# Elementary Logic

Department of Philosophy
Central South University
xieshenlixi@163.com
github

September 10, 2020

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Contents


Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 $\mathrm{Mod}(A)$ of its models. An update with new information $B$ reduces the current set of models $\mathrm{Mod}(A)$ to the overlap of $\mathrm{Mod}(A)$ and $\mathrm{Mod}(B)$.

# 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. *One day, the queen visits and announces that at least one husband has been unfaithful, and that any wife who discovers his husband's infidelity must kill him that very day.*
4. *What happens?*

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

### Test

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

# 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

# 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?

# Hardest Logic Puzzle Ever

## 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.*

# HLPE — Solution

## 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 $R$:*
   $Q[C/B, Q'/Q]$ $Q'$

# Contents


Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Outline

- Critical Thinking ✓
- History
- Term Logic
- Propositional Logic ✓
- Predicate Logic ✓
- Equational Logic
- Set Theory
- Recursion Theory
- Modal Logic

# Readings

1. P. J. Hurley: A Concise Introduction to Logic. — $B$
2. H. de Swart: Pilosophical and Mathematical Logic. — $P$
3. P. Smith: An Introduction to Formal Logic. — $P$
4. *P. Smith: Teach Yourself Logic.* — $P$
5. J. van Benthem: Logic in Action. — $P$
6. Open Logic Project. — $P$
7. H. Enderton: A Mathematical Introduction to Logic. — **L**
8. H. Ebbinghaus, J. Flum, W. Thomas: Mathematical Logic. — $L$
9. A. Nerode, R. A. Shore: Logic for Applications. — $C$
10. 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
- Philosophical Logic
- Philosophy of Logic
- Philosophy of Mathematics

- libgen
- sci-hub
- XX-Net
- ghelper
- Google Cloud
- JJQQKK

# 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

# Exams and Credits

- Question
- Discussion
- Exercises/Homework ✓
- Presentation
- Paper
- Examination ✓
- Techniques e.g. LaTeX / Coq ...
- ...

# Homework

Google/Wikipedia/Stanford Encyclopedia/Internet Encyclopedia

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

# Aim

- Critical thinking ✓
- 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
- Application in Math / CS / AI / Linguistics / Cognition / Physics / Information Theory / Game Theory / Social Science ...
- Mathematical Logic

# Contents

Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Example

一个受过良好教育的男性吹嘘自己比女性聪明，如同吹嘘他有勇气打败一个手脚被捆绑的人一样。

学问像大海，考试像鱼钩。老师怎么能把鱼挂在鱼钩上教它在大海中学习自由、平衡的游泳呢?

— Hermite

正如在潜水时身体有一个自然的漂浮到水面的趋势，它要求我们必须将身体尽力下沉；在思考问题时，我们必须将思维尽力发挥，使我们远离肤浅的表面，下潜到哲学的深度。

— Wittgenstein

# Example

## 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

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

1. 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。
2. 类比物的差异性越大，论证越强。
3. 类比物与目标物的相似性越多，论证越强。
4. 类比物与目标物的相似性之间越相关，论证越强。
5. 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。
6. 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

- 我认为性教育导致怀孕。
- 是的，正如驾驶教育导致交通事故。◎ô◎

# 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

有人认为，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”。照此推理，汽车也不可能代替马，因为汽车是铁做的，而马是活的血肉做的有机体。

## Refutation by Analogy

- 计算机会思考吗?
- 潜水艇会游泳吗?

# Examples — Does God Exist?

## Argument by Analogy

如果我们看见某个复杂精巧的机械装置，比如一块手表，我们会推测它是由某人制造的。我们所处的宇宙是一个错综复杂却运行精巧的自然机制，所以，我们应当推测它也有一个造物主。

## Refutation by Analogy

众多宇宙中的每一个都有各自的规律和参数。有些适合生命生存，有些不适合。有的甚至发展出了能提出人择问题的高级生命。但这就像是一场随机摸彩。总会有人赢，而没有人在刻意挑选赢家。仅仅因为一个宇宙具有一套独特的规律和参数，不能推出它是被造物主精心设计的。

# Contents


Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Method of Agreement

$$\frac{\begin{array}{c} ABCD \rightarrow wxyz \\ AEFG \rightarrow wtuv \end{array}}{A \rightarrow w}$$

某天下午很多同学突然腹泻，我们得了解原因。腹泻的人中午吃了什么？某些人吃了但不是所有病人都吃了的食物应该不是病因。

一天晚上老王看了两小时书，喝了很多浓茶，用热水泡了脚，结果失眠了；第二天晚上他看了两小时电视，抽了很多烟，用热水泡了脚，结果又失眠了；第三天他听了两小时音乐，喝了很多咖啡，用热水泡了脚，结果再次失眠。根据求同法，用热水泡脚是失眠的原因。◎ô◎

# Method of Difference

$$\frac{\begin{array}{c} ABCD \to wxyz \\ \overline{A}BCD \to \overline{w}xyz \end{array}}{A \to w}$$

秋末冬初街道旁的响叶杨纷纷开始落叶，但高压水银灯下的响叶杨却迟迟不落叶，因此，高压水银灯照射可能是响叶杨落叶迟的原因。

取一只蜘蛛，冲它大吼一声，蜘蛛被吓跑了。把它的腿砍掉，冲它大吼，蜘蛛纹丝不动。结论：蜘蛛的听觉器官长在腿上。◎ô◎

# Joint Method of Agreement and Difference

$$\frac{\begin{array}{cc} ABC \to xyz & ABC \to xyz \\ ADE \to xtw & \overline{A}BC \to \bar{x}yz \end{array}}{A \to x}$$

达尔文观察到不同类的生物在相同环境中常常具有相似的形态，鲨鱼属于鱼类，鲸鱼属于哺乳类，鱼龙属于爬行类，但形貌相似。又观察到同类生物在不同环境中呈现不同形态，鼹鼠、鲸鱼、蝙蝠同属哺乳类，却分别生活在陆、海、空，形态差别很大。通过对比，达尔文认为，生活环境是影响生物形态的重要原因。

# Method of Residues

$$\begin{array}{c} ABC \to xyz \\ B \to y \\ \underline{C \to z} \\ A \to x \end{array}$$

居里夫人知道铀的放射线的强度，也知道一定量的沥青矿石所含的铀数量。她观察到一定量的沥青矿石所发出的放射线要比它所含的铀所发出的放射线强许多倍。她推断：沥青矿石中还含有其它放射性极强的新元素。经过试验，她发现了镭。

# Method of Concomitant Variation

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

热胀冷缩、体温表

老王发现，抽烟越多肺病越严重，所以推测，抽烟是导致肺病的重要原因。
有没有可能，老王携带的某种基因是导致他容易抽烟和容易得肺病的共同原因?

# Contents

Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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！

今天在路边看见一条鱼，捡起一看，还是条活鱼，回家一炖可好吃了。又一想，做鱼要有油、有厨房，还要找个媳妇来做，媳妇一定有娘，又多了个丈母娘。要娶她家姑娘，丈母娘一定会开条件：要房、要车、要钱……恍然大悟，赶紧把鱼扔了，现在房价这么恐怖，这鱼肯定是开发商故意扔的。我的妈呀，差点上当……

天无二日，国无二主。

## 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 vs 孟子

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.
   - The world of the happy is quite different from the world of the unhappy.
2. Doublethink/Dialectic/Contradiction.
   - War is peace.
   - Freedom is slavery.
   - Ignorance is strength.
   - All animals are equal but some animals are more equal than others.
   - Everyone is the other, and no one is himself.
   - Man can do what he wills but he can't will what he wills.
   - To believe is to know you believe, and to know you believe is not to believe.

[1] Law: Bellieving Bullshit.
Frankfurt: On Bullshit.

# How to generate pseudo-profound bullshit?

3. Ambiguity/Metaphor/Parable.
   - Love is just a word.
   - There is no need for torture: Hell is other people.
   - Language is the house of the truth of Being.
   - What is reasonable is real; that which is real is reasonable.
   - Never stay up on the barren heights of cleverness, but come down into the green valleys of silliness.
   - The World and Life are one. Ethics and Aesthetics are one. Ethics does not treat of the world. Ethics must be a condition of the world, like logic.
   - When you gaze long into the abyss the abyss also gazes into you.
   - The limits of my language mean the limits of my world.
   - A person is neither a thing nor a process but an opening through which the Absolute can manifest.
   - My work consists of two parts: of the one which is here, and of everything which I have not written. And precisely this second part is the important one.
   - Making itself intelligible is suicide for philosophy. Those who idolize "facts" never notice that their idols only shine in a borrowed light.

# How to generate pseudo-profound bullshit?

4. Analogy.
   - Life is like a box of chocolates. You never know what you're gonna get.
   - Life is like a coin. You can spend it any way but only once.
   - Life is like a shell, which suddenly bursts into fragments, which fragments, being themselves shells, burst in their turn into fragments destined to burst again, and so on for a time incommensurably long.
   - 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.
   - My propositions serve as elucidations in the following way: anyone who understands me eventually recognizes them as nonsensical, when he has used them — as steps — to climb up beyond them. (He must throw away the ladder after he has climbed up it.)

# How to generate pseudo-profound bullshit?

5. Use jargon.
   - The Nothing itself nothings.
   - 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.
   - Dasein has always made some sort of decision as to the way in which it is in each case mine. That entity which in its Being has this very Being as an issue, comports itself towards its Being as its ownmost possibility. With death, Dasein stands before itself in its ownmost potentiality-for-Being.
   - The Absolute Idea. The Idea, as unity of the Subjective and Objective Idea, is the notion of the Idea — a notion whose object is the Idea as such, and for which the objective is Idea — an Object which embraces all characteristics in its unity.
   - 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"。
- 科学哲学对科学家的用处跟鸟类学对鸟的用处差不多。 — 费曼

- 哲学旨在感动那些混淆晦涩与深刻的人。 — 温伯格
- 哲学难道不是用蜜写成的吗？乍一看，很精彩，再一看，除了一团浆糊，什么都没留下。 — 爱因斯坦

# 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. — *James*
- 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.
- 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!"

# Elimination of Metaphysics?

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。[a]

[a] 卡尔纳普：通过语言的逻辑分析清除形而上学

Mystics exult in mystery and want it to stay mysterious. Scientists exult in mystery for a different reason: it gives them something to do.

— *Dawkins*

# 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”?

# Galilei's Leaning Tower of Pisa

*Philosophy is written in this grand book — I mean the universe — which stands continually open to our gaze, but it can't be understood unless one first learns to comprehend the language in which it is written. It is written in the language of mathematics.*

*— Galileo Galilei*

# 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 $2^{\text{nd}}$ 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 $1^{\text{st}}$ Law.

# Logic of Science

**How to *express* your thoughts precisely and succinctly?**

- Not only is the universe stranger than we imagine, it is stranger than we can imagine.
- A few lines of reasoning can change the way we see the world.
- Logic enlarges our abstract imagination, and provides all possible hypotheses to be applied in the analysis of complex facts. Nothing is forbidden except nonsense and contradiction.
- Logic is the immune system of the mind!
- The music of reason — the fulfillment of the human spirit.

# The Music of Reason

**How to *express* your thoughts <u>precisely</u> and <u>succinctly</u>?**

The glory of the human spirit!

What are the extent and limits of reason?

# Contents

Introduction
- Logic Puzzle
- Textbook and Homework
- Analogical Argument
- Mill's Five Methods
- Fallacy and Bullshit
- Logic and other Disciplines

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 other Disciplines

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

# Logic vs CS

- Computer Architecture.
  Logic gates and digital circuit design $\approx$ Propositional Logic
- Programming Languages.
  Semantics of programming languages via methods of logic
  LISP $\approx$ $\lambda$-calculus
  Prolog $\approx$ First Order Logic + Recursion
  Typing $\approx$ Type Theory
- Theory of Computation and Computational Complexity.
  Models of computation (Turing machines, finite automata)
  Logic provides *complete problems* for complexity classes.
  Logical characterizations of complexity classes
  Descriptive Complexity
- General Problem Solver (SAT solvers).
- Automated Theorem Proving.

# Logic vs CS

- Knowledge representation via logic rules.
- 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).
  Extensive use of formal methods based on logic
  Temporal Logic, Dynamic Logic and Automata, Hoare Logic, Model Checking
- Multi-agent Systems.
  Epistemic Logic
- Semantic Web.
  Web Ontology Language (OWL) $\approx$ Description Logic

# Branches of Logic

**Mathematical Logic**

- **First Order Logic**
- Set Theory
- Model Theory
- Proof Theory
- Recursion Theory

**Computational Logic**

- Automata Theory
- Computational Complexity
- Finite Model Theory
- Model Checking
- Lambda Calculus
- Categorical Logic
- (Homotopy) Type Theory
- Theorem Proving
- Description Logic
- Dynamic Logic
- Temporal Logic
- Hoare Logic
- Inductive Logic
- Fuzzy Logic
- Non-monotonic Logic
- Computability Logic
- Default Logic
- Situation Calculus

**Philosophical Logic**

- Intuitionistic Logic
- Algebraic Logic
- Quantum Logic
- Modal Logic
- Epistemic Logic
- Doxastic Logic
- Preference Logic
- Provability Logic
- Hybrid Logic
- Free Logic
- Conditional Logic
- Relevance Logic
- Linear 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

*Between theology and science there is a no man's land, exposed to attack from both sides; this no man's land is philosophy.*

— *Russell*

*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.*

— *van Benthem*

- Philosophy is a game with objectives and no rules.
- Logic is a game with rules and no objectives.

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

- 这 TM 也用证?
- 这 TM 也能证?

*If Church says it's obvious, then everybody has seen it half an hour ago. If Weyl says it's obvious, von Neumann might be able to prove it. If Lefschetz says it's obvious, it's false.*

— *Rosser*

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Contents

Introduction

History
- The Prehistory of Logic
- The Rise of Logic
- After Gödel

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Aristotle(384-322 BC) — Term Logic

- 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.

$$\frac{\begin{array}{c}\text{All men are mortal}\\ \text{Socrates is a man}\end{array}}{\text{Socrates is mortal}}$$

**A**: All $S$ are $P$.

**E**: No $S$ are $P$.

**I**: Some $S$ are $P$.

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

# Syllogism

$$\frac{\begin{array}{c} M—P \\ S—M \end{array}}{S—P} \qquad \frac{\begin{array}{c} P—M \\ S—M \end{array}}{S—P} \qquad \frac{\begin{array}{c} M—P \\ M—S \end{array}}{S—P} \qquad \frac{\begin{array}{c} P—M \\ M—S \end{array}}{S—P}$$

- 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.

No $P$ are $M$
Some $S$ are not $M$
---
Some $S$ 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.

No $M$ are $P$
All $M$ are $S$

---

Some $S$ are not $P$

# Syllogistic Rules

$S$ distributed

| | | |
|---|---|---|
| $P$ undistributed | **A**: <u>All</u> $S$ are $P$. | **E**: <u>No</u> $S$ are $P$. | $P$ distributed |
| | **I**: Some $S$ are $P$. | **O**: Some $S$ are <u>not</u> $P$. | |

$S$ 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 $1 - 4$

# 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

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

Everyone loves my baby
My baby loves only me
---
I am my baby

# Deduction/Induction/Abduction/Examplification

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

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

$$\frac{\begin{array}{r} H \to E \\ E \end{array}}{H}$$

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

$$\frac{\begin{array}{c} H \to E \\ \top \to E \end{array}}{\top \to H}$$

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

# 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。

# Leibniz 1646-1716

## Don't argue. Calculate!

- Principle of Contradiction: Nothing can be and not be, but everything either is or is not.
- Principle of Sufficient Reason: Nothing is without a reason.
- 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 logic, topology, game theory, cybernetic theory, fractal geometry, non-standard analysis, algorithmic information theory and digital philosophy*.
- Wolfram: "Leibniz had the idea of encoding logical properties using numbers. He thought about associating every possible attribute of a thing with a prime number, then characterizing the thing by the product of the primes for its attributes — and then representing logical inference by arithmetic operations."

# Leibniz's Dream — Deduction

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.

$$\text{sign} \rightleftarrows \text{idea}$$

$$\text{encyclopedia} \Rightarrow \text{fundamental principles} \Rightarrow \text{primitive notions}$$

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 Dream — Induction

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.

# Characteristica 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.

| **Characteristica 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 |

# Characteristica 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 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 |

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

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

- 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

# Contents

Introduction

History
- The Prehistory of Logic
- The Rise of Logic
- After Gödel

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Boole 1815-1864

- *The Laws of Thought.*
- Logic as Algebra.
- Propositional Logic.
- Algebra's strength emanates from the fact that the symbols that represent quantities and operations obey a small number of rules.

# Cantor 1845-1918

- Mathematics $\rightsquigarrow$ Set Theory.
- Diagonalization.
- There are many different levels of infinity.
- Cantor set.
- Continuum Hypothesis (CH).
  How many points on the line?

# Frege 1848-1925 (+Peirce)

- *Begriffsschrift, a formal language of pure thought modelled upon that of arithmetic.*
- Predicate Logic. (Relation & Quantification)
  (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)

$\boxed{\text{Logicism}}$ Mathematics $\rightsquigarrow$ Logic.[2]

[2] Frege: The Foundations of Arithmetic.

# 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.[3]

[3] Russell: On denoting.

# 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 $\rightsquigarrow$ Mathematics $\rightsquigarrow$ 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*)

# 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. $(1^{\text{st}}, 2^{\text{nd}}, 10^{\text{th}}, 24^{\text{th}})$
- Meta-mathematics — Proof Theory.
- Formalism Mathematics $\rightsquigarrow$ 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.

# Hilbert's Program

*When we consider the axiomatization of logic more closely we soon recognize that the question of the consistency of the integers and of sets is not one that stands alone, but that it belongs to a vast domain of difficult epistemological questions which have a specifically mathematical tint: e.g., the problem of the solvability in principle of every mathematical question, the problem of the subsequent checkability of the results of a mathematical investigation, the question of a criterion of simplicity for mathematical proofs, the question of the relationship between content and formalism in mathematics and logic, and finally the problem of the decidability of a mathematical question in a finite number of operations.*

*— Hilbert*

*All of this that's happening now with the computer taking over the world, the digitalization of our society, of information in human society, is the result of a philosophical question that was raised by Hilbert at the beginning of the century.*

*— Chaitin*

# Contents

Introduction

History
- The Prehistory of Logic
- The Rise of Logic
- After Gödel

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Leibniz & Hilbert — Dream Shattered. . .

# Gödel 1906-1978

"I am unprovable."[4]

- Completeness.
  I think (consistently), therefore I am.
  (Consistency implies existence.)
- Incompleteness.
  1. provable < true
  2. un-self-aware
- Consistency of AC and CH.

[4] Gödel: On formally undecidable propositions of Principia Mathematica and related systems.

# Tarski 1901-1983

"snow is white" is true iff snow is white.

"I am false."[5]

Model Theory

**Undefinability of Truth**

Arithetical truth can't be defined in arithmetic.

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

Banach-Tarski Paradox

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

# 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"?[6] — Recursion Theory

[6] Turing: On computable numbers, with an application to the Entscheidungsproblem.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Logic → Truth

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

— *Frege*

Natural Language

$\Downarrow$ represents

$\boxed{\text{Formal Language (Syntax)}}$

$\Downarrow$ expresses

$\boxed{\text{Theory (calculus } \vdash)}$

interprets $\Downarrow$ $\Uparrow$ characterizes

$\boxed{\text{Models (semantics } \vDash)}$

$\Uparrow$ represents

. . . . . semantic gap

Real World

# Contents

Introduction

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Propositional Logic

- Language.
  Building blocks of propositional logic language.
- Syntax.
  Propositional symbols and propositional formulae.
- Semantics.
  Assign "meaning" to propositional formulae by first assigning "meaning" to propositional symbols.
- Calculus.
  Axioms and inference rules.

# Syntax

## Language

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

where $\mathcal{P} := \{p_1, \ldots, p_n, (\ldots)\}$.

## Well-Formed Formula wff

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

- $\bot := (A \wedge (\neg A))$
- $\top := (\neg \bot)$

## Example

- Lily is (not) beautiful.
- If wishes are horses, then beggars will ride.
- Lily is beautiful and/or/iff $2$ is not a prime number.

# Well-Formed Formula

## Definition (Formula-Building Operator)

$$\mathcal{E}_{\neg}(A) := (\neg A)$$
$$\mathcal{E}_{\wedge}(A, B) := (A \wedge B)$$
$$\mathcal{E}_{\vee}(A, B) := (A \vee B)$$
$$\mathcal{E}_{\rightarrow}(A, B) := (A \rightarrow B)$$
$$\mathcal{E}_{\leftrightarrow}(A, B) := (A \leftrightarrow B)$$

$$\boxed{\begin{aligned} \mathcal{E}_{\neg}(A) &:= \neg A \\ \mathcal{E}_{\wedge}(A, B) &:= \wedge AB \\ \mathcal{E}_{\vee}(A, B) &:= \vee AB \\ \mathcal{E}_{\rightarrow}(A, B) &:= \rightarrow AB \\ \mathcal{E}_{\leftrightarrow}(A, B) &:= \leftrightarrow AB \end{aligned}}$$

# Well-Formed Formula

## Definition (Construction Sequence)

A construction sequence $(C_1, \ldots, C_n)$ 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 $(C_1, \ldots, C_n)$ and $C_n = A$.

$$\begin{aligned}
\mathrm{wff}_0 &\coloneqq \{p_1, p_2, \ldots\} \\
\mathrm{wff}_{n+1} &\coloneqq \mathrm{wff}_n \cup \big\{(\neg A) : A \in \mathrm{wff}_n\big\} \cup \big\{(A \rightarrow B) : A, B \in \mathrm{wff}_n\big\} \\
\mathrm{wff}_* &\coloneqq \bigcup_{n \in \mathbb{N}} \mathrm{wff}_n
\end{aligned}$$

# 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

$$C_0 := B$$

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

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

## Top Down

- A set $S$ is closed under a function $f$ if for all $\mathbf{x}$: $\mathbf{x} \in S \to f(\mathbf{x}) \in S$.
- A set $S$ is inductive if $B \subset S$ 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 $B := \{0\}, \mathcal{F} := \{S, P\}, S(x) := x + 1, P(x) := x - 1$

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

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.
$(C_* \subset C^*)$: consider $x \in C_*$ and a construction sequence $(x_1, \ldots, x_n)$ for $x$. First $x_1 \in B \subset C^*$. If for all $j < i$ we have $x_j \in C^*$, then $x_i \in C^*$. By induction, $x_1, \ldots, x_n \in C^*$.

# Induction Principle for wff

**Theorem (Induction Principle)**

*Let $P$ be a property of formulae, 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.**

$$\mathrm{wff}_* = \mathrm{wff}^* \subset P$$

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

$$P(k) := P(\mathrm{wff}_k)$$

# 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 $\mathrm{Sub}(A)$ of subformulae of a wff $A$ is the smallest set $\Gamma$ that satisfies

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

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

# Unique Readability, Unique Tree

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

subformula vs subtree

# Balanced-Parentheses

**Corollary (Balanced-Parentheses)**

*In any wff, the number of left parentheses is equal to the number of right parentheses.*

**Proof.**

Let $S$ be the set of "balanced" wffs.
Base step: the propositional symbols have zero parentheses.
Inductive step: obvious.

# Left-Weighted-Parentheses

## Lemma

*Any proper initial segment of a wff contains an excess of left parentheses. Thus no proper initial segment of a wff can itself be a wff.*

## Proof.

Consider $A = (C \wedge D)$. The proper initial segments of $(C \wedge D)$ are the following:

1. $($
2. $(C_0$ [inductive hypothesis]
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.

To show $\mathcal{E}_\wedge$ is injective.

$$(A \wedge B) = (C \wedge D)$$
$$\Downarrow$$
$$A \wedge B) = C \wedge D)$$
$$\Downarrow$$
$$A = C \qquad [Lemma]$$

then it follows $B = D$.
Similarly, we can prove

$$(A \wedge B) \neq (C \rightarrow D)$$

# 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

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Assignment

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

$$v : \mathcal{P} \to \{0, 1\}$$

- Such a truth assignment can be uniquely extended to $\overline{v} : \mathrm{wff} \to \{0, 1\}$ satisfying the following condition:

1. $\overline{v}(p) = v(p)$ for $p \in \mathcal{P}$
2. $\overline{v}(\neg A) = 1 - \overline{v}(A)$
3. $\overline{v}(A \wedge B) = \min\{\overline{v}(A), \overline{v}(B)\}$
4. $\overline{v}(A \vee B) = \max\{\overline{v}(A), \overline{v}(B)\}$
5. $\overline{v}(A \to B) = 1 - \overline{v}(A) + \overline{v}(A) \cdot \overline{v}(B)$
6. $\overline{v}(A \leftrightarrow B) = \overline{v}(A) \cdot \overline{v}(B) + (1 - \overline{v}(A)) \cdot (1 - \overline{v}(B))$

# 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 $f \in \mathcal{F}$: $f\restriction_C$ is injective.
2. the range of $f\restriction_C$ 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 $f \in \mathcal{F}$ we have $F_f : V^n \to V$, where $n = \mathrm{arity}(f)$. Then for every function $h : B \to V$, there exists a unique function $\overline{h} : C \to V$ s.t.*

1. $\overline{h}\restriction_B = h$
2. *for all $f \in \mathcal{F}$ and all $x_1, \ldots, x_n \in C$:*

$$\overline{h}(f(x_1, \ldots, x_n)) = F_f\left(\overline{h}(x_1), \ldots, \overline{h}(x_n)\right)$$

$$\begin{tikzcd} B \arrow[r] \arrow[dr, "h"'] & C \arrow[d, dashed, "\overline{h}"] \\ & V \end{tikzcd}$$

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

Danger! $F_f$ is saying "green" but $F_g$ is saying "red" for the same point.

# Truth Table & Truth/Boolean Function

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \rightarrow q$ | $p \leftrightarrow q$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |

## Example

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

# 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!

# Tautology

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

| $p$ | $q$ | $q \to p$ | $p \to q \to p$ |
|---|---|---|---|
| $0$ | $0$ | $1$ | $1$ |
| $0$ | $1$ | $0$ | $1$ |
| $1$ | $0$ | $1$ | $1$ |
| $1$ | $1$ | $1$ | $1$ |

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

- $\nu \vDash A$ if $\overline{\nu}(A) = 1$.
- Logical Consequence. $\Gamma \vDash A$ if for any truth assignment $\nu$ s.t. $(\text{for all } B \in \Gamma : \nu \vDash B) \implies \nu \vDash A$.
- Tautology. $\vDash A$ if $\emptyset \vDash A$.

$$\vDash (p \to q \to r) \to (p \to q) \to p \to r$$

| $p$ | $q$ | $r$ | $q \to r$ | $p \to q \to r$ | $p \to q$ | $p \to r$ | $(p \to q) \to p \to r$ | $(p \to q \to r) \to (p \to q) \to p \to r$ |
|---|---|---|---|---|---|---|---|---|
| 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

$$(\,p \to q \to r\,) \to (\,p \to q\,) \to p \to r$$

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | $\underline{0}$ | | | | | | | |
| | 1 | | | | 0 | | | | $\underline{0}$ | | | |
| | 1 | | | | 0 | | 1 | | 0 | | $\underline{0}$ | |
| 1 | 1 | | | 0 | 0 | 1 | $\underline{1}$ | | 0 | 1 | 0 | 0 |
| 1 | $\underline{1}$ | 1 | | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | $\underline{1}$ | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| | | | × | | | | | | | | | |

# Exercises — Translation

1. The answer is $3$ or $6$.
2. I am not good at logic.
3. If you can't say it clearly, you don't understand it yourself.
4. You understand something only if you can formalize it.
5. I will go out unless it rains.
6. You can pay by credit card or cheque.
7. Neither Sarah nor Peter was to blame for the mistake.
8. I want to buy either a new desktop computer or a laptop, but I have neither the cash nor the credit I need.
9. If I get in the lift then it breaks, and/or if you get in then the lift breaks. (?) (Natural language is ambiguous!)
10. If we both get in the lift, then the lift breaks.
11. $p \vee q \to r \vDash\!\dashv (p \to r) \wedge (q \to r)$
12. $p \wedge q \to r \vDash\!\dashv (p \to r) \vee (q \to r)$

# 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 — Validity

1. $p \vee q \mathrel{\vDash\!\dashv} \neg p \to q \mathrel{\vDash\!\dashv} (p \to q) \to q$
2. $p \wedge q \mathrel{\vDash\!\dashv} \neg(p \to \neg q)$
3. $p \leftrightarrow q \mathrel{\vDash\!\dashv} (p \to q) \wedge (q \to p)$
4. $p \wedge q \mathrel{\vDash\!\dashv} \neg(\neg p \vee \neg q)$
5. $p \to q \to r \mathrel{\vDash\!\dashv} (p \wedge q) \to r$
6. $p \to q \mathrel{\vDash\!\dashv} \neg q \to \neg p$
7. $p \wedge (q \vee r) \mathrel{\vDash\!\dashv} (p \wedge q) \vee (p \wedge r)$
8. $p \vee (q \wedge r) \mathrel{\vDash\!\dashv} (p \vee q) \wedge (p \vee r)$
9. $\neg(p \vee q) \mathrel{\vDash\!\dashv} \neg p \wedge \neg q$
10. $\neg(p \wedge q) \mathrel{\vDash\!\dashv} \neg p \vee \neg q$
11. $p \mathrel{\vDash\!\dashv} p \vee (p \wedge q)$
12. $p \mathrel{\vDash\!\dashv} p \wedge (p \vee q)$

1. $\neg\neg p \to p$
2. $p \to \neg\neg p$
3. $p \vee \neg p$
4. $\neg(p \wedge \neg p)$
5. $p \wedge \neg p \to q$
6. $(p \to q) \wedge (\neg p \to q) \to q$
7. $(p \to q) \wedge (p \to \neg q) \to \neg p$
8. $(\neg p \to q) \wedge (\neg p \to \neg q) \to p$
9. $((p \to q) \to p) \to p$

1. $\Gamma, A \vDash B \iff \Gamma \vDash A \to B$
2. $A \mathrel{\vDash\!\dashv} B \iff \vDash A \leftrightarrow B$
3. $A \vee B, \neg A \vee C \vDash B \vee C$

$$\frac{\begin{array}{r} p \to q \\ q \end{array}}{p} \qquad \frac{\begin{array}{r} p \to q \\ \neg p \end{array}}{\neg q} \qquad \frac{\begin{array}{r} p \vee q \\ p \end{array}}{\neg q}$$

$$\frac{\begin{array}{l} \text{I think, therefore I am} \\ \text{I do not think} \end{array}}{\text{Therefore I am not}}$$

$$\frac{\begin{array}{c} \text{Mickey is murdered by Tom or Jerry} \\ \text{Tom is the killer} \end{array}}{\text{Jerry is innocent}}$$

*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*

# 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，也浇不灭我对你爱情的火焰。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，也浇不灭我对你爱情的火焰。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。

$$p \to r, q \to s \vDash p \lor q \to r \lor s$$

$$p \to \neg s, q \to \neg r \vDash p \lor q \to \neg s \lor \neg r$$

- 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……

# 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。

$$w \to p, \neg w \to p, w \vee \neg w \vDash p$$

$$w \wedge j \to p, \neg w \wedge c \to p, w \vee \neg w \overset{?}{\vDash} p$$

$$\neg w \wedge j \to \neg p, w \wedge c \to \neg p, w \vee \neg w \overset{?}{\vDash} \neg p$$

$$w \wedge j \to p, \neg w \wedge c \to p, (w \wedge j) \vee (\neg w \wedge c) \vDash p$$

# The Crocodile Dilemma

## The Crocodile Dilemma

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

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

| $r$ | $(\neg r \leftrightarrow r) \rightarrow r$ |
|---|---|
| 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。

# 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。

$$x = ? \implies \vDash (x \leftrightarrow b \vee s) \rightarrow b$$

| $b$ | $s$ | $(\neg b \wedge \neg s \leftrightarrow b \vee s) \rightarrow b$ | $(\neg s \leftrightarrow b \vee s) \rightarrow b$ | $((s \rightarrow b) \leftrightarrow b \vee s) \rightarrow b$ |
|---|---|---|---|---|
| 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?

$$x = ? \implies \vDash (p \to (x \leftrightarrow q)) \land (\neg p \to (x \leftrightarrow \neg q))$$

- p: 你说真话。
- q: 左门通天堂。

| $p$ | $q$ | $(p \land q) \lor (\neg p \land \neg q)$ | report | $A$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 |

# Proof by Contradiction

$$(\neg p \to q) \land (\neg p \to \neg q) \to p$$

**Theorem (Euclid's Theorem)**

*There are infinitely many prime numbers.*

**Proof.**

Assume to the contrary that $\mathbb{P} := \{p_1, p_2, \ldots, p_k\}$ is finite. Let $N := \prod_{i=1}^{k} p_i$.

$\exists p \in \mathbb{P} : p \mid (N+1) \;\;\&\;\; p \mid N \implies p \mid 1.$

# Semantic Equivalence

- Semantic equivalence is an equivalence relation between formulae.
- Semantic equivalence is compatible with operators.

$$A \vDash\!\!\!\dashv A' \implies \neg A \vDash\!\!\!\dashv \neg A'$$

$$\left.\begin{array}{l} A \vDash\!\!\!\dashv A' \\ B \vDash\!\!\!\dashv B' \end{array}\right\} \implies A \star B \vDash\!\!\!\dashv A' \star B' \quad \text{where} \quad \star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$$

- Equivalence relation + Compatible with Operators = Congruence relation

# Substitution

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

$$(\neg A)[C_1/p_1, \ldots, C_n/p_n] \coloneqq \neg A[C_1/p_1, \ldots, C_n/p_n]$$

$$(A \to B)[C_1/p_1, \ldots, C_n/p_n] \coloneqq A[C_1/p_1, \ldots, C_n/p_n] \to B[C_1/p_1, \ldots, C_n/p_n]$$

## Theorem

*Consider a wff $A$ and a sequence $C_1, \ldots, C_n$ of wffs.*

1. *Let $\nu$ be a truth assignment for the set of all propositional symbols. Define $\mu$ to be the truth assignment for which $\mu(p_i) = \overline{\nu}(C_i)$. Then $\overline{\mu}(A) = \overline{\nu}\,(A[C_1/p_1, \ldots, C_n/p_n])$.*
2. $\vDash A \implies \vDash A[C_1/p_1, \ldots, C_n/p_n]$

## Example

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

# 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 $\neg A \Vdash\!\!\!\dashv A^*$.*

**Proof.**

Prove by induction.

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

# Contents

Introduction

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Connectives

Would we gain anything by adding more connectives to the language?

## Exclusive Disjunction

$$\begin{aligned} v(p \oplus q) &= v(p) + v(q) \mod 2 \\ &\Downarrow \\ p \oplus q &\vDash\!\!\!\dashv (\neg p \wedge q) \vee (p \wedge \neg q) \\ &\vDash\!\!\!\dashv (p \vee q) \wedge (\neg p \vee \neg q) \\ &\vDash\!\!\!\dashv \neg(p \leftrightarrow q) \end{aligned}$$

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

$$\frac{\begin{array}{c} p \oplus q \\ p \end{array}}{\neg q} \qquad \frac{\begin{array}{c} p \oplus q \\ \neg p \end{array}}{q} \qquad \frac{p}{p \oplus q}\ ?$$

# 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

$$\#(p,q,r) \vDash\!\!\!\dashv (p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$$

| $p$ | $q$ | $r$ | $\#(p,q,r)$ |
|---|---|---|---|
| 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 $\mathscr{L}^0$ is a function $v : \mathcal{P} \to \{0, 1\}$.

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $p \to q$ | $p \leftrightarrow q$ | $\cdots$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | $\cdots$ |
| 0 | 1 | 0 | 1 | 1 | 0 | $\cdots$ |
| 1 | 0 | 0 | 1 | 0 | 0 | $\cdots$ |
| 1 | 1 | 1 | 1 | 1 | 1 | $\cdots$ |

A $n$-place truth/Boolean function is a function $F : \{0, 1\}^n \to \{0, 1\}$.

| $x$ | $F_\neg(x)$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $x$ | $y$ | $F_\wedge(x, y)$ | $F_\vee(x, y)$ | $F_\to(x, y)$ | $F_\leftrightarrow(x, y)$ | $\cdots$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | $\cdots$ |
| 0 | 1 | 0 | 1 | 1 | 0 | $\cdots$ |
| 1 | 0 | 0 | 1 | 0 | 0 | $\cdots$ |
| 1 | 1 | 1 | 1 | 1 | 1 | $\cdots$ |

There are $2^{2^n}$ distinct truth functions with $n$ places.

# Truth Table & Truth/Boolean Function

$$v : \mathcal{P} \to \{0,1\}$$
$$F : \{0,1\}^n \to \{0,1\}$$

| $v(p_1),\ldots,v(p_n)$ | | $x_1,\ldots,x_n$ | $F_A(x_1,\ldots,x_n)$ | | $\overline{v}(A)$ |
|---|---|---|---|---|---|
| $v_1(p_1),\ldots,v_1(p_n)$ | $=$ | $0,\ldots,0$ | $F_A(0,\ldots,0)$ | $=$ | $\overline{v}_1(A)$ |
| $\vdots$ | | $\vdots$ | $\vdots$ | | $\vdots$ |
| $v_{2^n}(p_1),\ldots,v_{2^n}(p_n)$ | $=$ | $1,\ldots,1$ | $F_A(1,\ldots,1)$ | $=$ | $\overline{v}_{2^n}(A)$ |

## Definition

Suppose $A$ is a wff whose propositional symbols are $p_1,\ldots,p_n$.
A truth function $F : \{0,1\}^n \to \{0,1\}$ represented by $A$ is

$$F_A(v(p_1),\ldots,v(p_n)) = \overline{v}(A)$$

$$A \vDash B \iff F_A = F_B$$

## Theorem (Post1921)

*Every truth function $F : \{0,1\}^n \to \{0,1\}$ 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.

$$\neg A \vDash\!\!\!\dashv \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} \pm p_{ij} \implies A \vDash\!\!\!\dashv \neg \left( \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} \pm p_{ij} \right) \vDash\!\!\!\dashv \bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} \mp p_{ij}$$

# CNF Transformation

| subformula | replaced by |
|---|---|
| $A \leftrightarrow B$ | $(\neg A \vee B) \wedge (\neg B \vee A)$ |
| $A \rightarrow B$ | $\neg A \vee B$ |
| $\neg(A \wedge B)$ | $\neg A \vee \neg B$ |
| $\neg(A \vee B)$ | $\neg A \wedge \neg B$ |
| $\neg\neg A$ | $A$ |
| $(A_1 \wedge \cdots \wedge A_n) \vee B$ | $(A_1 \vee B) \wedge \cdots \wedge (A_n \vee B)$ |

# Adequate Sets of Connectives

## Definition

A set of connectives is adequate if every truth function can be represented by a wff containing only connectives from that set.

- $\{\neg, \wedge, \vee\}$
- $\{\neg, \wedge\}; \{\neg, \vee\}; \{\neg, \rightarrow\}; \{\bot, \rightarrow\}$
- $\{\uparrow\}; \{\downarrow\}$
- $\{\wedge, \vee, \rightarrow, \leftrightarrow\}; \{\neg, \leftrightarrow\}$ not adequate.

| $p$ | $\bot$ |
|---|---|
| 0 | 0 |
| 1 | 0 |

$$\begin{aligned}
\bot &\coloneqq p \wedge \neg p \\
p \uparrow q &\coloneqq \neg(p \wedge q) \\
p \downarrow q &\coloneqq \neg(p \vee q) \\
\neg p &\coloneqq p \uparrow p \\
p \wedge q &\coloneqq (p \uparrow q) \uparrow (p \uparrow q) \\
p \vee q &\coloneqq (p \uparrow p) \uparrow (q \uparrow q)
\end{aligned}$$

| $p$ | $q$ | $p \uparrow q$ | $p \downarrow q$ |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |

# 3-valued Logics

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| $u$ | $u$ |
| 1 | 0 |

| $\wedge$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | $u$ | 0 |
| $u$ | $u$ | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

| $\vee$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | $u$ | 1 |
| $u$ | $u$ | $u$ | $u$ |
| 1 | 1 | $u$ | 1 |

| $\rightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | $u$ | 1 |
| $u$ | $u$ | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

| $\leftrightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | $u$ | 0 |
| $u$ | $u$ | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

Table: Bochvar: $u$ as "meaningless"

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| $u$ | $u$ |
| 1 | 0 |

| $\wedge$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| $u$ | 0 | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

| $\vee$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | $u$ | 1 |
| $u$ | $u$ | $u$ | 1 |
| 1 | 1 | 1 | 1 |

| $\rightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| $u$ | $u$ | $u$ | 1 |
| 1 | 0 | $u$ | 1 |

| $\leftrightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | $u$ | 0 |
| $u$ | $u$ | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

Table: Kleene: $u$ as "undefined"

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| $u$ | $u$ |
| 1 | 0 |

| $\wedge$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| $u$ | 0 | $u$ | $u$ |
| 1 | 0 | $u$ | 1 |

| $\vee$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 0 | $u$ | 1 |
| $u$ | $u$ | $u$ | 1 |
| 1 | 1 | 1 | 1 |

| $\rightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| $u$ | $u$ | 1 | 1 |
| 1 | 0 | $u$ | 1 |

| $\leftrightarrow$ | 0 | $u$ | 1 |
|---|---|---|---|
| 0 | 1 | $u$ | 0 |
| $u$ | $u$ | 1 | $u$ |
| 1 | 0 | $u$ | 1 |

Table: Lukasiewicz: $u$ as "possible"

# Contents

Introduction

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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.

# Formal System = Axiom + Inference Rule

## Axiom Schema

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

## Inference Rule

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

# Deduction / Proof

This sentence can never be proved.

What is "proof"?

## Definition (Deduction)

A deduction from $\Gamma$ is a sequence of wff $(C_1, \ldots, C_n)$ 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 $j < k$, $C_i = C_j \to C_k$.

- $\Gamma \vdash A$ if $A$ is the last member of some deduction from $\Gamma$.
- $\vdash A := \emptyset \vdash A$

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.

# Example

**Theorem**

$$\vdash p \to p$$

**Proof.**

| | | |
|---|---|---|
| 1. | $p \to (p \to p) \to p$ | A1 |
| 2. | $(p \to (p \to p) \to p) \to (p \to p \to p) \to p \to p$ | A2 |
| 3. | $(p \to p \to p) \to p \to p$ | 1,2 MP |
| 4. | $p \to p \to p$ | A1 |
| 5. | $p \to p$ | 3,4 MP |

# Example

**Theorem**

$$\vdash (\neg p \to p) \to p$$

**Proof.**

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

# Example

**Theorem**

$$p \to q, q \to r \vdash p \to r$$

**Proof.**

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

# Example — Curry's Paradox ◎ô◎

If this sentence is true, then God exists.

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

Proof.

1. $p \leftrightarrow (p \to q)$
2. $p \to p \to q$
3. $(p \to p) \to p \to q$
4. $p \to q$
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.

$$x = ? \implies \vDash (a \leftrightarrow x) \to k$$

**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?

# Deduction Theorem

## Theorem (Deduction Theorem)

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

## Proof.

Prove by induction on the length of the deduction sequence $(C_1, \ldots, C_n)$ 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. $C_i = C_j \to B$

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

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

$\Gamma \vdash A \to B$

# Equivalent Replacement

**Theorem**

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

$$B \leftrightarrow C \vdash A \leftrightarrow A^*$$

**Proof.**

Prove by induction on the number of connective of $A$.

# 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.

$$\left.\begin{array}{r} p \vee q \\ q \leftrightarrow \neg p \end{array}\right\} \Longrightarrow p \vee \neg p \qquad \checkmark$$

# Formal System — Variant

## Axiom Schema

1. $A \to B \to A$
2. $(A \to B \to C) \to (A \to B) \to A \to C$
3. $A \wedge B \to A$
4. $A \wedge B \to B$
5. $(A \to B) \to (A \to C) \to A \to B \wedge C$
6. $A \to A \vee B$
7. $B \to A \vee B$
8. $(A \to C) \to (B \to C) \to A \vee B \to C$
9. $(A \to \neg B) \to (A \to B) \to \neg A$
10. $\neg A \to A \to B$
11. $\neg\neg A \to A$

## Reference Rule

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

$$p' := \neg\neg p$$

$$(A \star B)' := \neg\neg(A' \star B')$$

where $\star \in \{\wedge, \vee, \to\}$

$$\Gamma' := \{A' : A \in \Gamma\}$$

$$\Gamma \vdash_{\mathrm{C}} A \iff \Gamma' \vdash_{\mathrm{I}} A'$$

1–8+MP=**P**ositive Calculus  **P**+9=**M**inimal Calculus

**M**+10=**I**ntuitionistic Calculus  **I**+11=**C**lassical Calculus

# Tree Method for Propositional Logic

$\neg\neg A$

$A$

$A \to B$

$\neg A \qquad B$

$\neg(A \to B)$

$A$

$\neg B$

---

$A \wedge B$

$A$

$B$

$\neg(A \wedge B)$

$\neg A \qquad \neg B$

$A \vee B$

$A \qquad B$

$\neg(A \vee B)$

$\neg A$

$\neg B$

---

$A \leftrightarrow B$

$A \qquad \neg A$

$B \qquad \neg B$

$\neg(A \leftrightarrow B)$

$A \qquad \neg A$

$\neg B \qquad B$

✓

# 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 occurrance 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 if it contains a wff and its negation.
- *Closed tree.* A tree is closed if all its branches are closed.
- *Open branch.* A branch is open if it is not closed and no rule can be applied.
- *Open tree.* A tree is open if it has at least one open branch.

# 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.

**Definition (Deduction)**

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

**Theorem (Soundness & Completeness Theorem)**

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

**Remark:** If an inference with propositional formulae 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

$$\boxed{p \to q, \neg q \vee r \vdash \neg p \vee r}$$

$p \to q$ ✓

$\neg q \vee r$ ✓

$\neg(\neg p \vee r)$ ✓

$\neg\neg p$

$\neg r$

- $\neg p$ ×
- $q$
  - $\neg q$ ×
  - $r$ ×

# An open branch corresponds to a valuation

$$p \lor q, r \lor s, s \to t \overset{?}{\vDash} r$$

$v(r) = 0, \quad v(s) = 1, \quad v(t) = 1 \quad v(p) = 1 \quad v(q) = 1$ or $0$

$v(r) = 0, \quad v(s) = 1, \quad v(t) = 1 \quad v(q) = 1 \quad v(p) = 1$ or $0$

$$v \vDash p \lor q, \quad v \vDash r \lor s, \quad v \vDash s \to t, \quad v \nvDash r$$

**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

1. $p \to (\neg q \to q) \vdash p \to q$
2. $(p \to r) \land (q \to r) \vdash p \lor q \to r$
3. $(p \to q) \land (r \to s) \vdash \neg q \land r \to \neg q \land s$
4. $\Big(\big((p \to q) \to (\neg r \to \neg s)\big) \to r\Big) \to t \vdash (t \to p) \to s \to p$
5. $(p \to q) \lor (q \to r)$
6. $(p \to q) \to (\neg p \to q) \to q$
7. $((p \to q) \to p) \to p$
8. $(p \to q) \land (r \to s) \to p \lor r \to q \lor s$
9. $(p \to q) \land r \to \neg(p \land r) \lor (q \land r)$
10. $(p \leftrightarrow (p \to q)) \to q$
11. $\neg(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow q)$

# Exercises — Tree Method

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

1. $(p \vee q) \wedge r \overset{?}{\vDash} p \vee (q \wedge r)$
2. $p \vee (q \wedge r) \overset{?}{\vDash} (p \vee q) \wedge r$
3. $p \leftrightarrow (q \rightarrow r) \overset{?}{\vDash} (p \leftrightarrow q) \rightarrow r$
4. $(p \leftrightarrow q) \rightarrow r \overset{?}{\vDash} p \leftrightarrow (q \rightarrow r)$
5. $\neg(p \rightarrow q \wedge r), r \rightarrow p \wedge q \overset{?}{\vDash} \neg r$
6. $p \rightarrow (q \wedge r), \neg(p \vee q \rightarrow r) \overset{?}{\vDash} p$
7. $p \rightarrow q, r \rightarrow s, p \vee r, \neg(q \wedge s) \overset{?}{\vDash} (q \rightarrow p) \wedge (s \rightarrow r)$
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.

# Contents

Introduction

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Independence

## Definition (Independence)

An axiom $A$ in $\Gamma$ is independent if $\Gamma \setminus \{A\} \nvdash A$.

