = c \cdot p$

Toffoli Gate: CCNOT or $D(\frac{\pi}{2})$

c_1	c_2	t	x_1	x_2	x_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

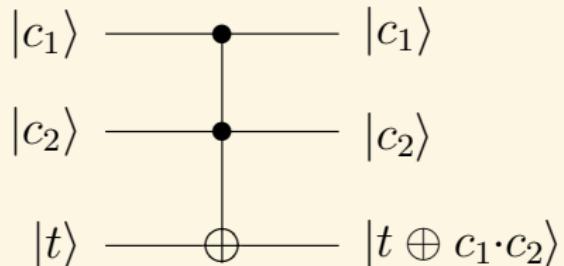


Figure: if the first two bits are 1, it inverts the third bit, otherwise all bits stay the same.

$$f : (c_1, c_2, t) \mapsto (c_1, c_2, t \oplus c_1 \cdot c_2)$$

$$\text{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\neg c_1 = c_2 = 1 \implies x_3 = \bar{t}$$

$$\wedge t = 0 \implies x_3 = c_1 \cdot c_2$$

Universal Quantum Gates

- ▶ Fredkin gate CSWAP is universal for classical computation, but not universal for quantum computation.
- ▶ Toffoli gate CCNOT is universal for classical computation, but not universal for quantum computation.
- ▶ $\{\text{CNOT}, H, R_{\frac{\pi}{4}}\}$ is universal for quantum computation.
- ▶ Deutsch gate $D(\theta)$ is universal for quantum computation.
- ▶ Toffoli gate and Hadamard gate $\{\text{CCNOT}, H\}$ constitute a universal set of quantum gates.

Deutsch Gate

$$D(\theta) : |a, b, c\rangle \mapsto \begin{cases} i \cos \theta |a, b, c\rangle + \sin \theta |a, b, 1 - c\rangle & \text{for } a = b = 1 \\ |a, b, c\rangle & \text{otherwise} \end{cases}$$

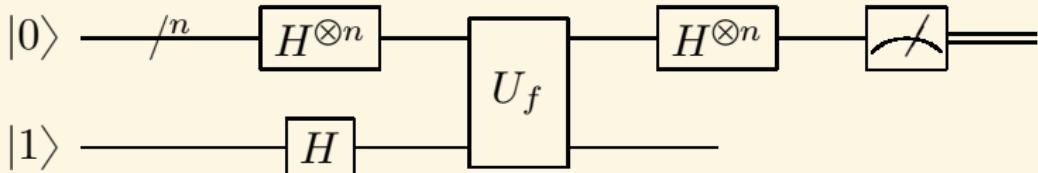
- ▶ Transformations on qubits are reversible: the number of input qubits always must equal the number of output qubits.
- ▶ Qubit transformations are operators on vector spaces. And an operator defined on an n -dim vector space (e.g. n -qubit space) that acts on n -dim vectors (e.g. n qubits) can only spit out n -dim vectors.

Quantum Algorithms

- I. **Initialization** Build an initial state $|\psi_i\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle$.
For example, $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$ (uniform superposition) can be build from $|0\rangle^{\otimes n}$ by application of Hadamard gate $H^{\otimes n}$.
- II. **Transformations** Transform $|\psi_i\rangle \rightarrow |\psi_f\rangle = \sum_{x \in \{0,1\}^n} b_x |x\rangle$ through a sequence of elementary quantum gates.
- III. **Measurement** Extract information by quantum measurement of $|\psi_f\rangle$.

The “balanced vs constant” Problem

- ▶ given a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ that is either constant (same output for all x) or balanced ($f(x)$ is equal to 0 for exactly half of the possible values of x).
- ▶ classically, we need to query the function $2^{n-1} + 1$ times to be sure whether the function is constant or balanced.
- ▶ but quantumly, the Deutsch-Jozsa Algorithm requires only 1 oracle call.—measuring the first n qubits allows us to determine with certainty whether the function is constant (measure all zeros) or balanced (measure at least one 1).