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

- $\nVdash A$
- for all $B$, $\Gamma \setminus \{A\} \vdash B \implies \Vdash B$

## Theorem

*Axiom3 is independent of Axiom1 and Axiom2.*

| $p$ | $\neg p$ |
|---|---|
| 0 | 0 |
| 1 | 0 |

| $\rightarrow$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |

Let $\nu(p) = 0$ and $\nu(q) = 1$, then $\nVdash (\neg p \rightarrow \neg q) \rightarrow (\neg p \rightarrow q) \rightarrow p$.

# Independence

Axiom$1$ and Axiom$2$ axiomatizes the conditional ($\to$) fragment of intuitionistic propositional logic. To axiomatize the conditional fragment of classical logic, we also need *Peirce's law*: $((p \to q) \to p) \to p$.

**Theorem**

*Peirce's law is independent of Axiom$1$ and Axiom$2$.*

| $\to$ | $1$ | $2$ | $3$ |
|---|---|---|---|
| $1$ | $1$ | $2$ | $3$ |
| $2$ | $1$ | $1$ | $3$ |
| $3$ | $1$ | $1$ | $1$ |

Here we interpret $1$ as "true", $3$ as "false", and $2$ as "maybe".
Let $v(p) = 2$ and $v(q) = 3$, then $v(((p \to q) \to p) \to p) = 2$.

# Model & Semantic Consequence

- $\mathrm{Mod}(A) := \{v : v \vDash A\}$
- $\mathrm{Mod}(\Gamma) := \bigcap_{A \in \Gamma} \mathrm{Mod}(A)$
- $\mathrm{Th}(v) := \{A : v \vDash A\}$
- $\mathrm{Th}(\mathcal{K}) := \bigcap_{v \in \mathcal{K}} \mathrm{Th}(v)$
- $\mathrm{Cn}(\Gamma) := \{A : \Gamma \vDash A\}$

- $\Gamma \subset \Gamma' \implies \mathrm{Mod}(\Gamma') \subset \mathrm{Mod}(\Gamma)$
- $\mathcal{K} \subset \mathcal{K}' \implies \mathrm{Th}(\mathcal{K}') \subset \mathrm{Th}(\mathcal{K})$
- $\Gamma \subset \mathrm{Th}(\mathrm{Mod}(\Gamma))$
- $\mathcal{K} \subset \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$
- $\mathrm{Mod}(\Gamma) = \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Gamma)))$
- $\mathrm{Th}(\mathcal{K}) = \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathcal{K})))$
- $\mathrm{Cn}(\Gamma) = \mathrm{Th}(\mathrm{Mod}(\Gamma))$
- $\Gamma \subset \Gamma' \implies \mathrm{Cn}(\Gamma) \subset \mathrm{Cn}(\Gamma')$
- $\mathrm{Cn}(\mathrm{Cn}(\Gamma)) = \mathrm{Cn}(\Gamma)$

# Consistency & Satisfiability

- $\Gamma$ is consistent if $\Gamma \nvdash \bot$.
- $\Gamma$ is Post-consistent if there is some wff $A : \Gamma \nvdash A$.

$$\boxed{\Gamma \text{ is consistent iff it is Post-consistent.}}$$

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

- If $\Gamma$ is consistent and $\Gamma \vdash A$, then $\Gamma \cup \{A\}$ is consistent.
- $\Gamma \cup \{\neg A\}$ is inconsistent iff $\Gamma \vdash A$.
- If $\Gamma$ 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:

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

## Corollary

*Any satisfiable set of wffs is consistent.*

# Compactness Theorem

**Theorem (Compactness Theorem)**

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

如果语言可以说无穷析取，则没有紧致性。$\left\{\bigvee_{i=1}^{\infty} p_i, \neg p_1, \neg p_2, \dots\right\}$

**Corollary**

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

**Proof.**

$$\begin{aligned}
\Gamma_0 \nvDash A \text{ for any } \Gamma_0 \subset \Gamma &\implies \Gamma_0 \cup \{\neg A\} \text{ is satisfiable for any } \Gamma_0 \subset \Gamma \\
&\implies \Gamma \cup \{\neg A\} \text{ is satisfiable} \\
&\implies \Gamma \nvDash A
\end{aligned}$$

# 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.

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

# Proof of Compactness Theorem

**Proof.**

part1. Extend the finitely satisfiable set $\Gamma$ to a maximal finitely satisfiable set $\Delta$.

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

$$\Delta_0 := \Gamma$$

$$\Delta_{n+1} := \begin{cases} \Delta_n \cup \{A_n\} & \text{if } \Delta_n \cup \{A_n\} \text{ is finitely satisfiable} \\ \Delta_n \cup \{\neg A_n\} & \text{otherwise} \end{cases}$$

$$\Delta := \bigcup_{n \in \mathbb{N}} \Delta_n$$

part2. Define a truth assignment that satisfies $\Gamma$.

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

# "Compactness Theorem"

**Theorem ("Compactness Theorem")**

*$\Gamma$ is consistent iff every finite subset of $\Gamma$ is consistent.*

**Proof.**

Suppose $\Gamma \vdash A$ and $\Gamma \vdash \neg A$.
Then there is a deduction sequence $(C_1, \ldots, C_n)$ of $A$ from $\Gamma$, and a deduction sequence $(D_1, \ldots, D_m)$ of $\neg A$ from $\Gamma$.
Let $\Sigma_0 := \{C_i \in \Gamma : 1 \leq i \leq n\}$ and $\Sigma_1 := \{D_i \in \Gamma : 1 \leq i \leq m\}$.
The finite set $\Sigma := \Sigma_0 \cup \Sigma_1$ is inconsistent.

# Weak Completeness Theorem

## Lemma

*Let $A$ be a wff whose only propositional symbols are $p_1, \ldots, p_n$. Let*

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

*then $p_1^\nu, \ldots, p_n^\nu \vdash A^\nu$.*

## Weak Completeness Theorem $\quad \vDash A \implies \vdash A$

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

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

# Completeness Theorem

$$\vDash A \iff \vdash A$$

$$+$$

Compactness

$$\Downarrow$$

$$\Gamma \vDash A \iff \Gamma \vdash A$$

# Completeness Theorem — Post1921

## Theorem (Completeness Theorem)

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

## Corollary

*Any consistent set of wffs is satisfiable.*

$$\begin{array}{ccc} \Gamma \vDash A & \Longleftrightarrow & \Gamma \vdash A \\ \Updownarrow & & \Updownarrow \\ \begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{unsatisfiable}\end{array} & \Longleftrightarrow & \begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{inconsistent}\end{array} \end{array}$$

## Corollary (Compactness Theorem)

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

# Proof of Completeness Theorem

**Proof.**

step1. Extend the consistent set $\Gamma$ to a maximal consistent set $\Delta$.
Let $\langle A_i : i \in \mathbb{N} \rangle$ be a fixed enumeration of the wffs.

$$\Delta_0 := \Gamma$$

$$\Delta_{n+1} := \begin{cases} \Delta_n \cup \{A_n\} & \text{if } \Delta_n \cup \{A_n\} \text{ is consistent} \\ \Delta_n \cup \{\neg A_n\} & \text{otherwise} \end{cases}$$

$$\Delta := \bigcup_{n \in \mathbb{N}} \Delta_n$$

step2. Define a truth assignment that satisfies $\Gamma$.

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

# Decidability — Post1921

**Theorem**

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

**Theorem**

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

**Theorem**

*If $\Gamma$ is a decidable set of wffs, then the set of logical consequences of $\Gamma$ is recursively enumerable.*

# Post 1897-1954

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

# Theory & Axiomatization

## What is "theory"?

- A set $\Gamma$ of sentences is a theory if $\Gamma = \mathrm{Cn}(\Gamma)$.
- A theory $\Gamma$ is complete if for every sentence $A$, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- A theory $\Gamma$ is axiomatizable if there is a decidable set $\Sigma$ of sentences s.t. $\Gamma = \mathrm{Cn}(\Sigma)$.
- A theory $\Gamma$ is finitely axiomatizable if $\Gamma = \mathrm{Cn}(\Sigma)$ for some finite set $\Sigma$ of sentences.

# Model Checking & Satisfiability Checking & Validity Checking[7]

- Given a model $\nu$ and a formula $A$. Is $\nu \vDash A$? —P
- Given a formula $A$. Is there a model $\nu$ s.t. $\nu \vDash A$? —NP
- Given a sentence $A$. Is $\vDash A$?

Figure: *Hamiltonian Circle(NP)*

Figure: *Eulerian Circle(P)*

Figure: *Graph Coloring(NP)*

[7] Aaronson: Why philosophers should care about computational complexity.

# Contents

Introduction

History

Propositional Logic
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Party and Friends

## Problem

- *We want to throw a party for Tweety, Gentoo and Tux.*
- *But they have different circles of friends and dislike some.*
- *Tweety tells you that he would like to see either his friend Kimmy or not to meet Gentoo's Alice, but not both.*
- *But Gentoo proposes to invite Alice or Harry or both.*
- *Tux, however, does not like Harry and Kimmy too much, so he suggests to exclude at least one of them.*

# Party and Friends

## Problem

- *We want to throw a party for Tweety, Gentoo and Tux.*
- *But they have different circles of friends and dislike some.*
- *Tweety tells you that he would like to see either his friend Kimmy or not to meet Gentoo's Alice, but not both.*
- *But Gentoo proposes to invite Alice or Harry or both.*
- *Tux, however, does not like Harry and Kimmy too much, so he suggests to exclude at least one of them.*

## Solution

$$(K \vee \neg A) \wedge \neg(K \wedge \neg A) \wedge (A \vee H) \wedge (\neg H \vee \neg K)$$

# Sudoku

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

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

- Every row/column contains every number.

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

- Every $3 \times 3$ 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 $n \neq n'$:

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

# Shannon — Digital Circuit Design

$$(A \wedge B) \vee ((C \vee A) \wedge \neg B) \equiv A \vee (C \wedge \neg B)$$

# Shannon — Digital Circuit Design

$$(A \vee \neg C) \wedge (B \vee \neg C) \equiv (A \wedge B) \vee \neg C$$

# McCulloch-Pitts Artificial Neural Network

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

## 《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：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。

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

$$w_1 \cdot 0 + w_2 \cdot 0 + b < 0 \qquad b < 0$$
$$w_1 \cdot 0 + w_2 \cdot 1 + b \geq 0 \qquad w_2 + b \geq 0$$
$$w_1 \cdot 1 + w_2 \cdot 0 + b \geq 0 \qquad w_1 + b \geq 0$$
$$w_1 \cdot 1 + w_2 \cdot 1 + b < 0 \qquad w_1 + w_2 + b < 0$$

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

# 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 |

$$y_1^+ = \bar{y}_1\bar{y}_2 + \bar{x}\bar{y}_2$$
$$y_2^+ = y_1\bar{y}_2 + xy_1$$

# 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.

$$f : (c, p, q) \mapsto (c, c \cdot q + \overline{c} \cdot p, c \cdot p + \overline{c} \cdot q)$$

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

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

# 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。

- 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

## 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。

## 谁是窃贼?

1. 钱要么是甲偷的要么是乙偷的。
2. 如果是甲偷的，则偷窃时间不会在午夜前。
3. 如果乙的证词正确，则午夜时灯光未灭。
4. 如果乙的证词不正确，则偷窃发生在午夜前。
5. 午夜时没有灯光。

# Exercise

## 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："只要小白或老王说真话，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"。

## 我在做什么?

1. 如果我不在打网球，那就在看网球。
2. 如果我不在看网球，那就在读网球杂志。
3. 但我不能同时做两件以上的事。

# Summary

- Syntax
- Semantics
- Formal System
- Expressiveness / Succinctness
- Satisfiability / Validity
- Soundness / Completeness / Compactness
- Decidability / Computational Complexity
- $\vdots$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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.

# Example

◎ô◎

What will a logician choose: an egg or eternal bliss in the afterlife? An egg! Because nothing is better than eternal bliss in the afterlife, and an egg is better than nothing.

$$b < 0 < e \implies b < e$$

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

◎ô◎

No cat has eight tails. A cat has one tail more than no cat. Therefore, a cat has nine tails.

Modeling
Statistics
Operations Research
Differential Equations
Probability
Cryptology
Number Theory
Knot Theory
Computational Math
Game Theory
Calculus
Numerical Analysis
Graph Theory
Topology
Linear Algebra
Complex Analysis
Real Analysis
Geometry
Algebra
Analysis
Number Systems
Set Theory
Logic
©2002 M Hale

GENERAL RELATIVITY
(3+1-dimensional pseudo-Riemannian manifolds with tensor fields obeying PDE's of, say, Einstein-Maxwell theory with perfect fluid component)
QUANTUM FIELD THEORY
(Operator-valued fields on R 4 obeying certain Lorentz-invariant PDE's and commutation relationships, acting on an abstract Hilbert space)
LORENTZ GROUP
SU(2)
Specialize
LIE GROUPS
LIE ALGEBRAS
DIFFERENTIAL OPERATORS
MANIFOLDS WITH TENSOR FIELDS
METRIC MANIFOLDS
ALGEBRAS
LINEAR OPERATORS
TENSOR SPACES
REAL MANIFOLDS
COMPLEX MANIFOLDS
HILBERT SPACES
DISTRI-BUTIONS
Define linear vector mappings
Define linear functions of n vectors
Define charts and atlases
Add inner product
Define linear functionals
TRIPLE FIELDS
Add 4th binary op. etc.
DOUBLE FIELDS
VECTOR SPACES
R n
C n
BANACH SPACES
REAL FUNCTIONS
Add new class (vectors), define vector sum & scalar product
Add ordering, least upper bound property
REAL NUMBERS
Define =, + & · for pairs
COMPLEX NUMBERS
COMPLEX FUNCTIONS
Add 3rd binary operation, etc.
ABELIAN FIELDS
Define =, + & · for Dedekind cuts
Add norm & complete-ness
MEASURABLE SPACES
RATIONAL NUMBERS
METRIC SPACES
Add measure
Add commutativity
ABELIAN GROUPS
FIELDS
Define =, + & · for equi-valence classes of pairs
Add metric
INTEGERS
Add multiplicative inverse
Add commutativity
GROUPS
RINGS
Define =, + & · for negative numbers
TOPOLOGICAL SPACES
Add inverse
Add commutativity and 2nd assoc. & distrib. binary operation
NATURAL NUMBERS
Add open set axioms
ABSTRACT GEOMETRIES
Specialize
SEMI-GROUPS
Add number theory symbols & axioms
DODECA-HEDRON GROUP
Add = & associative binary operation with identity
LOWER PREDICATE CALCULUS
Add symbols and axioms for =, in, subset, union & intersection
SETS
RELATIONS
Add cartesian products
Add quantifiers
BOOLEAN ALGEBRA
Add symbols & axioms for brackets, not, and, etc.
MODELS
FORMAL SYSTEMS

?
h→0
G→0
General Relativity
Quantum Field Theory
h→0
c→∞
G→0
Special Relativity
Nonrelativistic Quantum Mechanics
Nuclear Physics
Particle phenomenology
h→0
Electro-magnetism
Classical Mechanics
Atomic Physics
Solid State Physics
Statistical Mechanics
Chemistry
Electric properties of solids
Mechanics of solids
Hydro-dynamics
Thermo-dynamics
Astrophysics
Electrical Engineering
Mechanical Engineering
Earth Science
Evolution
Computer Science
Biology
Psychology
Medicine
Sociology

# Reductionism ≠ Emergence

# Contents

Introduction

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Syntax

## Language

$$\mathscr{L}^1 := \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, =, (, )\} \cup \mathcal{V} \cup \overbrace{\mathcal{F} \cup \mathcal{Q}}^{\text{signature}}$$

where

$$\mathcal{V} := \{x_i : i \in \mathbb{N}\}$$

$$\mathcal{F} := \bigcup_{k \in \mathbb{N}} \mathcal{F}^k \quad \mathcal{F}^k := \left\{f_1^k, \ldots, f_n^k, (\ldots)\right\}$$

$$\mathcal{Q} := \bigcup_{k \in \mathbb{N}} \mathcal{Q}^k \quad \mathcal{Q}^k := \left\{P_1^k, \ldots, P_n^k, (\ldots)\right\}$$

$f^k$ is a $k$-place function symbol.
$P^k$ is a $k$-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

## Term $\mathcal{T}$

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

where $x \in \mathcal{V}$ and $f \in \mathcal{F}$.

- $\mathcal{T}$ is freely generated from $\mathcal{V}$ by $\mathcal{F}$.

## Well-Formed Formula wff

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

where $t \in \mathcal{T}$ and $P \in \mathcal{Q}$.

- wff is freely generated from atomic formulae by connective and quantifier operators.

# Syntax

- $A \wedge B := \neg(A \to \neg B)$
- $A \vee B := \neg A \to B$
- $A \leftrightarrow B := (A \to B) \wedge (B \to A)$
- $\exists x A := \neg \forall x \neg A$
- $\bot := A \wedge \neg A$
- $\top := \neg \bot$

- Bottom up and Top down definitions of terms, subterms, wffs and subformulae.
- Induction Principle for terms and wffs.
- Unique readability theorem for terms and wffs.
- Omitting Parenthesis.
  1). outermost parentheses. 2). $\neg, \forall, \exists, \wedge, \vee, \to, \leftrightarrow$ 3). group to the right.

# Freedom & Bondage

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

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

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

$$\left( \sum_{x \in \mathcal{X}} |P(x) - Q(x)| \right)^2 \leq 2 \sum_{x \in \mathcal{X}} P(x) \ln \frac{P(x)}{Q(x)}$$

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

$$\int_0^t \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\,dx$$

$$f(x) = \sum_{n=1}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$$

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

# Freedom & Bondage

## Definition (Free Variable of a Term)

$$\mathrm{Fv}(t) := \begin{cases} x & \text{if } t = x \\ \emptyset & \text{if } t = c \\ \mathrm{Fv}(t_1) \cup \cdots \cup \mathrm{Fv}(t_n) & \text{if } t = f(t_1, \ldots, t_n) \end{cases}$$

## Definition (Free Variable of a wff)

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

# Freedom & Bondage

## Definition (Bound Variable)

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

- $t$ is a ground (closed) term if $\mathrm{Fv}(t) = \emptyset$.
- $A$ is a sentence (closed formula) if $\mathrm{Fv}(A) = \emptyset$.
- $A$ is an open formula if $\mathrm{Bv}(A) = \emptyset$.

Example: $c = d$ is clopen.

# Translation

How to 'speak' the language of first order logic?

1. **A**: $\forall x(Sx \to Px)$
2. **E**: $\forall x(Sx \to \neg Px)$
3. **I**: $\exists x(Sx \wedge Px)$
4. **O**: $\exists x(Sx \wedge \neg Px)$
5. Every boy loves some girl. $\forall x\big(Bx \to \exists y(Gy \wedge Lxy)\big)$
6. Whoever has a father has a mother. $\forall x(\exists y Fyx \to \exists y Myx)$
7. Grandmother is mother's mother. $\forall xy\big(Gxy \leftrightarrow \exists z(Mxz \wedge Mzy)\big)$ or $\forall xy\big(x = Gy \leftrightarrow \exists z(x = Mz \wedge z = My)\big)$
8. 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。
   $\forall xy(Fx \wedge Fy \wedge Bxy \to Sxy) \to \exists x(Fx \wedge \forall y(Fy \to Bxy)) \to \exists x(Fx \wedge \forall y(Fy \to Sxy))$
9. There are $n$ elements. $\exists x_1 \ldots x_n \left( \bigwedge_{1 \le i < j \le n} x_i \neq x_j \wedge \forall x \left( \bigvee_{i=1}^{n} x = x_i \right) \right)$

# Translation

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

1. Cogito, ergo sum. (I think, therefore I am.) *Descartes*
2. To be or not to be. *Shakespeare*
3. April is the cruellest month. *Eliot*
4. Those who do not weep, do not see. *Hugo*
5. It was the best of times, it was the worst of times. *Dickens*
6. All Children, except one, grow up. *Barrie*
7. All happy families are alike; each unhappy family is unhappy in it's own way. *Tolstoi*
8. You can fool all the people some of the time, and some of the people all the time, but you can't fool all the people all the time. *Lincoln*
9. There is but one truly serious philosophical problem and that is suicide. *Camus*
10. Hope is the thing with feathers that perches in the soul. *Dickinson*
11. All hope abandon, all you who enter here. *Dante*
12. One for all and all for one. *Dumas*
13. The only thing we have to fear is fear itself. *Roosevelt*
14. All animals are equal, but some animals are more equal than others. *Orwell*

# Exercises — Translation

1. If you can't solve a problem, then there is an easier problem that you can't solve.
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. Every farmer who owns a donkey is happy.
11. Every farmer who owns a donkey beats it.
12. All even numbers are divisible by $2$, but *only some* are divisible by $4$.

# Exercises — Translation

1. Everyone alive $2000BC$ is either an ancestor of nobody alive today or of everyone alive today.
2. John hates all people who do not hate themselves.
3. No barber shaves exactly those who do not shave themselves.
4. Andy and Bob have the same maternal grandmother. $\mathrm{mother}(x, y)$
5. Anyone who loves *two* different girls is Tony.
6. There is *exactly* one sun.
7. Socrates' wife *has* a face that *only* her mother could love.
8. If dogs are animals, every head of a dog is the head of an animal.
9. Someone *other than the girl* who loves Bob is stupid.
10. Morris only loves *the girl* who loves him.
11. *The one* who loves Alice is *the one* she loves.
12. *The shortest* English speaker loves *the tallest* English speaker.

# Translation

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

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

continuity vs uniform continuity

$$\forall x \in \mathbb{R} \forall\varepsilon > 0 \exists\delta > 0 \forall y \in \mathbb{R} \big(|x - y| < \delta \to |f(x) - f(y)| < \varepsilon\big)$$

$$\forall\varepsilon > 0 \exists\delta > 0 \forall xy \in \mathbb{R} \big(|x - y| < \delta \to |f(x) - f(y)| < \varepsilon\big)$$

# Translation

1. $\exists x\Big(Gx \land \forall y\big(By \land \forall z(Gz \land z \neq x \to \neg Lzy) \to Lxy\big)\Big) \to \forall x\Big(Bx \to \exists y\big(Gy \land Lyx\big)\Big)$
2. $\forall xy\Big(\big(Gx \land \forall y(By \to \neg Lxy)\big) \land \big(Gy \land \exists x(Bx \land Lyx)\big) \to \neg Lxy\Big)$

# Translation

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

# Exercises — 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 and Substitutable

## Definition (Substitution in a term/formula)

$$=, P, \neg, \rightarrow \cdots$$

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

## Definition (Substitutable)

$t$ is substitutable for $x$ in $A$:

$$=, P, \neg, \rightarrow \cdots$$

$A = \forall y B$ iff either

1. $x \notin \mathrm{Fv}(A)$ or
2. $y \notin \mathrm{Fv}(t)$ and $t$ is substitutable for $x$ in $B$.

Prevent the variables in $t$ from being captured by a quantifier in $A$.

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

# Contents

Introduction

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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* $\forall x\big(T(x) \leftrightarrow A(x)\big)$
2. *materially adequate* $A(s) \leftrightarrow p$
   where '$s$' is the name of a sentence of $\mathscr{L}$, and '$p$' is the translation of this sentence in $\mathscr{L}'$.

# Structure

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

- assigns to each constant symbol $c$ an element $I(c) \in M$,
- assigns to each function symbol $f^k$ a $k$-ary function $I(f^k) : M^k \to M$,
- assigns to each predicate symbol $P^k$ a $k$-ary relation $I(P^k) \subset M^k$.

We write $\mathcal{M} = \left(M, c^{\mathcal{M}}, f^{\mathcal{M}}, P^{\mathcal{M}}\right)$ for convenience.

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

# Structure

火
心
木生火
火生土
木
肝
疏肝理气
除湿解毒
脾
土
益气健脾
帮助消化
木克土
水克火
火克金
金克木
土克水
土生金
水生木
肾
水
滋阴壮阳
强筋壮骨
肺
金
祛风散寒
止嗽润肺
金生水

fire
wood
earth
water
metal

# Interpretation

An interpretation $(\mathcal{M}, \nu)$ is a structure $\mathcal{M}$ with a variable assignment $\nu : \mathcal{V} \to M$.
We extend $\nu$ to $\overline{\nu} : \mathcal{T} \to M$ by recursion as follows:

- $\overline{\nu}(x) := \nu(x)$
- $\overline{\nu}(c) := c^{\mathcal{M}}$
- $\overline{\nu}(f(t_1, \ldots, f_n)) := f^{\mathcal{M}}(\overline{\nu}(t_1), \ldots, \overline{\nu}(t_n))$

$$\begin{tikzcd}
\mathcal{T} \arrow[r, "\overline{\nu}"] \arrow[d, "\mathcal{E}_f"'] & M \arrow[d, "f^{\mathcal{M}}"] \\
\mathcal{T} \arrow[r, "\overline{\nu}"'] & M
\end{tikzcd}$$

# Tarski's Definition of Truth

**Definition ($\mathcal{M}, v \vDash A$)**

- $\mathcal{M}, v \vDash t_1 = t_2$ if $\overline{v}(t_1) = \overline{v}(t_2)$
- $\mathcal{M}, v \vDash P(t_1, \ldots, t_n)$ if $(\overline{v}(t_1), \ldots, \overline{v}(t_n)) \in P^{\mathcal{M}}$
- $\mathcal{M}, v \vDash \neg A$ if $\mathcal{M}, v \nvDash A$
- $\mathcal{M}, v \vDash A \to B$ if $\mathcal{M}, v \nvDash A$ or $\mathcal{M}, v \vDash B$
- $\mathcal{M}, v \vDash \forall x A$ if for every $a \in M : \mathcal{M}, v(a/x) \vDash A$ where

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

or, $\mathcal{M}, v \vDash \forall x A$ if for all $v' \sim_x v : \mathcal{M}, v' \vDash A$.
where $v' \sim_x v$ if 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

Let $h$ map atomic formulae to variable assignments $\mathrm{P}\left(M^{\mathcal{V}}\right)$.

- $h(t_1 = t_2) = \{v : \overline{v}(t_1) = \overline{v}(t_2)\}$
- $h(P(t_1, \ldots, t_k)) = \left\{v : (\overline{v}(t_1), \ldots, \overline{v}(t_n)) \in P^{\mathcal{M}}\right\}$

We extend $h$ to $\overline{h} : \mathrm{wff} \to \mathrm{P}\left(M^{\mathcal{V}}\right)$ by recursion as follows:

1. $\overline{h}(A) = h(A)$ for atomic $A$
2. $\overline{h}(\neg A) = M^{\mathcal{V}} \setminus \overline{h}(A)$
3. $\overline{h}(A \to B) = \left(M^{\mathcal{V}} \setminus \overline{h}(A)\right) \cup \overline{h}(B)$
4. $\overline{h}(\forall x A) = \bigcap_{a \in M} \left\{v : v(a/x) \in \overline{h}(A)\right\}$

$$\mathcal{M}, v \vDash A \;:=\; v \in \overline{h}(A)$$

# Tarski's Definition of Truth

- $\mathcal{M} \vDash A$ if for all $v : \mathcal{M}, v \vDash A$. (True)
- $\mathcal{M}, v \vDash \Gamma$ if for all $A \in \Gamma : \mathcal{M}, v \vDash A$.
- $\mathcal{M} \vDash \Gamma$ if for all $A \in \Gamma : \mathcal{M} \vDash A$.
- $\Gamma \vDash A$ if for all $\mathcal{M}, v : \mathcal{M}, v \vDash \Gamma \implies \mathcal{M}, v \vDash A$.
- $\Gamma \vDash^* A$ if for all $\mathcal{M} : \mathcal{M} \vDash \Gamma \implies \mathcal{M} \vDash A$.
- $\vDash A$ if $\emptyset \vDash A$. (Valid)
- $A$ is satisfiable if there exists $\mathcal{M}, v$ s.t. $\mathcal{M}, v \vDash A$.

$$Px \vDash \forall x Px \quad ?$$

$$Px \vDash^* \forall x Px \quad ?$$

# Example

## Example

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

- $c^{\mathcal{M}}$: green point
- $P^{\mathcal{M}}$: red circles
- $R^{\mathcal{M}}$: arrows

- $\mathcal{M} \overset{?}{\models} Pc$
- $\mathcal{M} \overset{?}{\models} Pc \vee Rcc$
- $\mathcal{M} \overset{?}{\models} \forall x(Px \vee Rxx)$
- $\mathcal{M} \overset{?}{\models} \exists x \forall y(y = x \vee Rxy)$
- $\mathcal{M}, \nu \overset{?}{\models} Rxy \rightarrow Rcy$
  where $\nu(x) = a_1, \nu(y) = a_3$.

# Example

## Example

$$\forall xyz(Rxy \wedge Ryz \rightarrow Rxz)$$

What arrows are missing to make the following a model?

(Add only those arrows that are really needed.)

# Counter Model

## Counter Model

$\forall x \exists y Rxy \nvDash \exists x \forall y Rxy$

$\forall x \exists y Rxy \nvDash \exists y \forall x Rxy$

$\exists y \forall x Rxy \nvDash \forall y \exists x Rxy$

# Is there a finite counter model?

**Exercise (Counter Model)**

*Give a counter model for*

1. $\forall x \exists y Rxy \wedge \forall xyz(Rxy \wedge Ryz \rightarrow Rxz) \nvDash \exists x Rxx$
2. $\forall x \exists y Rxy \wedge \forall xyz(Rxy \wedge Ryz \rightarrow Rxz) \nvDash \exists xy(Rxy \wedge Ryx)$

$$\frac{\begin{array}{c}\text{Everybody loves somebody}\\ \text{Everybody loves all persons who are loved by his loved ones}\end{array}}{\text{There is at least a pair of persons who love each other}}$$

$$(\mathbb{Z}, <)$$

# Mistakes to Avoid

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

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

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

# Coincidence Lemma

**Lemma (Coincidence Lemma)**

*Assume* $v_1, v_2 : \mathcal{V} \to M$*, and for all* $x \in \mathrm{Fv}(A) : v_1(x) = v_2(x)$*. Then*

$$\mathcal{M}, v_1 \vDash A \iff \mathcal{M}, v_2 \vDash A$$

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

# Substitution Lemma

## Lemma (Substitution Lemma)

- $\nu\,(s[t/x]) = \nu(\nu(t)/x)(s)$
- *If the term $t$ is substitutable for the variable $x$ in the wff $A$, then* $\mathcal{M}, \nu \vDash A[t/x] \iff \mathcal{M}, \nu(\nu(t)/x) \vDash A$

$$\begin{tikzcd}
s \arrow[rr, "{[t/x]}"] \arrow[dr, "\overline{\nu(\overline{\nu}(t)/x)}"'] & & s[t/x] \arrow[dl, "\overline{\nu}"] \\
& M &
\end{tikzcd}$$

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

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

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

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

# Equivalent Replacement

**Lemma**

*Suppose $B \in \mathrm{Sub}(A)$, and $A^*$ arises from $A$ by replacing zero or more occurrences of $B$ by $C$. Then*

$$\vDash B \leftrightarrow C \implies \vDash A \leftrightarrow A^*$$

# Alphabetic Variant

## Definition (Alphabetic Variant)

If $y \notin \mathrm{Fv}(A)$, 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*

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

If $y \notin \mathrm{Fv}(A)$, 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 $y_1, \ldots, y_n$ (occurring in $t$), we can always find a logically equivalent alphabetic variant $A^*$ of $A$ s.t. $y_1, \ldots, y_n$ do not occur bound in $A^*$.*

# Equality and Equivalence

## Lemma

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

$$\vDash \forall x_1 \ldots x_n (t = s) \to (A \leftrightarrow A^*)$$

$$\mathcal{M} \vDash t = s \implies \mathcal{M} \vDash A \leftrightarrow A^*$$

## Lemma

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

$$\vDash \forall x_1 \ldots x_n (B \leftrightarrow C) \to (A \leftrightarrow A^*)$$

$$\mathcal{M} \vDash B \leftrightarrow C \implies \mathcal{M} \vDash A \leftrightarrow A^*$$

# Remark

- $\vDash \forall x\big(Px \leftrightarrow Qx\big) \rightarrow \big(\forall xPx \leftrightarrow \forall xQx\big)$
  $\nvDash \big(Px \leftrightarrow Qx\big) \rightarrow \big(\forall xPx \leftrightarrow \forall xQx\big)$
- $\mathcal{M}, v \vDash t = s \;\not\Longrightarrow\; \mathcal{M}, v \vDash A \leftrightarrow A^*$
- $\mathcal{M}, v \vDash B \leftrightarrow C \;\not\Longrightarrow\; \mathcal{M}, v \vDash A \leftrightarrow A^*$

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

# Valid Formulas — Example

$\forall x A \to A[t/x]$

$\neg \forall x A \leftrightarrow \exists x \neg A$

$\forall x (A \wedge B) \leftrightarrow \forall x A \wedge \forall x B$

$\exists x (A \vee B) \leftrightarrow \exists x A \vee \exists x B$

$\forall x (A \to B) \to \forall x A \to \forall x B$

$\forall x y A \leftrightarrow \forall y x A$

$\exists x \forall y A \to \forall y \exists x A$

$\forall x (A \leftrightarrow B) \to (\forall x A \leftrightarrow \forall x B)$

$(\forall x A \to \exists x B) \leftrightarrow \exists x (A \to B)$

$A[t/x] \to \exists x A$

$\neg \exists x A \leftrightarrow \forall x \neg A$

$\forall x A \vee \forall x B \to \forall x (A \vee B)$

$\exists x (A \wedge B) \to \exists x A \wedge \exists x B$

$\forall x (A \to B) \to \exists x A \to \exists x B$

$\exists x y A \leftrightarrow \exists y x A$

# Valid Formulas — Example

$x \notin \mathrm{Fv}(A)$ :

$A \leftrightarrow \forall x A$

$\forall x(A \vee B) \leftrightarrow A \vee \forall x B$

$\forall x(A \wedge B) \leftrightarrow A \wedge \forall x B$

$\forall x(A \rightarrow B) \leftrightarrow (A \rightarrow \forall x B)$

$\forall x(B \rightarrow A) \leftrightarrow (\exists x B \rightarrow A)$

$A \leftrightarrow \exists x A$

$\exists x(A \vee B) \leftrightarrow A \vee \exists x B$

$\exists x(A \wedge B) \leftrightarrow A \wedge \exists x B$

$\exists x(A \rightarrow B) \leftrightarrow (A \rightarrow \exists x B)$

$\exists x(B \rightarrow A) \leftrightarrow (\forall x B \rightarrow A)$

$\exists x(A \rightarrow \forall x A)$

# Example

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

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

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

Assume $\mathcal{M}, \nu \vDash \exists x B$ and $\mathcal{M}, \nu \nvDash A$. Then there exists $a \in M$ s.t. $\mathcal{M}, \nu(a/x) \vDash B$. According to Coincidence Lemma and $x \notin \mathrm{Fv}(A)$, we have $\mathcal{M}, \nu(a/x) \nvDash A$. Therefore $\mathcal{M}, \nu(a/x) \nvDash B \to A$. This contradicts $\mathcal{M}, \nu \vDash \forall x(B \to A)$.

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

$\mathcal{M}, \nu \vDash \exists x B \to A \implies \mathcal{M}, \nu \nvDash \exists x B$ or $\mathcal{M}, \nu \vDash A$.
If $\mathcal{M}, \nu \nvDash \exists x B$, then for all $a \in M$, $\mathcal{M}, \nu(a/x) \nvDash B$. It follows that $\mathcal{M}, \nu(a/x) \vDash B \to A$. Therefore $\mathcal{M}, \nu \vDash \forall x(B \to A)$.
If $\mathcal{M}, \nu \vDash A$, then according to Coincidence Lemma and $x \notin \mathrm{Fv}(A)$, for all $a \in M$, $\mathcal{M}, \nu(a/x) \vDash A$. It follows that $\mathcal{M}, \nu(a/x) \vDash B \to A$.
Therefore $\mathcal{M}, \nu \vDash \forall x(B \to A)$.

$$(\forall x B \to A) \leftrightarrow \exists x (B \to A)$$

$$\operatorname{diam}(X) := \sup \left\{ |x - y| : x, y \in X \right\}$$

$$\big(\forall x \in X \ |x| \leq 1\big) \to \operatorname{diam}(X) \leq 2$$

$$\updownarrow ?$$

$$\exists x \in X \ \big(|x| \leq 1 \to \operatorname{diam}(X) \leq 2\big) ?$$

# Valid Formulas — Example

$$t = t$$

$$t = s \rightarrow s = t$$

$$t = s \rightarrow s = r \rightarrow t = r$$

$$t_1 = s_1 \rightarrow \cdots \rightarrow t_n = s_n \rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, t_n)$$

$$t_1 = s_1 \rightarrow \cdots \rightarrow t_n = s_n \rightarrow \big(P(t_1, \ldots, t_n) \leftrightarrow P(s_1, \ldots, s_n)\big)$$

$$t = s \rightarrow r[t/x] = r[s/x]$$

$$t = s \rightarrow \big(A[t/x] \leftrightarrow A[s/x]\big)$$

# Valid Formulas — Example

$x \notin \mathrm{Fv}(t)$ :

$$\exists x(x = t)$$

$$A[t/x] \leftrightarrow \exists x(x = t \wedge A)$$

$$A[t/x] \leftrightarrow \forall x(x = t \rightarrow A)$$

# Example

$$\boxed{A[t/x] \to \forall x(x = t \to A) \quad \text{where } x \notin \mathrm{Fv}(t)}$$

$\mathcal{M}, v \vDash A[t/x] \implies \mathcal{M}, v(v(t)/x) \vDash A$
Assume $v(t) = b$. Then for all $a \in M$, ether $a = b$ or $a \neq b$.
If $a = b$, then $\mathcal{M}, v(a/x) \vDash A$.
If $a \neq b$, then $v(a/x)(x) = a \neq b = v(t) = v(a/x)(t)$. So $\mathcal{M}, v(a/x) \nvDash x = t$.
Therefore we have $\mathcal{M}, v(a/x) \vDash x = t \to A$ for all $a \in M$.

$$\boxed{\forall x(x = t \to A) \to A[t/x] \quad \text{where } x \notin \mathrm{Fv}(t)}$$

$\mathcal{M}, v \vDash \forall x(x = t \to A) \implies$ for all $a \in M : \mathcal{M}, v(a/x) \vDash x = t \to A$
Let $v(t) = b$. Then $\mathcal{M}, v(b/x) \vDash x = t \to A$.
$v(b/x)(x) = b = v(t) = v(b/x)(t) \implies \mathcal{M}, v(b/x) \vDash x = t$
Therefore $\mathcal{M}, v(b/x) \vDash A$. By Substitution Lemma, $\mathcal{M}, v \vDash A[t/x]$.

# Application — Game

## Theorem (Zermelo's Theorem)

*Every finite game of perfect information with no tie is determined.*

## Proof.

First, color those end nodes black that are wins for player $1$, and color the other end nodes white, being the wins for $2$. 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.

## Proof.

$$\exists x_1 \forall y_1 \ldots \exists x_n \forall y_n A \vee \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \neg A$$

where $A$ states that a final position is reached where player $1$ wins.

# Contents

Introduction

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Formal Systems

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

# Hilbert System = Axiom + Inference Rule

## Axiom Schema

1. $A \to B \to A$
2. $(A \to B \to C) \to (A \to B) \to A \to C$
3. $(\neg A \to \neg B) \to (\neg A \to B) \to A$
4. $\forall x(A \to B) \to \forall x A \to \forall x B$
5. $\forall x A \to A[t/x]$ where $t$ is substitutable for $x$ in $A$.
6. $A \to \forall x A$ where $x \notin \mathrm{Fv}(A)$.
7. $x = x$
8. $x = y \to A \to A'$ where $A$ is atomic and $A'$ is obtained from $A$ by replacing $x$ in zero or more places by $y$.
9. $\forall x_1 \ldots x_n A$ where $n \geq 0$ and $A$ is any axiom of the preceding groups.

## Inference Rule

$$\frac{A \quad A \to B}{B}\ [\mathrm{MP}]$$

# Example

**Theorem**

$$A \vdash \exists x A$$

**Proof.**

| | | |
|---|---|---|
| 1. | $(\forall x \neg A \to \neg A) \to A \to \neg \forall x \neg A$ | Tautology |
| 2. | $\forall x \neg A \to \neg A$ | A5 |
| 3. | $A \to \neg \forall x \neg A$ | 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)

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

## Inference Rule

$$\frac{A}{\forall x A} \text{ [G]}$$

What if we remove Axiom$9$ and add the rule of generalization 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 $\Gamma \vdash A \to B$.*

# Meta-properties

- $\vDash A[B_1/p_1, \ldots, B_n/p_n]$ where $A \in \mathscr{L}^0$, $B_1, \ldots, B_n \in \mathscr{L}^1$. tautology
- $\Gamma, A \vdash B \wedge \neg B \implies \Gamma \vdash \neg A$ reductio ad absurdum
- $\Gamma, \neg A \vdash B \ \& \ \Gamma, \neg A \vdash \neg B \implies \Gamma \vdash A$ proof by contradiction
- $\Gamma, A \vdash \neg B \iff \Gamma, B \vdash \neg A$ contraposition
- $t = s \vdash r[t/x] = r[s/x]$ substitution
- $t = s \vdash A[t/x] \leftrightarrow A[s/x]$ substitution
- $\vdash B \leftrightarrow C \implies \vdash A \leftrightarrow A^*$ where $A^*$ arises from $A$ by replacing one or more occurrences of $B$ in $A$ by $C$. equivalent replacement
- $\vdash \forall x A \iff \vdash \forall y A[y/x]$ alphabetic variant

# Meta-properties

- $\Gamma \vdash A[t/x] \implies \Gamma \vdash \exists x A$ $\qquad \exists R$
- $\Gamma, A[t/x] \vdash B \implies \Gamma, \forall x A \vdash B$ $\qquad \forall L$
- $\Gamma, A \vdash B \ \& \ x \notin \mathrm{Fv}(\Gamma, B) \implies \Gamma, \exists x A \vdash B$ $\qquad \exists L$
- $\Gamma \vdash A \ \& \ x \notin \mathrm{Fv}(\Gamma) \implies \Gamma \vdash \forall x A$ $\qquad \forall R$
- $\Gamma, A[y/x] \vdash B \ \& \ y \notin \mathrm{Fv}(\Gamma, \exists x A, B) \implies \Gamma, \exists x A \vdash B$ $\qquad \exists L$
- $\Gamma \vdash A[y/x] \ \& \ y \notin \mathrm{Fv}(\Gamma, \forall x A) \implies \Gamma \vdash \forall x A$ $\qquad \forall R$
- $\Gamma, A[a/x] \vdash B \ \& \ a \notin \mathrm{Cst}(\Gamma, \exists x A, B) \implies \Gamma, \exists x A \vdash B$ $\qquad \exists L$
- $\Gamma \vdash A[a/x] \ \& \ a \notin \mathrm{Cst}(\Gamma, \forall x A) \implies \Gamma \vdash \forall x A$ $\qquad \forall R$
- $\Gamma \vdash A \ \& \ a \notin \mathrm{Cst}(\Gamma) \ \& \ x \notin \mathrm{Fv}(A) \implies \Gamma \vdash \forall x A[x/a]$

# Alphabetic Variant

**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. $A \vdash\dashv A^*$
2. *$t$ is substitutable for $x$ in $A^*$.*

# Strategy

$\rightarrow$ • $\Gamma \vdash A \rightarrow B \iff \Gamma, A \vdash B$

$\forall$ 1. if $x \notin \mathrm{Fv}(\Gamma)$, $\Gamma \vdash \forall x A \iff \Gamma \vdash A$

2. if $x \in \mathrm{Fv}(\Gamma)$,
$\Gamma \vdash \forall x A \iff \Gamma \vdash \forall y A[y/x] \iff \Gamma \vdash A[y/x]$ for some new $y$.

$\neg$ 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...

# Tree Method for Propositional Logic

$$\begin{array}{c} \neg\neg A \\ | \\ A \end{array} \qquad \begin{array}{c} A \to B \\ \diagup \quad \diagdown \\ \neg A \qquad B \end{array} \qquad \begin{array}{c} \neg(A \to B) \\ | \\ A \\ \neg B \end{array}$$

---

$$\begin{array}{c} A \wedge B \\ | \\ A \\ B \end{array} \qquad \begin{array}{c} \neg(A \wedge B) \\ \diagup \quad \diagdown \\ \neg A \qquad \neg B \end{array} \qquad \begin{array}{c} A \vee B \\ \diagup \quad \diagdown \\ A \qquad B \end{array} \qquad \begin{array}{c} \neg(A \vee B) \\ | \\ \neg A \\ \neg B \end{array}$$

---

$$\begin{array}{c} A \leftrightarrow B \\ \diagup \quad \diagdown \\ \begin{array}{c} A \\ B \end{array} \qquad \begin{array}{c} \neg A \\ \neg B \end{array} \end{array} \qquad \begin{array}{c} \neg(A \leftrightarrow B) \\ \diagup \quad \diagdown \\ \begin{array}{c} A \\ \neg B \end{array} \qquad \begin{array}{c} \neg A \\ B \end{array} \end{array}$$

✓

# Tree Method for Predicate Logic I

Ground Tree:

$$\begin{array}{c} \forall x A \\ | \\ A[t/x] \end{array}$$

where $t$ is a ground term.

$$\begin{array}{c} \exists x A \checkmark \\ | \\ A(a) \end{array}$$

where $a$ is a new constant.

---

$$\begin{array}{c} \neg\forall x A \checkmark \\ | \\ \exists x \neg A \end{array}$$

$$\begin{array}{c} \neg\exists x A \checkmark \\ | \\ \forall x \neg A \end{array}$$

# Tree Method for Predicate Logic II

Tree Method with Unification:

$$\begin{array}{c} \forall x A \checkmark \\ | \\ A[x_i/x] \end{array}$$

where $x_i$ is a new variable.

$$\begin{array}{c} \exists x A \checkmark \\ | \\ A[f(x_1, \ldots, x_m)/x] \end{array}$$

where $f$ is a new function and $\{x_1, \ldots, x_m\} = \mathrm{Fv}(\exists x A)$.

---

$$\begin{array}{c} \neg\forall x A \checkmark \\ | \\ \exists x \neg A \end{array}$$

$$\begin{array}{c} \neg\exists x A \checkmark \\ | \\ \forall x \neg A \end{array}$$

# 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 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 $\sigma$ is a *unifier* for a set $\Gamma$ of formulae if for every $A, B \in \Gamma : A\sigma = B\sigma$.
- A unifier $\sigma$ is a *most general unifier* for $\Gamma$ if for each unifier $\theta$ there exists a substitution $\lambda$ s.t. $\theta = \sigma\lambda$.

$$\sigma := \{t_1/x_1, \ldots, t_m/x_m\} \qquad \lambda := \{s_1/y_1, \ldots, s_n/y_n\}$$

$$\sigma\lambda = \left\{t_1\lambda/x_1, \ldots, t_m\lambda/x_m,\ s_1/y_1, \ldots, s_n/y_n\right\} \setminus \left\{s_i/y_i : y_i \in \{x_1, \ldots, x_m\}\right\}$$

- $(A\sigma)\lambda = A(\sigma\lambda)$ and $(t\sigma)\lambda = t(\sigma\lambda)$
- $(\sigma\lambda)\theta = \sigma(\lambda\theta)$

# Tree Method for Predicate Logic

$$\begin{array}{c} A(x) \\ x = y \\ | \\ A(y) \end{array} \qquad\qquad \begin{array}{c} A(x) \\ y = x \\ | \\ A(y) \end{array}$$

where $A(y)$ arises from the wff $A(x)$ by replacing one or more occurrences of $x$ by $y$.

# Deduction & Tactics

## Definition (Deduction)

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

- 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.

# Example — Ground Tree

$\boxed{\{\forall x \neg P(x), \exists x(P(x) \vee P(f(x)))\} \text{ is unsatisfiable.}}$

$$\forall x \neg P(x)$$
$$\exists x(P(x) \vee P(f(x))) \checkmark$$

$$P(a) \vee P(f(a)) \checkmark$$

$$P(a) \qquad\qquad P(f(a))$$

$$\neg P(a) \qquad\qquad \neg P(f(a))$$

$$\times \qquad\qquad \times$$

# Example — Tree Method with Unification

$\boxed{\{\forall x P(x), \neg Q(f(a)), \forall x(\neg P(f(x)) \vee Q(x))\} \text{ is unsatisfiable.}}$

$$\forall x P(x) \checkmark$$
$$\neg Q(f(a))$$
$$\forall x(\neg P(f(x)) \vee Q(x)) \checkmark$$
$$P(x_1)$$
$$\neg P(f(x_2)) \vee Q(x_2) \checkmark$$

| $\neg P(f(x_2))$ | $Q(x_2)$ |
|---|---|
| $x_1 = f(x_2)$ | $x_2 = f(a)$ |
| $\times$ | $\times$ |

# Unification — Greedy Unification (incomplete)

$$\neg P(a) \checkmark$$
$$\neg Q(c) \checkmark$$
$$\neg R(d) \checkmark$$
$$\forall x(((R(d) \vee \neg P(b)) \wedge P(x)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x))) \checkmark$$
$$((R(d) \vee \neg P(b)) \wedge P(x_1)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x_1)) \checkmark$$

$$(R(d) \vee \neg P(b)) \wedge P(x_1) \checkmark$$
$$R(d) \vee \neg P(b)$$
$$P(x_1)$$
$$x_1 = a$$
$$\times$$

$$(R(d) \vee \neg Q(b)) \wedge Q(a) \checkmark$$
$$R(d) \vee \neg Q(b) \checkmark$$
$$Q(a)$$

$$R(d)$$
$$\times$$

$$\neg Q(b)$$

Applying unification as soon as a branch can be closed by lead to incompleteness.

# Unification — Final Closure

$\neg P(a)$ ✓

$\neg Q(c)$ ✓

$\neg R(d)$ ✓

$\forall x(((R(d) \vee \neg P(b)) \wedge P(x)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x)))$ ✓

$((R(d) \vee \neg P(b)) \wedge P(x_1)) \vee ((R(d) \vee \neg Q(b)) \wedge Q(x_1))$ ✓

$(R(d) \vee \neg P(b)) \wedge P(x_1)$ ✓

$R(d) \vee \neg P(b)$ ✓

$P(x_1)$

$R(d)$

×

$\neg P(b)$

$x_1 = b$

×

$(R(d) \vee \neg Q(b)) \wedge Q(x_1)$ ✓

$R(d) \vee \neg Q(b)$ ✓

$Q(x_1)$

$R(d)$

×

$\neg Q(b)$

$x_1 = b$

×

Unification is applied only when it closes all open branches at the same time.

# Example — Unification vs Ground

There is someone such that if he is drinking, then everyone is drinking.

$$\boxed{\vdash \exists x\big(A(x) \to \forall x A(x)\big)}$$

$$\neg\exists x(A(x) \to \forall x A(x)) \checkmark$$

$$\forall x \neg(A(x) \to \forall x A(x)) \checkmark$$

$$\neg(A(x_1) \to \forall x A(x)) \checkmark$$

$$A(x_1)$$

$$\neg\forall x A(x) \checkmark$$

$$\neg A(a)$$

$$x_1 = a$$

$$\times$$

$$\forall x \neg(A(x) \to \forall x A(x))$$

$$\neg(A(a) \to \forall x A(x)) \checkmark$$

$$A(a)$$

$$\neg\forall x A(x) \checkmark$$

$$\neg A(b)$$

$$\neg(A(b) \to \forall x A(x)) \checkmark$$

$$A(b)$$

$$\neg\forall x A(x)$$

$$\times$$

# 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.*

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

**Remark:** If an inference with predicate wff 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.

# Exercises — Tree Method

1. $\forall x(Px \to Qx) \to \exists x Px \to \exists x Qx$
2. $\exists x \forall y Rxy \to \forall y \exists x Rxy$
3. $\exists x(Px \wedge Qx) \to \exists x Px \wedge \exists x Qx$
4. $\forall x\big(A \vee B(x)\big) \to A \vee \forall x B(x)$ where $x \notin \mathrm{Fv}(A)$
5. $\exists x\Big(\big(Px \wedge \forall y(Py \to y = x)\big) \wedge Qx\Big) \vdash\!\dashv \exists x \forall y\Big(\big(Py \leftrightarrow y = x\big) \wedge Qx\Big)$
6. $\exists x\big(Px \wedge \forall y(Py \to y = x)\big) \wedge \exists x\big(Qx \wedge \forall y(Qy \to y = x)\big) \wedge \neg\exists x(Px \wedge Qx) \to$
   $\exists xy\big(x \neq y \wedge (Px \vee Qx) \wedge (Py \vee Qy) \wedge \forall z(Pz \vee Qz \to z = x \vee z = y)\big)$

$*\mathbf{54} \cdot \mathbf{43}.\ \vdash :. \alpha, \beta \in 1. \supset : \alpha \cap \beta = \Lambda. \equiv .\alpha \cup \beta \in 2$

*Dem.*

$$
\begin{aligned}
&\vdash .*54 \cdot 26. \supset \vdash :. \alpha = \iota' x . \beta = \iota' y. \supset : \alpha \cup \beta \in 2. \equiv .x \neq y. \\
&[*51 \cdot 231] \qquad \equiv .\iota' x \cap \iota' y = \Lambda. \\
&[*13 \cdot 12] \qquad \equiv .\alpha \cap \beta = \Lambda \qquad (1) \\
&\vdash .(1). *11 \cdot 11 \cdot 35. \supset \\
&\qquad \vdash :. (\exists x, y). \alpha = \iota' x . \beta = \iota' y. \supset : \alpha \cup \beta \in 2. \equiv .\alpha \cap \beta = \Lambda \qquad (2) \\
&\vdash .(2). *11 \cdot 54. *52 \cdot 1. \supset \vdash .Prop
\end{aligned}
$$

From this proposition it will follow, when arithmetical addition has been defined, that $\mathbf{1} + \mathbf{1} = \mathbf{2}$.

# 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.

Kant: Mathematics is synthetic a priori.
Frege: Mathematics is analytic.

# Frege

- Arithmetic laws are analytic judgments, 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 |
|---|---|---|
| $\frac{\text{Mathematics}}{\text{Logic}}$ | $\frac{\frac{\text{Logic}}{\text{Mathematics}}}{\text{Mind}}$ | $\frac{\text{Mathematics}}{\text{Game}}$ |
| Realism | Conceptualism | Nominalism |

# 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?

# Exercises — Tree Method

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. 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.
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!

# Exercises — Tree Method

1. 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.
2. Any philosopher admires some logician. Some students admire *only* film stars. No film stars are logicians. Therefore not all students are philosophers.
3. 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.
4. Whoever stole the goods, knew the safe combination. Someone stole the goods, and *only* Jack knew the safe combination. Hence Jack stole the goods.
5. *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.
  $\forall x(\mathrm{contain}(x, 1) \rightarrow$
  $\exists y(\mathrm{adj}(x, y) \wedge \mathrm{mine}(y) \wedge \forall z(\mathrm{adj}(x, z) \wedge \mathrm{mine}(z) \rightarrow z = y)))$
- ...

# 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 round square is round."

# Russell's Theory of Descriptions

$$B(\iota_x A) := \exists! x A \wedge \exists x (A \wedge B)$$

$$\vDash \exists x \forall y \Big( \big( A(y) \leftrightarrow y = x \big) \wedge B(x) \Big)$$

The round square does not exist. $B(\iota_x A) \vee (\neg B)(\iota_x A)$ ?

$$\exists x \forall y \Big( \big( Ry \wedge Sy \leftrightarrow y = x \big) \wedge \neg Ex \Big) \quad (\neg B)(\iota_x A) \ ?$$

$$\neg \exists x \forall y \Big( \big( Ry \wedge Sy \leftrightarrow y = x \big) \wedge Ex \Big) \quad \neg B(\iota_x A) \ ?$$

$$Ex \overset{?}{:=} \exists P \big( Px \wedge \exists y \neg Py \big)$$

$$\iota_x A = \iota_x A \ ? \qquad \forall x B \to B(\iota_x A) \ ?$$

$$B(\iota_x^y A) := \big( \exists! x A \to \exists x (A \wedge B) \big) \wedge \big( \neg \exists! x A \to B[y/x] \big)$$

$$\vdash \forall x B \to B(\iota_x^y A)$$

# Russell's Theory of Descriptions & Church's $\lambda$-Abstraction

$$v(\iota_x A) = \begin{cases} a & \text{if there is a unique } a \in M : \mathcal{M}, v(a/x) \vDash A \\ \uparrow & \text{otherwise} \end{cases}$$

$$\begin{cases} \mathcal{M}, v \vDash (\lambda x.A)t \iff \mathcal{M}, v \vDash A[t/x] & \text{if } v(t)\downarrow \\ \mathcal{M}, v \nvDash (\lambda x.A)t & \text{if } v(t)\uparrow \end{cases}$$

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.

$$\mathbf{D}(\lambda x(Cx \wedge \neg Lx))$$

# Hilbert's Epsilon Calculus

$$\nu(\varepsilon_x A) = \Phi\left(\{a \in M : \mathcal{M}, \nu(a/x) \vDash A\}\right)$$

where $\Phi : \mathrm{P}(M) \to M :: \Phi(X) \in X$ whenever $X \neq \emptyset$ and $\Phi(\emptyset) \in M$.

## Axiom $\varepsilon$

$$A(t) \to A(\varepsilon_x A)$$

where $t$ is an arbitrary term.

## $\varepsilon$-Extensionality Axiom

$$\forall x(A(x) \leftrightarrow B(x)) \to \varepsilon_x A = \varepsilon_x B$$

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 $\varepsilon$-theorem: Suppose $A$ is a quantifier-free and $\varepsilon$-free wff. Then $\vdash_\varepsilon A \implies \vdash_{\mathrm{QF}} A$ in quantifier-free predicate logic.
- Extended first $\varepsilon$-theorem: Suppose $\exists x_1 \ldots \exists x_n A(x_1, \ldots, x_n)$ is a purely existential formula containing only the bound variables $x_1, \ldots, x_n$. Then $\vdash_\varepsilon \exists x_1 \ldots \exists x_n A(x_1, \ldots, x_n) \implies \vdash \bigvee_i A(t_{i1}, \ldots, t_{in})$ for some terms $t_{ij}$.
- Second $\varepsilon$-theorem: Suppose $A$ is an $\varepsilon$-free wff. Then $\vdash_\varepsilon A \implies \vdash A$.

Herbrand's Theorem is a corollary of the extended first $\varepsilon$-theorem.

- 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: $2^{\text{nd}}$ crisis of the Foundations of Mathematics
For $f(x) = x^2$,

$$\frac{\mathrm{d}f(x)}{\mathrm{d}x} = \frac{f(x+\mathrm{d}x) - f(x)}{\mathrm{d}x} = \frac{(x+\mathrm{d}x)^2 - x^2}{\mathrm{d}x} = \frac{2x\mathrm{d}x + (\mathrm{d}x)^2}{\mathrm{d}x} = 2x + \mathrm{d}x = 2x$$

$\frac{\mathrm{d}}{\mathrm{d}x}$ should be explained as a whole.

$$\frac{\mathrm{d}f(x)}{\mathrm{d}x} = \frac{\mathrm{d}}{\mathrm{d}x}f(x) = \lim_{\Delta x \to 0} \frac{f(x+\Delta x) - f(x)}{\Delta x}$$

# 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.
- If all you have is a hammer, everything looks like a nail.
- 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.

# Expressive Limitation of First Order Language

- Most boys are funny.
- Some critics admire only one another.

$$\exists X\Big(\exists x Xx \wedge \forall x(Xx \to Cx) \wedge \forall xy\big(Xx \wedge A(x,y) \to Xy \wedge x \neq y\big)\Big)$$

- There are some gunslingers each of whom has shot the right foot of at least one of the others.

$$\exists X\Big(\exists x Xx \wedge \forall x(Xx \to Gx) \wedge \forall x\big(Xx \to \exists y(Xy \wedge y \neq x \wedge Sxy)\big)\Big)$$

- Least Number Principle.

$$\forall X\Big(\exists x Xx \wedge \forall x(Xx \to Nx) \to \exists x\big(Xx \wedge \forall y(Xy \wedge y \neq x \to x < y)\big)\Big)$$

- A linear order $(P, <)$ is *complete* if every non-empty subset of $P$ that is bounded above has a supremum in $P$.

$$\forall X\Big(\exists x Xx \wedge \exists y \forall x(Xx \to x \leq y) \to \exists y\Big(\forall x(Xx \to x \leq y) \wedge \forall z\big(\forall x(Xx \to x \leq z) \to y \leq z\big)\Big)\Big)$$

# Gentzen

Figure: Gentzen 1909-1945

- Natural Deduction: one proposition on the right.
- Sequent Calculus: zero or more propositions on the right.

$$\Gamma \vdash \Delta \iff \vdash \bigwedge \Gamma \to \bigvee \Delta$$

- Consistency of $\mathrm{PA}$ (proof-theoretical strength of $\mathrm{PA}$)

# Natural Deduction

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

---

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

---

$$\frac{\begin{array}{c}[A]^n\\ \vdots \\ B\end{array}}{A \to B}\,[\to^+]^n \qquad \frac{A \to B \quad A}{B}\,[\to^-]$$

---

$$\frac{\begin{array}{c}[A]^n\\ \vdots \\ \bot\end{array}}{\neg A}\,[\neg^+]^n \qquad \frac{\neg\neg A}{A}\,[\neg^-] \qquad \frac{\neg A \quad A}{\bot}\,[\bot^+] \qquad \frac{\bot}{A}\,[\bot^-]$$

# Natural Deduction

$$\frac{A(a)}{\forall x A}\ [\forall^+] \qquad\qquad \frac{\forall x A}{A(t)}\ [\forall^-]$$

where $a \notin \mathrm{Cst}(\forall x A)$, and $a$ is not in any assumption which is undischarged in the derivation ending with $A(a)$.

---

$$\frac{A(t)}{\exists x A}\ [\exists^+] \qquad\qquad \frac{\exists x A \qquad \begin{array}{c}[A(a)]^n \\ \vdots \\ B\end{array}}{B}\ [\exists^-]^n$$

where $a \notin \mathrm{Cst}(\exists x A, B)$, and $a$ is not in any assumption which is undischarged in the derivations ending with $\exists x A, B$ except in $A(a)$.

---

$$\frac{}{t = t}\ [=^+] \qquad\qquad \frac{s = t \quad A(s)}{A(t)}\ [=^-]$$

# Natural Deduction — another version

$$\frac{A \in \Gamma}{\Gamma \vdash A}\,[\mathsf{I}] \qquad \frac{\Gamma \vdash A \qquad \Gamma \subset \Gamma'}{\Gamma' \vdash A}\,[\mathsf{M}]$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,[\wedge^+] \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,[\wedge^-] \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,[\wedge^-]$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,[\vee^+] \qquad \frac{\Gamma \vdash A}{\Gamma \vdash B \vee A}\,[\vee^+] \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,[\vee^-]$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,[\to^+] \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,[\to^-]$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,[\neg^+] \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\,[\neg^-] \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,[\bot^+] \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,[\bot^-]$$

# Natural Deduction — another version

$$\frac{\Gamma \vdash A(a) \qquad a \notin \mathrm{Cst}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A}\,[\forall^+] \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A(t)}\,[\forall^-]$$

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A}\,[\exists^+] \qquad \frac{\Gamma \vdash \exists x A \qquad \Gamma, A(a) \vdash B \qquad a \notin \mathrm{Cst}(\Gamma, \exists x A, B)}{\Gamma \vdash B}\,[\exists^-]$$

$$\frac{}{\Gamma \vdash t = t}\,[=^+] \qquad \frac{\Gamma \vdash s = t \qquad \Gamma \vdash A(s)}{\Gamma \vdash A(t)}\,[=^-]$$

# Example

## Theorem (Proof by Contradiction)

$$\neg A \to \bot \vdash A$$

## Proof.

$$\dfrac{\dfrac{\dfrac{\neg A \to \bot \quad [\neg A]^1}{\bot}\,[\to^-]}{\neg\neg A}\,[\neg^+]^1}{A}\,[\neg^-]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A \to \bot, \neg A \vdash \neg A \to \bot}\,[\mathsf{I}] \qquad \dfrac{}{\neg A \to \bot, \neg A \vdash \neg A}\,[\mathsf{I}]}{\neg A \to \bot, \neg A \vdash \bot}\,[\to^-]}{\neg A \to \bot \vdash \neg\neg A}\,[\neg^+]}{\neg A \to \bot \vdash A}\,[\neg^-]$$

# Example

$$\boxed{\text{If } x \notin \mathrm{Fv}(A), \text{ then } \vdash \forall x(A \to B(x)) \to A \to \forall x B(x).}$$

**Proof.**

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x(A \to B(x))]^2}{A \to B(a)}\,[\forall^-] \qquad [A]^1}{B(a)}\,[\to^-]}{\forall x B(x)}\,[\forall^+]}{A \to \forall x B(x)}\,[\to^+]^1}{\forall x(A \to B(x)) \to A \to \forall x B(x)}\,[\to^+]^2$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(A \to B(x)) \vdash \forall x(A \to B(x))}\,[\mathrm{I}]}{\forall x(A \to B(x)) \vdash A \to B(a)}\,[\forall^-]}{\forall x(A \to B(x)), A \vdash B(a)}\,[\to^-]}{\forall x(A \to B(x)), A \vdash \forall x B(x)}\,[\forall^+]}{\dfrac{\forall x(A \to B(x)) \vdash A \to \forall x B(x)}{\vdash \forall x(A \to B(x)) \to A \to \forall x B(x)}\,[\to^+]}\,[\to^+]$$

# Sequent Calculus

Axiom

$$\frac{}{A \vdash A}\ [\mathrm{I}]$$

Cut

$$\frac{\Gamma \vdash \Delta, A \qquad \Sigma, A \vdash \Theta}{\Gamma, \Sigma \vdash \Delta, \Theta}\ [\mathrm{Cut}]$$

Left structural rules

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ [\mathrm{WL}]$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ [\mathrm{CL}]$$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}\ [\mathrm{PL}]$$

Right structural rules

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ [\mathrm{WR}]$$

$$\frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ [\mathrm{CR}]$$

$$\frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2}\ [\mathrm{PR}]$$

# Sequent Calculus

Left logical rules:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ [\wedge L_1]$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ [\wedge L_2]$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \vee B \vdash \Delta, \Theta}\ [\vee L]$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Sigma, B \vdash \Theta}{\Gamma, \Sigma, A \rightarrow B \vdash \Delta, \Theta}\ [\rightarrow L]$$

Right logical rules:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta}\ [\vee R_1]$$

$$\frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ [\vee R_2]$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Sigma \vdash B, \Theta}{\Gamma, \Sigma \vdash A \wedge B, \Delta, \Theta}\ [\wedge R]$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta}\ [\rightarrow R]$$

# Sequent Calculus

Left logical rules: Right logical rules:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\,[\neg L] \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\,[\neg R]$$

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\,[\forall L] \qquad \frac{\Gamma \vdash A(a), \Delta \qquad a \notin \mathrm{Cst}(\Gamma, \Delta, \forall x A)}{\Gamma \vdash \forall x A, \Delta}\,[\forall R]$$

$$\frac{\Gamma, A(a) \vdash \Delta \qquad a \notin \mathrm{Cst}(\Gamma, \Delta, \exists x A)}{\Gamma, \exists x A \vdash \Delta}\,[\exists L] \qquad \frac{\Gamma \vdash A(t), \Delta}{\Gamma \vdash \exists x A, \Delta}\,[\exists R]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,[\mathrm{I}]}{\vdash \neg A, A}\,[\neg R]}{\vdash \neg A \vee A, A}\,[\vee R_2]}{\vdash A, A \vee \neg A}\,[PR]}{\vdash A \vee \neg A, A \vee \neg A}\,[\vee R_1]}{\vdash A \vee \neg A}\,[CR]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,[\mathrm{I}]}{A \vdash B, A}\,[WR]}{A, \neg A \vdash B}\,[\neg L] \qquad \dfrac{\dfrac{}{B \vdash B}\,[\mathrm{I}]}{A, B \vdash B}\,[WL]}{A, \neg A \vee B \vdash B}\,[\vee L]}{\neg A \vee B \vdash A \to B}\,[\to R]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A(a) \vdash A(a)}\,[\mathrm{I}]}{\forall x A(x) \vdash A(a)}\,[\forall L]}{\forall x A(x), \neg A(a) \vdash}\,[\neg L]}{\neg A(a) \vdash \neg \forall x A(x)}\,[\neg R]}{\exists x \neg A(x) \vdash \neg \forall x A(x)}\,[\exists L]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,[\mathrm{I}]}{A \wedge B \vdash A}\,[\wedge L_1]}{A \wedge B, \neg A \vdash}\,[\neg L] \qquad \dfrac{\dfrac{}{B \vdash B}\,[\mathrm{I}]}{A \wedge B \vdash B}\,[\wedge L_2]}{A \wedge B, \neg B \vdash}\,[\neg L]}{A \wedge B, \neg A \vee \neg B \vdash}\,[\vee L]}{\neg A \vee \neg B \vdash \neg(A \wedge B)}\,[\neg R]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A(a,b) \vdash A(a,b)}\,[\mathrm{I}]}{\forall x A(x,b) \vdash A(a,b)}\,[\forall L]}{\forall x A(x,b) \vdash \exists y A(a,y)}\,[\exists R]}{\exists y \forall x A(x,y) \vdash \exists y A(a,y)}\,[\exists L]}{\exists y \forall x A(x,y) \vdash \forall x \exists y A(x,y)}\,[\forall R]$$

# Natural Deduction — constant vs variable

$$\frac{\Gamma \vdash A(a) \qquad a \notin \mathrm{Cst}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A}\ [\forall^+]$$

$$\frac{\Gamma \vdash A[y/x] \qquad y \notin \mathrm{Fv}(\Gamma, \forall x A)}{\Gamma \vdash \forall x A}\ [\forall^+]$$

$$\frac{\Gamma \vdash \exists x A \qquad \Gamma, A(a) \vdash B \qquad a \notin \mathrm{Cst}(\Gamma, \exists x A, B)}{\Gamma \vdash B}\ [\exists^-]$$

$$\frac{\Gamma \vdash \exists x A \qquad \Gamma, A[y/x] \vdash B \qquad y \notin \mathrm{Fv}(\Gamma, \exists x A, B)}{\Gamma \vdash B}\ [\exists^-]$$

# Natural Deduction — another version — constant vs variable

$$\frac{A(a)}{\forall x A}\ [\forall^+] \qquad\qquad \frac{A[y/x]}{\forall x A}\ [\forall^+]$$

where $a \notin \mathrm{Cst}(\forall x A)$, and $a$ is not in any assumption which is undischarged in the derivation ending with $A(a)$.

where $y \notin \mathrm{Fv}(\forall x A)$, and $y$ is not free in any assumption which is undischarged in the derivation ending with $A[y/x]$.

---

$$\frac{\exists x A \qquad \begin{array}{c}[A(a)]^n\\ \vdots \\ B\end{array}}{B}\ [\exists^-]^n \qquad\qquad \frac{\exists x A \qquad \begin{array}{c}[A[y/x]]^n\\ \vdots \\ B\end{array}}{B}\ [\exists^-]^n$$

where $a \notin \mathrm{Cst}(\exists x A, B)$, and $a$ is not in any assumption which is undischarged in the derivations ending with $\exists x A, B$ except in $A(a)$.

where $y \notin \mathrm{Fv}(\exists x A, B)$, 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

$$\frac{\Gamma \vdash A(a), \Delta \qquad a \notin \mathrm{Cst}(\Gamma, \Delta, \forall x A)}{\Gamma \vdash \forall x A, \Delta}\ [\forall R]$$

$$\frac{\Gamma \vdash A[y/x], \Delta \qquad y \notin \mathrm{Fv}(\Gamma, \Delta, \forall x A)}{\Gamma \vdash \forall x A, \Delta}\ [\forall R]$$

$$\frac{\Gamma, A(a) \vdash \Delta \qquad a \notin \mathrm{Cst}(\Gamma, \Delta, \exists x A)}{\Gamma, \exists x A \vdash \Delta}\ [\exists L]$$

$$\frac{\Gamma, A[y/x] \vdash \Delta \qquad y \notin \mathrm{Fv}(\Gamma, \Delta, \exists x A)}{\Gamma, \exists x A \vdash \Delta}\ [\exists L]$$

# 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 formulae are subformulae of $\Gamma$ and $\Delta$.*

**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 $\Theta$ be a set of sentences. If $\Theta$ 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

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 $(X \in \mathrm{Def}(\mathcal{M}, Y))$ over $\mathcal{M}$ if there is a wff $A$ and $b_1, \ldots, b_m \in Y^m$ s.t.

$$X = \left\{(a_1, \ldots, a_n) : \mathcal{M} \vDash A[a_1, \ldots, a_n, b_1, \ldots, b_m]\right\}$$

- $X$ is definable in $\mathcal{M}$ if 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 $f : \mathbb{N}^n \to \mathbb{N}$ is representable in the theory $\mathrm{T}$ iff there is a wff $A(x_1, \ldots, x_n, y)$ s.t. for all $a_1, \ldots, a_n$,

$$\mathrm{T} \vdash \forall y \Big( A(\underline{a_1}, \ldots, \underline{a_n}, y) \leftrightarrow y = \underline{f(a_1, \ldots, a_n)} \Big)$$

## Definition (Representable Relations)

A $n$-ary relation $R \subset \mathbb{N}^n$ is representable in the theory $\mathrm{T}$ iff there is a wff $A$ s.t. for all $a_1, \ldots, a_n$,

$$(a_1, \ldots, a_n) \in R \implies \mathrm{T} \vdash A[a_1, \ldots, a_n]$$
$$(a_1, \ldots, a_n) \notin R \implies \mathrm{T} \vdash \neg A[a_1, \ldots, a_n]$$

A function/relation is representable in Robinson $\mathrm{Q}$ iff it is computable.

# Example

- The interval $[0, \infty)$ is definable in $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$, where the language is $\mathscr{L} = \{0, 1, +, \cdot\}$.

$$\mathcal{R} \vDash \exists y(x = y \cdot y)[a] \iff a \geq 0$$

- The ordering relation $<$ is definable in $\mathcal{N} = (\mathbb{N}, 0, S, +, \cdot)$, where the language is $\mathscr{L} = \{0, S, +, \cdot\}$.

$$\exists z\big(x + S(z) = y\big)$$

- The set of primes is definable in $\mathcal{N}$ by the formula

$$\exists y\big(x = S(0) + S(y)\big) \wedge \forall yz\big(x = y \cdot z \to y = S(0) \vee z = S(0)\big)$$

- $\mathbb{N}$ is definable in $(\mathbb{Z}, +, \cdot)$ by

$$\exists y_1 y_2 y_3 y_4 \Big(x = y_1^2 + y_2^2 + y_3^2 + y_4^2\Big) \quad \text{(Lagrange four-square theorem)}$$

- Exponentiation $\big\{(m, n, p) : p = m^n\big\}$ is definable in $\mathcal{N}$. (use the Chinese remainder theorem)

# Homomorphism & Isomorphism

## Definition (Homomorphism)

A homomorphism $h$ of $\mathcal{M}$ into $\mathcal{N}$ is a function $h : M \to N$ s.t.

- For each $n$-place predicate symbol $P$ and each $n$-tuple $(a_1, \ldots, a_n) \in M^n$,
$$(a_1, \ldots, a_n) \in P^{\mathcal{M}} \iff (h(a_1), \ldots, h(a_n)) \in P^{\mathcal{N}}$$
- For each $n$-place function symbol $f$ and each $n$-tuple $(a_1, \ldots, a_n) \in M^n$,
$$h : f^{\mathcal{M}}(a_1, \ldots, a_n) \mapsto f^{\mathcal{N}}\big(h(a_1), \ldots, h(a_n)\big)$$
In the case of a constant symbol $c$ this becomes $h : c^{\mathcal{M}} \mapsto c^{\mathcal{N}}$.

- 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 if 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 $v : \mathcal{V} \to M$.*

1. *For any term $t$, $h(\overline{v}(t)) = \overline{h \circ v}(t)$*
2. *For any open formula $A$ not containing $=$, $\mathcal{M}, v \vDash A \iff \mathcal{N}, h \circ v \vDash A$*
3. *If $h : M \rightarrowtail N$, we may delete the restriction "not containing $=$".*
4. *If $h : M \twoheadrightarrow N$, we may delete the restriction "open".*

## Definition (Elementary Equivalence)

$$\mathcal{M} \equiv \mathcal{N} \text{ if for any sentence } A : \mathcal{M} \vDash A \iff \mathcal{N} \vDash A$$

$$\mathcal{M} \cong \mathcal{N} \implies \mathcal{M} \equiv \mathcal{N}$$

## Theorem

$\mathcal{M} \equiv \mathcal{N} \ \ \& \ \ |M| < \infty \implies \mathcal{M} \cong \mathcal{N}$

## Proof.

Suppose $|M| = n$. Then $|N| = n$.
There are only finitely many functions $f_1, \ldots, f_m : M \to N$. Assume none of $f : M \to N$ is an isomorphism. For each $f_i, 1 \leq i \leq m$, there is a formula $A_i$ s.t. $\mathcal{M} \vDash A_i(a_1, \ldots, a_n)$ but $\mathcal{N} \nvDash A_i(f_i(a_1), \ldots, f_i(a_n))$. Then we have

$$\mathcal{M} \vDash \bigwedge_{i=1}^{m} A_i(a_1, \ldots, a_n) \quad \& \quad \mathcal{M} \vDash \exists x_1 \ldots x_n \bigwedge_{i=1}^{m} A_i(x_1, \ldots, x_n)$$

Since $\mathcal{M} \equiv \mathcal{N}$, then $\mathcal{N} \vDash \exists x_1 \ldots x_n \bigwedge_{i=1}^{m} A_i(x_1, \ldots, x_n)$, and
$\mathcal{N} \vDash \bigwedge_{i=1}^{m} A_i(b_1, \ldots, b_n)$ for some $b_1, \ldots, b_n \in N$.
Let $f_j : a_i \mapsto b_i$. But $\mathcal{N} \nvDash A_j(b_1, \ldots, b_n)$.

# 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. $f^{\mathcal{M}} = f^{\mathcal{N}} \restriction_{M^n}$ for any $n$-ary function symbol $f$.

Suppose $\mathcal{M} \subset \mathcal{N}$. Then

- for any term $t(x_1, \ldots, x_n)$, and any $a_1, \ldots, a_n \in M$,

$$t^{\mathcal{M}}[a_1, \ldots, a_n] = t^{\mathcal{N}}[a_1, \ldots, a_n]$$

- for any open formula $A(x_1, \ldots, x_n)$, and any $a_1, \ldots, a_n \in M$,

$$\mathcal{M} \vDash A[a_1, \ldots, a_n] \iff \mathcal{N} \vDash A[a_1, \ldots, a_n]$$

# Example

- $\mathscr{L} = \{0, 1, +, \cdot\}, \mathcal{N} = (\mathbb{N}, 0, 1, +, \cdot), \mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$

$$\mathcal{N} \subset \mathcal{R}$$

- $\mathscr{L} = \{<\}, \mathcal{M} = (\mathbb{N}, <), \mathcal{N} = (\{2n : n \in \mathbb{N}\}, <)$

$$h : n \mapsto 2n, \quad h : \mathcal{M} \cong \mathcal{N}, \quad \text{but} \quad \mathcal{M} \not\subset \mathcal{N}$$

- $\mathscr{L} = \{0, +\}$

$$\begin{aligned} \mathcal{M} &= (\mathbb{N}, 0^{\mathcal{M}}, +^{\mathcal{M}}), && \text{where} \quad 0^{\mathcal{M}} = 0, \quad +^{\mathcal{M}}(a, b) = a + b \\ \mathcal{N} &= (\{2^n : n \in \mathbb{N}\}, 0^{\mathcal{N}}, +^{\mathcal{N}}), && \text{where} \quad 0^{\mathcal{N}} = 1, \quad +^{\mathcal{N}}(a, b) = a \cdot b \end{aligned}$$

$$h : n \mapsto 2^n, \quad h : \mathcal{M} \cong \mathcal{N} \quad \text{but} \quad \mathcal{M} \not\subset \mathcal{N}.$$

# Example

*quasipolynomial* $2^{O((\log n)^c)}$

# A Joke

"Let $G_1$ be the group $\ldots$, and $G_2$ be the group $\ldots$ 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 $\ldots$, let $G_2$ be the group $\ldots$. 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 $h : M \to M$, and $R \subset M^n$ definable in $\mathcal{M}$. Then for any $a_1, \ldots, a_n \in M$,*

$$(a_1, \ldots, a_n) \in R \iff (h(a_1), \ldots, h(a_n)) \in R$$

**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 $\mathscr{L} = \{<\}$.

$h : a \mapsto a^3$ is an automorphism of $\mathbb{R}$.
It maps points outside of $\mathbb{N}$ into $\mathbb{N}$.

$$\boxed{\mathbb{N} \text{ is not definable in } (\mathbb{R}, 0, 1, +, \cdot, <)}$$

Natural numbers are not definable over the theory of real-closed fields.

# Example

## Example

The structure $\mathcal{M} := \big(\{a, b, c\}, \{(a, b), (a, c)\}\big)$
where the language is $\mathscr{L} = \{E\}$.

$$b \bullet \leftarrow \overset{a}{\bullet} \rightarrow \bullet\ c$$

- $\{b, c\}$ 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 $r$.

- $U := \{\mathbf{x} \in E : |\mathbf{x}| = 1\}$ is not definable in $\mathcal{E}$.
- $h : \mathbf{x} \mapsto 2\mathbf{x}$ 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 $\mathcal{N}$.
- *Spoler* wins the run otherwise.
- $\mathcal{M} \sim_n \mathcal{N}$ if *Duplicator* has a winning strategy in the $n$-move game.
- $\mathcal{M} \equiv_n \mathcal{N}$ if $\mathcal{M} \vDash A \iff \mathcal{N} \vDash A$ 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)

$$\mathcal{M} \sim_2 \mathcal{N} \qquad \mathcal{M} \nsim_3 \mathcal{N}$$

$$\mathcal{M} \vDash A \qquad \mathcal{N} \vDash \neg A$$

$$\forall xy \exists z (\neg Exy \to Exz \wedge Eyz)$$

# Isomorphic Embedding, Elementary Embedding

## Definition

- Isomorphic embedding $f : \mathcal{M} \subset \mathcal{N}$ if there is $\mathcal{A} \subset \mathcal{N}$ s.t. $f : \mathcal{M} \cong \mathcal{A}$.
- Elementary embedding $f : \mathcal{M} \prec \mathcal{N}$ if for any wff $A(x_1, \ldots, x_n)$ and any $a_1, \ldots, a_n \in M$,
$$\mathcal{M} \vDash A[a_1, \ldots, a_n] \iff \mathcal{N} \vDash A[f(a_1), \ldots, f(a_n)]$$
- Elementary substructure $\mathcal{M} \prec \mathcal{N}$ if $M \subset N$ & $1_M : \mathcal{M} \prec \mathcal{N}$.

## Example

- $(\mathbb{N} \setminus \{0\}, \leq) \subset (\mathbb{N}, \leq)$ $\quad (\mathbb{N} \setminus \{0\}, \leq) \cong (\mathbb{N}, \leq)$ $\quad (\mathbb{N} \setminus \{0\}, \leq) \not\prec (\mathbb{N}, \leq)$
$A(x) := \exists y(y \leq x \wedge \neg y = x)$ $\quad (\mathbb{N}, \leq) \vDash A[1]$ $\quad (\mathbb{N} \setminus \{0\}, \leq) \nvDash A[1]$
- $(2\mathbb{Z}, <) \subset (\mathbb{Z}, <)$ $\quad (2\mathbb{Z}, <) \cong (\mathbb{Z}, <)$ $\quad (2\mathbb{Z}, <) \not\prec (\mathbb{Z}, <)$
$A(x, y) := \exists z(x < z < y)$ $\quad (\mathbb{Z}, <) \vDash A[0, 2]$ $\quad (2\mathbb{Z}, <) \nvDash A[0, 2]$

$$f : \mathcal{M} \prec \mathcal{N} \iff \exists \mathcal{A}(f : \mathcal{M} \cong \mathcal{A} \prec \mathcal{N}) \iff \exists \mathcal{A}(\mathcal{M} \prec \mathcal{A} \cong \mathcal{N})$$

# 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 $t(x_1, \ldots, x_n)$, any wff $A(x_1, \ldots, x_n)$, and any $a_1, \ldots, a_n \in M$,

$$f(t^{\mathcal{M}}[a_1, \ldots, a_n]) = t^{\mathcal{N}}[f(a_1), \ldots, f(a_n)]$$

$$\mathcal{M} \vDash A[a_1, \ldots, a_n] \iff \mathcal{N} \vDash A[f(a_1), \ldots, f(a_n)]$$

- $f : \mathcal{M} \prec \mathcal{N}$ iff $f : \mathcal{M} \subset \mathcal{N}$ and for any wff $\exists x A(x_1, \ldots, x_n, x)$ and any $a_1, \ldots, a_n \in M$,

$$\mathcal{N} \vDash \exists x A[f(a_1), \ldots, f(a_n), x] \implies \exists a \in M : \mathcal{N} \vDash A[f(a_1), \ldots, f(a_n), f(a)]$$

$$\mathcal{M} \prec \mathcal{N} \iff \mathcal{M} \subset \mathcal{N} \ \& \ \forall X \in \mathrm{Def}(\mathcal{N}, M) : X \cap M \neq \emptyset$$

Let $M \subset \mathbb{R}$. $(M, <) \prec (\mathbb{R}, <)$ iff $(M, <)$ is a dense linear ordering without endpoints.

# Isomorphic Embedding, Elementary Embedding

- Let $\mathcal{M}$ be a $\mathscr{L}$-structure. $\mathcal{M}_M := (\mathcal{M}, a)_{a \in M}$ is a $\mathscr{L}_M$-structure by interpreting $c_a$ by $a$.
- Let $\mathcal{N}$ be a $\mathscr{L}$-structure, and $X \subset M$ & $f : X \to N$. $(\mathcal{N}, f(a))_{a \in X}$ is a $\mathscr{L}_X$-structure by interpreting $c_a$ by $f(a)$.

$\mathrm{diag}(\mathcal{M}) := \{A : A$ is an atomic or negated atomic sentence of $\mathscr{L}_M$ and $\mathcal{M}_M \vDash A\}$

- $f : \mathcal{M} \subset \mathcal{N} \iff (\mathcal{N}, f(a))_{a \in M} \vDash \mathrm{diag}(\mathcal{M})$
- $f : \mathcal{M} \prec \mathcal{N} \iff (\mathcal{N}, f(a))_{a \in M} \vDash \mathrm{Th}(\mathcal{M}_M)$

# Contents

Introduction

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 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 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*

# 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*

## What is Logic?[8]

Logic is the science that investigates the principles of valid reasoning.

$\boxed{\text{what follows from what}}$

*The art of thinking and reasoning in strict accordance with the limitations and incapacities of the human misunderstanding.* ◎Ô◎

— *The Devil's Dictionary*

The study of invariants under all automorphisms (symmetries).

[8] Tarski: 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" if 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

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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: $A_1 \vee A_2 \vee \cdots \vee A_n$, where $n \geq 1$ and $A_1, A_2, \ldots, A_n$ are literals.
- A Horn clause is a clause in which at most one literal is positive.
- An open formula is in conjuctive normal form (CNF) iff it is a conjuction of clause.
- 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) if each of its variables appears exactly once in every clause. (similarly, full disjunctive normal form)

# 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 $y \notin \mathrm{Fv}(A) \cup \mathrm{Bv}(A)$ |
| $A \vee Qx B$ | $Qx(A \vee B)$ | where $x \notin \mathrm{Fv}(A)$ |
| $A \wedge Qx B$ | $Qx(A \wedge B)$ | where $x \notin \mathrm{Fv}(A)$ |
| $A \rightarrow \forall x B$ | $\forall x (A \rightarrow B)$ | where $x \notin \mathrm{Fv}(A)$ |
| $A \rightarrow \exists x B$ | $\exists x (A \rightarrow B)$ | where $x \notin \mathrm{Fv}(A)$ |
| $\forall x A \rightarrow B$ | $\exists x (A \rightarrow B)$ | where $x \notin \mathrm{Fv}(A)$ |
| $\exists x A \rightarrow B$ | $\forall x (A \rightarrow B)$ | where $x \notin \mathrm{Fv}(A)$ |

# 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 $\forall x_1 \ldots \forall x_n \exists y A$ by $\forall x_1 \ldots \forall x_n A[f(x_1, \ldots, x_n)/y]$, 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* $A^{\mathrm{SNF}}$ without existential quantifiers.
- Any formula can be *equisatisfiably* transformed into SNF.

Warning: $A^{\mathrm{SNF}} \vDash A$ 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

$$\boxed{A \text{ is satisfiable iff } A^{\mathrm{SNF}} \text{ is satisfiable.}}$$

$$A^{\mathrm{HNF}} := \left(\neg(\neg A)^{\mathrm{SNF}}\right)^{\mathrm{NNF}}$$

$$\boxed{\vDash A \iff \vDash A^{\mathrm{HNF}}}$$

Example:

$$(\forall x \exists y \forall z A(x, y, z))^{\mathrm{SNF}} = \forall x z A(x, f(x), z)$$

$$(\forall x \exists y \forall z A(x, y, z))^{\mathrm{HNF}} = \exists y A(c, y, f(y))$$

# Herbrand Universe

## Definition (Herbrand Universe)

Given a sentence $A$ in Skolem normal form,

- $H_0 \coloneqq \{\text{all constants in } A\}$. If no constant in $A$ then $H_0 \coloneqq \{c\}$ for a new constant $c$.
- $H_{i+1} \coloneqq \left\{f(t_1, \ldots, t_n) : f \text{ in } A \text{ and } t_j \in H_i,\ j = 1, \ldots, n\right\}$
- $H_A \coloneqq \bigcup_{i \in \omega} H_i$

The Herbrand universe of a language $\mathscr{L}$ is the set of all ground terms of $\mathscr{L}$. If no constant in $\mathscr{L}$, then add a new constant to $\mathscr{L}$.

# Herbrand Structure

## Definition (Herbrand Structure)

A Herbrand structure for $\mathscr{L}$ is $(H, I)$ s.t.

- $H$ is the Herbrand universe of $\mathscr{L}$.
- 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 $(H_A, J) \vDash A$, where for each ground term $t : J(t) = t$, and for each predicate symbol $P$,
$J(P) = \{(t_1, \ldots, t_n) \in H_A : M, I \vDash P(t_1, \ldots, t_n)\}$.

# Herbrand's Theorem

For a quantifier-free wff $A(x_1, \ldots, x_n)$, the Herbrand expansion over a set $D$ of ground terms is $\mathcal{E}(A, D) \coloneqq \{A(t_1, \ldots, t_n) : t_i \in D\}$.

**Theorem (Herbrand's Theorem)**

*A sentence $\forall \mathbf{x} A(\mathbf{x})$ 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*

$$\vdash A \iff \vdash \bigvee_{i=1}^{m} A'(t_{i1}, \ldots, t_{in})$$

*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 $A^{\mathrm{HNF}}$ by dropping the quantifiers.*

# 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 $n$.*

# Contents

Introduction

History

Propositional Logic

Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- What is Logic?
- Normal Forms
- Meta-Theorems

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Model & Semantic Consequence

- $\mathrm{Mod}(A) := \{\mathcal{M} : \mathcal{M} \vDash A\}$
- $\mathrm{Mod}(\Gamma) := \bigcap_{A \in \Gamma} \mathrm{Mod}(A)$
- $\mathrm{Th}(\mathcal{M}) := \{A : \mathcal{M} \vDash A\}$
- $\mathrm{Th}(\mathcal{K}) := \bigcap_{\mathcal{M} \in \mathcal{K}} \mathrm{Th}(\mathcal{M})$
- $\mathrm{Cn}(\Gamma) := \{A : \Gamma \vDash A\}$

- $\Gamma \subset \Gamma' \implies \mathrm{Mod}(\Gamma') \subset \mathrm{Mod}(\Gamma)$
- $\mathcal{K} \subset \mathcal{K}' \implies \mathrm{Th}(\mathcal{K}') \subset \mathrm{Th}(\mathcal{K})$
- $\Gamma \subset \mathrm{Th}(\mathrm{Mod}(\Gamma))$
- $\mathcal{K} \subset \mathrm{Mod}(\mathrm{Th}(\mathcal{K}))$
- $\mathrm{Mod}(\Gamma) = \mathrm{Mod}(\mathrm{Th}(\mathrm{Mod}(\Gamma)))$
- $\mathrm{Th}(\mathcal{K}) = \mathrm{Th}(\mathrm{Mod}(\mathrm{Th}(\mathcal{K})))$
- $\mathrm{Cn}(\Gamma) = \mathrm{Th}(\mathrm{Mod}(\Gamma))$
- $\Gamma \subset \Gamma' \implies \mathrm{Cn}(\Gamma) \subset \mathrm{Cn}(\Gamma')$
- $\mathrm{Cn}(\mathrm{Cn}(\Gamma)) = \mathrm{Cn}(\Gamma)$

# Galois Correspondence

## Definition (Galois Correspondence)

The function $X \mapsto X^*$ from $\mathrm{P}(A)$ to $\mathrm{P}(B)$ and the function $Y \mapsto Y^\dagger$ from $\mathrm{P}(B)$ to $\mathrm{P}(A)$ constitute a *Golois correspondence* if

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

$$X^* := \bigcap_{x \in X} \{y \in B : Rxy\} \qquad Y^\dagger := \bigcap_{y \in Y} \{x \in A : Rxy\}$$

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 ploarities induced by a relation.

# Theory & Axiomatization

- A set $\Gamma$ of sentences is a theory if $\Gamma = \mathrm{Cn}(\Gamma)$.
- A theory $\Gamma$ is complete if for every sentence $A$, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- A theory $\Gamma$ is finitely axiomatizable if $\Gamma = \mathrm{Cn}(\Sigma)$ for some finite set $\Sigma$ of sentences.
- A theory $\Gamma$ is axiomatizable if there is a decidable set $\Sigma$ of sentences s.t. $\Gamma = \mathrm{Cn}(\Sigma)$.
- A class $\mathcal{K}$ of structures is an elementary class $(EC)$ if $\mathcal{K} = \mathrm{Mod}(A)$ for some sentence $A$.
- A class $\mathcal{K}$ of structures is an elementary class in wider sense $(EC_\Delta)$ if $\mathcal{K} = \mathrm{Mod}(\Sigma)$ for some set $\Sigma$ of sentences.

# Consistency & Satisfiability

- $\Gamma$ is consistent if $\Gamma \nvdash \bot$.
- $\Gamma$ is maximal if for every wff $A$, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- $\Gamma$ is maximal consistent if it is both consistent and maximal.
- $\Gamma$ is satisfiable if $\mathrm{Mod}(\Gamma) \neq \emptyset$.
- $\Gamma$ is finitely satisfiable if every finite subset of $\Gamma$ 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.*

# Completeness Theorem

**Theorem (Completeness Theorem — Gödel1930)**

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

**Corollary**

*Any consistent set of wffs is satisfiable.*

$$\begin{array}{ccc} \Gamma \vDash A & \Longleftrightarrow & \Gamma \vdash A \\ \Updownarrow & & \Updownarrow \\ \begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{unsatisfiable}\end{array} & \Longleftrightarrow & \begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{inconsistent}\end{array} \end{array}$$

# Proof of Completeness Theorem — step1

## Lemma (Lindenbaum Lemma)

*Any consistent set $\Theta$ of sentences can be extended to a maximal consistent set $\Delta$ of sentences of the same language.*

## Proof.

Arrange all the sentences in a sequence $\langle A_\xi : \xi < \kappa \rangle$.

$$\Theta_0 := \Theta$$

$$\Theta_{\xi+1} := \begin{cases} \Theta_\xi \cup \{A_\xi\} & \text{if } \Theta_\xi \cup \{A_\xi\} \text{ is consistent} \\ \Theta_\xi \cup \{\neg A_\xi\} & \text{otherwise} \end{cases}$$

$$\Theta_\xi := \bigcup_{\alpha<\xi} \Theta_\alpha \qquad \text{if } \xi \text{ is a limit ordinal}$$

$\Delta := \bigcup_{\xi<\kappa} \Theta_\xi$ is maximal consistent.

# Proof of Completeness Theorem — step2

A set $\Delta$ is Henkin iff $\Delta$ is maximally consistent and for any formula of the form $\exists x A$ there exists a closed term $t$ s.t. $\exists x A \to A[t/x] \in \Delta$.

## Lemma (Closure Lemma)

*If $\Gamma$ is consistent, then there is a Henkin set $\Delta \supset \Gamma$.*

## Proof.

Let $\mathcal{C}$ be a set of new constants. $\mathscr{L}^+ := \mathscr{L} \cup \mathcal{C}$, $\mathscr{L} \cap \mathcal{C} = \emptyset$, $|\mathcal{C}| = |\mathscr{L}|$. Assume $|\mathcal{C}| = \kappa$, and $\mathcal{C} = \{c_\xi : \xi < \kappa\}$. Arrange all formulae of $\mathscr{L}^+$ with at most one free variable in a sequence $\langle A_\xi : \xi < \kappa \rangle$. Let

$$\Gamma_0 := \Gamma$$

$$\Gamma_{\xi+1} := \Gamma_\xi \cup \{\exists x A_\xi(x) \to A_\xi[c_\beta/x]\}$$

where $c_\beta$ 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 $\Theta$ to a maximal consistent set $\Delta \supset \Theta$ by Lindenbaum lemma.