Deutsch-Jozsa Algorithm

1. prepare the initial state $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$

2. apply $H^{\otimes n} \otimes H$

$$|\psi_1\rangle = (H^{\otimes n} \otimes H) |\psi_0\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes |- \rangle$$

3. apply f as a quantum oracle $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$$|\psi_2\rangle = U_f |\psi_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \otimes |- \rangle$$

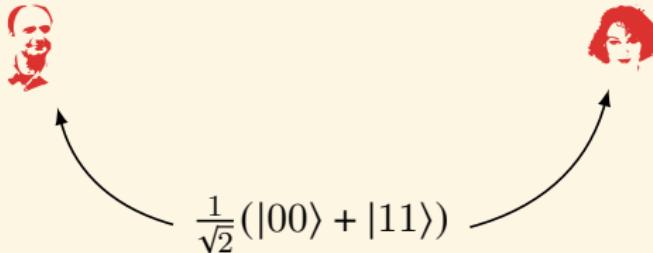
4. apply $H^{\otimes n} \otimes I$

$$|\psi_3\rangle = (H^{\otimes n} \otimes I) |\psi_2\rangle = \left(\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} |y\rangle \right) \otimes |- \rangle$$

5. examine the probability of measuring $|y\rangle = |0\rangle^{\otimes n}$

$$\left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|^2 = \begin{cases} 1 & \text{if } f(x) \text{ is constant} \\ 0 & \text{if } f(x) \text{ is balanced} \end{cases}$$

Teleportation & Superdense Coding



Teleportation Use a shared entanglement and **two bits** of classical information to transfer **one qubit**.

Superdense Coding Use a shared entanglement and **one qubit** of quantum information to transfer **two classical bits**.

Bell States

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Quantum Teleportation

Alice and Bob share $|\Phi^+\rangle$. Alice wants to teleport $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob. The joint state is

$$|\psi\rangle|\Phi^+\rangle = \frac{|\Phi^+\rangle\otimes(a|0\rangle+b|1\rangle)+|\Phi^-\rangle\otimes(a|0\rangle-b|1\rangle)+|\Psi^+\rangle\otimes(a|1\rangle+b|0\rangle)+|\Psi^-\rangle\otimes(a|1\rangle-b|0\rangle)}{\sqrt{2}}.$$

Alice measures her two qubits in the Bell basis $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$.

Then the joint state would collapse to one of the four states with equal probability.

- ▶ $|\Phi^+\rangle \otimes (a|0\rangle + b|1\rangle)$
- ▶ $|\Phi^-\rangle \otimes (a|0\rangle - b|1\rangle)$
- ▶ $|\Psi^+\rangle \otimes (a|1\rangle + b|0\rangle)$
- ▶ $|\Psi^-\rangle \otimes (a|1\rangle - b|0\rangle)$

Alice transmits two classical bits to Bob that indicate which of the above four states the system is in.

Bob uses this classical information to apply a correction to his qubit.

$a 0\rangle + b 1\rangle$	I	$a 0\rangle + b 1\rangle$
$a 0\rangle - b 1\rangle$	Z	$a 0\rangle + b 1\rangle$
$a 1\rangle + b 0\rangle$	X	$a 0\rangle + b 1\rangle$
$a 1\rangle - b 0\rangle$	ZX	$a 0\rangle + b 1\rangle$

Superdense Coding

By applying a quantum gate to $|\Phi^+\rangle$, Alice can transform $|\Phi^+\rangle$ into any of the four Bell states.