# Proof of Completeness Theorem — step3

## Lemma (Term Models Lemma)

*If $\Delta$ is maximal consistent, then there is an interpretation $\mathcal{M}, v$ s.t.*

$$\mathcal{M}, v \vDash A \iff A \in \Delta$$

## Proof.

- $M := \{[t] : t \in \mathcal{T}\}$ where $\mathcal{T}$ is the set of all terms of $\mathscr{L}^+$, $[t] := \{s : s \sim t\}$, $s \sim t := s = t \in \Delta$
- $([t_1], \ldots, [t_n]) \in P^{\mathcal{M}} := P(t_1, \ldots, t_n) \in \Delta$
- $f^{\mathcal{M}}([t_1], \ldots, [t_n]) := [f(t_1, \ldots, t_n)]$
- $c^{\mathcal{M}} = [c]$
- $v(x) := [x]$

# Stone Space of Lindenbaum Algebra

$$
\begin{tikzcd}
\mathrm{Str} \arrow[r, leftrightarrow, "\models"] \arrow[d, "\mathcal{M}\mapsto\mathrm{Th}(\mathcal{M})"'] & \mathrm{Sen} \arrow[d, "A\mapsto[A]"] \arrow[dl, leftrightarrow, "\ni"] \\
\mathrm{S}_0 \arrow[r, leftrightarrow] \arrow[d, "T\mapsto T/\sim"'] & \mathrm{Lin}_0 \arrow[dl, leftrightarrow, "\ni"] \\
\mathrm{Sto}(\mathrm{Lin}_0) &
\end{tikzcd}
$$

- $\mathrm{Str}$: the class of structures.
- $\mathrm{Sen}$: the set of sentences.
- $\mathrm{S}_0$: the set of complete theories.
- $\mathrm{Lin}_0 = \mathrm{Sen}/\sim$
- $\mathrm{Sto}(M)$: the set of ultrafilters of $M$.

1. The closed subsets of $\mathrm{Sen}$ are precisely the theories.
2. The closed subsets of $\mathrm{S}_0$ compose a Hausdorff topology.
3. $\mathcal{M} \mapsto \mathrm{Th}(\mathcal{M}) : \mathrm{Str} \to \mathrm{S}_0$ is continuous, and $[\mathcal{M}] \mapsto \mathrm{Th}(\mathcal{M})$ is a homomorphism, $\mathrm{S}_0$ is a Kolmogorov quotient $\mathrm{Str}/\equiv$.
4. For every theory $T$, $T/\sim$ is a filter of $\mathrm{Lin}_0$.
5. For every complete theory $T$, $T/\sim$ is an ultrafilter of $\mathrm{Lin}_0$.
6. $T \mapsto T/\sim : \mathrm{S}_0 \rightarrowtail \mathrm{Sto}(\mathrm{Lin}_0)$ is a homomorphism.
7. The image is dense in $\mathrm{Sto}(\mathrm{Lin}_0)$.
8. The image is a closed subspace of $\mathrm{Sto}(\mathrm{Lin}_0)$.
9. $T \mapsto T/\sim : \mathrm{S}_0 \rightarrowtail\!\!\!\!\rightarrow \mathrm{Sto}(\mathrm{Lin}_0)$ iff the topology on $\mathrm{S}_0$ is compact.

# Compactness Theorem

**Theorem (Compactness Theorem)**

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

**Corollary**

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

**Corollary**

*If a set* $\Gamma$ *of sentences has arbitrarily large finite models, then it has an infinite model.*

**Corollary**

*There is a countable structure* $\mathcal{M} \equiv \mathcal{N}$ *but* $\mathcal{M} \not\cong \mathcal{N}$*.*

# 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
  $f \sim g := \left\{ i \in I : f(i) = g(i) \right\} \in U$
- $P^{\mathcal{N}}\big([f_1], \ldots, [f_n]\big) := \left\{ i \in I : P^{\mathcal{M}_i}(f_1(i), \ldots, f_n(i)) \right\} \in U$
- $F^{\mathcal{N}}\big([f_1], \ldots, [f_n]\big) := [f]$ where $f(i) := F^{\mathcal{M}_i}\big(f_1(i), \ldots, f_n(i)\big)$

## Theorem (Łoś Theorem)

$$\prod_{i \in I} \mathcal{M}_i / U \vDash A\left([f_1], \ldots, [f_n]\right) \iff \left\{ i \in I : \mathcal{M}_i \vDash A\big(f_1(i), \ldots, f_n(i)\big) \right\} \in U$$

# 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 $\Gamma$ of wffs is satisfiable iff it is finitely satisfiable.*

## Proof.

Let $I := \{\Delta \subset \Gamma : |\Delta| < \infty\}$.
Then $\forall \Delta \in I \; \exists \mathcal{M}_\Delta : \mathcal{M}_\Delta \vDash \Delta$.
Let $\hat{A} := \{\Delta \in I : A \in \Delta\}$.
Then $F := \{\hat{A} : A \in \Gamma\}$ has the finite intersection property because

$$\{A_1, \ldots, A_n\} \in \hat{A}_1 \cap \cdots \cap \hat{A}_n$$

By the ultrafilter theorem, $F$ can be extended to an ultrafilter $U$ on $I$.
For $A \in \Gamma$,

$$\begin{aligned} \hat{A} \in U \;\; \& \;\; \hat{A} \subset \{\Delta \in I : \mathcal{M}_\Delta \vDash A\} &\implies \{\Delta \in I : \mathcal{M}_\Delta \vDash A\} \in U \\ &\implies \prod_{\Delta \in I} \mathcal{M}_\Delta / U \;\vDash A \end{aligned}$$

# 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* if 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.**

$$\mathrm{Th}(\mathcal{R}) \cup \{x > c_r : r \in \mathbb{R}\}$$

Figure: Robinson

# Nonstandard Analysis

Let $U$ be a nonprinciple ultrafilter on $\mathbb{N}$.

$$\prod_{i \in \mathbb{N}} \mathcal{R}/U \vDash \mathrm{Th}(\mathcal{R})$$

Let $\varepsilon := \left[(1, \frac{1}{2}, \frac{1}{3}, \dots)\right] \in \mathbb{R}$.
For any $n \in \mathbb{N}$,

$$\prod_{i \in \mathbb{N}} \mathcal{R}/U \vDash \varepsilon < \frac{1}{n}$$

**Theorem**

- *$\mathcal{K}$ is $EC_\Delta$ 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.*

# Applications of Compactness

- The class of all finite structures is not $EC_\Delta$. (Model finiteness is undefinable even by a set of formulae.)
- The class of all infinite structures is $EC_\Delta$ but not $EC$. (Model infiniteness is definable by a set of formulae 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 $EC_\Delta$ 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 $EC_\Delta$.

## 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 $n$?*

# Applications of Compactness

**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.*

**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 $N < 2^{\frac{k}{2}}$.

# 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 $\limsup_{n\to\infty} \frac{|A\cap[1,n]|}{\pi(n)} > 0$ 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* $\limsup_{n\to\infty} \frac{|A\cap[1,n]|}{n} > 0$ *contains arbitrarily long arithmetic progressions.*

**Theorem (Furstenberg Multiple Recurrence Theorem)**

*Let* $(X, \mathcal{B}, \mu, T)$ *be a measure-preserving system and* $A \in \mathcal{B}$ *with* $\mu(A) > 0$. *Then,*

$$\forall k \in \mathbb{N} : \liminf_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu\left(\bigcap_{j=0}^{k} T^{-jn} A\right) > 0$$

Szemerédi Theorem $\iff$ Furstenberg Multiple Recurrence Theorem

# Complete Disorder is Impossible!

## Theorem (Poincaré Recurrence Theorem)

*Let $(X, \mathcal{B}, \mu, T)$ be a measure-preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Then almost every $x \in A$ returns infinitely often to $A$.*

$$\mu\left(\{x \in A : \exists N \forall n > N : T^n x \notin A\}\right) = 0$$

## Lemma (Kac's Lemma)

*Let $(X, \mathcal{B}, \mu, T)$ be a measure-preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Then the recurrence time $\tau_A(x) := \min\left\{k \geq 1 : T^k x \in A\right\}$ satisfies*

$$\int_A \tau_A(x) \mathrm{d}\mu(x) = 1$$

*Equivalently, the mean recurrence time $\langle \tau_A \rangle := \frac{1}{\mu(A)} \int_A \tau_A(x) \mathrm{d}\mu(x) = \frac{1}{\mu(A)}$.*

# 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* if 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 $\lambda$ has a model of cardinality $\leq \lambda$.*

**Theorem (Upward Löwenheim-Skolem Theorem)**

*If a set of sentences in a language of cardinality $\lambda$ has an infinite model, then it has models of every cardinality $\geq \lambda$.*

# Skolem Paradox? — Models and Reality

- Cantor: $\mathrm{P}(\mathbb{N})$ is uncountable.
- There is a countable model $\mathcal{M} \vDash \mathrm{ZF} \vdash$"$\mathrm{P}(\mathbb{N})$ is uncountable".
- The statement "$\mathrm{P}(\mathbb{N})$ is uncountable" is interpreted in $\mathcal{M}$ as — within $\mathcal{M}$, there is a set $M_1$ that looks like $\mathrm{P}(\mathbb{N})$ 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 $\mathrm{P}(\mathbb{N})$ 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 $\mathrm{ZF}$.

# 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?

# The Interpolation Theorem

**Theorem (Craig's Interpolation Theorem)**

*If* $\vDash A \to B$*, then there is a sentence* $C$ *s.t.* $\vDash A \to C$ *and* $\vDash C \to B$*, and* $C$ *contains no non-logical symbols except such as are both in* $A$ *and in* $B$*.*

**Theorem (Robinson's joint Consistency Theorem)**

*Let* $\mathscr{L}_0, \mathscr{L}_1, \mathscr{L}_2$ *be languages, with* $\mathscr{L}_0 = \mathscr{L}_1 \cap \mathscr{L}_2$*. Let* $\mathrm{T}_i$ *be a theory in* $\mathscr{L}_i$ *for* $i = 1, 2$*. If* $\mathrm{T}_1$ *and* $\mathrm{T}_2$ *are consistent and if there is no formula* $A$ *of* $\mathscr{L}_0$ *s.t.* $\mathrm{T}_1 \vdash A$ *and* $\mathrm{T}_2 \vdash \neg A$*, then the union* $\mathrm{T}_1 \cup \mathrm{T}_2$ *is consistent.*

# Beth's Definability Theorem

## Definition (Explicit Definition)

Suppose $\mathscr{L}$ is a language not containing the predicate symbol $P$. A set $\Sigma(P)$ of sentences of $\mathscr{L} \cup \{P\}$ *explicitly defines* $P$ iff there is a wff $A(x_1, \ldots, x_n)$ of $\mathscr{L}$ s.t.

$$\Sigma(P) \vDash \forall x_1 \ldots \forall x_n (P(x_1, \ldots, x_n) \leftrightarrow A(x_1, \ldots, x_n))$$

## Definition (Implicit Definition)

Suppose $\mathscr{L}$ is a language not containing the predicate symbol $P$ and $P'$. A set $\Sigma(P)$ of sentences of $\mathscr{L} \cup \{P\}$ *implicitly defines* $P$ iff

$$\Sigma(P) \cup \Sigma(P') \vDash \forall x_1 \ldots \forall x_n (P(x_1, \ldots, x_n) \leftrightarrow P'(x_1, \ldots, x_n))$$

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?

# Abstract Logics

## Definition (Abstract Logic)

An *abstract logic* is a pair $\mathcal{L} := (\mathcal{S}, \vDash_{\mathcal{L}})$, where $\mathcal{S} : \mathrm{signatures} \to \mathrm{sets}$ assigns to signature $\tau$ a set $\mathcal{S}(\tau)$ of sentences, and $\vDash_{\mathcal{L}}$ is a relation between $\tau$-$\mathrm{structures}$ and elements of $\mathcal{S}(\tau)$ s.t.

1. (*Monotony*) $\tau \subset \tau' \implies \mathcal{S}(\tau) \subset \mathcal{S}(\tau')$
2. (*Isomorphism*) $\mathcal{M} \vDash_{\mathcal{L}} A \;\&\; \mathcal{M} \cong \mathcal{N} \implies \mathcal{N} \vDash_{\mathcal{L}} A$
3. (*Expansion*) If $\tau \subset \tau', A \in \mathcal{S}(\tau)$, and $\mathcal{M}$ is an $\tau'$-structure, then $\mathcal{M} \vDash_{\mathcal{L}} A \iff \mathcal{M}\restriction_{\tau} \vDash_{\mathcal{L}} A$

$$\mathrm{Mod}^{\tau}_{\mathcal{L}}(A) := \left\{\mathcal{M} \in \tau\text{-}structures : \mathcal{M} \vDash_{\mathcal{L}} A\right\}$$

# Example — $\mathcal{L}_{\kappa\lambda}$

For $\kappa \geq \lambda$, define the $\mathcal{L}_{\kappa\lambda}$ formulae as for first order logic, plus:

- Given a set of formulae $\{A_i : i \in I\}, |I| < \kappa$, then $\bigwedge_{i \in I} A_i$ and $\bigvee_{i \in I} A_i$ are formulae.
- 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 formulae.

Satisfaction relation:

- $\mathcal{M} \vDash_{\mathcal{L}_{\kappa\lambda}} \bigwedge_{i \in I} A_i$ if $\mathcal{M} \vDash_{\mathcal{L}_{\kappa\lambda}} A_i$ for all $i \in I$.
- $\mathcal{M} \vDash_{\mathcal{L}_{\kappa\lambda}} \exists(x_i : i \in J)A$ if $\mathcal{M} \vDash_{\mathcal{L}_{\kappa\lambda}} A[a_i : i \in J]$ 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* if it satisfies:

1. (*Bool*) For $A \in \mathcal{S}(\tau)$ there is $B \in \mathcal{S}(\tau)$ s.t. $\mathcal{M} \vDash_{\mathcal{L}} B \iff \mathcal{M} \nvDash_{\mathcal{L}} A$; and $\forall A, B \in \mathcal{S}(\tau)\ \exists C \in \mathcal{S}(\tau) : \mathcal{M} \vDash_{\mathcal{L}} C \iff \mathcal{M} \vDash_{\mathcal{L}} A \ \&\ \mathcal{M} \vDash_{\mathcal{L}} B$.
2. (*Quantifier*) $\forall c \in \tau \forall A \in \mathcal{S}(\tau)\ \exists B \in \mathcal{S}(\tau)$ :
$$\mathrm{Mod}_{\mathcal{L}}^{\tau \setminus \{c\}}(B) = \left\{\mathcal{M} : (\mathcal{M}, a) \in \mathrm{Mod}_{\mathcal{L}}^{\tau}(A) \text{ for some } a \in M\right\}$$
where $(\mathcal{M}, a)$ is the expansion of $\mathcal{M}$ to $\tau$ assigning $a$ to $c$.
3. (*Renaming*) Let $\pi : \tau \to \tau'$ be a bijection which respects arity, and we extend $\pi$ in a canonical way to $\hat{\pi} : \tau$-structures $\to \tau'$-structures. Then
$$\forall A \in \mathcal{S}(\tau)\ \exists A' \in \mathcal{S}(\tau) : \mathcal{M} \vDash_{\mathcal{L}} A \iff \hat{\pi}(\mathcal{M}) \vDash_{\mathcal{L}} A'$$
4. (*Relativization*) Given $A \in \mathcal{S}(\tau)$ and symbols $R$, $c_1, \ldots, c_n \notin \tau$, there is $B \in \mathcal{S}(\tau \cup \{R, c_1, \ldots, c_n\})$ called the *relativization* of $A$ to $R(x, c_1, \ldots c_n)$, s.t. for $\mathcal{M} : (\mathcal{M}, X, b_1, \ldots, b_n) \vDash_{\mathcal{L}} B \iff \mathcal{N} \vDash_{\mathcal{L}} A$ where $\mathcal{N} \subset \mathcal{M}$ with $N = \left\{a \in M : R^{\mathcal{M}}(a, b_1, \ldots, b_n)\right\}$, and $(\mathcal{M}, X, b_1, \ldots, b_n)$ is the expansion of $\mathcal{M}$ interpreting $R$, $c_1, \ldots, c_n$ by $X$, $b_1, , \ldots, b_n$ (with $X \subset M^{n+1}$).

# Lindström's Theorem

## Definition (Expressive Power)

$\mathcal{L}_2$ is *at least as expressive* as $\mathcal{L}_1$ ($\mathcal{L}_1 \leq \mathcal{L}_2$) if for each signature $\tau$ and $A \in \mathcal{S}_1(\tau)$ there is $B \in \mathcal{S}_2(\tau)$ s.t.

$$\mathrm{Mod}^{\tau}_{\mathcal{L}_1}(A) = \mathrm{Mod}^{\tau}_{\mathcal{L}_2}(B)$$

$$\mathcal{L}_1 \sim \mathcal{L}_2 \coloneqq \mathcal{L}_1 \leq \mathcal{L}_2 \ \& \ \mathcal{L}_2 \leq \mathcal{L}_1$$

## 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 formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \wedge$.
2. The set of *regular formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \wedge, \exists$.
3. The set of *coherent formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \bot, \wedge, \vee, \exists$.
4. The set of *first order formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \bot, \neg, \wedge, \vee, \rightarrow, \exists, \forall$.
5. The class of *geometric formulae* over is the smallest class containing the class of atomic formulae and closed under $\top, \bot, \wedge, \vee, \exists$ and infinitary disjunction.
6. The class of *infinitary first order formulae* is the smallest class containing the class of atomic formulae and closed under $\top, \bot, \neg, \wedge, \vee, \rightarrow, \exists, \forall$ and infinitary conjunction and infinitary disjunction.

- $\mathrm{T}$ is an algebraic theory if its signature has no relation symbols and its axioms are all of the form $\top \vdash_{\mathbf{x}} A$ where $A$ is an atomic formula of the form $s = t$ and $\mathbf{x}$ its canonical context.
- $\mathrm{T}$ is a Horn (resp. regular, coherent, geometric) theory if all the sequents in $\mathrm{T}$ are Horn (resp. regular, coherent, geometric).
- $\mathrm{T}$ is a universal Horn theory if its axioms are all of the form $A \vdash_{\mathbf{x}} B$, where $A$ is a finite conjunction of atomic formulae and $B$ is an atomic formula or the formula $\bot$.
- $\mathrm{T}$ is a propositional theory if it only consists of $0$-ary relation symbols.

Identity Axiom $A \vdash_{\mathbf{x}} A$

Equality $\top \vdash_x x = x$ and $\mathbf{x} = \mathbf{y} \wedge A \vdash_{\mathbf{z}} A[\mathbf{y}/\mathbf{x}]$ where $\mathrm{Fv}(\mathbf{x}, \mathbf{y}, A) \subset \mathbf{z}$.

Substitution $\dfrac{A \vdash_{\mathbf{x}} B}{A[\mathbf{t}/\mathbf{x}] \vdash_{\mathbf{y}} B[\mathbf{t}/\mathbf{x}]}$ where $\mathrm{Fv}(\mathbf{t}) \subset \mathbf{y}$.

Cut $\dfrac{A \vdash_{\mathbf{x}} B \quad B \vdash_{\mathbf{x}} C}{A \vdash_{\mathbf{x}} C}$

Conjunction $A \vdash_{\mathbf{x}} \top \qquad A \wedge B \vdash_{\mathbf{x}} A \qquad A \wedge B \vdash_{\mathbf{x}} B \qquad \dfrac{A \vdash_{\mathbf{x}} B \quad A \vdash_{\mathbf{x}} C}{A \vdash_{\mathbf{x}} B \wedge C}$

Disjunction $\bot \vdash_{\mathbf{x}} A \qquad A \vdash_{\mathbf{x}} A \vee B \qquad B \vdash_{\mathbf{x}} A \vee B \qquad \dfrac{A \vdash_{\mathbf{x}} C \quad B \vdash_{\mathbf{x}} C}{A \vee B \vdash_{\mathbf{x}} C}$

Implication $\dfrac{A \wedge B \vdash_{\mathbf{x}} C}{A \vdash_{\mathbf{x}} B \to C}$

Existential Quantification $\dfrac{A \vdash_{\mathbf{x}y} B}{\exists y A \vdash_{\mathbf{x}} B}$

Universal Quantification $\dfrac{A \vdash_{\mathbf{x}y} B}{A \vdash_{\mathbf{x}} \forall y B}$

Distributive Axiom $A \wedge (B \vee C) \vdash_{\mathbf{x}} (A \wedge B) \vee (A \wedge C)$

Frobenius Axiom $A \wedge \exists y B \vdash_{\mathbf{x}} \exists y (A \wedge B)$ where $y \notin \mathbf{x}$.

Law of Excluded Middle $\top \vdash_{\mathbf{x}} A \vee \neg A$

# 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 $(H, \bot, \top, \wedge, \vee, \rightarrow, \leq)$ is a bounded lattice $(H, \bot, \top, \wedge, \vee, \leq)$ 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. $a \leq b \ \ \& \ \ a \leq c \implies a \leq b \wedge c$
5. $\bot \leq a$
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 $\neg a := a \rightarrow \bot$.

- A proof of $A \wedge B$ is a pair $(a, b)$ where $a$ is a proof of $A$ and $b$ is a proof of $B$.
- A proof of $A \vee B$ is a pair $(a, b)$ where $a$ is $0$ and $b$ is a proof of $A$, or $a$ is $1$ and $b$ is a proof of $B$.
- A proof of $A \rightarrow B$ is a function $f$ that converts a proof $a$ of $A$ into a proof $f(a)$ of $B$.
- There is no proof of $\perp$.
- A proof of $\exists x A(x)$ is a pair $(a, b)$ where $a$ is an element of the domain of definition, and $b$ is a proof of $A(a)$.
- 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 $A(a)$.

# Continuity, Metric and Topology

- A function $f : X \to Y$ between metric spaces is *continuous* at point $a \in X$ if $\forall \varepsilon > 0 \exists \delta > 0 \forall x \in X : d_X(x, a) < \delta \to d_Y(f(x), f(a)) < \varepsilon$.
- A *metric space* $(X, d)$ is a set $X$ with a metric $d : X \times X \to \mathbb{R}$ 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. $d(x, z) \leq d(x, y) + d(y, z)$

  $$e.g. \quad d(x, y) = \left( \sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}} \qquad d(x, y) = \max_{1 \leq i \leq n} |x_i - y_i|$$
- 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 $f : X \to Y$ between topological spaces is *continuous* if 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 $a \in X$ if to each neighborhood $V$ of $f(a)$ there is a neighborhood $U$ of $a$ for which $f(U) \subset V$.

# Topological Semantics of Intuitionistic Propositional Logic

- A *topological space* $(X, \mathcal{O}(X))$ is a set $X$ with a family $\mathcal{O}(X) \subset \mathrm{P}(X)$ 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
$$A \to B := \big((X \setminus A) \cup B\big)^\circ = \bigcup \{U \in \mathcal{O}(X) : U \cap A \subset B\}$$
by definition, for all $U \in \mathcal{O}(X)$,
$$U \subset A \to B \iff U \cap A \subset B$$
Define $\neg A := A \to \bot$. Thus
$$\neg A = (X \setminus A)^\circ$$
- $A := (0,1) \cup (1,\infty), \neg A = (-\infty, 0), \neg\neg A = (0,\infty), A \cup \neg A \neq \mathbb{R}, A \subsetneq \neg\neg A$.
- A topological model of intuitionistic propositional logic is $(X, \mathcal{O}(X), \nu)$ where $\nu : \mathcal{P} \to \mathcal{O}(X)$.

# 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 ($\kappa$-categoricity)

A theory is $\kappa$-categorical if it has a unique model of cardinality $\kappa$.

## 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 (Łoś-Vaught Test)**

*If a theory with no finite model is $\kappa$-categorical, then it is complete.*

**Theorem**

*The theory $\mathrm{ACF}_p$ of algebraically closed fields of characteristic $p$ (for $p$ prime or $0$) is $\kappa$-categorical for all uncountable cardinals $\kappa$.*

**Corollary**

*For $p \in \mathbb{P}$ or $p = 0$, $\mathrm{ACF}_p$ is complete and decidable.*

**Theorem (Morley's Categoricity Theorem)**

*If a theory is $\kappa$-categorical for some $\kappa \geq |\mathscr{L}|$, then it is categorical in all cardinalities $\geq |\mathscr{L}|$.*

## Problem

- *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?*
- *Or is it rather the case that categoricity is a virtue in some theories but not in others?*

# Lefschetz's Transfer Principle

## Theorem (Lefschetz's Transfer Principle)

*For a sentence $A$ in the language of fields, the following are equivalent:*

1. $\mathbb{C} \vDash A$
2. $\mathrm{ACF}_0 \vDash A$
3. $\mathrm{ACF}_p \vDash A$ *for all sufficiently large primes* $p$.
4. $\mathrm{ACF}_p \vDash A$ *for infinitely many primes* $p$.

## Proof.

$(1 \leftrightarrow 2)$ follows from the completeness of $\mathrm{ACF}_0$.
$(2 \to 3)$ assume $\mathrm{ACF}_0 \vDash A$, since the deduction $\mathrm{ACF}_0 \vdash A$ only use finitely many instances of $\overbrace{1+1+\cdots+1}^{n \text{ times}} \neq 0$, then for some finite $\Delta \subset \mathrm{ACF}_0 : \Delta \vdash A$, and $\mathrm{ACF}_p \vDash \Delta$ for all sufficiently large primes $p$.
$(3 \to 4)$ is trivial.
$(4 \to 2)$ $\mathrm{ACF}_0 \nvdash A \implies \mathrm{ACF}_0 \vdash \neg A \implies \mathrm{ACF}_p \vdash \neg A$ for all sufficiently large primes $p$.

# Ax-Grothendieck Theorem

- An *affine variety* is a set $V \subset \mathbb{C}^n$ s.t. $V = \left\{(x_1, \ldots, x_n) : f_i(x_1, \ldots, x_n) = 0, 1 \leq i \leq k\right\}$ with $f_i \in \mathbb{C}[x_1, \ldots, x_n]$.
- For any field $K$ a map $f : K^n \to K^n$ is *polynomial* if $f(x_1, \ldots, x_n) = \big(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)\big)$ with $f_i \in K[x_1, \ldots, x_n]$.

**Theorem (Ax-Grothendieck Theorem)**

*Let $f : V \to V$ 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: $\mathbb{C}^n \to \mathbb{C}^n$ 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 $p$, $\mathrm{ACF}_p \vdash A$.
Moreover, for each $p$, by completeness of $\mathrm{ACF}_p$, we only need to show $A$ is true in *some* model of $\mathrm{ACF}_p$.
Consider the algebraic closure $F := \overline{\mathbb{F}}_p$ of the prime field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. We have $F = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.
Let $\{a_1, \cdots, a_k\}$ be the set of coefficients appearing in $f : F^n \to F^n$.
For $(b_1, \cdots, b_n) \in F^n$, let $K$ be the subfield of $F$ generated by $\{a_1, \cdots, a_k, b_1, \cdots, b_n\}$.
Since $K$ is finitely generated and $\exists N : K \subset \bigcup_{n=1}^{N} \mathbb{F}_{p^n}$, hence it is finite.
So $f\restriction_{K^n} : K^n \to K^n$ that is injective must be surjective.
Hence $f : F^n \to F^n$ is surjective.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Paradox of Material Implication

- 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!

# 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

History

Propositional Logic

Predicate Logic

Modal Logic
- Syntax
- Semantics
- Formal System
- Logic, Knowledge and Action

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Logics about Modalities

Mary _____ married.

- is possibly (basic modal logic)
- will be (temporal logic)
- is permitted to be (deontic logic)
- is known (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

$$\mathscr{L} := \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \Box, \Diamond, (, )\} \cup \mathcal{P}$$

where $\mathcal{P} := \{p_1, \ldots, p_n, (\ldots)\}$.

## 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 $\mathrm{T}$. $\Box_{\mathrm{T}} A$
- After the execution of the program $\alpha$, $A$ holds. $[\alpha]A$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic
- Syntax
- Semantics
- Formal System
- Logic, Knowledge and Action

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 $V : \mathcal{P} \to \mathrm{P}(W)$.

- $\mathcal{M}, w \Vdash p$ if $w \in V(p)$
- $\mathcal{M}, w \Vdash \neg A$ if $\mathcal{M} \nVdash A$
- $\mathcal{M}, w \Vdash A \wedge B$ if $\mathcal{M}, w \Vdash A$ and $\mathcal{M}, w \Vdash B$
- $\mathcal{M}, w \Vdash \Box A$ if $\forall v \in W : Rwv \implies \mathcal{M}, v \Vdash A$
- $\mathcal{M}, w \Vdash \Diamond A$ if $\exists v \in W : Rwv \ \& \ \mathcal{M}, v \Vdash A$

# 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 $\mathcal{M}, w$ if $\mathcal{M}, w \Vdash A$.
- $A$ is true in $\mathcal{M}$ ($\mathcal{M} \Vdash A$) if $\forall w \in W : \mathcal{M}, w \Vdash A$
- $A$ is valid in a pointed frame $\mathcal{F}, w$ ($\mathcal{F}, w \Vdash A$) if $\mathcal{M}, w \Vdash A$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- $A$ is valid in $\mathcal{F}$ ($\mathcal{F} \Vdash A$) if $\mathcal{M} \Vdash A$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- $\Vdash A$ if $\mathcal{F} \Vdash A$ for every $\mathcal{F}$.

*Truth is in the eye of the beholder.*

**Example**

$$\Vdash \Box(A \to B) \to \Box A \to \Box B$$

# Semantic Consequence

- local semantic consequence

$$\Gamma \Vdash_{\mathcal{C}} A \;:=\; \forall \mathcal{M} \in \mathcal{C} \forall w \in W : \mathcal{M}, w \Vdash \Gamma \implies \mathcal{M}, w \Vdash A$$

- global semantic consequence

$$\Gamma \Vdash^{g}_{\mathcal{C}} A \;:=\; \forall \mathcal{M} \in \mathcal{C} : \mathcal{M} \Vdash \Gamma \implies \mathcal{M} \Vdash A$$

**Example**

- $p \nVdash_{\mathcal{C}} \Box p$
- $p \Vdash^{g}_{\mathcal{C}} \Box p$

# Material Implication vs Strict Implication

$$p \mathrel{-\!\!\!\ni} q \coloneqq \Box(p \to q)$$

- $p \mathrel{-\!\!\!\ni} q \mathrel{-\!\!\!\ni} p$ ?
- $(p \mathrel{-\!\!\!\ni} q) \vee (q \mathrel{-\!\!\!\ni} r)$ ?
- $\neg(p \mathrel{-\!\!\!\ni} q) \to (p \wedge \neg q)$ ?
- $(p \wedge \neg p) \mathrel{-\!\!\!\ni} q$
- $p \mathrel{-\!\!\!\ni} (q \vee \neg q)$
- $\Box p \mathrel{-\!\!\!\ni} q \mathrel{-\!\!\!\ni} p$

# Accessibility

| | |
|---|---|
| serial | $\forall x \exists y : Rxy$ |
| reflexive | $\forall x : Rxx$ |
| symmetric | $\forall xy : Rxy \rightarrow Ryx$ |
| transitive | $\forall xyz : Rxy \wedge Ryz \rightarrow Rxz$ |
| euclidean | $\forall xyz : Rxy \wedge Rxz \rightarrow Ryz$ |
| 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**

| | | | |
|---|---|---|---|
| $D$ | $W, R \Vdash \Box p \to \Diamond p$ | $\iff$ | $R$ *is serial* |
| $T$ | $W, R \Vdash \Box p \to p$ | $\iff$ | $R$ *is reflexive* |
| $B$ | $W, R \Vdash p \to \Box\Diamond p$ | $\iff$ | $R$ *is symmetric* |
| $4$ | $W, R \Vdash \Box p \to \Box\Box p$ | $\iff$ | $R$ *is transitive* |
| $5$ | $W, R \Vdash \Diamond p \to \Box\Diamond p$ | $\iff$ | $R$ *is euclidean* |

# Counter-model for D,T,B,4,5

# Standard Translation

## Definition (Standard Translation)

$$T_x(p) = P(x) \qquad T_y(p) = P(y)$$

$$T_x(\neg A) = \neg T_x(A) \qquad T_y(\neg A) = \neg T_y(A)$$

$$T_x(A \wedge B) = T_x(A) \wedge T_x(B) \qquad T_y(A \wedge B) = T_y(A) \wedge T_y(B)$$

$$T_x(\Box A) = \forall y(Rxy \to T_y(A)) \qquad T_y(\Box A) = \forall x(Ryx \to T_x(A))$$

## Theorem (Correspondence on Models)

$$\mathcal{M}, w \Vdash A \iff \mathcal{M} \vDash T_x(A)[w]$$

$$\mathcal{M} \Vdash A \iff \mathcal{M} \vDash \forall x T_x(A)$$

$$\mathcal{F}, w \Vdash A \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n T_x(A)[w]$$

$$\mathcal{F} \Vdash A \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n \forall x T_x(A)$$

# Tree Method for Modal Logic

$$\begin{array}{c} w \Vdash \Box A \\ | \\ w' \Vdash A \end{array}$$

if $Rww'$ is already in the branch.

$$\begin{array}{c} w \nVdash \Box A \\ | \\ Rww' \\ w' \nVdash A \end{array}$$

where $w'$ is new in the branch.

$$\begin{array}{c} w \Vdash \Diamond A \\ | \\ Rww' \\ w' \Vdash A \end{array}$$

where $w'$ is new in the branch.

$$\begin{array}{c} w \nVdash \Diamond A \\ | \\ w' \nVdash A \end{array}$$

if $Rww'$ is already in the branch.

# Example — Tree Method for Modal Logic

$$\boxed{\Vdash \Box p \wedge \Diamond q \rightarrow \Diamond(p \wedge q)}$$

$$w \Vdash \Box p \wedge \Diamond q$$
$$w \Vdash \neg\Diamond(p \wedge q)$$

$$w \Vdash \Box p$$
$$w \Vdash \Diamond q$$

$$Rwv$$
$$v \Vdash q$$

$$v \Vdash p$$

$$v \Vdash \neg(p \wedge q)$$

$$v \Vdash \neg p \qquad\qquad v \Vdash \neg q$$
$$\times \qquad\qquad\qquad \times$$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic
- Syntax
- Semantics
- Formal System
- Logic, Knowledge and Action

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Formal System = Axiom + Inference Rule

## Axiom Schema

| | |
|---|---|
| | tautologies |
| Dual | $\Diamond A \leftrightarrow \neg\Box\neg A$ |
| K | $\Box(A \to B) \to \Box A \to \Box B$ |
| D | $\Box A \to \Diamond A$ |
| T | $\Box A \to A$ |
| B | $A \to \Box\Diamond A$ |
| 4 | $\Box A \to \Box\Box A$ |
| 5 | $\Diamond A \to \Box\Diamond A$ |
| L | $\Box(\Box A \to A) \to \Box A$ |

## Inference Rule

$$\frac{A \quad A \to B}{B}\ [\text{MP}] \qquad\qquad \frac{A}{\Box A}\ [\text{N}]$$

# Intuitionistic Logic vs Modal Logic

$$\mathrm{S4} := K + T + 4$$

$$\mathrm{Grz} := \mathrm{S4} + \Box(\Box(A \to \Box A) \to A) \to A$$

$$p^* := \Box p$$
$$(\neg A)^* := \Box\neg A^*$$
$$(A \wedge B)^* := A^* \wedge B^*$$
$$(A \vee B)^* := A^* \vee B^*$$
$$(A \to B)^* := \Box(A^* \to B^*)$$

$$\vdash_{\mathrm{I}} A \iff \vdash_{\mathrm{S4}} A^* \iff \vdash_{\mathrm{Grz}} A^*$$

$$\mathrm{GL} := K + L$$

$$p' := p$$
$$(\neg A)' := \neg A'$$
$$(A \wedge B)' := A' \wedge B'$$
$$(A \vee B)' := A' \vee B'$$
$$(A \to B)' := A' \to B'$$
$$(\Box A)' := A' \wedge \Box A'$$

$$\vdash_{\mathrm{Grz}} A \iff \vdash_{\mathrm{GL}} A'$$
$$\vdash_{\mathrm{I}} A \iff \vdash_{\mathrm{GL}} (A^*)'$$

$$\boxed{\Box(\Box A \to A) \to \Box A \vdash_{\mathrm{GL}} \Box A \to \Box\Box A}$$

- $A \wedge \Box A \wedge \Box\Box A \to A \wedge \Box A$
- $A \to \Box(A \wedge \Box A) \to A \wedge \Box A$ $\qquad \Box(p \wedge q) \leftrightarrow \Box p \wedge \Box q$
- $\Box(\Box(A \wedge \Box A) \to A \wedge \Box A) \to \Box(A \wedge \Box A)$ $\qquad$ L
- $\Box A \to \Box(A \wedge \Box A)$
- $\Box A \to \Box\Box A$

## Theorem

$W, R \Vdash \Box(\Box A \to A) \to \Box A \iff R$ *is transitive &* $R$ *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 $\Box(\Box p \to p)$ — 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* $\mathrm{GL} \vdash A \to B$*, then there is a* $C$ *with* $\mathrm{Var}(C) \subset \mathrm{Var}(A) \cap \mathrm{Var}(B)$ *s.t.*

$$\mathrm{GL} \vdash A \to C \quad \textit{and} \quad \mathrm{GL} \vdash C \to B$$

## Corollary (Beth Definability)

*Assume* $\mathrm{GL} \vdash A(p) \wedge A(q) \to (p \leftrightarrow q)$ *where* $q \notin \mathrm{Var}(A)$ *and* $A(q)$ *is obtained from* $A(p)$ *by replacing all occurrences of* $p$ *by* $q$*. Then there exists a formula* $B$ *with* $\mathrm{Var}(B) \subset \mathrm{Var}(A) \setminus \{p\}$ *s.t.*

$$\mathrm{GL} \vdash A(p) \to (p \leftrightarrow B)$$

## Proof.

Let $B$ be an interpolant for $\mathrm{GL} \vdash A(p) \wedge p \to (A(q) \to q)$.

## Theorem (Uniqueness of Fixpoint)

*If $p$ occurs only boxed in $A(p)$ and $q \notin \mathrm{Var}(A)$, then*

$$\mathrm{GL} \vdash \boxdot\Big(\big(p \leftrightarrow A(p)\big) \wedge \big(q \leftrightarrow A(q)\big)\Big) \to (p \leftrightarrow q)$$

*where $\boxdot A := A \wedge \Box A$.*

## Corollary

*If $p$ occurs only boxed in $A(p)$, then*

$$\mathrm{GL} \vdash B \leftrightarrow A(B) \ \ \& \ \ \mathrm{GL} \vdash C \leftrightarrow A(C) \implies \mathrm{GL} \vdash B \leftrightarrow C$$

## Theorem (Existence of Fixpoint)

*If $p$ occurs only boxed in $A(p)$, then there exists a formula $B$ with $\mathrm{Var}(B) \subset \mathrm{Var}(A) \setminus \{p\}$ s.t.*

$$\mathrm{GL} \vdash B \leftrightarrow A(B)$$

$$\boxed{\text{Uniqueness of Fixpoint + Beth Definability} \implies \text{Existence of Fixpoint}}$$

$$\mathrm{GL} \vdash \neg\Box\bot \leftrightarrow \neg\Box(\neg\Box\bot) \qquad \mathrm{GL} \vdash \top \leftrightarrow \Box\top$$

# Soundness & Completeness

## Definition (Theorem & Local Syntactic Consequence)

- $\vdash_S A$
- $\Gamma \vdash_S A$ if $\vdash_S \bigwedge_{i=1}^{n} B_i \to A$ for some finite subset $\{B_1, \ldots, B_n\} \subset \Gamma$.

## Theorem (Soundness & Completeness)

*Let $S$ be the normal system $KX_1 \ldots X_n$ 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 $Z : \mathcal{M} \leftrightarrows \mathcal{M}'$ 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

$\not\leftrightarrow$

$\Box_a(\Diamond_b \top \wedge \Diamond_c \top)$

# 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 $\mathcal{F}$ : $\mathcal{F} \vDash A \iff \mathcal{F}$ 是反对称的。考虑如上两个框架：$\mathcal{F} \vDash A, \mathcal{F}' \nvDash A$，这意味着 $\mathcal{F}'$ 有赋值 $V'$ 和点 $v$ 使得 $\mathcal{F}', V', v \nvDash A$，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 $\mathcal{F}', V', v \leftrightarrows \mathcal{F}, V, w$，因而 $\mathcal{F}, V, w \nvDash A$，这与 $\mathcal{F} \vDash A$ 矛盾。

# Bisimulation

**Theorem (van Benthem Characterization Theorem)**

*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.*

**Theorem (van Benthem2007)**

*An abstract modal logic extending basic modal logic and satisfying compactness and bisimulation invariance is equally expressive as the basic modal logic $K$.*

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic
- Syntax
- Semantics
- Formal System
- Logic, Knowledge and Action

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 only good is knowledge and the only evil is ignorance." — *Socrates*

$\boxed{\text{know the unknown from the known}}$

- 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.

$$\exists x K K x \wedge \exists x K \neg K x \wedge \exists x \neg K \neg K x$$

- 知之为知之，不知为不知，是知也。

$$K p \rightarrow K K p \quad \& \quad \neg K p \rightarrow K \neg K p$$

"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 $G \subset \{1 \ldots n\}$ of agents, everyone in $G$ knows $A$:

$$E_G A \;:=\; \bigwedge_{i \in G} K_i A$$

$$R_E \;:=\; \bigcup_{i \in G} R_i$$

$$\mathcal{M}, w \Vdash E_G A \quad \text{iff} \;\; \forall v \in W : R_E w v \implies \mathcal{M}, v \Vdash A$$

# Distributed Knowledge

$$R_D \coloneqq \bigcap_{i \in G} R_i$$

$$\mathcal{M}, w \Vdash D_G A \quad \text{iff} \quad \forall v \in W : R_D wv \implies \mathcal{M}, v \Vdash A$$

$$w_2 \vDash K_1 p \wedge \neg K_1 q \wedge K_2 q \wedge \neg K_2 p \wedge D_{\{1,2\}}(p \wedge q)$$

# Common Knowledge

$$E_G^1 A := E_G A$$
$$E_G^{k+1} A := E_G E_G^k A$$
$$C_G A := \bigwedge_{k=1}^{\infty} E_G^k A$$

$$R^1 := R$$
$$R^{k+1} := R \circ R^k$$
$$R \circ S := \{(x, y) : \exists z (Rxz \wedge Szy)\}$$
$$R^* := \bigcup_{k=1}^{\infty} R^k$$

$$R_C := \left( \bigcup_{i \in G} R_i \right)^*$$

$$\mathcal{M}, w \Vdash C_G A \text{ iff } \forall v \in W : R_C wv \implies \mathcal{M}, v \Vdash A$$

## 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?

$$w_1 \vDash E_{\{1,2\}}p \wedge \neg C_{\{1,2\}}p$$

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?

$$(0,1) \overset{B}{\longleftrightarrow} (2,1) \overset{A}{\longleftrightarrow} \underline{(2,3)} \overset{B}{\longleftrightarrow} (4,3) \overset{A}{\longleftrightarrow} (4,5) \overset{B}{\longleftrightarrow} (6,5) \cdots$$

$$(2,3) \Vdash \neg K_B K_A K_B (x + y \leq 10)$$

$A$ 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，即使你知道我把你也想象成善意的，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。简而言之，如果出发点信息是公共知识，则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 nonempty 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 $w$.
- $K_i : \mathrm{P}(W) \to \mathrm{P}(W)$ 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 $\mathrm{S5} := K + T + 4 + 5$

  知之为知之(4)，不知为不知(5)，是知也

- Belief $K + D + 4 + 5$
- Common Knowledge

$$\mathrm{S5}$$
$$+$$
$$C_G A \leftrightarrow A \wedge E_G C_G A$$
$$+$$
$$A \wedge C_G(A \rightarrow E_G A) \rightarrow C_G A$$

- Distributed Knowledge

$$\mathrm{S5}$$
$$+$$
$$D_{\{i\}} A \leftrightarrow K_i A$$
$$+$$
$$D_G A \rightarrow D_{G'} A \ \text{ if } \ G \subset G'$$

# Knowledge vs Belief

1. $K(p \to q) \to Kp \to Kq$
2. $Kp \to p$
3. $Kp \to KKp$
4. $\neg Kp \to K\neg Kp$

1. $Kp \to Bp$
2. $Bp \to BKp$
3. $Bp \to KBp$
4. $\neg Kp \to K\neg Bp$

1. $B(p \to q) \to Bp \to Bq$
2. $Bp \to \neg B\neg p$
3. $Bp \to Bp$
4. $\neg Bp \to B\neg Bp$

$$\boxed{Bp \leftrightarrow \neg K\neg Kp}$$

# Fitch's Paradox

All knowable truths are known.

$\forall p(p \to \Diamond Kp) \vdash \forall p(p \to Kp)$

| | | |
|---|---|---|
| 1. | $K(p \wedge \neg Kp)$ | Assumption |
| 2. | $Kp \wedge K\neg Kp$ | $K(p \wedge q) \to Kp \wedge Kq$ |
| 3. | $Kp$ | |
| 4. | $K\neg Kp$ | |
| 5. | $\neg Kp$ | $Kp \to p$ |
| 6. | $\neg K(p \wedge \neg Kp)$ | |
| 7. | $\neg\Diamond K(p \wedge \neg Kp)$ | $\vdash \neg p \implies \vdash \neg\Diamond p$ |
| 8. | $p \wedge \neg Kp$ | Assumption |
| 9. | $\Diamond K(p \wedge \neg Kp)$ | $p \to \Diamond Kp$ |
| 10. | $\neg(p \wedge \neg Kp)$ | |
| 11. | $p \to Kp$ | |

# Fitch's Paradox

| | | |
|---|---|---|
| 1. | $B(p \wedge \neg Bp)$ | Assumption |
| 2. | $Bp \wedge B\neg Bp$ | $B(p \wedge q) \to Bp \wedge Bq$ |
| 3. | $Bp$ | |
| 4. | $BBp$ | $Bp \to BBp$ |
| 5. | $B\neg Bp$ | |
| 6. | $BBp \wedge B\neg Bp$ | |
| 7. | $\neg(BBp \wedge B\neg Bp)$ | $\neg(Bp \wedge B\neg p)$ |
| 8. | $\neg B(p \wedge \neg Bp)$ | |

# 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. $B\bot$

# 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

$$A ::= p \mid \neg A \mid A \wedge A \mid K_i A \mid [A]A$$

$$\mathcal{M}, w \Vdash [B]A \;\text{ iff }\; \mathcal{M}, w \Vdash B \implies \mathcal{M}\restriction_B, w \Vdash A$$

$$\mathcal{M}, w \Vdash \langle B \rangle A \;\text{ iff }\; \mathcal{M}, w \Vdash B \;\;\&\;\; \mathcal{M}\restriction_B, w \Vdash A$$

where

$$\mathcal{M}\restriction_B := \left(W', \{R'_i\}_{i \in G}, V'\right)$$

and

$$W' := \{w \in W : \mathcal{M}, w \Vdash B\} \quad R'_i := R_i\restriction_{W' \times W'} \quad V'(p) := V(p) \cap W'$$

# Muddy Children Problem

$\mathcal{M}, mmc \Vdash m_1 \wedge m_2 \wedge \neg m_3$

$\mathcal{M}, mmc \Vdash E_{\{1,2,3\}}P$

$\mathcal{M}, mmc \Vdash \neg C_{\{1,2,3\}}P$

$\mathcal{M}, mmc \Vdash \neg K_1 m_1 \wedge K_1 m_2$

$\mathcal{M}, mmc \Vdash K_1 K_3 m_2 \wedge K_1 \neg K_2 m_2$

$\mathcal{M}\restriction_P, mcc \Vdash K_1 m_1$

$\mathcal{M}\restriction_P, mmc \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$

$\mathcal{M}\restriction_P, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$

$\mathcal{M}\restriction_P \restriction_{\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3}, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$

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

$$\Vdash [p]C_G p$$

$$\Vdash [C_G A]C_G A$$

$$\overset{?}{\Vdash} [A]C_G A \qquad \overset{?}{\Vdash} [A]KA \qquad \overset{?}{\Vdash} [A]A$$

$$\mathcal{M}, w \Vdash (p \wedge \neg Kp) \wedge [p \wedge \neg Kp]\, Kp$$

**Remark:** If the goal of the announcing person was to "spread the truth of this formula," then this attempt was clearly unsuccessful.

# Unsuccessful Update

$$\mathcal{M}, w \Vdash (p \wedge \neg K_j p) \wedge K_i(p \wedge \neg K_j p) \wedge \left[K_i(p \wedge \neg K_j p)\right] K_i K_j p$$

- $\langle B\rangle A \leftrightarrow B \wedge [B]A$
- $[B](A \rightarrow C) \leftrightarrow ([B]A \rightarrow [B]C)$
- $[B]p \leftrightarrow (B \rightarrow p)$
- $[B]\neg A \leftrightarrow (B \rightarrow \neg A)$ ?
- $[B]\neg A \leftrightarrow \neg[B]A$ ?
- $[B]\neg A \leftrightarrow (B \rightarrow \neg[B]A)$
- $[B]K_i A \leftrightarrow (B \rightarrow K_i(B \rightarrow [B]A))$
- $[B]K_i A \leftrightarrow (B \rightarrow K_i[B]A)$
- $[B][C]A \leftrightarrow [B \wedge C]A$ ?
- $[B][C]A \leftrightarrow [B \wedge [B]C]A$
- $\dfrac{A}{[B]A}$ $\quad \dfrac{A(p)}{A(B)}$ ? $\quad \dfrac{A \leftrightarrow B}{[A]C \leftrightarrow [B]C}$ $\quad \dfrac{A \leftrightarrow B}{[C]A \leftrightarrow [C]B}$

# Public Announcement Logic (PAL)

## Axiom Schema

1. tautologies
2. $K_i(A \to B) \to K_i A \to K_i B$
3. $[B]p \leftrightarrow (B \to p)$
4. $[B]\neg A \leftrightarrow (B \to \neg[B]A)$
5. $[B](A \wedge C) \leftrightarrow [B]A \wedge [B]C$
6. $[B]K_i A \leftrightarrow (B \to K_i[B]A)$
7. $[B][C]A \leftrightarrow [B \wedge [B]C]A$

## Inference Rule

$$\frac{A \quad A \to B}{B}\ [\text{MP}] \qquad\qquad \frac{A}{K_i A}\ [\text{N}]$$

# Expressive Power

**Theorem**

PAL *is equally expressive as basic modal logic.*

**Proof.**

$$t(\top) = \top$$
$$t(p) = p$$
$$t(\neg A) = \neg t(A)$$
$$t(A \wedge B) = t(A) \wedge t(B)$$
$$t(K_i A) = K_i t(A)$$

$$t([B]\top) = t(B \to \top)$$
$$t([B]p) = t(B \to p)$$
$$t([B]\neg A) = t(B \to \neg[B]A)$$
$$t([B](A \wedge C)) = t([B]A \wedge [B]C)$$
$$t([B]K_i A) = t(B \to K_i[B]A)$$
$$t([B][C]A) = t([B \wedge [B]C]A)$$

$$\Vdash A \leftrightarrow t(A)$$

# Succinctness

**Theorem**

$\mathrm{PAL}$ *is complete w.r.t. the standard semantics of Public Announcement Logic.*

**Proof.**

$$\Vdash A \implies \Vdash t(A) \implies \vdash_{\mathrm{K}} t(A) \implies \vdash_{\mathrm{PAL}} t(A) \implies \vdash_{\mathrm{PAL}} A$$

**Theorem**

$\mathrm{PAL}$ *is exponentially more succinct than modal logic on arbitrary models.*

$$A_0 \coloneqq \top$$

$$A_{n+1} \coloneqq \langle\langle A_n \rangle \Diamond_1 \top \rangle \Diamond_2 \top$$

where $\Diamond_i A \coloneqq \neg K_i \neg A$ and $\langle B \rangle A \coloneqq \neg [B] \neg A$.

# Announcement and Common Knowledge

$$\frac{P \to [Q]A \quad P \wedge Q \to E_G P}{P \to [Q]C_G A}$$

'Common knowledge induction' is a special case.
Take $P := A$ and $Q := \top$.

$$C_G(A \to E_G A) \to A \to C_G A$$

# Propositional Dynamic Logic

$$A ::= \top \mid p \mid \neg A \mid A \wedge A \mid [\alpha]A$$
$$\alpha ::= a \mid A? \mid \alpha;\alpha \mid \alpha \cup \alpha \mid \alpha^*$$

$$\mathcal{M}, w \Vdash [\alpha]A \;\text{ iff }\; \forall v \in W : R_\alpha wv \implies \mathcal{M}, v \Vdash A$$

where

$$\begin{aligned}
R_{A?} &:= \{(w,w) : \mathcal{M}, w \Vdash A\} \\
R_{\alpha;\beta} &:= \big\{(w,v) : \exists u \big(R_\alpha wu \wedge R_\beta uv\big)\big\} \\
R_{\alpha\cup\beta} &:= R_\alpha \cup R_\beta \\
R_{\alpha^*} &:= \bigcup_{n=0}^{\infty} R_{\alpha^n}
\end{aligned}$$

# Propositional Dynamic Logic (PDL)

## Axiom Schema

1. tautologies
2. $[\alpha](A \to B) \to [\alpha]A \to [\alpha]B$
3. $[B?]A \leftrightarrow (B \to A)$
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. $A \wedge [\alpha^*](A \to [\alpha]A) \to [\alpha^*]A$

## Inference Rule

$$\frac{A \quad A \to B}{B}\ [\text{MP}] \qquad\qquad \frac{A}{[\alpha]A}\ [\text{N}]$$

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

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

$$\frac{A \to [\alpha^n]B, \quad n \in \omega}{A \to [\alpha^*]B} \text{ [IC]}$$

$$\frac{A}{[\alpha]A} \text{ [N]}$$

$$\frac{A}{\forall x A} \text{ [G]}$$

# Application

$$\begin{aligned}
\textbf{skip} &:= \top? \\
\textbf{fail} &:= \bot? \\
\textbf{if } B \textbf{ then } \alpha \textbf{ else } \beta &:= B?; \alpha \cup \neg B?; \beta \\
\textbf{while } B \textbf{ do } \alpha &:= (B?; \alpha)^*; \neg B? \\
\textbf{repeat } \alpha \textbf{ until } B &:= \alpha; (\neg B?; \alpha)^*; B? \\
\{A\}\ \alpha\ \{B\} &:= A \rightarrow [\alpha]B
\end{aligned}$$

$$[(x = m \wedge y = n)?]\left\langle (x \neq y?; (x > y?; x \leftarrow x - y) \cup (x < y?; y \leftarrow y - x))^*; x = y?\right\rangle x = \gcd(m, n)$$

# Hoare Logic

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}}$$

$$\frac{}{\{P[t/x]\}\ x := t\ \{P\}}$$

$$\frac{\{P\}\ \alpha\ \{Q\} \quad \{Q\}\ \beta\ \{R\}}{\{P\}\ \alpha; \beta\ \{R\}}$$

$$\frac{\{B \wedge P\}\ \alpha\ \{Q\} \quad \{\neg B \wedge P\}\ \beta\ \{Q\}}{\{P\}\ \textbf{if}\ B\ \textbf{then}\ \alpha\ \textbf{else}\ \beta\ \{Q\}}$$

$$\frac{P_1 \rightarrow P_2 \quad \{P_2\}\ \alpha\ \{Q_2\} \quad Q_2 \rightarrow Q_1}{\{P_1\}\ \alpha\ \{Q_1\}}$$

$$\frac{\{P \wedge B\}\ \alpha\ \{P\}}{\{P\}\ \textbf{while}\ B\ \textbf{do}\ \alpha\ \{\neg B \wedge P\}}$$

$$\{x = 4 \wedge y = 3\}\ \textbf{if}\ x < y\ \textbf{then}\ z := x; y := y + 1\ \textbf{else}\ z := y; z := z + 1\ \{x = 4 \wedge y = 3 \wedge z = 4\}$$

# 庄子《秋水》

## 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?
3. 庄子：子非我，安知我不知鱼之乐?
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。
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。

# 庄子《秋水》

- 惠子：子非鱼，安知鱼之乐?

$$\forall xy(K_x Hy \vee K_x \neg Hy \to Fy \to Fx)$$

$$\forall x(K_x Hf \vee K_x \neg Hf \to x = f)$$

- 庄子：子非我，安知我不知鱼之乐?

$$\forall xy(K_x K_y Hf \vee K_x \neg K_y Hf \to x = y)$$

- 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 $A$,

$$\frac{\forall xy\big(K_x A(y) \vee K_x \neg A(y) \to x = y\big) \quad h \neq z \quad z \neq f}{\neg K_z Hf \wedge \neg K_h \neg K_z Hf}$$

Moore's Paradox?

# Proof of God's Existence?

**安瑟尔谟**

当人们思考上帝时，人们是把上帝作为一切完美性的总和来思考的。因为不存在的必然是不完美的，所以必须把存在算在上帝的完美性之中。因此上帝存在。

# 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. $G(x) \coloneqq \forall X[P(X) \rightarrow X(x)]$

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.
$E(X,x) \coloneqq X(x) \wedge \forall Y(Y(x) \rightarrow \Box \forall y(X(y) \rightarrow Y(y)))$

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. $N(x) \coloneqq \forall X[E(X,x) \rightarrow \Box \exists y X(y)]$

Ax.5 Necessary existence is a positive property. $P(N)$

Th.4 Necessarily, God exists. $\Box \exists x G(x)$

# Pride and Prejudice

$$C_{\text{Human}}\Big(\forall x\Big(\text{Man}(x) \land \text{Single}(x) \land \text{Fortune}(x) \rightarrow \text{Desire}_x\Big(\exists y\big(\text{Woman}(y) \land \text{Marry}(x, y)\big)\Big)\Big)\Big)$$

— *Jane Austen*

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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

$$\mathscr{L}^{=} := \{=, (, )\} \cup \mathcal{V} \cup \overbrace{\mathcal{F}}^{signature}$$

where

$$\mathcal{V} := \{x_i : i \in \mathbb{N}\}$$

$$\mathcal{F} := \bigcup_{k \in \mathbb{N}} \mathcal{F}^k \quad \mathcal{F}^k := \{f_1^k, \ldots, f_n^k, (\ldots)\}$$

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

# Term & Formula

## Term $\mathcal{T}$

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

where $x \in \mathcal{V}$ and $f \in \mathcal{F}$.

## Well-Formed Formula $\mathrm{wff}$

$$A ::= s = t$$

where $s, t \in \mathcal{T}$.

# Semantics

A structure is a pair $\mathcal{M} := (M, I)$, where $M$ is a non-empty set, and $I$ is a mapping which assigns to each constant symbol an element $I(c) \in M$, and assigns each function symbol $f^k$ a $k$-ary function $I(f^k) : M^k \to M$.
We write $\mathcal{M} = (M, c^{\mathcal{M}}, f^{\mathcal{M}})$ for convenience.
An interpretation $(\mathcal{M}, \nu)$ is a structure $\mathcal{M}$ with a variable assignment $\nu : \mathcal{V} \to M$.
We extend $\nu$ to $\overline{\nu} : \mathcal{T} \to M$ by recursion as follows:

## Assignment over Terms

- $\overline{\nu}(x) = \nu(x)$
- $\overline{\nu}(c) = c^{\mathcal{M}}$
- $\overline{\nu}(f(t_1, \ldots, f_n)) = f^{\mathcal{M}}(\overline{\nu}(t_1), \ldots, \overline{\nu}(t_n))$

$$\begin{tikzcd}
\mathcal{T} \arrow[r, "\overline{\nu}"] \arrow[d, "\mathcal{E}_f"'] & M \arrow[d, "f^{\mathcal{M}}"] \\
\mathcal{T} \arrow[r, "\overline{\nu}"'] & M
\end{tikzcd}$$

# Semantics

- $\mathcal{M}, v \vDash s = t$ if $\overline{v}(s) = \overline{v}(t)$. (Satisfaction)
- $\mathcal{M} \vDash s = t$ if for all $v : \mathcal{M}, v \vDash s = t$. (True)
- $\mathcal{M} \vDash \mathrm{T}$ if for all $A \in \mathrm{T} : \mathcal{M} \vDash A$. (Model)
- $\mathrm{T} \vDash s = t$ if for all $\mathcal{M} : \mathcal{M} \vDash \mathrm{T} \implies \mathcal{M} \vDash s = t$.
- $\vDash s = t$ if $\emptyset \vDash s = t$. (Valid)

# Formal System

## Birkhoff's Rules

$$\frac{}{t = t}\ [\text{REFL}] \qquad \frac{s = t}{t = s}\ [\text{SYMM}]$$

$$\frac{r = s \qquad s = t}{r = t}\ [\text{TRANS}] \qquad \frac{s = t}{r(\ldots s \ldots) = r(\ldots t \ldots)}\ [\text{REP}]$$

$$\frac{r(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)}{r[t_1/x_1, \ldots, t_n/x_n] = s[t_1/x_1, \ldots, t_n/x_n]}\ [\text{SUBST}]$$

where $r(\ldots t \ldots)$ arises from $r(\ldots s \ldots)$ by replacing an occurrence of $s$ in $r$ by $t$.

$\mathrm{T} \vdash s = t$: An equation $s = t$ is a *theorem* of a theory $\mathrm{T}$ if $s = t$ is the last member of some deduction from $\mathrm{T}$.

# Meta-Theorems

**Theorem (Soundness & Completeness)**

$$\mathrm{T} \vdash s = t \iff \mathrm{T} \vDash s = t$$

- Determining Validity? Undecidable!

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic
- Boolean Algebra

Lambda Calculus and Combinatory Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Semigroup/Monoid/Group

Group $\mathscr{L} = \{e, \cdot, ^{-1}\}$

1. $\forall xyz : x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x : e \cdot x = x$
3. $\forall x : x \cdot e = x$
4. $\forall x : x^{-1} \cdot x = e$
5. $\forall x : x \cdot x^{-1} = e$

Group $\mathscr{L} = \{\cdot\}$

1. $\forall xyz : x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall xy \exists z : xz = y$
3. $\forall xy \exists z : zx = y$

Group $\mathscr{L} = \{e, \cdot\}$

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

$$\begin{array}{ccccccc} \dagger & \clubsuit & \divideontimes & \oint & \blacklozenge & \nabla & \$ \\ \hline \divideontimes & \blacklozenge & \nabla & \clubsuit & \oint & \$ & \dagger \end{array} \iff \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 3 & 5 & 6 & 2 & 4 & 7 & 1 \end{array} = (1,3,6,7)(2,5,4)$$

$$\{e, r, r^2, m, mr, mr^2\}$$

*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 symmetry 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 $(\mathrm{Aut}(G), 1_G, \circ)$ of symmetries.

$$\lambda_e = 1_G \qquad \lambda_{g \cdot h} = \lambda_g \circ \lambda_h \qquad (\lambda_g)^{-1} = \lambda_{g^{-1}}$$

# Ring/Boolean Ring BR

Ring $\mathscr{L} = \{0, 1, \oplus, \odot, -\}$

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 $\mathscr{L} = \{0, 1, \oplus, -, \odot, ^{-1}\}$

- $\forall xy : x \odot y = y \odot x$
- $\forall x \neq 0 : x \odot x^{-1} = x^{-1} \odot x = 1$

# Logic as Algebra — Boolean Algebra $\mathrm{BA}$

Boolean Algebra $\mathscr{L} = \{0, 1, +, \cdot, \overline{\phantom{x}}\}$

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

$$\begin{tikzcd}
\text{proposition} \arrow[r, "\text{Logic deduce}"] \arrow[d, "\text{translate}"'] & \text{proposition} \\
\text{equation} \arrow[r, "\text{calculate Algebra}"'] & \text{equation} \arrow[u, "\text{translate}"']
\end{tikzcd}$$

# Power Set Algebra

$$(\mathrm{P}(A), \emptyset, A, \cup, \cap, \overline{\phantom{x}})$$

$$x \oplus y \coloneqq (x \cdot \overline{y}) + (\overline{x} \cdot y)$$

$$x = y \iff x \oplus y = 0$$

# Boolean Ring $\mathrm{BR}$ vs Boolean Algebra $\mathrm{BA}$

$\mathrm{BR} \implies \mathrm{BA}$

$$x \cdot y = x \odot y$$
$$x + y = x \oplus y \oplus (x \odot y)$$
$$\overline{x} = 1 \oplus x$$

$\mathrm{BA} \implies \mathrm{BR}$

$$x \odot y = x \cdot y$$
$$x \oplus y = (x \cdot \overline{y}) + (\overline{x} \cdot y)$$
$$-x = x$$

# Boole's Four Main Theorems

$$\mathbf{x}^\sigma := x_1^{\sigma_1} \cdots x_n^{\sigma_n} \qquad x_i^{\sigma_i} := \begin{cases} x_i & \text{if } \sigma_i = 1 \\ \bar{x}_i & \text{if } \sigma_i = 0 \end{cases} \qquad \sigma : \{1, \ldots, n\} \to \{0, 1\}$$

1. Expansion

$$f(\mathbf{x}, \mathbf{y}) = \sum_\sigma f(\sigma, \mathbf{y}) \cdot \mathbf{x}^\sigma$$

2. Reduction

$$\bigwedge_i \big(f_i(\mathbf{x}) = 0\big) \iff \sum_i f_i(\mathbf{x}) = 0$$

3. Elimination

$$\exists \mathbf{x} \big(f(\mathbf{x}, \mathbf{y})\big) = 0 \iff \prod_\sigma f(\sigma, \mathbf{y}) = 0$$

4. Solution

$$q(\mathbf{y}) \cdot x = p(\mathbf{y})$$

$$\Updownarrow$$

$$p(\mathbf{y}) \cdot \big(p(\mathbf{y}) - q(\mathbf{y})\big) = 0 \quad \& \quad \exists v : x = \sum_{\tau : p(\tau) = q(\tau) \neq 0} \mathbf{y}^\tau + v \cdot \sum_{\tau : p(\tau) = q(\tau) = 0} \mathbf{y}^\tau$$

# Boole's Method

1. Translation. Translate premises into equational form.
   **A**: $x \cdot \overline{y} = 0$; **E**: $x \cdot y = 0$; **I**: $v = v \cdot x \cdot y$; **O**: $v = v \cdot x \cdot \overline{y}$.
2. Reduction. Combine the premise-equations into a single equation.

$$f_1(\mathbf{x}) = 0, \ldots, f_k(\mathbf{x}) = 0 \iff \sum_{i=1}^{k} f_i(\mathbf{x}) = 0$$

3. Elimination. Given the single premise $\sum_{i=1}^{k} f_i(\mathbf{y}, \mathbf{z}) = 0$, the most general conclution involving only $\mathbf{z}$ is $f(\mathbf{z}) = 0$, where

$$f(\mathbf{z}) := \left(\sum_{i=1}^{k} f_i(1, \ldots, 1, \mathbf{z})\right) \cdot \ldots \cdot \left(\sum_{i=1}^{k} f_i(0, \ldots, 0, \mathbf{z})\right)$$

4. Expansion. $f(\mathbf{z}) = f(1, \ldots, 1) \cdot z_1 \cdot \ldots \cdot z_n + \ldots + f(0, \ldots, 0) \cdot \overline{z}_1 \cdot \ldots \cdot \overline{z}_n$
5. Translation. Interpret the conclusion-equations as propositions.

# Boole's Method — Syllogism

$$\frac{MAP \quad SAM}{SAP}$$

$$\underbrace{m \cdot \overline{p} = 0 \qquad s \cdot \overline{m} = 0}$$

$$\Downarrow \textit{Reduction}$$

$$m \cdot \overline{p} + s \cdot \overline{m} = 0$$

$$\Downarrow \textit{Elimination}$$

$$(1 \cdot \overline{p} + s \cdot 0) \cdot (0 \cdot \overline{p} + s \cdot 1) = 0$$

$$\Downarrow \textit{Expansion}$$

$$(1 \cdot 0 + 1 \cdot 0) \cdot (0 \cdot 1 + 1 \cdot 1) \cdot s \cdot p + \ldots + (1 \cdot 1 + 0 \cdot 0) \cdot (0 \cdot 1 + 0 \cdot 1) \cdot \overline{s} \cdot \overline{p} = 0$$

$$\Downarrow$$

$$s \cdot \overline{p} = 0$$

$$s \cdot \overline{p} = s \cdot 1 \cdot \overline{p} = s \cdot (m + \overline{m}) \cdot \overline{p} = s \cdot m \cdot \overline{p} + s \cdot \overline{m} \cdot \overline{p} = 0 + 0 = 0$$

# Boole's Method — Syllogism

**A** : $x \cdot \overline{y} = 0$; **E** : $x \cdot y = 0$; **I** : $x \cdot y \neq 0$; **O** : $x \cdot \overline{y} \neq 0$.

$$\frac{PAM \quad SOM}{SOP}$$

$$p \cdot \overline{m} = s \cdot \overline{m} \cdot p + \overline{s} \cdot \overline{m} \cdot p = 0$$

$$s \cdot \overline{m} = s \cdot \overline{m} \cdot p + s \cdot \overline{m} \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$p \cdot \overline{m} + s \cdot \overline{m} = s \cdot \overline{m} \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$s \cdot \overline{m} \cdot \overline{p} + s \cdot m \cdot \overline{p} = s \cdot \overline{p} \neq 0$$

$$\frac{MEP \quad MIS}{SOP}$$

$$m \cdot p = s \cdot m \cdot p + \overline{s} \cdot m \cdot p = 0$$

$$m \cdot s = s \cdot m \cdot p + s \cdot m \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$m \cdot p + m \cdot s = s \cdot m \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$s \cdot m \cdot \overline{p} + s \cdot \overline{m} \cdot \overline{p} = s \cdot \overline{p} \neq 0$$

# Propositional Logic vs Boolean Algebra

$$
\begin{aligned}
(\bot)^* &:= 0 \\
(\top)^* &:= 1 \\
(p)^* &:= p \\
(\neg A)^* &:= \overline{A^*} \\
(A \vee B)^* &:= A^* + B^* \\
(A \wedge B)^* &:= A^* \cdot B^*
\end{aligned}
$$

$$
\begin{aligned}
(0)' &:= \bot \\
(1)' &:= \top \\
(p)' &:= p \\
\left(\overline{A}\right)' &:= \neg A' \\
(A + B)' &:= A' \vee B' \\
(A \cdot B)' &:= A' \wedge B'
\end{aligned}
$$

$$A \vdash B \iff \mathrm{BA} \vdash A^* \leq B^*$$

$$\mathrm{BA} \vdash A \leq B \iff A' \vdash B'$$

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.

$$A \rightarrow \neg B \wedge C$$
$$B \wedge D \rightarrow (A \wedge \neg C) \vee (\neg A \wedge C)$$
$$\neg B \wedge C \rightarrow \neg A \wedge D$$

$$A \cdot (B + \overline{C}) = 0$$
$$B \cdot D \cdot (\overline{A} \cdot \overline{C} + A \cdot C) = 0$$
$$\overline{B} \cdot C \cdot (A + \overline{D}) = 0$$

# General Solution?[9]

## Exercise — Save Yourself

You can say one sentence. If you lie I will hang you. If you tell the truth I will shoot you.

$$x = ? \implies \vDash (\neg x \to h) \land (x \to s) \land (s \leftrightarrow \neg h) \to \neg h \land \neg s$$

$$\vDash (\neg h \to h) \land (h \to s) \land (s \leftrightarrow \neg h) \to \neg h \land \neg s$$

## Problem (General Solution?)

$$x = ? \implies \vDash A(x)$$

[9] Brown: Boolean Reasoning.

# 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.

$$x = ? \implies \vDash (a \leftrightarrow x) \to k$$

# 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.

$$x = ? \implies \vDash (a \leftrightarrow x) \to k$$

## Solution

$$(a \cdot x + \overline{a} \cdot \overline{x}) \cdot \overline{k} = 0 \quad \implies \quad x = \overline{a} \cdot \overline{k} + \theta \cdot (\overline{a} + k)$$

$$\vDash (a \leftrightarrow \neg a \wedge \neg k) \to k$$

$$\vDash (a \leftrightarrow (a \to k)) \to k$$

# General Solution of Boolean Equation

## Theorem (General Solution of Boolean Equation)

*Given the Boolean function* $f : \{0,1\}^n \to \{0,1\}$, *define* $f_0, f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)$ *by means of the recursion*

$$f_n \coloneqq f$$
$$f_{i-1}(x_1, \ldots, x_{i-1}) \coloneqq f_i(x_1, \ldots, x_{i-1}, 0) \cdot f_i(x_1, \ldots, x_{i-1}, 1)$$

*then*

$$f_0 = 0$$
$$f_i(x_1, \ldots, x_{i-1}, 0) \leq x_i \leq \overline{f_i(x_1, \ldots, x_{i-1}, 1)} \qquad (i = 1, \ldots, n)$$

*is a genereal solution of* $f(x_1, \ldots, x_n) = 0$.

# Homomorphism

- Let $\mathcal{M}$ and $\mathcal{N}$ be Boolean algebras. A (Boolean) homomorphism is a mapping $h : M \to N$ s.t. for all $x, y \in M$:
  1. $h(0) = 0$
  2. $h(1) = 1$
  3. $h(\overline{x}) = \overline{h(x)}$
  4. $h(x + y) = h(x) + h(y)$
  5. $h(x \cdot y) = h(x) \cdot h(y)$
- If $h : M \rightarrowtail N$, it is an isomorphic embedding of $\mathcal{M}$ into $\mathcal{N}$.
- If $h : M \rightarrowtail\!\!\!\!\twoheadrightarrow N$, then $\mathcal{M}$ and $\mathcal{N}$ are isomorphic ($\mathcal{M} \cong \mathcal{N}$).

# Example — Lindenbaum Algebra of Propositional Logic

## Lindenbaum Algebra of Propositional Logic

$$\mathrm{Lin} := \left(\mathrm{wff}/{\sim}, 0, 1, +, \cdot, {}^{-}\right)$$

where

$$\begin{aligned}
\sim &:= \vdash \\
[A] &:= \left\{B \in \mathrm{wff} : A \sim B\right\} \\
\mathrm{wff}/{\sim} &:= \left\{[A] : A \in \mathrm{wff}\right\} \\
0 &:= [\bot] \\
1 &:= [\top] \\
\overline{[A]} &:= [\neg A] \\
[A] + [B] &:= [A \vee B] \\
[A] \cdot [B] &:= [A \wedge B]
\end{aligned}$$

$$\mathbf{2} := \left(\{0, 1\}, 0, 1, \max, \min, 1 - \right)$$

$$\mathrm{Lin} \overset{?}{\cong} \mathbf{2}$$

If $\nu$ is a truth assignment, then $h : [A] \mapsto \nu(A)$ is a homomorphism. If $h : \mathrm{Lin} \to \mathbf{2}$ 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 $\mathcal{B} = (B, 0, 1, +, \cdot, \overline{\phantom{x}})$ be a Boolean algebra. A subset $F \subset B$ is a filter if
  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 if $0 \notin F$.
- A proper filter $F$ is an ultrafilter if either $x \in F$ or $\overline{x} \in F$.
- Ultrafilter Theorem: every proper filter can be extended to an ultrafilter.

Ultrafilter theorem on Lindenbaum Algebra of Propositional Logic $\Longleftrightarrow$ 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 $\mathrm{Sto}(B) := \{w : w \text{ is an ultrafilter on } B\}$. Define a map $h : B \to \mathrm{P}\left(\mathrm{Sto}(B)\right)$ by

$$x \mapsto \{w \in \mathrm{Sto}(B) : x \in w\}$$

Then

$$\mathcal{B} \cong (h(B), \emptyset, \mathrm{Sto}(B), \cup, \cap, \setminus)$$

$\boxed{\vDash A \implies \vdash A}$

$$\nvdash A$$
$$\Downarrow$$
$$[A] \neq [\top]$$
$$\Downarrow$$
$$[\neg A] \neq [\bot]$$
$$\Downarrow$$
$$h([\neg A]) \neq \emptyset$$
$$\Downarrow$$
$$\exists w \in \mathrm{Sto}(\mathrm{Lin})\big([\neg A] \in w\big)$$
$$\Downarrow$$
$$\chi_w([\neg A]) = 1$$

**A set of wffs $\Gamma$ is satisfiable iff it is finitely satisfiable.**

Let $2 := \{0, 1\}$ be the discrete topology, and $2^{\mathcal{P}}$ be the product topology.
By Tychonoff Theorem, $2^{\mathcal{P}}$ is a compact, Hausdorff space.
For any wff $A$, let $\mathrm{Mod}(A) := \left\{\nu \in 2^{\mathcal{P}} : \nu(A) = 1\right\}$.
It can be shown that $\mathrm{Mod}(A)$ is clopen in $2^{\mathcal{P}}$.
By hypothesis, for each finite $\Gamma_0 \subset \Gamma$, there is a truth assignment making $\Gamma_0$ true, i.e. $\mathrm{Mod}(\Gamma_0) \neq \emptyset$. That is to say, $\{\mathrm{Mod}(A) : A \in \Gamma\}$ has the Finite Intersection Property. By the compactness of $2^{\mathcal{P}}$, $\mathrm{Mod}(\Gamma) \neq \emptyset$.

# Arrow's Impossibility Theorem

Let $N$ be a set of voters, and $C$ a set of candidates. A social welfare function (SWF) is $f : \mathcal{S}_C^N \to \mathcal{S}_C$, where $\mathcal{S}_C$ is the set of all permutations on $C$. We write $a \succ_i b$ to indicate that voter $i \in N$ ranks $a$ above $b$. Given $\sigma \in \mathcal{S}_C^N$, $N_{a \succ b}^{\sigma} := \{i \in N : a \succ_i b \text{ under } \sigma\}$.

- Unanimity ($\mathbf{U}$): If all voters rank $a$ above $b$, then so does society: $N_{a \succ b}^{\sigma} = N \implies a \succ_{f(\sigma)} b$.
- Irrelevant Alternatives ($\mathbf{IA}$): the relative social ranking of two candidates only depends on their relative individual rankings: $N_{a \succ b}^{\sigma} = N_{a \succ b}^{\sigma'} \implies \left(a \succ_{f(\sigma)} b \iff a \succ_{f(\sigma')} b\right)$.
- Nondictatorship ($\mathbf{ND}$): There is no $i \in N$ s.t. $\sigma_i = f(\sigma)$.

**Theorem (Arrow's Impossibility Theorem)**

*If $N$ is finite and $|C| \geq 3$, then any SWF that satisfy $\mathbf{U}$ and $\mathbf{IA}$ must be a dictatorship.*

# Proof Sketch of Arrow's Impossibility Theorem

1. We call a subset $A \subset N$ decisive if whenever all $x \in A$ present the same ranking, the SWF $f$ outputs that ranking.
2. The set of decisive sets of voters $\mathcal{F} := \{A \subset N : A \text{ is decisive}\}$ is an ultrafilter.
3. If $N$ is finite, then the ultrafilter $\mathcal{F}$ must be a principle ultrafilter.

Let $\mathcal{F}$ be an ultrafilter on $N$. We can define a SWF $f$ by declaring the output to be that unique permutation $\sigma$ with the property that $\{i \in N : \sigma_i = \sigma\} \in \mathcal{F}$.

**Theorem (Arrow's Theorem)**

*Assume $|C| \geq 3$. There is a $1-1$ correspondence between ultrafilters on $N$ and SWF that satisfy $\mathbf{U}$ and $\mathbf{IA}$. The non-dictatorship SWFs are those corresponding to non-principle ultrafilters. In particular, Arrow's impossibility theorem is equivalent to the assertion that all ultrafilters on a finite set are principle.*

# Social Choice Theory

- 计算社会选择理论：用计算复杂性防止坏情况的发生
- 用逻辑做投票协议验证
  - 隐私性：没有别人能知道你投的是谁
  - 无收据性：你不能证明给别人你投了特定人的票
  - 可核查性：你自己能检查你的票是不是被算进去了
  - 公平性：之前投票的部分结果不会影响之后投票的结果

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic
- Boolean Algebra

Lambda Calculus and Combinatory Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Church 1903-1995

- Lambda Calculus
- Church-Turing Thesis
- Undecidability
- Church-Rosser Theorem
- Frege-Church Ontology

# Lambda Calculus

$\mathscr{L} = \{\lambda, .\}$

## Definition ($\lambda$-Terms)

$$\Lambda ::= x \mid \Lambda\Lambda \mid \lambda x.\Lambda$$

**Notation**:

- $M_0 M_1 \cdots M_n$ denotes $(\cdots((M_0 M_1)M_2 \cdots M_n)$
- $\lambda x_0 x_1 \cdots x_n.M$ denotes $(\lambda x_0.(\lambda x_1.(\cdots(\lambda x_n.M))\cdots))$

## Definition (Free Variable)

$$\mathrm{Fv}(\Lambda) := \begin{cases} \{x\} & \text{if } \Lambda = x \\ \mathrm{Fv}(M) \cup \mathrm{Fv}(N) & \text{if } \Lambda = MN \\ \mathrm{Fv}(M) \setminus \{x\} & \text{if } \Lambda = \lambda x.M \end{cases}$$

# Reduction Rules

## Definition (Substitution)

$$y[N/x] = \begin{cases} N & \text{if } x = y \\ y & \text{otherwise} \end{cases}$$

$$(M_1 M_2)[N/x] = (M_1[N/x])\,(M_2[N/x])$$

$$(\lambda y.M)[N/x] = \begin{cases} \lambda y.M & \text{if } x = y \\ \lambda y.M[N/x] & \text{if } x \neq y \text{ and } y \notin \mathrm{Fv}(N) \end{cases}$$

## Reduction Rules

$$\lambda x.M \stackrel{\alpha}{=} \lambda y.M[y/x] \quad \text{if } y \text{ does not occur in } M.$$

$$(\lambda x.M)N \stackrel{\beta}{=} M[N/x]$$

$$\lambda x.Mx \stackrel{\eta}{=} M \quad \text{if } x \notin \mathrm{Fv}(M)$$

# $\lambda$-definability

$$\underline{n} \coloneqq \lambda f x.f^n x$$
$$f^0 x \coloneqq x$$
$$f^{n+1} x \coloneqq f(f^n x)$$

## Definition ($\lambda$-definability)

An $n$-ary function $f(x_1, \ldots, x_n)$ is $\lambda$-definable if there is a $\lambda$-term $F$ s.t. for all $a_1, \ldots, a_n$,

$$F\underline{a_1} \ldots \underline{a_n} \overset{\beta}{=} \underline{f(a_1, \ldots, a_n)}$$

$\boxed{\text{A function } f \text{ is computable iff it is } \lambda\text{-definable.}}$

$$\mathbf{succ} \coloneqq \lambda n f x.f(nfx)$$
$$\mathbf{add} \coloneqq \lambda m n f x.mf(nfx)$$
$$\mathbf{mult} \coloneqq \lambda m n f.m(nf)$$
$$\mathbf{exp} \coloneqq \lambda m n.nm$$

$$\begin{tikzcd}
\mathbb{N}^* \arrow[r, "f"] \arrow[d, "-"'] & \mathbb{N} \arrow[d, "-"] \\
\Lambda^* \arrow[r, "F"'] & \Lambda
\end{tikzcd}$$

# Combinator

## Definition (Combinator)

A $\lambda$-term $M$ is called a combinator if $\mathrm{Fv}(M) = \emptyset$.

$$\mathbf{K} = \lambda xy.x$$
$$\mathbf{S} = \lambda xyz.xz(yz)$$
$$\mathbf{I} = \lambda x.x$$
$$\omega = \lambda x.xx$$
$$\Omega = \omega\omega$$
$$\mathbf{Y} = \lambda y.(\omega(\lambda x.y(xx)))$$

$$\mathbf{F} = \lambda xy.y$$
$$\mathbf{T} = \mathbf{K}$$
$$\mathbf{B} = \mathbf{S}(\mathbf{KS})\mathbf{K}$$
$$\mathbf{C} = \mathbf{S}(\mathbf{BBS})(\mathbf{KK})$$
$$\mathbf{W} = \mathbf{SS}(\mathbf{SK})$$
$$\mathbf{D} = \mathbf{SII}$$
$$\mathbf{L} = \mathbf{D}(\mathbf{BDD})$$
$$\mathbf{neg} = \lambda x.x\mathbf{FT}$$
$$\mathbf{and} = \lambda xy.xy\mathbf{F}$$
$$\mathbf{or} = \lambda xy.x\mathbf{T}y$$
$$\mathbf{iszero} = \lambda x.x(\lambda y.\mathbf{F})\mathbf{T}$$

$$\iota = \lambda x.x\mathbf{SK}$$

$$\mathbf{K} = \iota(\iota(\iota\iota))$$
$$\mathbf{S} = \iota(\iota(\iota(\iota\iota)))$$

$$\iota\iota x = \mathbf{SK}(\mathbf{KK})x = x = \mathbf{I}x$$

# Exercises

- $\mathbf{B}xyz = x(yz)$ (composition)
- $\mathbf{C}xyz = xzy$ (swap)
- $\mathbf{W}xy = xyy$ (duplicate)
- $\mathbf{D}x = xx$ (doubling)
- $\mathbf{L} = \mathbf{LL}$ (self-doubling)

# Fixpoint Theorem in Lambda Calculus

**Theorem (Fixpoint Theorem in Lambda Calculus)**

*For every $\lambda$-term $F$ there is a $\lambda$-term $G$ s.t. $FG = G$.*

**Proof.**

Let $W := \lambda x.F(xx)$ and $G := WW$.

$$\mathbf{Y} = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx))$$

$$\mathbf{O} := \mathbf{YK} \implies \mathbf{O}x = \mathbf{O} \qquad \mathbf{L} := \mathbf{YD} \implies \mathbf{L} = \mathbf{LL}$$

**Corollary**

*For any $\lambda$-term $C(f, \vec{x})$, there exists a $\lambda$-term $M$ s.t. for all $\lambda$-terms $\vec{N}$*

$$M\vec{N} = C(M, \vec{N})$$

**Proof.**

Let $M := \mathbf{Y}(\lambda f\vec{x}.C(f, \vec{x}))$.

# Fixpoint Combinator

| | |
|---|---|
| $\mathbf{Y} = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx))$ | **Curry** |
| $\Theta = (\lambda xy.y(xxy))(\lambda xy.y(xxy))$ | **Turing** |

$$\mathbf{fac}\ n = \mathbf{if_then_else}\ (\mathbf{iszero}\ n)\ (1)\ (\mathbf{mult}\ n\ (\mathbf{fac}\ (\mathbf{pred}\ n)))$$

$$\mathbf{fac} = \lambda n.\mathbf{if_then_else}\ (\mathbf{iszero}\ n)\ (1)\ (\mathbf{mult}\ n\ (\mathbf{fac}\ (\mathbf{pred}\ n)))$$

$$\mathbf{fac} = (\lambda f.\lambda n.\mathbf{if_then_else}\ (\mathbf{iszero}\ n)\ (1)\ (\mathbf{mult}\ n\ (f\ (\mathbf{pred}\ n))))\ \mathbf{fac}$$

$$F := \lambda f.\lambda n.\mathbf{if_then_else}\ (\mathbf{iszero}\ n)\ (1)\ (\mathbf{mult}\ n\ (f\ (\mathbf{pred}\ n)))$$

$$\mathbf{fac} := \mathbf{Y}F$$

$$\mathbf{Y}F = F(\mathbf{Y}F)$$

$$\mathbf{fac} = F\ \mathbf{fac}$$

# Church-Rosser Theorem

We write $M \twoheadrightarrow_\beta N$ if $M$ $\beta$-reduces to $N$ in zero or more steps.

## Definition ($\beta$-nf)

A term is in $\beta$ normal form if it can't be $\beta$-reduced.
A term $M$ has a $\beta$ normal form if it $\beta$ reduces to some $N$ that is in $\beta$-nf.

## Theorem (Church-Rosser Theorem)

*Let $\twoheadrightarrow$ denote either $\twoheadrightarrow_\beta$ or $\twoheadrightarrow_{\beta\eta}$. Suppose $M, P, Q$ are $\lambda$-terms s.t. $M \twoheadrightarrow P$ and $M \twoheadrightarrow Q$. Then there exists a $\lambda$-term $N$ s.t. $P \twoheadrightarrow N$ and $Q \twoheadrightarrow N$.*

$$\begin{tikzcd}
 & M \arrow[dl, two heads] \arrow[dr, two heads] & \\
P \arrow[dr, two heads, dashed] & & Q \arrow[dl, two heads, dashed] \\
 & N &
\end{tikzcd}$$

# Fixpoint Theorem in Lambda Calculus

We write $\ulcorner M \urcorner$ to denote the $\lambda$-term representing the Gödel number of $M$.

**Theorem (Fixpoint Theorem in Lambda Calculus)**

*For every $\lambda$-term $F$ there is a $\lambda$-term $G$ s.t. $F\ulcorner G \urcorner = G$.*

**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. $A\ulcorner M \urcorner\ulcorner N \urcorner = \ulcorner MN \urcorner$.
Take $W := \lambda n.F(An(Cn))$. Then let $G := W\ulcorner W \urcorner$.

$$\begin{aligned} G &= W\ulcorner W \urcorner \\ &= F(A\ulcorner W \urcorner(C\ulcorner W \urcorner)) \\ &= F(A\ulcorner W \urcorner(\ulcorner\ulcorner W \urcorner\urcorner)) \\ &= F\ulcorner W\ulcorner W \urcorner\urcorner \\ &= F\ulcorner G \urcorner \end{aligned}$$

# Undecidability

## Theorem (Church1936)

*There is no term that will decide whether two terms have the same normal form.*

## Theorem (Church1936)

*There is no $\lambda$-term $D$ s.t. for all $\underline{n}$,*

$$D\underline{n} = \begin{cases} \underline{0} & \textit{if term with Gödel number } n \textit{ has a } \beta\textit{-nf} \\ \underline{1} & \textit{otherwise} \end{cases}$$

## Proof.

Suppose there was such a $D$. Then define $G := \lambda n.\mathbf{iszero}(Dn)\Omega\mathbf{I}$.
By the fixpoint theorem, there is $X$ s.t. $G(\ulcorner X \urcorner) = X$.
$X$ has a $\beta$-nf $\implies D\ulcorner X \urcorner = \underline{0} \implies G\ulcorner X \urcorner = \Omega \implies X$ has no $\beta$-nf
$X$ has no $\beta$-nf $\implies D\ulcorner X \urcorner = \underline{1} \implies G\ulcorner X \urcorner = \mathbf{I} \implies X$ has a $\beta$-nf

# Undecidability

**Theorem (Church1936)**

*There is no $D$ s.t. for all $M$,*

$$DM = \begin{cases} \mathbf{T} & \textit{if } M \textit{ has a normal form} \\ \mathbf{F} & \textit{otherwise} \end{cases}$$

**Proof.**

let $G := \mathbf{C}(\mathbf{C}(\mathbf{B}D(\mathbf{SII}))\Omega)\mathbf{I}$ and $X := GG$. Then

$$X = D(X)\Omega\mathbf{I}$$

If $X$ has a normal form, then $D(X)\Omega\mathbf{I} = \Omega$, but $\Omega$ has no normal form.
If $X$ has no normal form, then $D(X)\Omega\mathbf{I} = \mathbf{I}$, but $\mathbf{I}$ is in normal form.

## Theorem (Curry, Scott, Rice)

*Suppose $A \subset \Lambda$ is closed under $\overset{\beta}{=}$. Then $A$ is decidable iff $A = \Lambda$ or $A = \emptyset$.*

## Proof.

Define $B := \{M : M\ulcorner M \urcorner \in A\}$.
There exists a term $D \in \Lambda$ s.t.

$$M \in B \iff D\ulcorner M \urcorner = \underline{0}$$
$$M \notin B \iff D\ulcorner M \urcorner = \underline{1}$$

Let $P \in A$ and $Q \in \Lambda \setminus A$.

$$G := \lambda n.\mathbf{iszero}(Dn)QP$$

$$G \in B \iff D\ulcorner G \urcorner = \underline{0} \implies G\ulcorner G \urcorner = Q \implies G\ulcorner G \urcorner \notin A \implies G \notin B$$
$$G \notin B \iff D\ulcorner G \urcorner = \underline{1} \implies G\ulcorner G \urcorner = P \implies G\ulcorner G \urcorner \in A \implies G \in B$$

# Combinatory Logic

## Definition (Combinatory Terms)

$$\mathcal{C} ::= x \mid \mathbf{K} \mid \mathbf{S} \mid (\mathcal{C}\mathcal{C})$$

## 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 $\lambda$-term $P$ and variable $x$, there is a combinator $\lambda^* x.P$ s.t.*

$$(\lambda^* x.P)Q = P[Q/x]$$

## Proof.

$$\lambda^* x.P := \begin{cases} \mathbf{I} & \text{if } P \equiv x \\ \mathbf{K}P & \text{if } x \notin \mathrm{Fv}(P) \\ \mathbf{S}(\lambda^* x.M)(\lambda^* x.N) & \text{if } P \equiv MN \end{cases}$$

# Lambda Calculus subsumes Combinatory Logic

| $M$ | $(M)_\lambda$ |
|---|---|
| $\mathbf{I}$ | $\lambda x.x$ |
| $\mathbf{K}$ | $\lambda xy.x$ |
| $\mathbf{S}$ | $\lambda xyz.xz(yz)$ |
| $PQ$ | $(P)_\lambda(Q)_\lambda$ |

Table: translation: $()_\lambda : \mathrm{CL} \to \Lambda$

$$\vdash_{\mathrm{CL}} M = N \implies \vdash_\lambda (M)_\lambda = (N)_\lambda$$

But not the other way around:
$\nvdash_{\mathrm{CL}} \mathbf{SKI} = \mathbf{I}$, $\vdash_\lambda (\mathbf{SKI})_\lambda = (\mathbf{I})_\lambda$.

# Combinatory Logic subsumes Lambda Calculus

| $M$ | $(M)_{\mathrm{C}}$ |
|---|---|
| $x$ | $x$ |
| $\lambda x.P$ | $\lambda^* x.(P)_{\mathrm{C}}$ |
| $PQ$ | $(P)_{\mathrm{C}}(Q)_{\mathrm{C}}$ |

Table: translation: $()_{\mathrm{C}} : \Lambda \to \mathrm{CL}$

$$\vdash_{\lambda} M = N \iff \vdash_{\mathrm{CL}} (M)_{\mathrm{C}} = (N)_{\mathrm{C}}$$

# Simply-Typed Lambda Calculus (STLC)

- Type

$$T ::= 1 \mid T \times T \mid T \to T$$

- Term

$$\Lambda ::= x \mid * \mid \Lambda\Lambda \mid \lambda x.\Lambda \mid \langle \Lambda, \Lambda \rangle \mid \pi_1 \Lambda \mid \pi_2 \Lambda$$

- Judgment

$$x_1 : T_1, \ldots, x_n : T_n \vdash t : T$$

1. $t$ is a proof of $T$ from assumptions $T_1, \ldots, T_n$.
2. $t$ is a program of type $T$ with free variables $x_1, \ldots, x_n$ of type $T_1, \ldots, T_n$.