Alice's Bits	Initial State	Operation	Final State
00	$ \Phi^+\rangle$	I	$ \Phi^+\rangle$
01	$ \Phi^+\rangle$	X	$ \Psi^+\rangle$
10	$ \Phi^+\rangle$	Z	$ \Phi^-\rangle$
11	$ \Phi^+\rangle$	ZX	$ \Psi^-\rangle$

Bob's correction:

Initial State	After CNOT	After H on 1 st qubit
$ \Phi^+\rangle$	$ +\rangle 0\rangle$	$ 00\rangle$
$ \Psi^+\rangle$	$ +\rangle 1\rangle$	$ 01\rangle$
$ \Phi^-\rangle$	$ -\rangle 0\rangle$	$ 10\rangle$
$ \Psi^-\rangle$	$ -\rangle 1\rangle$	$ 11\rangle$

Quantum Kolmogorov Complexity

Definition (Quantum Kolmogorov Complexity — Vitányi's Version)

The quantum Kolmogorov complexity of $|x\rangle$ with respect to quantum Turing machine M is

$$K^Q(x) = \min_p \left\{ \ell(p) + \lceil -\log \|\langle z|x\rangle\|^2 \rceil : M(p) = |z\rangle \right\}$$

Definition (Quantum Kolmogorov Complexity — Müller's Version)

Given a QTM M and a finite error $\delta > 0$, the finite-error quantum Kolmogorov complexity of a qubit string $|x\rangle$ is

$$K_\delta^Q(x) = \min_p \left\{ \ell(p) : \|x - M(p)\|_{\text{tr}} < \delta \right\}$$

and the approximate-scheme quantum Kolmogorov complexity of $|x\rangle$ is

$$K^Q(x) = \min_p \left\{ \ell(p) : \forall k \in \mathbb{N} : \|x - M(p, k)\|_{\text{tr}} < \frac{1}{k} \right\}$$

where $\|\cdot\|_{\text{tr}}$ is the trace norm, i.e. $\|\rho - \sigma\|_{\text{tr}} := \frac{1}{2} \text{Tr} \left(\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} \right)$.

Quantum Logic

- ▶ Any closed linear subspace of — or, equivalently, any projection operator on — a Hilbert space corresponds to a proposition.
- ▶ The conjunction \wedge is identified with the intersection of two subspaces. For propositions p, q and their associated closed linear subspaces M_p, M_q : $M_{p \wedge q} = M_p \cap M_q$.
- ▶ The disjunction \vee is identified with the closure of the linear span \oplus of the subspaces corresponding to the two propositions.
$$M_{p \vee q} = M_p \oplus M_q = \{ax + by : a, b \in \mathbb{C}, x \in M_p, y \in M_q\}.$$
- ▶ The negation \neg is identified with operation of taking the orthogonal subspace \perp . $M_{\neg p} = M_p^\perp = \{x : \forall y \in M_p : \langle x | y \rangle = 0\}$.
- ▶ The implication \rightarrow is identified with the subset relation.
$$p \rightarrow q \iff M_p \subseteq M_q.$$
- ▶ A trivial true statement T is represented by the entire Hilbert space H .
$$M_T = H.$$
- ▶ An absurd statement \perp is represented by the zero vector 0 .
$$M_\perp = 0.$$

- De Morgan's Law

$$U^\perp \cap V^\perp = (U \oplus V)^\perp$$

$$U^\perp \oplus V^\perp = (U \cap V)^\perp$$

- Law of Double Negation

$$(V^\perp)^\perp = V$$

- Law of Excluded Middle

$$V \oplus V^\perp = H$$

- Law of Non-Contradiction

$$V \cap V^\perp = \{0\}$$

- Law of Contrapositive

$$U \subset V \iff V^\perp \subset U^\perp$$

- In **FdHilb**, $U \subset V \implies V \cap (U \oplus W) = U \oplus (V \cap W)$.
- In **Hilb**, $U \subset V \implies U = V \cap (U \oplus V^\perp)$.