# The System of Simply-Typed Lambda Calculus

$$\frac{x : A \in \Gamma}{\Gamma \vdash x : A}\ \text{var} \qquad \frac{}{\Gamma \vdash * : 1}\ \text{unit}$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash u : B}{\Gamma \vdash \langle t, u \rangle : A \times B}\ \times^{+} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_1 t : A}\ \times^{-} \qquad \frac{\Gamma \vdash t : A \times B}{\Gamma \vdash \pi_2 t : B}\ \times^{-}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\ \text{abs} \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}\ \text{app}$$

## Reduction rules

$$(\lambda x.t)u \to t[u/x] \qquad (\beta_{\to})$$

$$\lambda x.tx \to t \quad \text{where } x \notin \mathrm{Fv}(t) \qquad (\eta_{\to})$$

$$\pi_1\langle t, u \rangle \to t \qquad (\beta_{\times,1})$$

$$\pi_2\langle t, u \rangle \to u \qquad (\beta_{\times,2})$$

$$\langle \pi_1 t, \pi_2 t \rangle \to t \qquad (\eta_{\times})$$

# What does $\beta/\eta$-reduction correspond to?

$$\dfrac{\dfrac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B} \qquad \Gamma \vdash u : A}{\Gamma \vdash (\lambda x.t)u : B} \quad \overset{\text{cut}}{\Longrightarrow} \quad \Gamma \vdash t[u/x] : B$$

$$\Gamma \vdash t : A \to B \quad \overset{\text{expansion}}{\Longrightarrow} \quad \dfrac{\dfrac{\Gamma, x : A \vdash t : A \to B \qquad \Gamma, x : A \vdash x : A}{\Gamma, x : A \vdash tx : B}}{\Gamma \vdash \lambda x.tx : A \to B}$$

# Example

$$
\dfrac{\dfrac{\dfrac{\dfrac{[x : A \to B \to C]^3 \qquad [z : A]^1}{xz : B \to C} \qquad \dfrac{[y : A \to B]^2 \qquad [z : A]^1}{yz : B}}{xz(yz) : C}}{\lambda z.xz(yz) : A \to C}\,[\to^+]^1}{\lambda y.\lambda z.xz(yz) : (A \to B) \to A \to C}\,[\to^+]^2}{\lambda x.\lambda y.\lambda z.xz(yz) : (A \to B \to C) \to (A \to B) \to A \to C}\,[\to^+]^3
$$

- $\mathbf{I} := \lambda x.x : A \to A$
- $\mathbf{K} := \lambda x.\lambda y.x : A \to B \to A$
- $\mathbf{S} := \lambda x.\lambda y.\lambda z.xz(yz) : (A \to B \to C) \to (A \to B) \to A \to C$

**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)**

$$\Gamma \vdash t : A \ \ \& \ \ t \twoheadrightarrow_\beta u \implies \Gamma \vdash u : A$$

**Theorem (Church-Rosser property for typable terms)**

*Suppose that $\Gamma \vdash t : A$. If $t \twoheadrightarrow_\beta u$ and $t \twoheadrightarrow_\beta v$, then there exists a term $w$ s.t. $u \twoheadrightarrow_\beta w, v \twoheadrightarrow_\beta w$ and $\Gamma \vdash w : A$.*

**Theorem (Strong Normalization Theorem)**

*If $\Gamma \vdash t : A$, then there is no infinite $\beta$-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.

| Type | Logic | Set | Homotopy |
|---|---|---|---|
| $A$ | proposition | set | space |
| $a : A$ | proof | element | point |
| $x : A \vdash B(x)$ | predicate | family of sets indexed by $A$ | fibration $B \to A$ with fibers $B(x)$ |
| $b(x) : B(x)$ | conditional proof | family of elements | section |
| $0, 1$ | $\bot, \top$ | $\emptyset, \{\emptyset\}$ | $\emptyset, *$ |
| $A + B$ | $A \vee B$ | disjoint union | coproduct |
| $A \times B$ | $A \wedge B$ | set of pairs | product space |
| $A \to B$ | $A \to B$ | set of functions | function space |
| $\sum_{x:A} B(x)$ | $\exists_{x:A} B(x)$ | disjoint sum | total space of fibration $B \to A$ |
| $\prod_{x:A} B(x)$ | $\forall_{x:A} B(x)$ | product | space of sections of fibration $B \to A$ |
| $\mathsf{Id}_A$ | equality $=$ | $\{(x, x) : x \in A\}$ | path space $A^I$ |

| Type | Category |
|---|---|
| coproduct types $A + B$ | binary coproducts |
| empty type $0$ | initial object |
| product types $A \times B$ | binary products |
| unit type $1$ | terminal object |
| natural numbers $\mathbb{N}$ | natural numbers object |
| identity type $(x = y)$ | diagonal/equalizer |
| function type $A \to B$ | exponential object (cartesian closure) |
| dependent sum $\sum_{x:A} B$ | left adjoint to pullback |
| dependent product $\prod_{x:A} B$ | right adjoint to pullback (lcc) |
| proposition type $\Omega$ | subobject classifier (elementary topos) |
| universe type $U$ | object classifier ($\infty$-topos) |
| coequalizer type $\mathrm{coeq}(f, g)$ | coequalizer |

# What is a Formalization of Math?

$$\begin{tikzcd}
\boxed{\begin{array}{c}\text{A formal}\\ \text{deduction}\\ \text{system}\end{array}} \arrow[r, "Semantics"] & \boxed{\begin{array}{c}\text{Class of objects}\\ \text{directly described}\\ \text{by the system}\end{array}} & \boxed{\text{Math}} \arrow[l, "Encoding"'] \\
Syntax \arrow[u] & &
\end{tikzcd}$$

- set theory
- category theory
- homotopy type theory

$$\mathrm{Contr}(X) \coloneqq \sum_{c:X} \prod_{x:X} \mathrm{Id}_X(c, x)$$

$$\mathrm{Fib}_f(y) \coloneqq \sum_{x:X} \mathrm{Id}_X(f(x), y)$$

$$X \simeq Y \coloneqq \sum_{f:X \to Y} \prod_{y:Y} \mathrm{Contr}\left(\mathrm{Fib}_f(y)\right)$$

$$X \cong Y \coloneqq \sum_{f:X \to Y} \sum_{g:Y \to X} \left[\left(\prod_{x:X} \mathrm{Id}_X(gfx, x)\right) \times \left(\prod_{y:Y} \mathrm{Id}_Y(fgy, y)\right)\right]$$

# 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*

- Structure Invariance Principle

$$(X \cong Y) \to \mathrm{Id}_U(X, Y)$$

  Isomorphic structures are identical.

- Voevodsky's Univalence Axiom

$$\mathrm{Id}_U(X, Y) \simeq (X \simeq Y)$$

  Identity is equivalent to equivalence.

# Consequences of the Univalence Axiom

- Function extensionality

$$\prod_{f,g:X\to Y} \mathrm{Id}(f,g) \simeq \left(\prod_{x:X} \mathrm{Id}_Y(fx,gx)\right)$$

- Propositional extensionality

$$\prod_{X,Y:\mathrm{Prop}} \mathrm{Id}(X,Y) \simeq (X \leftrightarrow Y)$$

- Paths are isomorphisms for sets

$$\prod_{X,Y:\mathrm{Set}} \mathrm{Id}(X,Y) \simeq (X \cong Y)$$

# Morning Star = Evening Star

$$\begin{tikzcd} m \star \arrow[r, bend left, "p"] \arrow[r, bend right, "q"'] \arrow[r, phantom, "\Downarrow"] & \star\ e \end{tikzcd}$$

$$\mathrm{Id}_A(m, e)$$

$$\mathrm{Id}_{\mathrm{Id}_A(m,e)}(p, q)$$

- 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.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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. M. Barr, C. Wells: Category Theory for Computing Science.
7. B. Fong, D. I. Spivak: Seven Sketches in Compositionality — An Invitation to Applied Category Theory.
8. D. I. Spivak: Category Theory for the Sciences.
9. F. W. Lawvere, S. H. Schanuel: Conceptual Mathematics.
10. F. W. Lawvere, R. Rosebrugh: Sets for Mathematics.
11. T. Streicher: Introduction to Category Theory and Categorical Loigc.
12. B. Jacobs: Categorical Logic and Type Theory.
13. R. Goldblatt: Topoi — The Categorical Analysis of Logic.
14. P. Johnstone: Sketches of an Elephant.
15. S. Mac Lane, I. Moerdijk: Sheaves in Geometry and Logic.
16. J. Adamek, H. Herrlich, G. E. Strecher: Abstract and Concrete Categories — The Joy of Cats.
17. nLab

# Category

## Definition (Category)

A category $\mathbf{C}$ consists of a class of objects $\mathrm{ob}(\mathbf{C})$ and a class of morphisms $\mathbf{C}(A, B) := \{f : A \to B\}$ for $A, B \in \mathrm{ob}(\mathbf{C})$ with the following properties:

- for $A \in \mathrm{ob}(\mathbf{C})$, there exists the identity $1_A : A \to A$;
- for $A, B, C \in \mathrm{ob}(\mathbf{C})$, there exists the composition $\circ : \mathbf{C}(A, B) \times \mathbf{C}(B, C) \to \mathbf{C}(A, C)$ such that
  - $\forall AB \in \mathrm{ob}(\mathbf{C}) \forall f : A \to B \left[ f \circ 1_A = f \ \& \ 1_B \circ f = f \right]$
  - $\forall ABCD \in \mathrm{ob}(\mathbf{C}) \forall fgh : A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \left[ h \circ (g \circ f) = (h \circ g) \circ f \right]$

$$\begin{tikzcd}
 & \bullet \arrow[r, "f"] & \bullet \\
\bullet \arrow[ur, "f"] \arrow[r, "f"'] & \bullet \arrow[u, "1"] \arrow[ur, "f"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & \bullet \arrow[dr, "h"] & \\
\bullet \arrow[ur, "g \circ f"] \arrow[rr, dashed, "f"] \arrow[rr, bend right, "h \circ (g \circ f) = (h \circ g) \circ f"'] & & \bullet \arrow[ul, "g"'] \arrow[d, "h \circ g"] \\
 & & \bullet
\end{tikzcd}$$

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.

# Examples

- A *discrete category* is a category that contains no morphisms apart from identities.
- A *monoid* $(M, \cdot, e)$ is a category that has only one object $\bullet$ s.t. $\mathbf{C}(\bullet, \bullet) = M$.
- A *group* is a category that has only one object and in which every morphism is an isomorphism.

- A *groupoid* is a category in which every morphism is an isomorphism.

# Examples

- $\mathbf{Set}$ sets and functions.
- $\mathbf{Rel}$ sets and relations.
- $\mathbf{Poset}$ partial order sets and monotone maps.
- $\mathbf{Graph}$ directed graphs and graph homomorphisms.
- $\mathbf{Type}$ types and computable functions.
- $\mathbf{Grp}$ groups and homomorphisms.
- $\mathbf{Ab}$ abelian groups and homomorphisms.
- $\mathbf{Rng}$ rings and ring homomorphisms.
- $\mathbf{Vect}_k$ vector spaces over a field $k$ and linear maps.
- $\mathbf{Diff}$ smooth manifolds and smooth maps.
- $\mathbf{Top}$ topological spaces and 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 | ✓ | ✓ | ✓ | ✓ | ✓ |

# 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 $\mathbf{C}$ is an internal criterion of identity, that is a criterion of identity for the entities within the category. From a categorical point of view, The identity relation is contextual. Entities are entities in a context.

# Opposite Category

## Definition (Opposite Category)

The *opposite category* $\mathbf{C}^{\mathrm{op}}$ of $\mathbf{C}$ is formed by reversing the morphisms. Formally, $\mathrm{ob}(\mathbf{C}^{\mathrm{op}}) = \mathrm{ob}(\mathbf{C})$, and for each morphism $f : A \to B$ of $\mathbf{C}$ a morphism $f^{\mathrm{op}} : B \to A$ in $\mathbf{C}^{\mathrm{op}}$, with the same identities and a composition defined (when possible) by $f^{\mathrm{op}} \circ g^{\mathrm{op}} := (g \circ f)^{\mathrm{op}}$.

$$
\begin{tikzcd}
A \arrow[d, "f"] \\
B \arrow[d, "g"] \\
C
\end{tikzcd}
\quad \leftrightsquigarrow \quad
\begin{tikzcd}
A \\
B \arrow[u, "f^{\mathrm{op}}"'] \\
C \arrow[u, "g^{\mathrm{op}}"']
\end{tikzcd}
$$

# Subcategory

## Definition (Subcategory)

We say that $\mathbf{C}'$ is a subcategory of $\mathbf{C}$ if:

1. $\mathrm{ob}(\mathbf{C}') \subset \mathrm{ob}(\mathbf{C})$;
2. $\mathbf{C}'(A, B) \subset \mathbf{C}(A, B)$ for $A, B \in \mathrm{ob}(\mathbf{C}')$;
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* if all objects of $\mathbf{C}'$ are also objects of $\mathbf{C}$.
$\mathbf{C}'$ is called *full* if for $A, B \in \mathrm{ob}(\mathbf{C}') : \mathbf{C}'(A, B) = \mathbf{C}(A, B)$.

# Monic / Epic / Bimorphism / Isomorphism

- A morphism $f : A \to B$ is a:
  1. monomorphism (monic) if $\forall X \forall g_1 g_2 : X \to A : fg_1 = fg_2 \implies g_1 = g_2$.
  2. epimorphism (epic) if $\forall X \forall g_1 g_2 : B \to X : g_1 f = g_2 f \implies g_1 = g_2$.
  3. bimorphism if $f$ is both monic and epic.
  4. isomorphism if $\exists g : B \to A : gf = 1_A \ \& \ fg = 1_B$.
  5. endomorphism if $A = B$.
  6. automorphism if $f$ is both an endomorphism and an isomorphism.
  7. retraction if a right inverse of $f$ exists, i.e. $\exists g : B \to A : fg = 1_B$.
  8. section if a left inverse of $f$ exists, i.e. $\exists g : B \to A : gf = 1_A$.

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[dr, "1_B"'] & A \arrow[d, "f"] \\ & B \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "1_A"'] & B \arrow[d, "g"] \\ & A \end{tikzcd}$$

- Every retraction is epic.
- Every section is a monic.
- 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.

# 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 $!_A : 0 \to A$.
- A *terminal object* in $\mathbf{C}$ is an object $1$ s.t. for every object $A$, there is a unique morphism $!_A : A \to 1$.
- If an object is both initial and terminal, it is called a *zero object*.
- An initial object $0$ is called a *strict initial object* if every morphism $x \to 0$ is an isomorphism.

- An initial object of $\mathbf{C}$ is a terminal object of $\mathbf{C}^{\mathrm{op}}$, and vice-versa.
- Initial and terminal objects are unique up to isomorphism.

# Product & Coproduct

- A *product* of $A$ and $B$ is an object $A \times B$ with a pair of morphisms $A \xleftarrow{\pi_1} A \times B \xrightarrow{\pi_2} B$ s.t

$$\forall C \forall f g : A \xleftarrow{f} C \xrightarrow{g} B \; \exists! u : C \to A \times B \big[ f = \pi_1 \circ u \;\; \& \;\; g = \pi_2 \circ u \big]$$

$$\begin{tikzcd}
A & A \times B \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & B \\
& C \arrow[ul, "f"] \arrow[u, dashed, "u"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Example: $\min\{x, y\}$ in $(\mathbb{R}, \leq)$. $x \cap y$ in $(\mathrm{P}(A), \subset)$. $\gcd(x, y)$ in $(\mathbb{N}, |)$.

- A *coproduct* of $A$ and $B$ is an object $A + B$ with a pair of morphisms $A \xrightarrow{\iota_1} A + B \xleftarrow{\iota_2} B$ s.t

$$\forall C \forall f g : A \xrightarrow{f} C \xleftarrow{g} B \; \exists! u : A + B \to C \big[ f = u \circ \iota_1 \;\; \& \;\; g = u \circ \iota_2 \big]$$

$$\begin{tikzcd}
A \arrow[r, "\iota_1"] \arrow[dr, "f"'] & A + B \arrow[d, dashed, "u"] & B \arrow[l, "\iota_2"'] \arrow[dl, "g"] \\
& C &
\end{tikzcd}$$

# Exponential & Cartesian Closed Category ($\mathbf{CCC}$)

- An *exponential* of objects $A, B$ is an object $B^A$ with a morphism $\mathrm{ev} : B^A \times A \to B$ s.t.

$$\forall C \forall f : C \times A \to B \; \exists! \hat{f} : C \to B^A \left[ \mathrm{ev} \circ (\hat{f} \times 1_A) = f \right]$$

$$\begin{tikzcd} B^A & B^A \times A \arrow[r, "\mathrm{ev}"] & B \\ C \arrow[u, dashed, "\hat{f}"] & C \times A \arrow[u, dashed, "\hat{f} \times 1_A"] \arrow[ur, "f"'] & \end{tikzcd}$$

- **Cartesian Closed Category** ($\mathbf{CCC}$) is a category with a terminal object, all products and all exponentials.
- **Bicartesian Closed Category** ($\mathbf{BCCC}$) is a $\mathbf{CCC}$ with an initial object and all coproducts, with products distributing over coproducts.

# Curry-Howard-Lambek Isomorphism

- **Objects** types/formulae $\top \mid A \times B \mid A \to B$
- **Morphisms** terms/proofs $1_A \mid ! \mid \mathrm{ev} \mid \pi_1 \mid \pi_2 \mid \hat{f} \mid \langle f, g \rangle \mid g \circ f$
  $f : A \to B \iff A \vdash B$

$$\frac{}{1_A : A \vdash A} \qquad \frac{}{! : A \vdash \top} \qquad \frac{f : A \vdash B \qquad g : B \vdash C}{g \circ f : A \vdash C}$$

$$\frac{f : A \vdash B \qquad g : A \vdash C}{\langle f, g \rangle : A \vdash B \times C} \qquad \frac{}{\pi_1 : A \times B \vdash A} \qquad \frac{}{\pi_2 : A \times B \vdash B}$$

$$\frac{f : A \times B \vdash C}{\hat{f} : A \vdash B \to C} \qquad \frac{}{\mathrm{ev} : (A \to B) \times A \vdash B}$$

# Curry-Howard-Lambek Isomorphism

| **Logic** | **Type Theory** | **Categories** |
|---|---|---|
| Formula | Type | Object |
| Proof | Term/Program | Morphism |
| true $\top$ | unit type $1$ | terminal object $1$ |
| false $\bot$ | bottom type $0$ | initial object $0$ |
| conjunction $\wedge$ | product type $\times$ | product $\times$ |
| disjunction $\vee$ | sum type $+$ | coproduct $+$ |
| implication $\rightarrow$ | function type $\rightarrow$ | exponential $B^A$ |
| cut-elimination | $\beta$-reduction | composition $\circ$ |
| modus ponens | application $\mathrm{app}$ | evaluation $\mathrm{ev}$ |

$$\begin{tikzcd}
\text{Logic} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \text{Computation} \arrow[dl, leftrightarrow] \\
& \text{Categories} &
\end{tikzcd}$$

*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** | **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 $\mathrm{Hom}$ | 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

# Internalization

- Every category has a set $\mathrm{Hom}(X, Y)$ 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 $f : X \to Y$ in $\mathrm{Hom}(X, Y)$ we can convert it into its *name* $\ulcorner f \urcorner : 1 \to Y^X$ in $\mathrm{Hom}(1, Y^X)$.
- In functional programming, objects are data types, morphisms are programs and any program $f : X \to Y$ have a name $\ulcorner f \urcorner \in \mathrm{Hom}(1, Y^X)$.
- *Internalization* is the process of taking math that lives in $\mathbf{Set}$ and moving it into some category $\mathbf{C}$.

# Groups in a Category

## Definition

Let $\mathbf{C}$ be a category with finite products. A group in $\mathbf{C}$ consists of objects and morphisms

$$\begin{tikzcd} G \times G \arrow[r, "m"] & G & G \arrow[l, "i"'] \\ & 1 \arrow[u, "e"'] & \end{tikzcd}$$

such that,

1. $m$ is associative,

$$\begin{tikzcd} (G \times G) \times G \arrow[rr, "\cong"] \arrow[d, "m \times 1_G"'] & & G \times (G \times G) \arrow[d, "1_G \times m"] \\ G \times G \arrow[r, "m"'] & G & G \times G \arrow[l, "m"] \end{tikzcd}$$

2. $e$ is a unit,

$$\begin{tikzcd} 1 \times G \arrow[d, "e \times 1_G"'] & G \arrow[l, "\cong"'] \arrow[r, "\cong"] \arrow[d, "1_G"] & G \times 1 \arrow[d, "1_G \times e"] \\ G \times G \arrow[r, "m"'] & G & G \times G \arrow[l, "m"] \end{tikzcd}$$

3. $i$ is an inverse,

$$\begin{tikzcd} G \times G \arrow[dd, "1_G \times i"'] & G \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, "!_G"] & G \times G \arrow[dd, "i \times 1_G"] \\ & 1 \arrow[d, "e"] & \\ G \times G \arrow[r, "m"'] & G & G \times G \arrow[l, "m"] \end{tikzcd}$$

# Groups in a Category

## Definition

A *group homomorphism* from $G$ to $H$ is a morphism $f : G \to H$ in $\mathbf{C}$ s.t.

$$\begin{tikzcd} G \times G \arrow[r, "f \times f"] \arrow[d, "m_1"'] & H \times H \arrow[d, "m_2"] \\ G \arrow[r, "f"'] & H \end{tikzcd} \qquad \begin{tikzcd} G \arrow[rr, "f"] & & H \\ & 1 \arrow[ul, "e_1"] \arrow[ur, "e_2"'] & \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "f"] \arrow[d, "i_1"'] & H \arrow[d, "i_2"] \\ G \arrow[r, "f"'] & H \end{tikzcd}$$

# Groups in a Category

- A group in the usual sense is a group in the category $\mathbf{Set}$.
- If $\mathbf{C}$ is the category of algebraic varieties, a group in $\mathbf{C}$ is an algebraic group.
- If $\mathbf{C} = \mathbf{Top}$, a group in $\mathbf{C}$ is a topological group.
- If $\mathbf{C} = \mathbf{Diff}$, a group in $\mathbf{C}$ is a Lie group.
- If $\mathbf{C} = \mathbf{Grp}$, a group in $\mathbf{C}$ is an abelian group.

Suppose $\circ$ is a group homomorphism $(G, \bullet) \times (G, \bullet) \to (G, \bullet)$. 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 $f : G \to H$ is exactly the same thing as a *group homomorphism*.
- What is a functor $R : G \to \mathbf{C}$ from a group $G$ to another category $\mathbf{C}$? If $\mathbf{C} = \mathbf{Vect}_k$, then $R$ is a "linear representation" of $G$.
- In general, any functor $R : G \to \mathbf{C}$ 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 $\mathbf{Set}$.

# Diagonalization[10]

## Definition (Weakly Point-Surjective)

A morphism $f : X \times X \to Y$ is *weakly point-surjective* if for every $g : X \to Y$, there is a $t : 1 \to X$ such that, for all $x : 1 \to X$:

$$gx = f\langle x, t\rangle$$

## Theorem (Lawvere's Fixpoint Theorem)

*Let* $\mathbf{C}$ *be a category with a terminal object and binary products. If* $f : X \times X \to Y$ *is weakly point-surjective, then every morphism* $\alpha : Y \to Y$ *has a fixpoint* $y : 1 \to Y$.

[10] Lawvere: Diagonal arguments and cartesian closed categories.
Yanofsky: A universal approach to self-referential paradoxes, incompleteness and fixed points.

# Lindenbaum Category

- Consider a first-order theory $\mathrm{T}$.
  We form $\mathbf{C}_{\mathrm{T}}$ a classifying category of $\mathrm{T}$ in the following way:
  The $\mathbf{C}_{\mathrm{T}}$-objects are generated by a sort object $A$ (more object if the theory is multi-sorted), and an object $2$.
  The $\mathbf{C}_{\mathrm{T}}$-morphisms are equivalence classes of (tuples of) formulas $A^n \to 2$ or terms $A^n \to A$ of $\mathrm{T}$.
  In particular, morphisms $1 \to 2$ are sentences, and morphisms $1 \to A$ are constant terms.
- A theory is *consistent* if $\mathrm{Hom}(1,2)$ contains at least two elements $\mathrm{Hom}(1,2) \supset \{\top, \bot\}$.
  A theory is *complete* if $\mathrm{Hom}(1,2) = \{\top, \bot\}$.

# Tarski & Gödel

- **Undefinability of** $\mathrm{sat}$**.** Suppose that the satisfiabilty predicate is definable in $\mathrm{T}$: $\vdash \mathrm{sat}(a, \ulcorner\varphi\urcorner) \leftrightarrow \varphi(a)$ for all $\varphi, a$.
  In categorical terms, we have a Gödel encoding $\ulcorner\urcorner : \mathrm{Hom}(A^n, 2) \to \mathrm{Hom}(1, A)$, and a formula $\mathrm{sat} : A^2 \to 2$, such that for $\varphi : A \to 2$ and $a : 1 \to A$, $\mathrm{sat}\langle a, \ulcorner\varphi\urcorner\rangle = \varphi a$.
  But this is exactly the condition for weak point-surjectivity!
- **Undefinability of** $\mathrm{truth}$**.** Suppose that $\mathrm{T}$ has a *truth* predicate: $\mathrm{true} \circ \ulcorner\varphi\urcorner = \varphi$ for all $\varphi \in \mathrm{Hom}(1, 2)$.
  Suppose that $\mathrm{T}$ supports "*substitution*": $\mathrm{subst}\langle a, \ulcorner\varphi\urcorner\rangle = \ulcorner\varphi(a)\urcorner$.
  Then we can define $\mathrm{sat} := \mathrm{true} \circ \mathrm{subst}$.
- **Incomplenteness** Suppose that *provability* is representable in $\mathrm{T}$: $\mathrm{T} \vdash \varphi \iff \mathrm{T} \vdash \mathrm{prov}(\ulcorner\varphi\urcorner)$.
  If $\mathrm{T}$ is complete, then $\varphi = \top$ or $\varphi = \bot$.
  And $\varphi = \top \implies \mathrm{prov}(\ulcorner\varphi\urcorner) = \top$, $\varphi = \bot \implies \mathrm{prov}(\ulcorner\varphi\urcorner) = \bot$.
  Therefore, for all $\varphi \in \mathrm{Hom}(1, 2) : \mathrm{prov} \circ \ulcorner\varphi\urcorner = \varphi$, i.e. $\mathrm{true}$ is $\mathrm{prov}$.

# Functor

## Definition (Functor)

A functor $F : \mathbf{C} \to \mathbf{D}$ between categories $\mathbf{C}$ and $\mathbf{D}$ is a mapping of objects to objects and morphisms to morphisms, in such a way that:

- $F(f : A \to B) = Ff : FA \to FB$
- $F(1_A) = 1_{FA}$
- $F(g \circ f) = Fg \circ Ff$

identity functor $1_{\mathbf{C}}$ and composition of functors

$$\begin{tikzcd} A \arrow[d, "f", "1_{\mathbf{C}}"'] \\ B \end{tikzcd} = \begin{tikzcd} A \arrow[d, "f"] \\ B \end{tikzcd} \qquad \begin{tikzcd} A \arrow[d, "f", "G \circ F"'] \\ B \end{tikzcd} = \begin{tikzcd} G(FA) \arrow[d, "G(Ff)"] \\ G(FB) \end{tikzcd}$$

# Functor — Example

- Let $\mathbf{Top}_*$ be the category of *pointed topological spaces*, where
  - objects $(X, x_0)$ are topological spaces with a distinguished *base point*.
  - a morphism $f : (X, x_0) \to (Y, y_0)$ is a continuous map $f : X \to Y$ which preserves the base point $f(x_0) = y_0$.
- A *loop in $X$ based at $x_0$* is a continuous function $l : [0,1] \to X$ such that $l(0) = l(1) = x_0$.
- Consider loops $l, m : [0,1] \to X$ at $x_0$. The *concatenation of loops* $lm : [0,1] \to X$ is the loop at $x_0$ given by:

$$lm(t) := \begin{cases} l(2t) & 0 \leq t \leq 1/2 \\ m(2t-1) & 1/2 < t \leq 1 \end{cases}$$

- A *homotopy* between the loops $l, m : [0,1] \to X$ at $x_0$ is a continuous map $h : [0,1] \times [0,1] \to X$ such that:
  - For $t \in [0,1]$, $h(0,t) = x_0$;
  - For $t \in [0,1]$, $h(1,t) = x_0$;
  - For $r \in [0,1]$, $h(r,0) = l(r)$ and $h(r,1) = m(r)$.
- Intuitively, $h$ is a way to deform the loop $l$ continuously into the loop $m$, while keeping the base points fixed.

# Functor — Example

- If there exists a homotopy $h$ between $l$ and $m$ we say that $l$ and $m$ are *homotopic*. This is an equivalence relation. We denote the space of homotopy classes by
$$\pi_1(X, x_0) := \{\text{all loops } l : [0,1] \to X \text{ based at } x_0\}/\text{homotopy}$$
- The concatenation of loops induces a concatenation between the homotopy classes $[l][m] = [lm]$ which equips $\pi_1(X, x_0)$ with a group structure. The unit is given by the constant loop at $x_0$, and the inverse is given by "walking the loop backwards" $l^{-1}(t) := l(1-t)$. We call $\pi_1(X, x_0)$ the *fundamental group of $X$ at $x_0$*.
- Let $f : (X, x_0) \to (Y, y_0)$ 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, $\pi_1(X, x_0) \to \pi_1(Y, y_0)$. 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 $\pi_1 : \mathbf{Top}_* \to \mathbf{Grp}$.
- $\pi_1(S^1) \cong (\mathbb{Z}, +)$ where $S^1 = \left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\right\}$.

## Theorem (Brouwer Fixpoint Theorem)

*Any continuous endomorphism of a 2-dimensional disk $D^2$ has a fixpoint.*

## Proof.

Suppose $f : D^2 \to D^2$ has no fixpoint. Then there is a continuous function $r : D^2 \to S^1$ 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 $r$ fixes the points on $S^1$. The function $r$ defines a retraction of the inclusion $i : S^1 \hookrightarrow D^2$.

Pick any basepoint on the boundary $S^1$ and apply the functor $\pi_1$ 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 $\mathbb{Z} \rightarrowtail 0$.

# 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 $f : (\mathbb{R}^n, x) \to (\mathbb{R}^m, y)$ we take smooth (i.e. differentiable infinitely many times) functions $\mathbb{R}^n \to \mathbb{R}^m$ such that $f(x) = y$.

The derivative is a functor $D : \mathbf{Euc}_* \to \mathbf{Vect}$ 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 $f : (\mathbb{R}^n, x) \to (\mathbb{R}^m, y)$ to the derivative $Df|_x$.

The derivative is functorial because:

- The derivative of the identity map $(\mathbb{R}^n, x) \to (\mathbb{R}^n, x)$ 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.,

$$\frac{\partial (g \circ f)^k}{\partial x^i} = \sum_{j=1}^{m} \frac{\partial g^k}{\partial y^j} \frac{\partial f^j}{\partial x^i} \quad \text{for } i = 1, \ldots, n \text{ and } k = 1, \ldots, p.$$

# Functors

## Definition

A functor $F : \mathbf{C} \to \mathbf{D}$ is:

- *faithful* if for $A, B \in \mathbf{C}$ each $F : \mathbf{C}(A, B) \to \mathbf{D}(FA, FB)$ is injective;
- *full* if for $A, B \in \mathbf{C}$ each $F : \mathbf{C}(A, B) \to \mathbf{D}(FA, FB)$ is surjective;
- an *embedding* if $F$ is full, faithful, and injective on objects;
- *essentially surjective* if for every $B \in \mathbf{D}$ there is $A \in \mathbf{C}$ s.t. $F(A) \cong B$;
- an *isomorphism* if there is a functor $G : \mathbf{D} \to \mathbf{C}$ 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 $F : \mathbf{C} \to \mathbf{D}$ is a functor then $FA \cong FB$.*

## Definition (Contravariant Functor)

A *contravariant functor* $F : \mathbf{C} \to \mathbf{D}$ between categories $\mathbf{C}$ and $\mathbf{D}$ is a functor $F : \mathbf{C}^{\mathrm{op}} \to \mathbf{D}$.

# Natural Transformation

## Definition (Natural Transformation)

Given categories and functors $F, G : \mathbf{C} \to \mathbf{D}$, a natural transformation $\alpha : F \to G$ is a family of $\mathbf{D}$-morphisms $\{\alpha_A : FA \to GA\}_{A \in \mathbf{C}}$, such that for all $\mathbf{C}$-morphisms $f : A \to B$, the diagram commutes:

$$\begin{tikzcd}
FA \arrow[r, "Ff"] \arrow[d, "\alpha_A"'] & FB \arrow[d, "\alpha_B"] \\
GA \arrow[r, "Gf"'] & GB
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbf{C} \arrow[r, bend left, "F"] \arrow[r, bend right, "G"'] \arrow[r, phantom, "\Downarrow\alpha"] & \mathbf{D}
\end{tikzcd}$$

A natural transformation is a mapping between functors preserving specified actions, symmetries, or other structures

# Equivalence of Categories

## Definition (Natural Isomorphism)

A natural transformation $\alpha : F \to G$ is a natural isomorphism ($F \cong G$) if each morphism $\alpha_A : FA \to GA$ is an isomorphism.

## Definition (Equivalence of Categories)

The categories $\mathbf{C}$ and $\mathbf{D}$ are equivalent ($\mathbf{C} \simeq \mathbf{D}$) if there are functors $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ and natural isomorphisms $G \circ F \cong 1_{\mathbf{C}}, F \circ G \cong 1_{\mathbf{D}}$.

- The categories $\mathbf{C}$ and $\mathbf{D}$ are isomorphic ($\mathbf{C} \cong \mathbf{D}$) if there are functors $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ 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".

## Theorem

*A functor $F : \mathbf{C} \to \mathbf{D}$ is an equivalence functor iff $F$ is fully faithful and essentially surjective on objects.*

## Proof.

( $\Longrightarrow$ ) Easy.
( $\Longleftarrow$ ) Suppose $F : \mathbf{C} \to \mathbf{D}$ is fully faithful and essentially surjective on objects. For each $B \in \mathbf{D}$, choose $GB \in \mathbf{C}$ and an isomorphism $\alpha_B : F(GB) \to B$. For $f : B \to B'$, let $Gf : GB \to GB'$ 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 $G : \mathbf{D} \to \mathbf{C}$.
In addition, $\alpha$ is a natural isomorphism $\alpha : FG \to 1_{\mathbf{D}}$.
It remains to show that $GF \cong 1_{\mathbf{C}}$. For $A \in \mathbf{C}$, let $\beta_A : A \to G(FA)$ be the unique morphism s.t. $F\beta_A = \alpha_{FA}^{-1}$. Because $F$ reflects isomorphisms, $\beta_A$ is an isomorphism for every $A$. Naturality of $\beta_A$ follows from functoriality of $F$ and naturality of $\alpha$.

# Vertical and Horizontal Composition

$$\begin{tikzcd}
\mathbf{C} \arrow[r, bend left=60, "F"] \arrow[r, bend right=60, "H"'] \arrow[r, "G"] \arrow[r, phantom, shift left=3, "\Downarrow\alpha"] \arrow[r, phantom, shift right=3, "\Downarrow\beta"] & \mathbf{D}
\end{tikzcd}
\Longrightarrow
\begin{tikzcd}
\mathbf{C} \arrow[r, bend left=60, "F"] \arrow[r, bend right=60, "H"'] \arrow[r, phantom, "\Downarrow\beta\alpha"] & \mathbf{D}
\end{tikzcd}$$

$$(\beta\alpha)_A := \beta_A \alpha_A$$

$$\begin{tikzcd}
\mathbf{C} \arrow[r, bend left=60, "F_1"] \arrow[r, bend right=60, "F_2"'] \arrow[r, phantom, "\Downarrow\alpha"] & \mathbf{D} \arrow[r, bend left=60, "G_1"] \arrow[r, bend right=60, "G_2"'] \arrow[r, phantom, "\Downarrow\beta"] & \mathbf{E}
\end{tikzcd}
\Longrightarrow
\begin{tikzcd}
\mathbf{C} \arrow[r, bend left=60, "G_1F_1"] \arrow[r, bend right=60, "G_2F_2"'] \arrow[r, phantom, "\Downarrow\beta\alpha"] & \mathbf{E}
\end{tikzcd}$$

$$\begin{tikzcd}
G_1F_1 \arrow[r, "G_1\alpha"] \arrow[d, "\beta F_1"'] \arrow[dr, "\beta\alpha"] & G_1F_2 \arrow[d, "\beta F_2"] \\
G_2F_1 \arrow[r, "G_2\alpha"'] & G_2F_2
\end{tikzcd}$$

# Whiskering

$$\begin{tikzcd} \mathbf{C} \arrow[r, "F"] & \mathbf{D} \arrow[r, bend left, "G_1"] \arrow[r, bend right, "G_2"'] \arrow[r, phantom, "\Downarrow\beta"] & \mathbf{E} \end{tikzcd} \qquad \begin{tikzcd} \mathbf{C} \arrow[r, bend left, "G_1"] \arrow[r, bend right, "G_2"'] \arrow[r, phantom, "\Downarrow\beta"] & \mathbf{D} \arrow[r, "F"] & \mathbf{E} \end{tikzcd}$$

The prewhiskering of $\beta$ by $F$, denoted $\beta F := \beta 1_F : G_1 F \to G_2 F$ (resp. the postwhiskering of $\beta$ by $F$, denoted $F\beta := 1_F \beta : F G_1 \to F G_2$) is defined as follows.

$$\begin{tikzcd} \mathbf{C} \arrow[r, bend left, "G_1 F"] \arrow[r, bend right, "G_2 F"'] \arrow[r, phantom, "\Downarrow\beta F"] & \mathbf{E} \end{tikzcd} \qquad \begin{tikzcd} \mathbf{C} \arrow[r, bend left, "F G_1"] \arrow[r, bend right, "F G_2"'] \arrow[r, phantom, "\Downarrow F\beta"] & \mathbf{E} \end{tikzcd}$$

$$(\beta F)_A := \beta_{F A}$$
$$(F\beta)_A := F\beta_A$$

# Vertical and Horizontal Composition

$$
\begin{tikzcd}
\mathbf{C} \arrow[r, bend left=60, "F_1"] \arrow[r, "G_1"] \arrow[r, bend right=60, "H_1"'] \arrow[r, phantom, shift left=3, "\Downarrow\alpha_1"] \arrow[r, phantom, shift right=3, "\Downarrow\beta_1"] & \mathbf{D} \arrow[r, bend left=60, "F_2"] \arrow[r, "G_2"] \arrow[r, bend right=60, "H_2"'] \arrow[r, phantom, shift left=3, "\Downarrow\alpha_2"] \arrow[r, phantom, shift right=3, "\Downarrow\beta_2"] & \mathbf{E}
\end{tikzcd}
$$

$$(\beta_2\beta_1)(\alpha_2\alpha_1) = (\beta_2\alpha_2)(\beta_1\alpha_1)$$

# Product Category

## Definition (Product Category)

Given categories $\mathbf{C}$ and $\mathbf{D}$, the product category $\mathbf{C} \times \mathbf{D}$ has

- objects $(A, B)$ for $A \in \mathbf{C}$ and $B \in \mathbf{D}$.
- morphisms $(f, g) : (A, B) \to (A', B')$ for $f : A \to A'$ and $g : B \to B'$.
- identity $1_{(A,B)} := (1_A, 1_B)$.
- composition $(f', g') \circ (f, g) := (f' \circ f, g' \circ g)$.

$$(A, B) \xrightarrow{(f,g)} (A', B') \xrightarrow{(f',g')} (A'', B'')$$

$$(A, B) \xrightarrow{(f' \circ f, g' \circ g)} (A'', B'')$$

# Functor Category

## Definition (Functor Category)

Given categories $\mathbf{C}$ and $\mathbf{D}$, the functor category $\mathbf{D}^{\mathbf{C}}$ has

- objects: functors $F : \mathbf{C} \to \mathbf{D}$
- morphisms: natural transformations $\alpha : F \to G$
- identity natural transformation $(1_F)_A \coloneqq 1_{FA}$
  given a functor $F : \mathbf{C} \to \mathbf{D}$, define $1_F : F \to F$ with
  $(1_F)_A \coloneqq FA \xrightarrow{1_{FA}} FA$.
- composition of natural transformations $(\beta \circ \alpha)_A \coloneqq \beta_A \circ \alpha_A$
  given functors $F, G, H : \mathbf{C} \to \mathbf{D}$ and natural transformations
  $F \xrightarrow{\alpha} G \xrightarrow{\beta} H$, define $\beta \circ \alpha : F \to H$ with

$$(\beta \circ \alpha)_A \coloneqq FA \xrightarrow{\alpha_A} GA \xrightarrow{\beta_A} HA$$

# The Category of Small Categories $\mathbf{Cat}$

- Assume there is an infinite sequence $U_0 \in U_1 \in U_2 \in \ldots$ 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 $\mathbf{C}$ is locally small if $\forall AB \in \mathbf{C} : \mathbf{C}(A, B) \in \mathbf{Set}_0$.
- A category $\mathbf{C}$ is small if it is both locally small and $\mathrm{ob}(\mathbf{C}) \in \mathbf{Set}_0$.

**Definition (The Category of Small Categories $\mathbf{Cat}$)**

The category of small categories $\mathbf{Cat}$ has

- objects: small categories.
- morphisms: functors $F : \mathbf{C} \to \mathbf{D}$.
- identity and composition as for functors.

$\mathbf{Cat}$ is large.

# Cat is CCC

- $\mathbf{Cat}$ has a terminal object $\mathbf{1} := \overset{1}{\bullet}\circlearrowleft$ .
- $\mathbf{Cat}$ has products.
- There is a functor $\mathrm{ev} : \mathbf{D}^{\mathbf{C}} \times \mathbf{C} \to \mathbf{D}$ that makes $\mathbf{D}^{\mathbf{C}}$ the exponential.
- $\mathbf{Cat}$ is cartesian closed.

# Equalizer

- A *fork* in a category $\mathbf{C}$ consists of $C \xrightarrow{h} A \underset{g}{\overset{f}{\rightrightarrows}} B$ s.t. $fh = gh$.
- Let $\mathbf{C}$ be a category and take $A \underset{g}{\overset{f}{\rightrightarrows}} B$. An *equalizer* of $f$ and $g$ is an object $E$ with a morphism $E \xrightarrow{e} A$ s.t. $E \xrightarrow{e} A \underset{g}{\overset{f}{\rightrightarrows}} B$ is a fork, and for any fork $C \xrightarrow{h} A \underset{g}{\overset{f}{\rightrightarrows}} B$, there exists a unique morphism $C \xrightarrow{u} E$ s.t.

$$\begin{tikzcd}
\mathbf{C} \arrow[d, dashed, "u"'] \arrow[dr, "h"] & & \\
E \arrow[r, "e"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B
\end{tikzcd}$$

Example: In $\mathbf{Set}$, $E := \{x \in A : f(x) = g(x)\}$.

# Coequalizer

- A *cofork* in a category $\mathbf{C}$ consists of $A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{h} C$ s.t. $hf = hg$.
- Let $\mathbf{C}$ be a category and take $A \underset{g}{\overset{f}{\rightrightarrows}} B$. An *coequalizer* of $f$ and $g$ is an object $Q$ with a morphism $B \xrightarrow{q} Q$ s.t. $A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{q} Q$ is a cofork, and for any cofork $A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{h} C$, there exists a unique morphism $Q \xrightarrow{u} C$ s.t.

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \arrow[r, "q"] \arrow[dr, "h"'] & Q \arrow[d, dashed, "u"] \\ & & C \end{tikzcd}$$

Example: In $\mathbf{Set}$, let $y \sim y' := \exists x\big(f(x) = y \wedge g(x) = y'\big)$. Then $Q := B/{\sim}$ is a coequalizer.

**Theorem**

*If* $C \xrightarrow{h} A \underset{g}{\overset{f}{\rightrightarrows}} B$ *is an equalizer,* $h$ *is monic.*

**Theorem**

*If* $A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{h} C$ *is a coequalizer,* $h$ *is epic.*

# Pullback

Let $\mathbf{C}$ be a category. A *pullback* of
$$\begin{tikzcd} & B \arrow[d, "g"] \\ A \arrow[r, "f"] & C \end{tikzcd}$$
is an object $P$ with $P \xrightarrow{p_1} A$ and $P \xrightarrow{p_2} B$ s.t.
$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$
, and for any
$$\begin{tikzcd} Q \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$
there is a unique morphism $Q \xrightarrow{u} P$ s.t.
$$\begin{tikzcd} Q \arrow[dr, dashed, "u"] \arrow[drr, bend left, "q_2"] \arrow[ddr, bend right, "q_1"'] & & \\ & P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ & A \arrow[r, "f"'] & C \end{tikzcd}$$
.

Example: In $\mathbf{Set}$, $P := A \times_C B := \{(x, y) \in A \times B : f(x) = g(y)\}$.

# Pullback

$$\begin{tikzcd} P \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

In $\mathbf{Set}$, $P := A \times_C B := \{(x, y) \in A \times B : f(x) = g(y)\}$.
We also say that we pull back $g$ along $f$ and think of $f^*g : f^*B \to A$ as the inverse image of $B$ along $f$. This terminology is explained by looking at the pullback of a subset inclusion $i : B \hookrightarrow C$.

$$\begin{tikzcd} f^*B \arrow[r, "p_2"] \arrow[d, "f^*g"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd} \qquad \begin{tikzcd} f^*B \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, hook, "i"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

In this case $\{(x, y) \in A \times B : fx = y\} \cong \{x \in A : fx \in B\} = f^*B$.

# products & equalizers $\implies$ pullbacks

## Theorem

*In a category with products and equalizers, given* $A \xrightarrow{f} C \xleftarrow{g} B$ *, consider the diagram:*

$$\begin{tikzcd}
E \arrow[dr, "e"] & & \\
& A \times B \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & B \arrow[d, "g"] \\
& A \arrow[r, "f"'] & C
\end{tikzcd}$$

*Then* $e : E \to A \times B$ *is an equalizer of* $A \times B \underset{g \circ \pi_2}{\overset{f \circ \pi_1}{\rightrightarrows}} C$ *iff*

$$\begin{tikzcd}
E \arrow[r, "\pi_2 \circ e"] \arrow[d, "\pi_1 \circ e"'] \arrow[dr, phantom, "\lrcorner"] & B \arrow[d, "g"] \\
A \arrow[r, "f"'] & C
\end{tikzcd}$$

*is a pullback.*

# pullbacks & terminal objects $\Longrightarrow$ products & equalizers

- $A \times B \cong A \times_1 B$

$$\begin{tikzcd} A \times B \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "!_B"] \\ A \arrow[r, "!_A"'] & 1 \end{tikzcd}$$

- The equalizer $E \overset{e}{\rightarrowtail} A \underset{g}{\overset{f}{\rightrightarrows}} B$ is constructed as the following pullback,

$$\begin{tikzcd} E \arrow[r, "h"] \arrow[d, "e"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "\Delta"] \\ A \arrow[r, "\langle f, g \rangle"'] & B \times B \end{tikzcd}$$

## Theorem

$$\begin{tikzcd} A \times_C B \arrow[r, "q"] \arrow[d, "p"'] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, "g"] \\ A \arrow[r, "f"'] & C \end{tikzcd}$$

*If $g$ is monic, so is $p$.*

## Theorem

$$\begin{tikzcd} F \arrow[r] \arrow[d] & E \arrow[r] \arrow[d] & D \arrow[d] \\ A \arrow[r] & B \arrow[r] & C \end{tikzcd}$$

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

Let $\mathbf{C}$ be a category. A *pushout* of
$$\begin{tikzcd} C \arrow[r, "g"] \arrow[d, "f"'] & B \\ A & \end{tikzcd}$$
is an object $P$ with

$A \xrightarrow{p_1} P$ and $B \xrightarrow{p_2} P$ s.t.
$$\begin{tikzcd} C \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[d, "p_2"] \\ A \arrow[r, "p_1"'] \arrow[ur, phantom, "\ulcorner"] & P \end{tikzcd}$$
, and for any
$$\begin{tikzcd} C \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[d, "q_2"] \\ A \arrow[r, "q_1"'] \arrow[ur, phantom, "\ulcorner"] & Q \end{tikzcd}$$

there is a unique morphism $P \xrightarrow{u} Q$ s.t.
$$\begin{tikzcd} C \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[d, "p_2"] \arrow[ddr, bend left, "q_2"] & \\ A \arrow[r, "p_1"'] \arrow[drr, bend right, "q_1"'] \arrow[ur, phantom, "\ulcorner"] & P \arrow[dr, dashed, "u"] & \\ & & Q \end{tikzcd}$$
.

# Cone

- A *diagram* of a small category $\mathbf{I}$ in category $\mathbf{C}$ is a functor $D : \mathbf{I} \to \mathbf{C}$.
- 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.

$$\begin{tikzcd} & D_i \arrow[d, "Df"] \\ C \arrow[ur, "c_i"] \arrow[r, "c_j"'] & D_j \end{tikzcd}$$

A cone $(C, c)$ over $D$ can be taken as a natural transformation $c : \Delta C \to D$.

- A morphism of cones $\theta : (C, c) \to (C', c')$ is a morphism $\theta$ s.t.

$$\begin{tikzcd} C \arrow[r, "\theta"] \arrow[dr, "c_i"'] & C' \arrow[d, "c'_i"] \\ & D_i \end{tikzcd}$$

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.

$$\begin{tikzcd} D_i \arrow[r, "c_i"] \arrow[d, "Df"'] & C \\ D_j \arrow[ur, "c_j"'] & \end{tikzcd}$$

A cocone $(C, c)$ over $D$ can be taken as a natural transformation $c : D \to \Delta C$.

- A morphism of cocones $\theta : (C, c) \to (C', c')$ is a morphism $\theta$ s.t.

$$\begin{tikzcd} C \arrow[r, "\theta"] & C' \\ & D_i \arrow[ul, "c_i"] \arrow[u, "c'_i"'] \end{tikzcd}$$

Then we have a category $\mathbf{Cocone}(D)$ of cones over $D$.

# Limit

- A *limit* $\left(\varprojlim D, p\right)$ for a diagram $D : \mathbf{I} \to \mathbf{C}$ 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 $i \in \mathbf{I}$.

$$\begin{tikzcd}
 & & D_i \\
C \arrow[urr, "c_i"] \arrow[r, dashed, "u"] \arrow[drr, "c_j"'] & \varprojlim D \arrow[ur, "p_i"] \arrow[dr, "p_j"'] & \\
 & & D_j
\end{tikzcd}$$

# Colimit

- A *colimit* $\left(\varinjlim D, p\right)$ for a diagram $D : \mathbf{I} \to \mathbf{C}$ 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 $i \in \mathbf{I}$.

# Examples

- Take $\mathbf{I} := \emptyset$. Then a limit for $D : \mathbf{I} \to \mathbf{C}$ is a terminal object in $\mathbf{C}$: $\varprojlim D \cong 1$.
- Take $\mathbf{I} := \boxed{\bullet \qquad \bullet}$. Then a limit for $D$ is a product $\varprojlim D \cong D_1 \times D_2$.
- Take $\mathbf{I} := \boxed{\bullet \underset{g}{\overset{f}{\rightrightarrows}} \bullet}$. Then a cone over $D$ is
$$\begin{tikzcd} & C \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ D_1 \arrow[rr, shift left, "f"] \arrow[rr, shift right, "g"'] & & D_2 \end{tikzcd}.$$
Thus a limit for $D$ is an equalizer for $f, g$.
- Take $\mathbf{I} := \boxed{\begin{tikzcd} & \bullet \arrow[d] \\ \bullet \arrow[r] & \bullet \end{tikzcd}}$. Then a limit for $D$ is a pullback.

# products & equalizers $\implies$ limits

Let $D : \mathbf{I} \to \mathbf{C}$. 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 $\alpha : i \to j \in \operatorname{mor} \mathbf{I}$.

$$\begin{tikzcd}
C \arrow[d, dashed, "u"'] \arrow[dr, "c"] & & & \\
E \arrow[r, tail, "e"] & \prod\limits_{i \in \operatorname{ob}\mathbf{I}} D_i \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] \arrow[d, "\pi_i"'] \arrow[dr, "\pi_j"] & \prod\limits_{\alpha : i \to j \in \operatorname{mor}\mathbf{I}} D_j \arrow[d, "\pi_\alpha"] & \\
& D_i \arrow[r, "D\alpha"'] \arrow[ur, phantom, "?"] & D_j &
\end{tikzcd}$$

but generally $D\alpha \circ \pi_i \neq \pi_j$

Take any $c : C \to \prod\limits_{i \in \operatorname{ob}\mathbf{I}} D_i$. For $\alpha : i \to j$ 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 $c : C \to \prod\limits_{i \in \operatorname{ob}\mathbf{I}} D_i$, there is a unique $u : C \to E$ s.t. $c = e \circ u$.
Then $u : C \to E$ is also the required factorization of the cone $(C, c_i)$ through $(E, e_i)$ s.t. $c_i = e_i \circ u$. Therefore $E = \varprojlim D$.

# Preserving/Reflecting/Creating Limits

- A functor $F : \mathbf{C} \to \mathbf{D}$ is said to *preserve limits of* $\mathbf{I}$ iff, for all diagrams $D : \mathbf{I} \to \mathbf{D}$ and all cones $(C, c)$ over $D$,

$$(C, c) \text{ is a limit over } D \Longrightarrow (FC, Fc) \text{ is a limit over } FD : \mathbf{I} \to \mathbf{D}$$

- A functor $F : \mathbf{C} \to \mathbf{D}$ is said to *reflect limits of* $\mathbf{I}$ iff, for all diagrams $D : \mathbf{I} \to \mathbf{D}$ and all cones $(C, c)$ over $D$,

$$(C, c) \text{ is a limit over } D \Longleftarrow (FC, Fc) \text{ is a limit over } FD : \mathbf{I} \to \mathbf{D}$$

- A functor $F : \mathbf{C} \to \mathbf{D}$ is said to *create limits of* $\mathbf{I}$ iff, for all diagrams $D : \mathbf{I} \to \mathbf{C}$, if $(M, m)$ is a limit cone over $FD : \mathbf{I} \to \mathbf{D}$, 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* if it has all small limits.
- A functor is *continuous* if it preserves all small limits.

Obviously, if $F$ preserves limits then $F\left(\varprojlim D\right) \cong \varprojlim(FD)$.

**Theorem**

*The following are equivalent for a category* $\mathbf{C}$*:*

- $\mathbf{C}$ *has all pullbacks and a terminal object.*
- $\mathbf{C}$ *has all equalizers and finite products.*
- $\mathbf{C}$ *has has finite limits.*

**Theorem**

*The following are equivalent for a category* $\mathbf{C}$*:*

- $\mathbf{C}$ *has all equalizers and small products.*
- $\mathbf{C}$ *has small limits.*

**Theorem**

*A functor preserves finite (small) limits iff it preserves equalizers and finite (small) products.*

# Topos

- A *subobject* of an object $A \in \mathbf{C}$ is a monomorphism $m : M \rightarrowtail A$.
- Let $\mathbf{E}$ be a category with all finite limits. A *subobject classifier* in $\mathbf{E}$ is a monomophism $t : 1 \rightarrowtail \Omega$ such that for every monomorphism $m : M \rightarrowtail E$, there is a unique morphism $\chi : E \to \Omega$ making the following diagram a pullback:

$$\begin{tikzcd} M \arrow[r, "!_M"] \arrow[d, tail, "m"'] \arrow[dr, phantom, "\lrcorner", very near start] & 1 \arrow[d, tail, "t"] \\ E \arrow[r, dashed, "\chi"'] & \Omega \end{tikzcd}$$

- A *topos* is a cartesian closed category with finite limits and a subobject classifier.

- Given subobjects $m$ and $m'$, define

$$m \subset m' \coloneqq \exists f : m \to m' \in \mathbf{C}/X \qquad \begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, tail, "m"'] & & M' \arrow[dl, tail, "m'"] \\ & X & \end{tikzcd}$$

- $m \sim m' \coloneqq m \subset m' \;\&\; m' \subset m$
- $\mathrm{Sub}(X) \coloneqq \big\{[m] : m \text{ is monic with } \mathrm{cod}(m) = X\big\}$
- $[m] \subset [m'] \coloneqq m \subset m'$
- In terms of generalized elements of an object $X$, $z : Z \to X$, one can define a local membership relation,

$$z \in_X M \coloneqq \exists f : Z \to M [z = mf] \qquad \begin{tikzcd} Z \arrow[r, "f"] \arrow[dr, "z"'] & M \arrow[d, "m"] \\ & X \end{tikzcd}$$

## Theorem

*If $\mathbf{C}$ has finite limits and is in addition a locally small category, then it has a subobject classifier iff $\mathrm{Sub} : \mathbf{C}^{\mathrm{op}} \to \mathbf{Set} :: X \mapsto \{M \rightarrowtail X\}/\sim$ is representable, with representing object $\Omega$. In this case there is a natural isomorphism*

$$\mathrm{Sub}_{\mathbf{C}}(X) \cong \mathrm{Hom}_{\mathbf{C}}(X, \Omega)$$

$$\mathrm{Sub}_{\mathbf{Set}}(X) \cong \mathrm{P}(X)$$

## Theorem

*In any topos $\mathbf{E}$, for any object $X \in \mathbf{E}$, $(\mathrm{Sub}_{\mathbf{E}}(X), \subset)$ 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* if for any $X \in \mathbf{E}$, $(\mathrm{Sub}_{\mathbf{E}}(X), \subset)$ is a Boolean algebra.

## Theorem

*For any small category $\mathbf{C}$, the category of diagrams $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ is a topos.*

# Lawvere's Elementary Theory of the Category of Sets ETCS

- *Well-pointed Topos:* a topos is called *well-pointed* if
  1. for $A \underset{g}{\overset{f}{\rightrightarrows}} B$ , if $\forall x : 1 \to A[fx = gx]$ then $f = g$.
  2. $0 \ncong 1$.
- *Natural Numbers Object:* a *natural numbers object* is an object $N$ with morphisms $0 : 1 \to N$ and $s : N \to N$ such that: given morphisms $a : 1 \to X$ and $g : X \to X$, there is a unique morphism $f : N \to X$ making the following diagram commute:

$$\begin{tikzcd} 1 \arrow[r, "0"] \arrow[dr, "a"'] & N \arrow[r, "s"] \arrow[d, dashed, "f"] & N \arrow[d, dashed, "f"] \\ & X \arrow[r, "g"'] & X \end{tikzcd}$$

- *Choice:* for any epimorphism $f : A \to B$, there exists $g : B \to A$ s.t. $fg = 1_B$. (every epimorphism has a section.)
- $\mathrm{ETCS}$ is a well-pointed topos with natural numbers object and Choice.

# NNO — Example

- Addition

$$\begin{tikzcd}
1 \arrow[r, "0"] \arrow[dr, "a"'] & N \arrow[r, "s"] \arrow[d, dashed, "f_a"] & N \arrow[d, dashed, "f_a"] \\
& N \arrow[r, "s"'] & N
\end{tikzcd}$$

$$f_a(0) = a$$
$$f_a(s(n)) = s(f_a(n))$$

- Multiplication

$$\begin{tikzcd}
1 \arrow[r, "0"] \arrow[dr, "0"'] & N \arrow[r, "s"] \arrow[d, dashed, "f_a"] & N \arrow[d, dashed, "f_a"] \\
& N \arrow[r, "a+(-)"'] & N
\end{tikzcd}$$

$$f_a(0) = 0$$
$$f_a(s(n)) = a + f_a(n)$$

# NNO — Example

- Iteration

$$
\begin{tikzcd}
1 \arrow[r, "0"] \arrow[dr, "\mathrm{id}"'] & \mathbb{N} \arrow[r, "s"] \arrow[d, dashed, "f"] & \mathbb{N} \arrow[d, dashed, "f"] \\
& \mathbf{C}^{\mathbf{C}} \arrow[r, "F^{\mathbf{C}}"'] & \mathbf{C}^{\mathbf{C}}
\end{tikzcd}
\quad \Longrightarrow \quad
\begin{tikzcd}
1 \times \mathbf{C} \arrow[r, "0 \times 1_{\mathbf{C}}"] \arrow[d, "\cong"'] & \mathbb{N} \times \mathbf{C} \arrow[r, "s \times 1_{\mathbf{C}}"] \arrow[d, dashed, "\overline{f}"] & \mathbb{N} \times \mathbf{C} \arrow[d, dashed, "\overline{f}"] \\
\mathbf{C} \arrow[r, "1_{\mathbf{C}}"'] & \mathbf{C} \arrow[r, "F"'] & \mathbf{C}
\end{tikzcd}
$$

where $\mathrm{id}$ is the transpose of $1_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$.

$$
\left.
\begin{aligned}
\overline{f}(0, C) &= C \\
\overline{f}(sn, C) &= F\big(\overline{f}(n, C)\big)
\end{aligned}
\right\}
\quad \Longrightarrow \quad
\overline{f}(n, C) = F^n(C)
$$

# 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.

# 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*

# Hom Functor

## Definition (Hom Functor)

- For $A \in \mathbf{C}$, the hom functor $\mathbf{C}(A, -)$ maps $X \in \mathbf{C}$ to $\mathbf{C}(A, X)$, and maps $f : X \to Y$ to $\mathbf{C}(A, f) : \mathbf{C}(A, X) \to \mathbf{C}(A, Y) :: g \mapsto fg$.

$$X \xrightarrow{f} Y$$

$$C(A, X) \xrightarrow{C(A,f)} C(A, Y)$$

$$g \xmapsto{f \circ -} fg$$

- For $B \in \mathbf{C}$, the hom functor $\mathbf{C}(-, B)$ maps $X \in \mathbf{C}$ to $\mathbf{C}(X, B)$, and maps $f : Y \to X$ to $\mathbf{C}(f, B) : \mathbf{C}(X, B) \to \mathbf{C}(Y, B) :: g \mapsto gf$.

$$Y \xrightarrow{f} X$$

$$C(X, B) \xrightarrow{C(f,B)} C(Y, B)$$

$$g \xmapsto{- \circ f} gf$$

$\mathbf{C}(-,-) : \mathbf{C}^{\mathrm{op}} \times \mathbf{C} \to \mathbf{Set}$ maps $A, B \in \mathbf{C}$ to $\mathbf{C}(A,B)$, and maps $f : A' \to A, g : B \to B'$ to $\mathbf{C}(f,g) : \mathbf{C}(A,B) \to \mathbf{C}(A',B') :: h \mapsto ghf$.

$$
\begin{tikzcd}
 & h \arrow[rr, mapsto, "-\circ f"] \arrow[dd, mapsto, "g\circ -"'] & & hf \arrow[dd, mapsto, "g\circ -"] \\
B \arrow[d, "g"'] & & & \\
B' & & & \\
 & \mathbf{C}(A,B) \arrow[r, "\mathbf{C}(f,B)"] \arrow[d, "\mathbf{C}(A,g)"'] & \mathbf{C}(A',B) \arrow[d, "\mathbf{C}(A',g)"] & \\
 & \mathbf{C}(A,B') \arrow[r, "\mathbf{C}(f,B')"'] & \mathbf{C}(A',B') & \\
 & gh \arrow[rr, mapsto, "-\circ f"'] & & ghf
\end{tikzcd}
$$

$$
\begin{tikzcd}
A' \arrow[r, "f"] & A
\end{tikzcd}
$$

# Yoneda Embedding

## Definition (Yoneda Embedding)

Let $\mathbf{C}$ be a locally small category. Define $\mathrm{y} : \mathbf{C} \to \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ as follows.

- For $A \in \mathbf{C}$, $\mathrm{y} : A \mapsto \mathbf{C}(-, A) : \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$.
- For $f \in \mathbf{C}(A, B)$, $\mathrm{y} : f \mapsto \mathbf{C}(-, f) : \mathbf{C}(-, A) \to \mathbf{C}(-, B)$.

## Definition (Yoneda Embedding)

Let $\mathbf{C}$ be a locally small category. Define $\mathrm{y} : \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}^{\mathbf{C}}$ as follows.

- For $A \in \mathbf{C}^{\mathrm{op}}$, $\mathrm{y} : A \mapsto \mathbf{C}(A, -) : \mathbf{C} \to \mathbf{Set}$.
- For $f \in \mathbf{C}^{\mathrm{op}}(A, B)$, $\mathrm{y} : f \mapsto \mathbf{C}(f, -) : \mathbf{C}(A, -) \to \mathbf{C}(B, -)$.

$$\widehat{\mathbf{C}} := \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$$

# Yoneda Lemma

## Theorem (Yoneda Lemma)

*For any locally small category* $\mathbf{C}$*, object* $A \in \mathbf{C}$ *and functor* $F : \mathbf{C} \to \mathbf{Set}$*,*

$$\mathbf{Set}^{\mathbf{C}}(\mathrm{y}\, A, F) \cong FA$$

*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* $F : \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$*,*

  $$\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}(\mathbf{C}(-, A), F) \cong FA$$

  *naturally in both* $A$ *and* $F$*.*
- *For any locally small category* $\mathbf{C}$*, object* $A \in \mathbf{C}$ *and functor* $F : \mathbf{C} \to \mathbf{Set}$*,*

  $$\mathbf{Set}^{\mathbf{C}}(\mathbf{C}(A, -), F) \cong FA$$

  *naturally in both* $A$ *and* $F$*.*

# Proof Sketch of Yoneda Lemma

**Proof.**

Let $\varphi : \mathrm{Hom}(\mathbf{C}(A,-),F) \to FA :: \alpha \mapsto \alpha_A(1_A)$.
Our first aim is to define an inverse function $\psi : FA \to \mathrm{Hom}(\mathbf{C}(A,-),F)$ that constructs a natural transformation $\psi(a) : \mathbf{C}(A,-) \to F$ from any $a \in FA$.
To this end, we must define components $\psi(a)_B : \mathbf{C}(A,B) \to FB$ 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 $\psi(a)_B(f) \coloneqq Ff(a)$.
By construction, $\varphi(\psi(a)) = a$. It remains to verify that $\psi(\varphi(\alpha)) = \alpha$.
$\psi(\varphi(\alpha))_B(f) = \psi(\alpha_A(1_A))_B(f) = Ff(\alpha_A(1_A)) = \alpha_B(f)$

$$\begin{tikzcd}
\mathbf{C}(A,A) \arrow[r, "\mathbf{C}(A,f)"] \arrow[d, "\psi(a)_A"'] & \mathbf{C}(A,B) \arrow[d, "\psi(a)_B"] \\
FA \arrow[r, "Ff"'] & FB
\end{tikzcd}$$

$$\begin{tikzcd}
1_A \arrow[r, mapsto] \arrow[d, mapsto] & f \arrow[d, mapsto] \\
a \arrow[r, mapsto] & \psi(a)_B(f) = Ff(a)
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbf{C}(A,A) \arrow[r, "\mathbf{C}(A,f)"] \arrow[d, "\alpha_A"'] & \mathbf{C}(A,B) \arrow[d, "\alpha_B"] \\
FA \arrow[r, "Ff"'] & FB
\end{tikzcd}$$

# Proof Sketch of Yoneda Lemma

## Proof continued.

To show that $\varphi$ is natural in $F$, suppose given a natural transformation $\beta : F \to G$.

$$\begin{tikzcd}
\mathbf{Set}^{\mathbf{C}}(\mathbf{C}(A,-),F) \arrow[r, "\beta\circ-"] \arrow[d, "\varphi_F"'] & \mathbf{Set}^{\mathbf{C}}(\mathbf{C}(A,-),G) \arrow[d, "\varphi_G"] \\
FA \arrow[r, "\beta_A"'] & GA
\end{tikzcd}$$

$$\beta_A(\varphi_F(\alpha)) = \beta_A(\alpha_A(1_A)) = (\beta \circ \alpha)_A(1_A) = \varphi_G(\beta \circ \alpha)$$

To show that $\varphi$ is natural in $A$, suppose given $f : A \to B$.

$$\begin{tikzcd}
\mathbf{Set}^{\mathbf{C}}(\mathbf{C}(A,-),F) \arrow[r, "-\circ\mathbf{C}(f,-)"] \arrow[d, "\varphi_A"'] & \mathbf{Set}^{\mathbf{C}}(\mathbf{C}(B,-),F) \arrow[d, "\varphi_B"] \\
FA \arrow[r, "Ff"'] & FB
\end{tikzcd}$$

$Ff(\varphi_A(\alpha)) = Ff(\alpha_A(1_A)) = \alpha_B \circ \mathbf{C}(A,f)(1_A) = \alpha_B(f) =$
$\alpha_B \circ \mathbf{C}(f,-)_B(1_B) = (\alpha \circ \mathbf{C}(f,-))_B(1_B) = \varphi_B(\alpha \circ \mathbf{C}(f,-))$

$$
\begin{tikzcd}
\mathbf{C}(A,A) \arrow[rr, "\mathbf{C}(A,f)"] \arrow[dd, "\psi(a)_A"'] & & \mathbf{C}(A,B) \arrow[dd, "\psi(a)_B"] \\
& 1_A \arrow[r, mapsto] \arrow[d, mapsto] & f \arrow[d, mapsto] \\
& a \arrow[r, mapsto] & \psi(a)_B(f) = Ff(a) \\
FA \arrow[rr, "Ff"'] & & FB
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbf{C}^{\mathrm{op}} \times \mathbf{Set}^{\mathbf{C}} \arrow[r, bend left, "\mathrm{Hom}(\mathrm{y}(-),\bullet)"] \arrow[r, bend right, "\bullet(-)"'] \arrow[r, phantom, "\Downarrow\varphi"] & \mathbf{Set}
\end{tikzcd}$$

## Theorem (Restricted Yoneda Lemma)

*For any locally small category* $\mathbf{C}$*, object* $A, B \in \mathbf{C}$*,*

- $\mathbf{Set}^{\mathbf{C}}(\mathbf{C}(A,-), \mathbf{C}(B,-)) \cong \mathbf{C}(B,A)$
- $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}(\mathbf{C}(-,A), \mathbf{C}(-,B)) \cong \mathbf{C}(A,B)$

## Proof.

Let $F := \mathbf{C}(B,-)$ or $F := \mathbf{C}(-,B)$.

### Corollary

*The Yoneda embedding functor* $\mathrm{y} : \mathbf{C} \to \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ *is fully faithful, and injective on objects.*

Hence, $\mathrm{y}$ is an embedding $\mathbf{C} \hookrightarrow \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$.

### Definition (Concrete Category & Abstract Category)

A category $\mathbf{C}$ is *concrete* if there is a faithful functor $F : \mathbf{C} \to \mathbf{Set}$. 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* $A, B \in \mathbf{C}$*,*
$A \cong B \iff \mathrm{y}\, A \cong \mathrm{y}\, B$*.*

Figure: If $\mathbf{C}(X, A) \cong \mathbf{C}(X, B)$ naturally in $X$, then $A \cong B$.

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 $\mathrm{Hom}(\bullet, X) \cong \mathrm{Hom}(\bullet, Y)$.
- $X$ and $Y$ have the same path space iff $\mathrm{Hom}(I, X) \cong \mathrm{Hom}(I, Y)$.
- $X$ and $Y$ have the same loop space iff $\mathrm{Hom}(S^1, X) \cong \mathrm{Hom}(S^1, Y)$.
- Probing $X$ and $Y$ with various spaces gives us more information.
- Probing them with all spaces gives us all information.

Given any objects $A, B$ in a locally small category $\mathbf{C}$, to find an arrow $h : A \to B$ it suffices to give one $\theta : \mathrm{y}\, A \to \mathrm{y}\, B$ in $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$, for then there is a unique $h$ with $\theta = \mathrm{y}\, h$. Why should it be easier to give $\mathrm{y}\, A \to \mathrm{y}\, B$ than $A \to B$? The key difference is that in general $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ has much more structure to work with than does $\mathbf{C}$. The category $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ 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.

## Theorem

*For a locally small category $\mathbf{C}$, the Yoneda embedding $\mathrm{y}$ preserves all limits that exist in $\mathbf{C}$.*

## Proof.

Suppose $(L, \lambda)$ is a limit of $D : \mathbf{I} \to \mathbf{C}$. The Yoneda embedding maps $D$ to the diagram $\mathrm{y}\, D : \mathbf{I} \to \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ defined by $(\mathrm{y}\, D)_i = \mathrm{y}\, D_i = \mathbf{C}(-, D_i)$, and it maps $(L, \lambda)$ to $(\mathrm{y}\, L, \mathrm{y}\, \lambda)$ on $\mathrm{y}\, D$ defined by $(\mathrm{y}\, \lambda)_i = \mathrm{y}\, \lambda_i = \mathbf{C}(-, \lambda_i)$.
To see that $(\mathrm{y}\, L, \mathrm{y}\, \lambda)$ is a limit cone on $\mathrm{y}\, D$, consider a cone $(M, \mu)$ on $\mathrm{y}\, D$. Then $\mu : \Delta M \to D$ consists of a family of functions, one for each $i \in \mathbf{I}$ and $A \in \mathbf{C}$,

$$(\mu_i)_A : MA \to \mathbf{C}(A, D_i)$$

For $A \in \mathbf{C}$ and $m \in MA$, we get a cone on $D$ consisting of morphisms $(\mu_i)_A m : A \to D_i$. There exists a unique morphism $\varphi_A m : A \to L$ s.t. $(\mu_i)_A m = \lambda_i \circ \varphi_A m$. Then $\varphi_A : MA \to \mathbf{C}(A, L) = (\mathrm{y}\, L)A$ forms a unique factorization $\varphi : M \to \mathrm{y}\, L$.

- $\mathbf{C}(A, \varprojlim D_i) \cong \varprojlim \mathbf{C}(A, D_i)$
- $\mathbf{C}(\varinjlim D_i, A) \cong \varprojlim \mathbf{C}(D_i, A)$

# Cayley Theorem

## Theorem (Cayley Theorem)

*Every group $G$ is isomorphic to a subgroup of the symmetry group on $G$.*

## Proof.

Any group $G$ can be viewed as a single object $\bullet$ category, call it $\mathbf{G}$.

$$\mathbf{Set}^{\mathbf{G}^{\mathrm{op}}}(\mathbf{G}(-,\bullet),\mathbf{G}(-,\bullet)) \cong \mathbf{G}(\bullet,\bullet)$$

The right-hand side is just $G$.
$\mathrm{y} : g \mapsto \mathbf{G}(-,g) : \mathbf{G}(\bullet,\bullet) \to \mathbf{G}(\bullet,\bullet)$ 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

- Klein[11] 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 $\mathrm{Aut}(X)$.

$$\mathrm{Aut}(X) \to \mathrm{End}(X) \to \mathrm{Hom}(X, Y)$$

$$\frac{\text{Space}}{\text{Transformation group}} \sim \frac{\text{Category}}{\text{Algebra of mappings}}$$

[11] Klein'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 $G \times X \to X$ can be seen as a group representation $G \to \mathrm{Aut}(X)$. A group representation provides a way to view the abstract group elements as concrete linear transformations of some vector space.
- For example, $D_3 \to \mathrm{Aut}(\mathbb{R}^2)$.

$$D_3 = \langle r, s | r^3 = s^2 = rsrs = e \rangle$$

$$r \mapsto R = \begin{bmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix} \qquad s \mapsto S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- We can think of a group $G$ as providing the syntax while automorphisms $\mathrm{Aut}(X)$ provide the semantics. So a group representation is like a functor

$$\text{syntax} \;\to\; \text{semantics}$$

# Representable Functor & Universal Element

## Definition (Representable Functor)

A functor $F : \mathbf{C} \to \mathbf{Set}$ is *representable* if there is a natural isomorphism $\alpha : \mathbf{C}(A, -) \xrightarrow{\cong} F$ for some $A \in \mathbf{C}$. We say that the pair $(A, \alpha)$ is a *representation* of $F$.

## Definition (Universal Element)

A *universal element* of the functor $F : \mathbf{C} \to \mathbf{Set}$ 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 $f : A \to B$ such that $Ff(a) = b$.

- If $(A, \alpha)$ is a representation of $F : \mathbf{C} \to \mathbf{Set}$, then $(A, \alpha_A(1_A))$ is a universal element of $F$.
- The natural transformation $\psi(a) : \mathbf{C}(A, -) \to F$ induced by $a \in FA$ in Yoneda lemma is an isomorphism iff $(A, a)$ is a universal element of $F$.

# Category of Elements

## Definition

- The *category of elements* $\int^{\mathbf{C}} F$ of a covariant functor $F : \mathbf{C} \to \mathbf{Set}$ has
  1. as objects $(A, a)$, where $A \in \mathbf{C}$ and $a \in FA$, and
  2. as morphisms $(A, a) \to (B, b)$ with $f : A \to B$ in $\mathbf{C}$ s.t. $Ff(a) = b$.
- The *category of elements* $\int_{\mathbf{C}} P$ of a contravariant functor $P : \mathbf{C}^{\mathrm{op}} \to \mathbf{Set}$ has
  1. as objects $(A, a)$ where $A \in \mathbf{C}$ and $a \in PA$, and
  2. as morphisms $(A, a) \to (B, b)$ with $f : A \to B$ 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:

$$\pi_P : \int_{\mathbf{C}} P \to \mathbf{C} :: (A, a) \mapsto A$$

**Theorem**

*If $F : \mathbf{C} \to \mathbf{D}$ is a functor from a small category $\mathbf{C}$ to a cocomplete category $\mathbf{D}$, the functor $R : \mathbf{D} \to \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$ given by*

$$R(B) : A \mapsto \mathrm{Hom}_{\mathbf{D}}(FA, B)$$

*has a left adjoint $L : \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}} \to \mathbf{D}$ given by*

$$L(P) = \varinjlim \left( \int_{\mathbf{C}} P \xrightarrow{\pi_P} \mathbf{C} \xrightarrow{F} \mathbf{D} \right)$$

*In other words,*

$$\mathrm{Hom}_{\mathbf{D}}(LP, B) \cong \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}(P, RB) \qquad L \dashv R$$

## Proof.

For a natural transformation $\alpha : P \to RB$,

$$\alpha_A : PA \to \mathbf{D}(FA, B)$$

$\{\alpha_A\}_{A \in \mathbf{C}}$ is natural in $A$.

$$\begin{tikzcd}
A & PA \arrow[r, "\alpha_A"] \arrow[d, "Pf"'] & \mathbf{D}(FA, B) \arrow[d, "\mathbf{D}(Ff, B)"] \\
A' \arrow[u, "f"'] & PA' \arrow[r, "\alpha_{A'}"'] & \mathbf{D}(FA', B)
\end{tikzcd}$$

Such an $\alpha$ can also be considered as $\{\alpha_A(a) : FA \to B\}_{(A,a) \in \int_{\mathbf{C}} P}$. Then

$$\begin{tikzcd}
A & FA = F\pi_P(A, a) \arrow[dr, "\alpha_A(a)"] & \\
 & & B \\
A' \arrow[uu, "f"] & FA' = F\pi_P(A', a') \arrow[uu, "Ff"] \arrow[ur, "\alpha_{A'}(a')"'] &
\end{tikzcd}$$

This means that $(B, \alpha_A)$ constitute a cocone over $F\pi_P : \int_{\mathbf{C}} P \to \mathbf{D}$.
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,

$$R_{\mathrm{y}}(B)(A) = \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}(\mathrm{y}\,A, B) \cong B(A)$$

this means that $R_{\mathrm{y}}$ is isomorphic to the identity functor of $\mathbf{Set}^{\mathbf{C}^{\mathrm{op}}}$.
Its left adjoint $L$ must also be isomorphic to the identity functor.

$$P \cong \varinjlim \left( \int_{\mathbf{C}} P \xrightarrow{\pi_P} \mathbf{C} \xrightarrow{\mathrm{y}} \mathbf{Set}^{\mathbf{C}^{\mathrm{op}}} \right)$$

# 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 $f : B \to A$. A morphism of $\mathbf{C}/A$ from $(B, f)$ to $(B', f')$ is a morphism $g : B \to B'$ s.t.

$$\begin{tikzcd} & B \arrow[dl, "f"'] \arrow[d, "g"] \\ A & B' \arrow[l, "f'"] \end{tikzcd}$$

- 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 $f : A \to B$. A morphism of $A/\mathbf{C}$ from $(B, f)$ to $(B', f')$ is a morphism $g : B \to B'$ s.t.

$$\begin{tikzcd} & B \arrow[d, "g"] \\ A \arrow[ur, "f"] \arrow[r, "f'"'] & B' \end{tikzcd}$$

$$\boxed{\mathbf{Set}/I \simeq \mathbf{Set}^I}$$

$$\Phi : \mathbf{Set}/I \to \mathbf{Set}^I$$

$$\Psi : \mathbf{Set}^I \to \mathbf{Set}/I$$

$$\Phi : A \xrightarrow{f} I \mapsto \left(f^{-1}(i)\right)_{i \in I}$$

$$\Psi : (A_i)_{i \in I} \mapsto \coprod_{i \in I} A_i \xrightarrow{\pi} I \quad \text{(the indexing projection)}$$

where the coproduct is conveniently taken to be

$$\coprod_{i \in I} A_i := \bigcup_{i \in I} A_i \times \{i\}$$

# Slice Category

- There is a forgetful functor $U_A : \mathbf{C}/A \to \mathbf{C}$ which maps $(B, f)$ to $B$.
- Furthermore, for $h : A \to A'$ there is a functor "*composition by h*" $\mathbf{C}/h : \mathbf{C}/A \to \mathbf{C}/A'$ which maps $(B, f)$ to $(B, hf)$ and

$$\begin{tikzcd} & B \arrow[dl, "f"'] \arrow[d, "g"] \\ A & B' \arrow[l, "f'"] \end{tikzcd} \quad \text{to} \quad \begin{tikzcd} & B \arrow[dl, "hf"'] \arrow[d, "g"] \\ A' & B \arrow[l, "hf'"] \end{tikzcd}$$

- For any small category $\mathbf{C}$, the construction of slice categories itself is a functor $\mathbf{C}/- : \mathbf{C} \to \mathbf{Cat}$.
- The functor $\mathbf{C}/-$ then factors through the forgetful functor $U_{\mathbf{C}} : \mathbf{Cat}/\mathbf{C} \to \mathbf{Cat}$ via a functor $\overline{\mathbf{C}} : \mathbf{C} \to \mathbf{Cat}/\mathbf{C}$.

$$\begin{tikzcd} \mathbf{C} \arrow[r, "\overline{\mathbf{C}}"] \arrow[dr, "\mathbf{C}/-"'] & \mathbf{Cat}/\mathbf{C} \arrow[d, "U_{\mathbf{C}}"] \\ & \mathbf{Cat} \end{tikzcd} \quad \text{where } \overline{\mathbf{C}}{:}A \mapsto (\mathbf{C}/A, U_A) \text{ and } \overline{\mathbf{C}}{:}h \mapsto \quad \begin{tikzcd} \mathbf{C}/A \arrow[rr, "\mathbf{C}/h"] \arrow[dr, "U_A"'] & & \mathbf{C}/A' \arrow[dl, "U_{A'}"] \\ & \mathbf{C} & \end{tikzcd}$$

# 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 $f : FA \to GB$.
- the morphisms from $(A, B, f)$ to $(A', B', f')$ are pairs $(a, b)$ where $a : A \to A'$ in $\mathbf{A}$ and $b : B \to B'$ in $\mathbf{B}$ s.t.

$$\begin{tikzcd} FA \arrow[r, "f"] \arrow[d, "Fa"'] & GB \arrow[d, "Gb"] \\ FA' \arrow[r, "f'"'] & GB' \end{tikzcd}$$

- If $\mathbf{B} = \mathbf{1}$ and $G : \mathbf{1} \to \mathbf{C}$ 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 $F : \mathbf{1} \to \mathbf{C}$ 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 $(f, g)$ where $f : A \rightarrow A', g : B \rightarrow B'$ s.t.

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[d, "f"'] & B \arrow[d, "g"] \\ A' \arrow[r, "h'"'] & B' \end{tikzcd}$$

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 $G : \mathbf{D} \to \mathbf{C}$ 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 $u : A \to GB$ with the following property: for any $f : A \to GB'$, there exists a unique morphism $g : B \to B'$ s.t.

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[dr, "f"'] & GB \arrow[d, dashed, "Gg"] \\ & GB' \end{tikzcd}$$

- A universal morphism from $G$ to $A$ is a unique pair $(B, u)$ where $u : GB \to A$ with the following property: for any $f : GB' \to A$, there exists a unique morphism $g : B' \to B$ s.t.

$$\begin{tikzcd} A & GB \arrow[l, "u"'] \\ & GB' \arrow[u, dashed, "Gg"'] \arrow[ul, "f"] \end{tikzcd}$$

# Comma Category

## Definition (Comma Category)

Let $G : \mathbf{D} \to \mathbf{C}$ 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 $f : A \to GB$. A morphism from $(B, f)$ to $(B', f')$ is given by $g : B \to B'$ s.t.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "f'"'] & GB \arrow[d, dashed, "Gg"] \\ & GB' \end{tikzcd}$$

- The *comma category* $G \downarrow A$ has objects all pairs $(B, f)$ with $B \in \mathbf{D}$ and $f : GB \to A$. A morphism from $(B, f)$ to $(B', f')$ is given by $g : B' \to B$ s.t.

$$\begin{tikzcd} A & GB \arrow[l, "f"'] \\ & GB' \arrow[u, dashed, "Gg"'] \arrow[ul, "f'"] \end{tikzcd}$$

- 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 $f : A \to GB$ in $\mathbf{C}$. The $A \downarrow G$-morphisms from $(\bullet, B, f)$ to $(\bullet, B', f')$ are pairs $(1_\bullet, g)$ with $g : B \to B'$ in $\mathbf{D}$ s.t.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "1_A"'] & GB \arrow[d, "Gg"] \\
A \arrow[r, "f'"'] & GB'
\end{tikzcd}$$

- Let $G : \mathbf{D} \to \mathbf{C}$ 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 $\mathbf{C}(A, G(-))$.
- The dual statements are also equivalent:
  1. $(B, u)$ is a universal morphism from $G$ to $A$.
  2. $(B, u)$ is a termianl object of the comma category $G \downarrow A$.
  3. $(B, u)$ is a representation of $\mathbf{C}(G(-), A)$.
- A universal element can be viewed as a universal morphism from the one-point set $\{\bullet\}$ to the functor $G : \mathbf{D} \to \mathbf{Set}$.

# Universal Property — Product

Let $X$ and $Y$ be objects of a category $\mathbf{D}$.

$$\begin{tikzcd} X & X \times Y \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & Y \\ & Z \arrow[ul, "f"] \arrow[u, dashed, "h"] \arrow[ur, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} (X,Y) & \Delta(X \times Y) \arrow[l, "(\pi_1,\pi_2)"'] \\ & \Delta(Z) \arrow[ul, "(f,g)"] \arrow[u, dashed, "\Delta(h)"'] \end{tikzcd}$$

Take $\mathbf{C}$ to be the product category $\mathbf{D} \times \mathbf{D}$, and let $\Delta$ be the diagonal functor $\Delta : \mathbf{C} \to \mathbf{C}^{\mathbf{I}}$.

Then $(X \times Y, (\pi_1, \pi_2))$ is a universal morphism from $\Delta$ to the object $(X, Y)$ of $\mathbf{D} \times \mathbf{D}$.

One can generalize the above example to arbitrary limits and colimits.

- Given $D : \mathbf{I} \to \mathbf{C}$ (thought of as an object in $\mathbf{C}^{\mathbf{I}}$), the limit $\varprojlim D$ is a universal morphism from $\Delta$ to $D$.
- Dually, the colimit $\varinjlim D$ is a universal morphism from $D$ to $\Delta$.

# Left/Right Adjoint

## Definition (Left/Right Adjoint)

Functors $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ are *adjoint* $F \dashv G$ if 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 $\theta$ means that for $f : A \to A'$ and $g : B \to B'$,

$$\begin{tikzcd}
\mathbf{D}(FA', B) \arrow[r, "\mathbf{D}(Ff, B)"] \arrow[d, "\theta_{A',B}"'] & \mathbf{D}(FA, B) \arrow[d, "\theta_{A,B}"] \\
\mathbf{C}(A', GB) \arrow[r, "\mathbf{C}(f, GB)"'] & \mathbf{C}(A, GB)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbf{D}(FA, B) \arrow[r, "\mathbf{D}(FA, g)"] \arrow[d, "\theta_{A,B}"'] & \mathbf{D}(FA, B') \arrow[d, "\theta_{A,B'}"] \\
\mathbf{C}(A, GB) \arrow[r, "\mathbf{C}(A, Gg)"'] & \mathbf{C}(A, GB')
\end{tikzcd}$$

## Theorem

*Given* $\mathbf{D}(FA, B) \underset{\sharp}{\overset{\flat}{\rightleftarrows}} \mathbf{C}(A, GB)$ *, the naturality condition of the adjunction implies that for every* $f : A \to A'$, $g : B \to B'$, $h^\sharp : FA \to B$, $k^\sharp : FA' \to B'$,

$$\begin{tikzcd} A \arrow[r, "h^\flat"] \arrow[d, "f"'] & GB \arrow[d, "Gg"] \\ A' \arrow[r, "k^\flat"'] & GB' \end{tikzcd} \iff \begin{tikzcd} FA \arrow[r, "h^\sharp"] \arrow[d, "Ff"'] & B \arrow[d, "g"] \\ FA' \arrow[r, "k^\sharp"'] & B' \end{tikzcd}$$

## Proof.

$$\begin{tikzcd} \mathbf{D}(FA', B') \arrow[r, "-\circ Ff"] \arrow[d, "\flat"'] & \mathbf{D}(FA, B') \arrow[d, "\flat"] \\ \mathbf{C}(A', GB') \arrow[r, "-\circ f"'] & \mathbf{C}(A, GB') \end{tikzcd} \qquad \begin{tikzcd} \mathbf{D}(FA, B) \arrow[r, "g\circ -"] \arrow[d, "\flat"'] & \mathbf{D}(FA, B') \arrow[d, "\flat"] \\ \mathbf{C}(A, GB) \arrow[r, "Gg\circ -"'] & \mathbf{C}(A, GB') \end{tikzcd}$$

$$k^\flat \circ f = (k^\sharp \circ Ff)^\flat \qquad Gg \circ h^\flat = (g \circ h^\sharp)^\flat$$

# Left/Right Adjoint

## Example

$$\frac{A \wedge B \vdash C}{\overline{A \vdash B \to C}}$$

$$F_B : X \mapsto X \wedge B \qquad G_B : X \mapsto B \to X \qquad F_B \dashv G_B$$

## Example

$$\frac{A \cap B \subset C}{\overline{A \subset B \to C}} \qquad \text{where } B \to C := \overline{B} \cup C$$

$$F_B : X \mapsto X \cap B \qquad G_B : X \mapsto B \to X \qquad F_B \dashv G_B$$

## Example $([0, \infty], \geq, +, 0)$

$$\frac{A + B \geq C}{\overline{A \geq B \to C}} \qquad \text{where } B \to C := \max\{0, C - B\}$$

$$F_B : X \mapsto X + B \qquad G_B : X \mapsto B \to X \qquad F_B \dashv G_B$$

# Left/Right Adjoint

## Example

$$\mathbf{C}(A \times B, C) \cong \mathbf{C}(A, C^B)$$

$$F_B : X \mapsto X \times B \qquad G_B : X \mapsto X^B \qquad F_B \dashv G_B$$

Figure: In $\mathbf{Set}$, a map $A \times B \to C$ can be seen as a way of assigning to each element of $A$ a map $B \to C$.

# Left/Right Adjoint

## Example

The forgetful functor $U : \mathbf{Grp} \to \mathbf{Set}$ has as a left adjoint $F : \mathbf{Set} \to \mathbf{Grp}$ which sends a set to the free group on that set. $F \dashv U$.

## Example

The functor $\mathrm{ob} : \mathbf{Cat} \to \mathbf{Set}$ has a left adjoint $D$ sending $A$ to the discrete category whose objects are the members of $A$. (since a functor $DA \to \mathbf{C}$ is uniquely determined by its effect on objects) and a right adjoint $I$ sending $A$ to the preorder with objects $a \in A$ and one morphism $a \to b$ for all $(a, b) \in A \times A$. (Again, a functor $\mathbf{C} \to IA$ is uniquely determined by its effect on objects.) In this case $D$ also has a left adjoint $\pi_0$ sending $\mathbf{C}$ to its set of connected components, i.e. equivalences of objects $A$ with $U \sim V$ if there exists a morphism $U \to V$. (Once again, a functor $\mathbf{C} \to DA$ is determined by its effect on objects, but the functor $\mathrm{ob}(\mathbf{C}) \to A$ has to be ordered on connected components.)

$$\pi_0 \dashv D \dashv \mathrm{ob} \dashv I$$

# Left/Right Adjoint

## 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 $z \in \mathbb{Z}, r \in \mathbb{R}$:

$$\frac{r \leq i(z)}{\lceil r \rceil \leq z} \qquad \frac{i(z) \leq r}{z \leq \lfloor r \rfloor}$$

## 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 $c : X \to Y$ 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 $\mathcal{O}(X) \subset \mathrm{P}(X)$ 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 $S \in \mathrm{P}(X)$, topological interior is a right adjoint to the inclusion of $\mathcal{O}(X)$ into $\mathrm{P}(X)$.

$$\frac{i\,U \subset S}{\overline{U \subset S^\circ}}$$

$$\begin{tikzcd} \mathcal{O}(X) \arrow[r, shift left, "i"] \arrow[r, phantom, "\perp"] & \mathrm{P}(X) \arrow[l, shift left, "(\,)^\circ"] \end{tikzcd}$$

# Left/Right Adjoint

$A$ $\qquad$ $\Box A$ $\qquad$ $\Diamond A$

$\Box A$ squares that are completely covered by $A$.

$\Diamond A$ squares that are partly or totally covered by $A$.

$$\frac{\Diamond A \subset B}{A \subset \Box B} \qquad \Diamond \dashv \Box$$

# Left/Right Adjoint

## Example

Assume $R \subset X \times Y$, and let $F_R : \mathrm{P}(X) \to \mathrm{P}(Y) :: A \mapsto \bigcup_{x \in A} \{y : Rxy\}$.

This has a right adjoint $[R] : \mathrm{P}(Y) \to \mathrm{P}(X)$:

$$\frac{F_R(A) \subset B}{\overline{\overline{A \subset [R]B}}}$$

The definition of $[R]$ which satisfies this condition is:

$$[R]B \coloneqq \big\{x : \forall y \big(Rxy \to y \in B\big)\big\}$$

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 $f : X \to Y$, consider
$f^* : \mathrm{P}(Y) \to \mathrm{P}(X) :: B \mapsto \{x \in X : fx \in B\}$.
Take the subset $B \subset Y$ as a predicate $B(y)$ over $Y$,
and $f^*B$ as $f^*B(x)$ over $X$.
By the pullback, $f^*B(x) = B(fx) =: (Bf)(x)$.

$$\begin{tikzcd} f^*B \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, hook, "i"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

Then $f^*$ has both a left and a right adjoint $\exists_f, \forall_f : \mathrm{P}(X) \to \mathrm{P}(Y)$.

$$\frac{A \subset f^*B}{\exists_f A \subset B} \qquad \frac{f^*B \subset A}{B \subset \forall_f A} \qquad \text{i.e.} \qquad \frac{A \vdash_X Bf}{\exists_f A \vdash_Y B} \qquad \frac{Bf \vdash_X A}{B \vdash_Y \forall_f A}$$

$$\boxed{\exists_f \dashv f^* \dashv \forall_f}$$

The unique functions satisfying these conditions can be defined as

$$\exists_f A := \bigcap \{B : A \subset f^*B\} = fA = \big\{y \in Y : \exists x\big(fx = y \wedge x \in A\big)\big\}$$

$$\forall_f A := \bigcup \{B : f^*B \subset A\} = \{y \in Y : f^*y \subset A\} = \big\{y \in Y : \forall x\big(fx = y \to x \in A\big)\big\}$$

$$\frac{A \subset f^{-1}B}{\overline{\overline{f\,A \subset B}}} \qquad \frac{A \vdash_X B f}{\overline{\overline{\exists_f A \vdash_Y B}}}$$

# $\exists_\pi \dashv \pi^* \dashv \forall_\pi$

Let $f$ be the projection $\pi : X \times Y \to Y$. Hence $\pi^* : \mathrm{P}(Y) \to \mathrm{P}(X \times Y)$.

$$\begin{tikzcd} \pi^* B \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & B \arrow[d, hook, "i"] \\ X \times Y \arrow[r, "\pi"'] & Y \end{tikzcd}$$

By the pullback, $\pi^* B(x, y) = B\pi(x, y)$.
Then $\pi^*$ has both a left and a right adjoint $\exists_\pi, \forall_\pi : \mathrm{P}(X \times Y) \to \mathrm{P}(Y)$.

$$\boxed{\exists_\pi \dashv \pi^* \dashv \forall_\pi}$$

We write $\exists_\pi A$ as $\exists x A(x, y)$, $\forall_\pi A$ as $\forall x A(x, y)$, and $\subset$ as $\vdash$.

$$\exists x A(x, y) = \exists_\pi A = \{y \in Y : \exists x \ (x, y) \in A\}$$

$$\forall x A(x, y) = \forall_\pi A = \{y \in Y : \forall x \ (x, y) \in A\}$$

$$\frac{A \subset \pi^* B}{\exists_\pi A \subset B} \qquad \frac{\pi^* B \subset A}{B \subset \forall_\pi A} \qquad \frac{A(x, y) \vdash_{X \times Y} B(y)}{\exists x A(x, y) \vdash_Y B(y)} \qquad \frac{B(y) \vdash_{X \times Y} A(x, y)}{B(y) \vdash_Y \forall_x A(x, y)}$$

# Quantifiers are Adjoints

For a list $\mathbf{y} = y_1, \ldots, y_n$ of distinct variables, let $\mathrm{Form}(\mathbf{y})$ be the set of formulae that has at most $\mathbf{y}$ free. Then $\mathrm{Form}(\mathbf{y})$ is a preorder under $\vdash$. Let $x$ be a variable not in $\mathbf{y}$. We have a trivial operation

$$* : \mathrm{Form}(\mathbf{y}) \to \mathrm{Form}(x, \mathbf{y})$$

The operation $*$ is trivially a functor, since

$$A(\mathbf{y}) \vdash B(\mathbf{y}) \text{ in } \mathrm{Form}(\mathbf{y}) \implies A(x, \mathbf{y}) \vdash B(x, \mathbf{y}) \text{ in } \mathrm{Form}(x, \mathbf{y})$$

For any $A \in \mathrm{Form}(x, \mathbf{y})$, obviously $x \notin \mathrm{Fv}(\exists x A)$ and $x \notin \mathrm{Fv}(\forall x A)$. We have $\exists x / \forall x : \mathrm{Form}(x, \mathbf{y}) \to \mathrm{Form}(\mathbf{y})$.