Distributivity Fails

Let A, B, C be three distinct states in \mathbb{C}^2 , then:

- ▶ the meet of any two of them is $\{0\}$;
- ▶ the join of any two of them is the whole space \mathbb{C}^2 .

$$(A \cap B) \oplus C = C \neq \mathbb{C}^2 = (A \oplus C) \cap (B \oplus C)$$

$$(A \oplus B) \cap C = C \neq \{0\} = (A \cap C) \oplus (B \cap C)$$

Contents

Introduction	Recursion Theory
Term Logic	Equational Logic
Propositional Logic	Homotopy Type Theory
Predicate Logic	Category Theory
Modal Logic	Quantum Computing
Set Theory	Answers to the Exercises References 1436

Answers to the Exercises — Translation

1. $\forall x(\neg Sx \rightarrow \exists y(Eyx \wedge \neg Sy))$
2. $\forall x(Mx \vee Wx \rightarrow Ax)$
3. $\forall x(\neg(Rx \wedge Bx) \rightarrow \neg Ex)$
4. $Hs \wedge Hp \wedge \forall x(Hx \rightarrow x = s \vee x = p)$
5. $\forall x(x \neq s \wedge x \neq p \rightarrow Hx)$
6. $\forall x(Bx \rightarrow \exists y\exists z(Gy \wedge Gz \wedge y \neq z \wedge Lxy \wedge Lxz))$
7. $\neg\forall x(Jx \rightarrow Dx)$
8. $\forall x(Jx \rightarrow \neg Dx)$
9. $\neg\forall x(\text{Glitter}(x) \rightarrow \text{Gold}(x))$
10. $\forall xyz(\text{City}(z) \wedge \text{In}(x, z) \wedge \text{In}(y, z) \rightarrow \text{first(zip}(x)) = \text{first(zip}(y)))$
11. $\forall x\forall y(Fx \wedge Dy \wedge Oxy \rightarrow Hx)$
12. $\forall x\forall y(Fx \wedge Dy \wedge Oxy \rightarrow Bxy)$
13. $\forall x(Ex \rightarrow Dx2) \wedge \exists x(Ex \wedge Dx4) \wedge \exists x(Ex \wedge \neg Dx4)$

Answers to the Exercises — Translation

14. $\forall x(Fx \rightarrow \exists y(Cy \wedge Byx))$
15. $\forall x(Cx \wedge Ex \rightarrow \neg \exists y(Py \wedge Sy) \rightarrow Dx)$
16. $\forall x(Bx \rightarrow \neg \exists y(Ty \wedge Axy) \vee \forall y(Ty \rightarrow Axy))$
17. $\forall x(\neg Hxx \rightarrow Hjx)$
18. $\neg \exists x(Bx \wedge \forall y(Sxy \leftrightarrow \neg Syy))$
19. $\exists x \exists y \exists z(Mxa \wedge Myb \wedge Mzx \wedge Mzy) \wedge \forall u \forall v \forall x \forall y(Mua \wedge Mvb \wedge Mxu \wedge Myv \rightarrow x = y)$
 $m(m(a)) = m(m(b))$
20. $\forall x \exists y \exists z(Gy \wedge Gz \wedge y \neq z \wedge Lxy \wedge Lxz \rightarrow x = t)$
21. $\forall x(L(x, f(w(s))) \rightarrow x = m(w(s)))$
22. $\forall x(Dx \rightarrow Ax) \rightarrow \forall x(\exists y(Dy \wedge Hxy) \rightarrow \exists y(Ay \wedge Hxy))$
 $\forall x(Dx \rightarrow Ax) \rightarrow \forall x(Dx \rightarrow \exists y(Ay \wedge hx = hy))$
23. $\exists x(Dx \wedge \forall y(Dy \rightarrow y = x) \wedge \neg \exists z(Tz \wedge Hxz))$
24. $\exists x(Gx \wedge Lxb \wedge \forall y(Gy \wedge Lyb \rightarrow y = x) \wedge \exists y(y \neq x \wedge Sy))$
25. $\exists x(Gx \wedge Lxm \wedge \forall y(Gy \wedge Lym \rightarrow y = x) \wedge Lmx \wedge \forall y(Lmy \rightarrow y = x))$
26. $\exists x(Lxa \wedge \forall y(Lya \rightarrow y = x) \wedge \exists y(Lay \wedge \forall z(Laz \rightarrow z = y) \wedge y = x))$
27. $\exists x(Ex \wedge \forall z(Ez \rightarrow Tzx) \wedge \exists y(Ey \wedge \forall z(Ez \rightarrow Tyz) \wedge Lxy))$

1. $\neg \exists x \forall y (Txy \leftrightarrow \neg \exists z (Tyz \wedge Tzy))$
2. $\forall x (Dx \rightarrow Ax) \rightarrow \forall x (\exists y (Dx \wedge Hxy) \rightarrow \exists y (Ay \wedge Hxy))$
3. $\forall x (\neg Ax \wedge Mx \rightarrow Vx \vee Fx), \forall x (Px \rightarrow \neg Ax \wedge \neg Vx \wedge \neg Fx) \vdash \forall x (Px \rightarrow \neg Mx)$
4. $\exists x Jx, \neg \exists x (Ax \wedge Jx) \vdash \exists x \neg Ax$
5. $\exists x \forall y ((Ky \leftrightarrow y = x) \wedge Bx), \forall x (Bx \rightarrow Sx) \vdash \forall x (Kx \rightarrow Sx)$
6. $\forall x (Px \rightarrow x = r), Pw \wedge Sw \vdash Sr$
7. $\forall x Fxd, \forall x (Fdx \rightarrow x = i) \vdash i = d$
8. $\forall x \forall y (\exists z Lyz \rightarrow Lxy), Lrj \vdash Liu$
9. $\forall x \forall y (\exists z Lyz \rightarrow Lxy) \vdash \exists x \exists y Lxy \rightarrow \forall x \forall y Lxy$
10. $\neg \exists x \exists y (Gx \wedge Sy \wedge Lxy), Gc \wedge \forall x (Lxc \rightarrow Lcx), Lhc \vdash \neg Sh$
11. $Pi, \forall x \forall y (Px \wedge Axy \rightarrow Py), \neg \exists x (Px \wedge \neg Ex), Ri, \forall x (Ex \wedge Rx \rightarrow \exists y (Gy \wedge Axy)), \forall x (Ex \rightarrow Cx) \vdash \exists x (Gx \wedge Cx)$
12. $\forall x (Px \rightarrow \exists y (Ly \wedge Axy)), \exists x (Sx \wedge \forall y (Axy \rightarrow Fy)), \neg \exists x (Fx \wedge Lx) \vdash \neg \forall x (Sx \rightarrow Px)$
13. $\forall x \forall y (Sxy \rightarrow \exists z Izxy), \forall x \forall y \forall z (Izxy \rightarrow Kzx \wedge Kzy), \forall x Sxf \vdash \forall x \exists y (Iyx f \wedge Kyf)$
14. $\forall x (Sx \rightarrow Kx), \exists x Sx, \forall x (Kx \rightarrow x = j) \vdash Sj$
15. $Aac \wedge Abc \wedge a \neq b \wedge \forall x (Axc \rightarrow x = a \vee x = b), \forall x (Axc \leftrightarrow Lxc) \vdash \exists x \exists y (Lxc \wedge Lyc \wedge x \neq y \wedge \forall z (Lzc \rightarrow z = x \vee z = y))$

References I

- [Gir11] Jean-Yves Girard. “The Blind Spot: Lectures on Logic”. In: European Mathematical Society, 2011.
- [Law69] F William Lawvere. “Diagonal arguments and cartesian closed categories”. In: *Category theory, homology theory and their applications II*. Springer, 1969, pp. 134–145.
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [San20] Paulo Guilherme Santos. *Diagonalization in Formal Mathematics*. Springer Spektrum, Wiesbaden, 2020.
- [SV84] Jorge Soto-Andrade and Francisco J. Varela. “Self-reference and fixed points: A discussion and an extension of Lawvere’s Theorem”. In: *Acta Applicandae Mathematica* 2 (1984), pp. 1–19.

References II

- [Svo18] Karl Svozil. *Physical (A)Causality Determinism, Randomness and Uncaused Events*. Fundamental Theories of Physics, 192. Cham: Springer International Publishing, 2018.
- [Uni13] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study: <https://homotopytypetheory.org/book>, 2013.

Thank U