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. $\forall x A(x, \mathbf{y}) \vdash A(x, \mathbf{y})$ is just the counit of $* \dashv \forall$, and $A(x, \mathbf{y}) \vdash \exists x A(x, \mathbf{y})$ is the unit of $\exists \dashv *$.

$$\begin{aligned}
\forall x A(x, y) &\vdash A(x, y) && \text{(counit of } * \dashv \forall) \\
A(x, y) &\vdash \exists y A(x, y) && \text{(unit of } \exists \dashv *) \\
\forall x A(x, y) &\vdash \exists y A(x, y) && \text{(transitivity of } \vdash) \\
\exists y \forall x A(x, y) &\vdash \exists y A(x, y) && (\exists \dashv *) \\
\exists y \forall x A(x, y) &\vdash \forall x \exists y A(x, y) && (* \dashv \forall)
\end{aligned}$$

# Quantifiers are Adjoints

Given a wff $A$. Let $[\![A]\!] := \{(a, \mathbf{b}) : \mathcal{M} \vDash A[a, \mathbf{b}]\}$. Take the projection $\pi : (a, \mathbf{b}) \mapsto \mathbf{b}$. It can be regarded as $\pi : \nu(a/x) \mapsto \nu$.

$$\boxed{\exists_\pi \dashv \pi^* \dashv \forall_\pi}$$

$$\frac{[\![A]\!] \subset \pi^*[\![B]\!]}{\exists_\pi[\![A]\!] \subset [\![B]\!]} \qquad \frac{\pi^*[\![B]\!] \subset [\![A]\!]}{[\![B]\!] \subset \forall_\pi[\![A]\!]}$$

Explicitly,

$$\exists_\pi[\![A]\!] = \left\{\mathbf{b} : \exists a\Big(\mathcal{M} \vDash A[a, \mathbf{b}]\Big)\right\} = \bigcup_{a \in M} \left\{\nu : \mathcal{M}, \nu(a/x) \vDash A\right\}$$

$$\forall_\pi[\![A]\!] = \left\{\mathbf{b} : \forall a\Big(\mathcal{M} \vDash A[a, \mathbf{b}]\Big)\right\} = \bigcap_{a \in M} \left\{\nu : \mathcal{M}, \nu(a/x) \vDash A\right\}$$

And we have

$$[\![\exists x A]\!] = \exists_\pi[\![A]\!] \qquad [\![\forall x A]\!] = \forall_\pi[\![A]\!]$$

# Internal Logic

| Logical operator | Operation on $\mathrm{Sub}(A)$ |
|---|---|
| truth: $\top$ | top element ($A$ itself) |
| falsity: $\bot$ | 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 |

# $0_{\mathbf{C}} \dashv !_{\mathbf{C}} \dashv 1_{\mathbf{C}}$

An object $A \in \mathbf{C}$ can be viewed as a functor from the terminal category $\mathbf{1}$ to $\mathbf{C}$, i.e., $A : \bullet \to A$ and $A : 1_\bullet \to 1_A$. Since $\mathbf{1}$ is the terminal object of $\mathbf{Cat}$, there exists a unique functor $!_{\mathbf{C}} : \mathbf{C} \to \mathbf{1}$, which maps every object $A \in \mathbf{C}$ to $\bullet$.

Now we ask whether the functor $!_{\mathbf{C}} : \mathbf{C} \to \mathbf{1}$ has any adjoints. Indeed, it has a right adjoint just if $\mathbf{C}$ has a terminal object $1_{\mathbf{C}}$, for the corresponding functor $1_{\mathbf{C}} : \mathbf{1} \to \mathbf{C}$ has the property that, for every $A \in \mathbf{C}$ we have a trivial natural bijective correspondence:

$$\frac{1_\bullet : !_{\mathbf{C}} A \to \bullet}{\overline{!_A : A \to 1_{\mathbf{C}}\bullet}} \qquad \text{similarly,} \qquad \frac{1_\bullet : \bullet \to !_{\mathbf{C}} A}{\overline{!_A : 0_{\mathbf{C}}\bullet \to A}}$$

$$0_{\mathbf{C}} \dashv !_{\mathbf{C}} \dashv 1_{\mathbf{C}}$$

# $+ \dashv \Delta \dashv \times$

**Theorem**

1. *$\Delta$ has a right adjoint iff $\mathbf{C}$ has binary products, and the right adjoint is $\times : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$.*
2. *$\Delta$ has a left adjoint iff $\mathbf{C}$ has binary coproducts, and the left adjoint is $+ : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$.*

$$\mathbf{C} \times \mathbf{C}(\Delta X, (A, B)) \cong \mathbf{C}(X, A) \times \mathbf{C}(X, B) \cong \mathbf{C}(X, A \times B)$$

$$\mathbf{C}(A + B, X) \cong \mathbf{C}(A, X) \times \mathbf{C}(B, X) \cong \mathbf{C} \times \mathbf{C}((A, B), \Delta X)$$

$$\begin{tikzcd}
A & A \times B \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & B \\
& Z \arrow[ul, "f"] \arrow[u, dashed, "u"] \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\iota_1"] \arrow[dr, "f"'] & A + B \arrow[d, dashed, "u"] & B \arrow[l, "\iota_2"'] \arrow[dl, "g"] \\
& Z &
\end{tikzcd}$$

# $\varinjlim \dashv \Delta \dashv \varprojlim$

Consider the constant diagram functor $\Delta : \mathbf{C} \to \mathbf{C}^{\mathbf{I}}$. It maps $X \in \mathbf{C}$ to the constant diagram $\Delta X : \mathbf{I} \to \mathbf{C}$ which maps every object to $X$ and every morphism to $1_X$. The limit construction is a functor $\varprojlim : \mathbf{C}^{\mathbf{I}} \to \mathbf{C}$ that maps each diagram $D \in \mathbf{C}^{\mathbf{I}}$ to its limit $\varprojlim D$.

The cones over $D : \mathbf{I} \to \mathbf{C}$ with vertex $X$ is the hom-set $\mathbf{C}^{\mathbf{I}}(\Delta X, D)$.

The cones over $D : \mathbf{I} \to \mathbf{C}$ with vertex $X$ correspond one-to-one with $\mathbf{C}(X, \varprojlim D)$.

If $\mathbf{C}$ has all limits of shape $\mathbf{I}$, then

$$\mathbf{C}^{\mathbf{I}}(\Delta X, D) \cong \mathbf{C}(X, \varprojlim D)$$

$$\varinjlim \dashv \Delta \dashv \varprojlim$$

# Galois Connection

## Definition (Galois Connection)

- Let $(\mathbf{C}, \prec)$ and $(\mathbf{D}, \sqsubset)$ be two partially ordered sets. A monotone Galois connection between these posets consists of two monotone functions: $F : \mathbf{C} \to \mathbf{D}, G : \mathbf{D} \to \mathbf{C}$ s.t.,
$$\forall A \in \mathbf{C} \forall B \in \mathbf{D} : F(A) \sqsubset B \iff A \prec G(B)$$
- Let $(\mathbf{C}, \prec)$ and $(\mathbf{D}, \sqsubset)$ be two partially ordered sets. An antitone Galois connection between these posets consists of two order-reversing functions: $F : \mathbf{C} \to \mathbf{D}, G : \mathbf{D} \to \mathbf{C}$ s.t.,
$$\forall A \in \mathbf{C} \forall B \in \mathbf{D} : B \sqsubset F(A) \iff A \prec G(B)$$

Example: $B \to \neg A \iff A \to \neg B, \quad F = G = \neg$

- A Galois correspondence is an antitone Galois connection.
- An antitone Galois connection between $\mathbf{C}$ and $\mathbf{D}$ is just a monotone Galois connection between $\mathbf{C}$ and the order dual $\mathbf{D}^{\mathrm{op}}$.
- A Galois connection is a pair of adjoint functors between two categories that arise from partially ordered sets.

# Fundamental Theorem of Galois Theory

## Theorem (Fundamental Theorem of Galois Theory)

*Let $K \to L$ be a finite separable normal field extension with Galois group $G := \mathrm{Aut}(L/K)$. For any subfiled $F$ of $L$ containing $K$, any subgroup $H < G$, let*

$$F^* := \mathrm{Aut}(L/F) := \left\{\sigma \in \mathrm{Aut}(L) : \forall x \in F\big(\sigma(x) = x\big)\right\}$$

$$H^\dagger := \left\{x \in L : \forall \sigma \in H\big(\sigma(x) = x\big)\right\}$$

*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* $F^* \lhd G$.
4. $F^* \lhd G \implies \mathrm{Aut}(F/K) \cong G/F^*$.

## Theorem

$$\begin{tikzcd} \mathbf{C} \arrow[r, shift left, "F"] \arrow[r, phantom, "\perp"] & \mathbf{D} \arrow[l, shift left, "G"] \arrow[r, shift left, "F'"] \arrow[r, phantom, "\perp"] & \mathbf{E} \arrow[l, shift left, "G'"] \end{tikzcd} \quad \Longrightarrow \quad \begin{tikzcd} \mathbf{C} \arrow[r, shift left, "F'F"] \arrow[r, phantom, "\perp"] & \mathbf{E} \arrow[l, shift left, "G'G"] \end{tikzcd}$$

## 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* $\mathbf{C} \underset{G}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}$ *are adjoint iff there are two natural transformations* $\eta : 1_{\mathbf{C}} \to GF$ *and* $\varepsilon : FG \to 1_{\mathbf{D}}$ *s.t.*

$$\begin{tikzcd} F \arrow[r, "F\eta"] \arrow[dr, "1_F"'] & FGF \arrow[d, "\varepsilon F"] \\ & F \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "\eta G"] \arrow[dr, "1_G"'] & GFG \arrow[d, "G\varepsilon"] \\ & G \end{tikzcd}$$

The natural transformations $\eta$ and $\varepsilon$ are called the *unit* and *counit* of the adjoint.

**Remark:** The triangle identities have the virtue of being entirely "algebraic" — no quantifiers, limits, $\mathrm{Hom}$-sets, infinite conditions, etc. Thus, anything defined by adjoints such as free groups, product spaces, quantifiers, ... can be defined equationally.

$$\begin{aligned} \text{category} &= \text{country} \\ \text{object} &= \text{citizen} \\ \text{morphism} &= \text{speaking in country's language} \\ \text{functor} &= \text{translation} \end{aligned}$$

- 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.

# Adjoints and Equivalent Categories

- An equivalence between categories $\mathbf{C}$ and $\mathbf{D}$ is a pair of functors $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ and a pair of natural *isomorphisms* $\eta : 1_{\mathbf{C}} \to GF$ and $\varepsilon : FG \to 1_{\mathbf{D}}$.
- An adjoint between categories $\mathbf{C}$ and $\mathbf{D}$ is a pair of functors $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ and a pair of natural *transformations* $\eta : 1_{\mathbf{C}} \to GF$ and $\varepsilon : FG \to 1_{\mathbf{D}}$ s.t.

$$\begin{tikzcd} F \arrow[r, "F\eta"] \arrow[dr, "1_F"'] & FGF \arrow[d, "\varepsilon F"] \\ & F \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "\eta G"] \arrow[dr, "1_G"'] & GFG \arrow[d, "G\varepsilon"] \\ & G \end{tikzcd}$$

**Theorem**

*If there is an equivalence* $\mathbf{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{D}$ *and a pair of natural isomorphisms* $\eta : 1_{\mathbf{C}} \to GF$ *and* $\gamma : FG \to 1_{\mathbf{D}}$, *then there is an adjoint* $F \dashv G$ *with unit* $\eta$ *and counit* $\varepsilon : FG \xrightarrow{FG\gamma^{-1}} FGFG \xrightarrow{F\eta^{-1}G} FG \xrightarrow{\gamma} 1_{\mathbf{D}}$.

Let $\theta : \mathbf{D}(F-,-) \to \mathbf{C}(-,G-)$ be the natural isomorphism witnessing $F \dashv G$. For any $A \in \mathbf{C}$, there is a distinguished morphism $\eta_A := \theta_{A,FA} 1_{FA} : A \to G(FA)$.

$$\frac{1_{FA} : FA \to FA}{\eta_A : A \to G(FA)}$$

In fact, we can recover $\theta$ from $\eta$ as follows, for $g : FA \to B$,

$$\theta_{A,B} g = \theta_{A,B}(g \circ 1_{FA}) = Gg \circ \theta_{A,FA}(1_{FA}) = Gg \circ \eta_A$$

$$\begin{tikzcd}
\mathbf{D}(FA,B) \arrow[d, "\theta_{A,B}"'] & \mathbf{D}(FA,FA) \arrow[l, "\mathbf{D}(FA,g)"'] \arrow[d, "\theta_{A,FA}"] \\
\mathbf{C}(A,GB) & \mathbf{C}(A,GFA) \arrow[l, "\mathbf{C}(A,Gg)"]
\end{tikzcd}$$

Similarly, for any $B \in \mathbf{D}$, there is a distinguished morphism $\varepsilon_B := \theta^{-1}_{GB,B} 1_{GB} : F(GB) \to B$.

$$\frac{1_{GB} : GB \to GB}{\varepsilon_B : F(GB) \to B}$$

In fact, we can recover $\theta^{-1}$ from $\varepsilon$ as follows, for $f : A \to GB$,

$$\theta^{-1}_{A,B} f = \theta^{-1}_{A,B}(1_{GB} \circ f) = \theta^{-1}_{GB,B} 1_{GB} \circ Ff = \varepsilon_B \circ Ff$$

$$\begin{tikzcd}
\mathbf{D}(FA, B) & \mathbf{D}(FGB, B) \arrow[l, "\mathbf{D}(Ff, B)"'] \\
\mathbf{C}(A, GB) \arrow[u, "\theta^{-1}_{A,B}"] & \mathbf{C}(GB, GB) \arrow[l, "\mathbf{C}(f, GB)"] \arrow[u, "\theta^{-1}_{GB,B}"']
\end{tikzcd}$$

- $1_{FA} = \varepsilon_{FA} \circ F(\eta_A)$ (substitut $FA$ for $B$ and $\eta_A$ for $f$)
- $1_{GB} = G(\varepsilon_B) \circ \eta_{GB}$ (substitut $GB$ for $A$ and $\varepsilon_B$ for $g$)

## Theorem

- *Functors* $\mathbf{C} \underset{G}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}$ *are adjoint iff there is a natural transformation* $\eta : 1_{\mathbf{C}} \to GF$, *for which for any* $f : A \to GB$ *in* $\mathbf{C}$ *there is a unique* $g : FA \to B$ *in* $\mathbf{D}$ *s.t.* $f = Gg \circ \eta_A$.

$$\begin{tikzcd} A \arrow[r, "\eta_A"] \arrow[dr, "f"'] & G(FA) \arrow[d, dashed, "Gg"] \\ & GB \end{tikzcd}$$

- *Functors* $\mathbf{C} \underset{G}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}$ *are adjoint iff there is a natural transformation* $\varepsilon : FG \to 1_{\mathbf{D}}$, *for which for any* $g : FA \to B$ *in* $\mathbf{D}$ *there is a unique* $f : A \to GB$ *in* $\mathbf{C}$ *s.t.* $g = \varepsilon_B \circ Ff$.

$$\begin{tikzcd} B & F(GB) \arrow[l, "\varepsilon_B"'] \\ & FA \arrow[ul, "g"] \arrow[u, dashed, "Ff"'] \end{tikzcd}$$

# Left/Right Adjoint & Unit/Counit

## Example

$$\frac{A \wedge B \vdash C}{\overline{A \vdash B \to C}}$$

$$F_B : X \mapsto X \wedge B \qquad G_B : X \mapsto B \to X \qquad F_B \dashv G_B$$

$$\eta_A : A \to B \to A \wedge B$$

$$\varepsilon_A : (B \to A) \wedge B \to A$$

## Example

$$\mathbf{C}(A \times B, C) \cong \mathbf{C}(A, C^B)$$

$$F_B : X \mapsto X \times B \qquad G_B : X \to X^B \qquad F_B \dashv G_B$$

$$\eta_A : A \to (A \times B)^B$$

$$\varepsilon_A : A^B \times B \to A$$

# Left/Right Adjoint via Universal Property

- A functor $F : \mathbf{C} \to \mathbf{D}$ has a right adjoint, iff, for any $B \in \mathbf{D}$, there is an object $GB \in \mathbf{C}$ and a morphism $\varepsilon_B : F(GB) \to B$ such that $(GB, \varepsilon_B)$ is a universal morphism from $F$ to $B$.

$$\begin{tikzcd} B & F(GB) \arrow[l, "\varepsilon_B"'] \\ & FA \arrow[u, dashed, "Ff"'] \arrow[ul, "g"] \end{tikzcd}$$

- A functor $G : \mathbf{D} \to \mathbf{C}$ has a left adjoint, iff, for any $A \in \mathbf{C}$, there is an object $FA \in \mathbf{D}$ and a morphism $\eta_A : A \to G(FA)$ such that $(FA, \eta_A)$ is a universal morphism from $A$ to $G$.

$$\begin{tikzcd} A \arrow[r, "\eta_A"] \arrow[dr, "f"'] & G(FA) \arrow[d, dashed, "Gg"] \\ & GB \end{tikzcd}$$

$$\boxed{\text{Universality} \equiv \text{Adjoints}}$$

## Theorem

- *Right adjoints preserve limits.*
- *Left adjoints preserve colimits.*

## Proof.

Given $\mathbf{C} \underset{G}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}$ , 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

$$\mathbf{C}^{\mathbf{I}} \underset{G_*}{\overset{F_*}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}^{\mathbf{I}}$$

Since the diagram of right-adjoints of the functors in a commutative square commutes up to natural isomorphism, then

$$\begin{tikzcd} \mathbf{C} \arrow[r, "F"] \arrow[d, "\Delta"'] & \mathbf{D} \arrow[d, "\Delta"] \\ \mathbf{C}^{\mathbf{I}} \arrow[r, "F_*"'] & \mathbf{D}^{\mathbf{I}} \end{tikzcd} \implies \begin{tikzcd} \mathbf{C} & \mathbf{D} \arrow[l, "G"'] \\ \mathbf{C}^{\mathbf{I}} \arrow[u, "\varprojlim"] & \mathbf{D}^{\mathbf{I}} \arrow[l, "G_*"] \arrow[u, "\varprojlim"'] \end{tikzcd}$$

$$G \varprojlim D \cong \varprojlim GD$$

# Example

- Right adjoints preserve limits.

$$C \to A \wedge B \vdash (C \to A) \wedge (C \to B)$$

$$\forall x(Ax \wedge Bx) \vdash \forall x Ax \wedge \forall x Bx$$

- Left adjoints preserve colimits.

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

$$\exists x(Ax \vee Bx) \vdash \exists x Ax \vee \exists x Bx$$

## 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:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta C \to D}{\Delta FC \to FD}\ (F \text{ fully faithful})}{FC \to \varprojlim FD}\ (\Delta \dashv \varprojlim)}{FC \to FL}\ (FL \cong \varprojlim FD)}{C \to L}\ (F \text{ fully faithful})$$

# Adjoint Functor Theorem for Posets

## Theorem (Adjoint Functor Theorem for Posets)

*Let $(X, \leq)$ and $(Y, \leq)$ be posets. Suppose that $Y$ has all infima, and let $g : Y \to X$ be a monotone function preserving all infima. Then $g$ has a left adjoint $f : X \to Y$, given by*

$$f(x) \coloneqq \inf \left\{ y \in Y : x \leq g(y) \right\}$$

*In particular, a monotone map $g : Y \to X$ is the right adjoint of a Galois connection iff it preserves all infima.*

## Corollary

*Suppose that $X$ has all suprema. A monotone map $f : X \to Y$ has a right adjoint iff it preserves all suprema.*

Proof.

$$g(f(x)) = g\big(\inf\{y \in Y : x \leq g(y)\}\big) = \inf\{g(y) : y \in Y \;\&\; x \leq g(y)\}$$

$$x \leq \inf\{g(y) : y \in Y \;\&\; x \leq g(y)\} = g(f(x))$$

This inequality is the unit of the adjunction.
For the counit, let $z \in Y$. Then

$$f(g(z)) = \inf\{y \in Y : g(z) \leq g(y)\}$$

Since $g(z) \leq g(z)$, we have

$$z \geq \inf\{y \in Y : g(z) \leq g(y)\} = f(g(z))$$

# Adjoint Functor Theorem

## Lemma

*A functor $G : \mathbf{D} \to \mathbf{C}$ 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 $g_i : B_i \to B$.*

## Theorem (Adjoint Functor Theorem)

*Suppose $\mathbf{D}$ is locally small and complete. Then $G : \mathbf{D} \to \mathbf{C}$ 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 $(B_i, f_i : A \to GB_i)_{i \in I}$ in $A \downarrow G$ s.t. for any $(B, f : A \to GB)$ there exists some $i \in I$ and $g_i : B_i \to B$ with $f = Gg_i \circ f_i$.*

$$\begin{tikzcd} A \arrow[r, "f_i"] \arrow[dr, "f"'] & GB_i \arrow[d, "Gg_i"] \\ & GB \end{tikzcd}$$

# Kan Extension

## Definition (Left Kan Extension)

Given functors $F : \mathbf{C} \to \mathbf{E}$ and $K : \mathbf{C} \to \mathbf{D}$, a *left Kan extension* of $F$ along $K$ is a functor $\mathrm{Lan}_K F : \mathbf{D} \to \mathbf{E}$ with a natural transformation $\eta : F \to \mathrm{Lan}_K F \circ K$ s.t. for any such pair $(G : \mathbf{D} \to \mathbf{E}, \gamma : F \to GK)$, there exists a unique natural transformation $\alpha : \mathrm{Lan}_K F \to G$ with $\gamma = \alpha K \circ \eta$.

$$\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & \arrow[d, phantom, "\Downarrow\eta"] & \mathbf{E} \\
& \mathbf{D} \arrow[ur, dashed, "\mathrm{Lan}_K F"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & \arrow[d, phantom, "\Downarrow\gamma"] & \mathbf{E} \\
& \mathbf{D} \arrow[ur, "G"'] &
\end{tikzcd}
\quad = \quad
\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & \arrow[d, phantom, "\Downarrow\eta"] & \mathbf{E} \\
& \mathbf{D} \arrow[ur, bend left, "\mathrm{Lan}_K F"] \arrow[ur, bend right, "G"'] \arrow[ur, phantom, "\Downarrow\alpha"] &
\end{tikzcd}$$

# Kan Extension

## Definition (Right Kan Extension)

Given functors $F : \mathbf{C} \to \mathbf{E}$ and $K : \mathbf{C} \to \mathbf{D}$, a *right Kan extension* of $F$ along $K$ is a functor $\mathrm{Ran}_K F : \mathbf{D} \to \mathbf{E}$ with a natural transformation $\varepsilon : \mathrm{Ran}_K F \circ K \to F$ s.t. for any such pair $(G : \mathbf{D} \to \mathbf{E}, \delta : GK \to F)$, there exists a unique natural transformation $\beta : G \to \mathrm{Ran}_K F$ with $\delta = \varepsilon \circ \beta K$.

$$\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & & \mathbf{E} \\
& \mathbf{D} \arrow[ur, dashed, "\mathrm{Ran}_K F"'] \arrow[u, phantom, "\Uparrow\varepsilon"] &
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & & \mathbf{E} \\
& \mathbf{D} \arrow[ur, "G"'] \arrow[u, phantom, "\Uparrow\delta"] &
\end{tikzcd}
\quad = \quad
\begin{tikzcd}
\mathbf{C} \arrow[rr, "F"] \arrow[dr, "K"'] & & \mathbf{E} \\
& \mathbf{D} \arrow[ur, bend left, "\mathrm{Ran}_K F"] \arrow[ur, bend right, "G"'] \arrow[u, phantom, "\Uparrow\varepsilon"] \arrow[ur, phantom, "\Leftarrow\beta"] &
\end{tikzcd}$$

# Example

For any object $A \in \mathbf{C}$ and any $F : \mathbf{C} \to \mathbf{Set}$, there is a bijection between elements $x \in FA$ and natural transformations with boundary as displayed

$$\begin{tikzcd}
\mathbf{1} \arrow[rr, "*"] \arrow[dr, "A"'] & \arrow[d, phantom, "\Downarrow x"] & \mathbf{Set} \\
& \mathbf{C} \arrow[ur, "F"'] &
\end{tikzcd}$$

By the Yoneda lemma, the representable functor $\mathbf{C}(A, -)$ and the identity $1_A : A \to A$ define the left Kan extension of $* : \mathbf{1} \to \mathbf{Set}$ along $A : \mathbf{1} \to \mathbf{C}$.

$$\begin{tikzcd}
\mathbf{1} \arrow[rr, "*"] \arrow[dr, "A"'] & \arrow[d, phantom, "\Downarrow 1_A"] & \mathbf{Set} \\
& \mathbf{C} \arrow[ur, dashed, "\mathbf{C}(A,-)"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbf{1} \arrow[rr, "*"] \arrow[dr, "A"'] & \arrow[d, phantom, "\Downarrow 1_A"] & \mathbf{Set} \\
& \mathbf{C} \arrow[ur, bend left, "\mathbf{C}(A,-)"] \arrow[ur, bend right, "F"'] \arrow[ur, phantom, "\Downarrow \psi(x)"] &
\end{tikzcd}$$

The required unique factorization is the natural transformation $\psi(x) : \mathbf{C}(A, -) \to F$ with $\psi(x)_A(1_A) = x$.

# $\mathrm{Lan}_K \dashv K^* \dashv \mathrm{Ran}_K$

## Theorem

*If the Kan extensions exist for all $F$, then $\mathrm{Lan}_K \dashv K^* \dashv \mathrm{Ran}_K$, where $K^* := - \circ K$.*

$$\begin{tikzcd}
\mathbf{E}^{\mathbf{C}} \arrow[rr, bend left=60, "\mathrm{Lan}_K"] \arrow[rr, bend right=60, "\mathrm{Ran}_K"'] \arrow[rr, phantom, "\perp"] \arrow[rr, phantom, "\perp"'] & & \mathbf{E}^{\mathbf{D}} \arrow[ll, "K^*"']
\end{tikzcd}$$

## Proof.

By the Yoneda Lemma, any pair $(G, \gamma)$, as in the definition for the left Kan extension, yields a natural transformation by $\gamma^*_H(\alpha) := \alpha K \circ \gamma$.

$$\gamma^* : \mathbf{E}^{\mathbf{D}}(G, -) \to \mathbf{E}^{\mathbf{C}}(F, - \circ K)$$

The universal property of the left Kan extension says that $(\mathrm{Lan}_K, \eta)$ yields a natural isomorphism.

$$\mathbf{E}^{\mathbf{D}}(\mathrm{Lan}_K F, -) \cong \mathbf{E}^{\mathbf{C}}(F, - \circ K)$$

# (Co)Limits as Kan Extensions

## Theorem ((Co)Limits as Kan Extensions)

1. *The left Kan extension* $\mathrm{Lan}_! D$ *of* $D : \mathbf{I} \to \mathbf{C}$ *along* $! : \mathbf{I} \to \mathbf{1}$ *defines the colimit* $\varinjlim D$.

$$\begin{tikzcd} \mathbf{I} \arrow[rr, "D"] \arrow[dr, "!"'] & \arrow[d, phantom, "\Downarrow\eta"] & \mathbf{C} \\ & \mathbf{1} \arrow[ur, "C"'] & \end{tikzcd} = \begin{tikzcd} \mathbf{I} \arrow[r, "D"] \arrow[rr, bend right, "\Delta C"'] & \arrow[d, phantom, "\Downarrow\eta"] & \mathbf{C} \end{tikzcd}$$

2. *Dually, the right Kan extension* $\mathrm{Ran}_! D$ *defines the limit* $\varprojlim D$.

$$\begin{tikzcd} \mathbf{I} \arrow[rr, "D"] \arrow[dr, "!"'] & \arrow[d, phantom, "\Uparrow\varepsilon"] & \mathbf{C} \\ & \mathbf{1} \arrow[ur, "C"'] & \end{tikzcd} = \begin{tikzcd} \mathbf{I} \arrow[r, "D"] \arrow[rr, bend right, "\Delta C"'] & \arrow[d, phantom, "\Uparrow\varepsilon"] & \mathbf{C} \end{tikzcd}$$

# Adjoints as Kan Extensions

## Theorem (Adjoints as Kan Extensions)

1. *If $F \dashv G$ is an adjoint with unit $\eta : 1_{\mathbf{C}} \to GF$ and counit $\varepsilon : FG \to 1_{\mathbf{D}}$, then $(G, \eta)$ is a left Kan extension of the identity functor $1_{\mathbf{C}}$ along $F$ and $(F, \varepsilon)$ is a right Kan extension of the identity functor $1_{\mathbf{D}}$ along $G$.*

$$\begin{tikzcd}
\mathbf{C} \arrow[rr, "1_{\mathbf{C}}"] \arrow[dr, "F"'] & \arrow[d, phantom, "\Downarrow \eta"] & \mathbf{C} \\
& \mathbf{D} \arrow[ur, dashed, "G \cong \mathrm{Lan}_F\, 1_{\mathbf{C}}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbf{D} \arrow[rr, "1_{\mathbf{D}}"] \arrow[dr, "G"'] & \arrow[d, phantom, "\Uparrow \varepsilon"] & \mathbf{D} \\
& \mathbf{C} \arrow[ur, dashed, "F \cong \mathrm{Ran}_G\, 1_{\mathbf{D}}"'] &
\end{tikzcd}$$

   *Moreover, both Kan extensions are absolute(preserved by all functors).*

2. *Conversely, if $(G, \eta : 1_{\mathbf{C}} \to GF)$ is a left Kan extension of the identity functor $1_{\mathbf{C}}$ along $F$ and if $F$ preserves this Kan extension, then $F \dashv G$ with unit $\eta$.*

# Monad

## Definition (Monad)

A *monad* $(T, \eta, \mu)$ on a category $\mathbf{C}$ consists of

- an endofunctor $T : \mathbf{C} \to \mathbf{C}$,
- a unit natural transformation $\eta : 1_{\mathbf{C}} \to T$,
- a multiplication natural transformation $\mu : T^2 \to T$

such that:

- $\mu \circ T\mu = \mu \circ \mu T$ (as natural transformations $T^3 \to T$);
- $\mu \circ T\eta = \mu \circ \eta T = 1_T$ (as natural transformations $T \to T$).

$$\begin{tikzcd} T^3 \arrow[r, "\mu T"] \arrow[d, "T\mu"'] & T^2 \arrow[d, "\mu"] \\ T^2 \arrow[r, "\mu"'] & T \end{tikzcd} \qquad \begin{tikzcd} T \arrow[r, "\eta T"] \arrow[d, "T\eta"'] \arrow[dr, equal] & T^2 \arrow[d, "\mu"] \\ T^2 \arrow[r, "\mu"'] & T \end{tikzcd}$$

# Monad

The first axiom is akin to the associativity in monoids if we think of $\mu$ 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.

$$\begin{tikzcd} T^3 \arrow[r, "\mu T"] \arrow[d, "T\mu"'] & T^2 \arrow[d, "\mu"] \\ T^2 \arrow[r, "\mu"'] & T \end{tikzcd} \qquad \begin{tikzcd} T \arrow[r, "\eta T"] \arrow[d, "T\eta"'] \arrow[dr, equal] & T^2 \arrow[d, "\mu"] \\ T^2 \arrow[r, "\mu"'] & T \end{tikzcd}$$

$$\begin{tikzcd} TTTX \arrow[r, "\mu_{TX}"] \arrow[d, "T\mu_X"'] & TTX \arrow[d, "\mu_X"] \\ TTX \arrow[r, "\mu_X"'] & TX \end{tikzcd} \qquad \begin{tikzcd} TX \arrow[r, "\eta_{TX}"] \arrow[d, "T\eta_X"'] \arrow[dr, equal] & TTX \arrow[d, "\mu_X"] \\ TTX \arrow[r, "\mu_X"'] & TX \end{tikzcd}$$

A *comonad* for a category $\mathbf{C}$ is a monad for the opposite category $\mathbf{C}^{\mathrm{op}}$.

# Comonad

## Definition (Comonad)

A *comonad* $(W, \varepsilon, \delta)$ on a category $\mathbf{C}$ consists of

- an endofunctor $W : \mathbf{C} \to \mathbf{C}$,
- a counit natural transformation $\varepsilon : W \to 1_{\mathbf{C}}$,
- a multiplication natural transformation $\delta : W \to W^2$

such that:

- $W\delta \circ \delta = \delta W \circ \delta$ (as natural transformations $W \to W^3$);
- $W\varepsilon \circ \delta = \varepsilon W \circ \delta = 1_W$ (as natural transformations $W \to W$).

$$\begin{tikzcd} W \arrow[r, "\delta"] \arrow[d, "\delta"'] & W^2 \arrow[d, "\delta W"] \\ W^2 \arrow[r, "W\delta"'] & W^3 \end{tikzcd} \qquad \begin{tikzcd} W \arrow[r, "\delta"] \arrow[d, "\delta"'] \arrow[dr, equal] & W^2 \arrow[d, "\varepsilon W"] \\ W^2 \arrow[r, "W\varepsilon"'] & W \end{tikzcd}$$

# 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 $\mathbf{Set}$.
  - $T : A \mapsto \mathrm{P}(A)$, and $T(f) : A \mapsto f(A)$ for object $A$ and morphism $f$.
  - $\eta_A : A \to \mathrm{P}(A)$ given by $\eta_A(a) := \{a\}$.
  - $\mu_A : \mathrm{P}(\mathrm{P}(A)) \to \mathrm{P}(A)$ given by $\mu_A(B) := \bigcup B$.
- Consider $\mathbf{Set}$ and a monoid $(M, e, \cdot)$, the functor $M \times - : \mathbf{Set} \to \mathbf{Set}$ has a monad structure with
  - $T : A \mapsto M \times A$, and $T(f) : (m, a) \mapsto (m, f(a))$.
  - $\eta_A : A \to M \times A :: a \mapsto (e, a)$.
  - $\mu_A : M \times M \times A \to M \times A :: (m, (n, a)) \mapsto (mn, a)$.
- A preorder $(P, \leq)$ yields a category where endofunctors are monotone functions. Given a monad $(T, \eta, \mu)$, the natural transformations $\eta$ and $\mu$ give that, for $a \in P$, $a \leq Ta$ and $TTa \leq Ta$, since $\eta_a : a \to Ta$, and $\mu_a : TTa \to Ta$. Then $Ta \leq TTa \leq Ta \implies TTa = Ta$. Monads on $(P, \leq)$ are closure operators[12].

[12] A *closure operator* on a poset $(P, \leq)$ is $T : P \to P$ s.t. for $x, y \in P$,

- $x \leq T(x)$
- $x \leq y \to T(x) \leq T(y)$
- $T(T(x)) = T(x)$

# Monads from Adjoints

## Monads from Adjoints

Any adjoint $\mathbf{C} \underset{G}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{D}$ gives rise to a monad on the category $\mathbf{C}$, with

- the endofuntor $T := GF$,
- the unit natural transformation $\eta : 1_{\mathbf{C}} \to GF$,
- the multiplication natural transformation $\mu := G\varepsilon F : GFGF \to GF$.

- $(GF, \eta, G\varepsilon F)$ is a monad.
- $(FG, \varepsilon, F\eta G)$ is a comonad.

# $\mathbb{T}$-Algebra

## Definition

Let $\mathbb{T} = (T, \eta, \mu)$ be a monad on $\mathbf{C}$. A $\mathbb{T}$-algebra is a pair $(A, \alpha)$ where $A \in \mathbf{C}$ and $\alpha : TA \to A$ s.t.

$$\begin{tikzcd} TTA \arrow[r, "T\alpha"] \arrow[d, "\mu A"'] & TA \arrow[d, "\alpha"] \\ TA \arrow[r, "\alpha"'] & A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\eta A"] \arrow[dr, "1_A"'] & TA \arrow[d, "\alpha"] \\ & A \end{tikzcd}$$

A homomorphism of $\mathbb{T}$-algebras $f : (A, \alpha) \to (B, \beta)$ is $f : A \to B$ s.t.

$$\begin{tikzcd} TA \arrow[r, "Tf"] \arrow[d, "\alpha"'] & TB \arrow[d, "\beta"] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

The category of $\mathbb{T}$-algebras and $\mathbf{T}$-algebra homomorphisms is denoted $\mathbf{C}^{\mathbf{T}}$. This is called the Eilenberg-Moore category.

## Theorem

*Every monad* $\mathrm{T} = (T, \eta, \mu)$ *arises from an adjoint* $\mathbf{C} \underset{U}{\overset{F}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{C}^{\mathrm{T}}$ .

*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 $(A, \mu_A)$ is a $\mathrm{T}$-algebra.
Clearly $UF(A) = U(TA, \mu_A) = T(A)$, and we have a natural transformation $\dot{\eta} = \eta : 1_{\mathbf{C}} \to UF$.
Define $\dot{\varepsilon} : FU \to 1_{\mathbf{C}^{\mathrm{T}}}$ by $\dot{\varepsilon}_{(A,\alpha)} = \alpha : TA \to A$.
It is easy to check that $(\dot{\eta}, \dot{\varepsilon}) : F \dashv U$.
For $A \in \mathbf{C}$, $U\dot{\varepsilon}F(A) = U\dot{\varepsilon}_{FA} = U\dot{\varepsilon}_{(TA,\mu_A)} = U\mu_A = \mu_A$.

# 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 $\otimes : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$ 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 $\alpha$, 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 $\lambda$ and $\rho$, 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 $\alpha, \lambda$ and $\rho$ are identities.

# Monoidal Category

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[r, "\alpha_{A,B,C\otimes D}"] \arrow[d, "1_A \otimes \alpha_{B,C,D}"'] & (A \otimes B) \otimes (C \otimes D) \arrow[r, "\alpha_{A\otimes B,C,D}"] & ((A \otimes B) \otimes C) \otimes D \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "\alpha_{A,B\otimes C,D}"'] & & (A \otimes (B \otimes C)) \otimes D \arrow[u, "\alpha_{A,B,C} \otimes 1_D"']
\end{tikzcd}$$

$$\begin{tikzcd}
A \otimes (I \otimes B) \arrow[rr, "\alpha_{A,I,B}"] \arrow[dr, "1_A \otimes \lambda_B"'] & & (A \otimes I) \otimes B \arrow[dl, "\rho_A \otimes 1_B"] \\
& A \otimes B &
\end{tikzcd}$$

# 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: $\mathbf{Set}$ and $\mathbf{Cat}$.
4. The category of all endofunctors on a category $\mathbf{C}$ 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 $\sigma$ called the *braiding* that assigns to every pair of objects $A, B \in \mathbf{C}$ an isomorphism $\sigma_{A,B} : A \otimes B \to B \otimes A$ such that,

$$\begin{tikzcd}
A \otimes (B \otimes C) \arrow[r, "\alpha_{A,B,C}"] \arrow[d, "\sigma_{A,B\otimes C}"'] & (A \otimes B) \otimes C \arrow[r, "\sigma_{A,B} \otimes 1_C"] & (B \otimes A) \otimes C \arrow[d, "\alpha^{-1}_{B,A,C}"] \\
(B \otimes C) \otimes A & B \otimes (C \otimes A) \arrow[l, "\alpha_{B,C,A}"] & B \otimes (A \otimes C) \arrow[l, "1_B \otimes \sigma_{A,C}"]
\end{tikzcd}$$

$$\begin{tikzcd}
(A \otimes B) \otimes C \arrow[r, "\alpha^{-1}_{A,B,C}"] \arrow[d, "\sigma_{A\otimes B,C}"'] & A \otimes (B \otimes C) \arrow[r, "1_A \otimes \sigma_{B,C}"] & A \otimes (C \otimes B) \arrow[d, "\alpha_{A,C,B}"] \\
C \otimes (A \otimes B) & (C \otimes A) \otimes B \arrow[l, "\alpha^{-1}_{C,A,B}"] & (A \otimes C) \otimes B \arrow[l, "\sigma_{A,C} \otimes 1_B"]
\end{tikzcd}$$

# Symmetric Monoidal Category

## Definition (Symmetric Monoidal Category)

A *symmetric monoidal category* is a braided monoidal category where the braiding satisfies $\sigma_{B,A} \circ \sigma_{A,B} = 1_{A \otimes B}$.

## Theorem

*Every (symmetric) monoidal category is monoidally equivalent to a (symmetric) strict monoidal category.*

# Dagger Category

## Definition (Dagger Category)

A *dagger category* is a category $\mathbf{C}$ such that for any morphism $f : A \to B$ in $\mathbf{C}$ there is a specified morphism $f^\dagger : B \to A$ such that for all $f : A \to B$ and $g : B \to C$,

- $1_A^\dagger = 1_A$
- $(gf)^\dagger = f^\dagger g^\dagger$
- $(f^\dagger)^\dagger = f$

## Definition

A morphism $f : A \to B$ in a dagger category is:

- the *adjoint* of $g : B \to A$ if $g = f^\dagger$;
- *self-adjoint* if $f = f^\dagger$ (and $A = B$);
- *idempotent* if $ff = f$ (and $A = B$);
- a *projection* if it is idempotent and self-adjoint;
- *unitary* if both $f^\dagger f = 1_A$ and $ff^\dagger = 1_B$;
- an *isometry* if $f^\dagger f = 1_A$;
- a *partial isometry* if $f^\dagger f$ is a projection;
- *positive* if $f = g^\dagger g$ for some morphism $g : A \to B$ (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 $\eta_A : I \to A^* \otimes A$, and a counit $\varepsilon_A : A \otimes A^* \to I$ such that

$$\begin{tikzcd}
A \arrow[r, "\rho_A^{-1}"] \arrow[d, "1_A"'] & A \otimes I \arrow[r, "1_A \otimes \eta_A"] & A \otimes (A^* \otimes A) \arrow[d, "\alpha_{A,A^*,A}"] \\
A & I \otimes A \arrow[l, "\lambda_A"] & (A \otimes A^*) \otimes A \arrow[l, "\varepsilon_A \otimes 1_A"]
\end{tikzcd}$$

$$\begin{tikzcd}
A^* \arrow[r, "\lambda_{A^*}^{-1}"] \arrow[d, "1_{A^*}"'] & I \otimes A^* \arrow[r, "\eta_A \otimes 1_{A^*}"] & (A^* \otimes A) \otimes A^* \arrow[d, "\alpha^{-1}_{A^*,A,A^*}"] \\
A^* & A^* \otimes I \arrow[l, "\rho_{A^*}"] & A^* \otimes (A \otimes A^*) \arrow[l, "1_{A^*} \otimes \varepsilon_A"]
\end{tikzcd}$$

# 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:

$$\begin{tikzcd} I \arrow[r, "\varepsilon_A^\dagger"] \arrow[dr, "\eta_A"'] & A \otimes A^* \arrow[d, "\sigma_{A,A^*}"] \\ & A^* \otimes A \end{tikzcd}$$

## Examples

- The category $\mathbf{Rel}$ of Sets and relations. The product is the Cartesian product. The dagger is the relational converse.
- The category $\mathbf{FdHilb}$ 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.

# Enrichment in a Monoidal Category

## Definition (Enrichment in a Monoidal Category)

Let $(V, \otimes, I, \lambda, \rho)$ be a monoidal category. Then a $V$-category $\mathbf{C}$ consists of

- a class $\mathrm{ob}(\mathbf{C})$ of objects.
- a hom-object $\mathbf{C}(a, b)$ in $V$ for each pair $a, b \in \mathrm{ob}(\mathbf{C})$.
- an arrow $\mathrm{id}_a : I \to \mathbf{C}(a, a)$ in $V$ for each $a \in \mathrm{ob}(\mathbf{C})$.
- an arrow $\circ_{abc} : \mathbf{C}(b, c) \otimes \mathbf{C}(a, b) \to \mathbf{C}(a, c)$ in $V$ for each triple $a, b, c \in \mathrm{ob}(\mathbf{C})$ such that

$$
\begin{tikzcd}
(\mathbf{C}(c,d) \otimes \mathbf{C}(b,c)) \otimes \mathbf{C}(a,b) \arrow[rr, "\alpha"] \arrow[d, "\circ_{bcd} \otimes 1"'] & & \mathbf{C}(c,d) \otimes (\mathbf{C}(b,c) \otimes \mathbf{C}(a,b)) \arrow[d, "1 \otimes \circ_{abc}"] \\
\mathbf{C}(b,d) \otimes \mathbf{C}(a,b) \arrow[r, "\circ_{abd}"'] & \mathbf{C}(a,d) & \mathbf{C}(c,d) \otimes \mathbf{C}(a,c) \arrow[l, "\circ_{acd}"] \\
\mathbf{C}(b,b) \otimes \mathbf{C}(a,b) \arrow[r, "\circ_{abb}"] & \mathbf{C}(a,b) & \mathbf{C}(a,b) \otimes \mathbf{C}(a,a) \arrow[l, "\circ_{aab}"'] \\
I \otimes \mathbf{C}(a,b) \arrow[u, "\mathrm{id}_b \otimes 1"] \arrow[ur, "\lambda"'] & & \mathbf{C}(a,b) \otimes I \arrow[u, "1 \otimes \mathrm{id}_a"'] \arrow[ul, "\rho"]
\end{tikzcd}
$$

# Lawvere Metric Space

## Definition (Lawvere Metric Space)

A Lawvere metric space is a set $X$ with a function $d : X \times X \to [0, \infty]$ 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 $\mathbf{Cost} := ([0, \infty], \geq, +, 0)$, where the tensor product is $+$, and the identity is $0$.

$$\mathrm{Hom}(x, y) := d(x, y) \in \mathrm{ob}(\mathbf{Cost})$$

# Sheaf

- The topology $\mathcal{O}(X)$ of $X$, i.e. the poset of open subsets of $X$, ordered by inclusion, can be considered to be a category.
- A presheaf $F : \mathcal{O}(X)^{\mathrm{op}} \to \mathbf{Set}$ is a *sheaf* if it satisfies:
  1. (Locality) For any open cover $(U_i)_{i \in I}$ of $U$, and for $s, t \in F(U)$, and $\forall i : s\restriction_{U_i} = t\restriction_{U_i}$, 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 $\forall i, j : s_i\restriction_{U_i \cap U_j} = s_j\restriction_{U_i \cap U_j}$, then there exists some $s \in F(U)$ such that $\forall i : s\restriction_{U_i} = s_i$.
- 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

- A presheaf $F$ is a *sheaf* if for any open cover $(U_i)_{i \in I}$ of $U$, the following diagram is an equalizer:

$$F(U) \xrightarrow{e} \prod_i F(U_i) \underset{g}{\overset{f}{\rightrightarrows}} \prod_{i,j} F(U_i \cap U_j)$$

Where $e, f, g$ are given by the restriction maps:

$$\mathrm{res}^{U}_{U_i} : F(U) \to F(U_i)$$

$$\mathrm{res}^{U_i}_{U_i \cap U_j} : F(U_i) \to F(U_i \cap U_j)$$

$$\mathrm{res}^{U_j}_{U_i \cap U_j} : F(U_j) \to F(U_i \cap U_j)$$

$$\begin{tikzcd}
 & F(U_i) \arrow[r, "F(U_i \cap U_j \hookrightarrow U_i)"] & F(U_i \cap U_j) \\
F(U) \arrow[ur, "F(U_i \hookrightarrow U)"] \arrow[r, tail, "e"] \arrow[dr, "F(U_j \hookrightarrow U)"'] & \prod_i F(U_i) \arrow[u, "\pi_i"'] \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] \arrow[d, "\pi_j"] & \prod_{i,j} F(U_i \cap U_j) \arrow[u, "\pi_{ij}"'] \arrow[d, "\pi_{ij}"] \\
 & F(U_j) \arrow[r, "F(U_i \cap U_j \hookrightarrow U_j)"'] & F(U_i \cap U_j)
\end{tikzcd}$$

# Sheaf

- Let $\mathbf{I}$ be a category with $\mathrm{ob}(\mathbf{I}) := \{U_i : i \in I\} \cup \{U_i \cap U_j : i, j \in I\}$, and the morphisms are the inclusions of $U_i \cap U_j$ in $U_i$ and $U_j$.

$$U_i \hookleftarrow U_i \cap U_j \hookrightarrow U_j$$

Then $U$ can be taken as a colimit of $\mathbf{I}$.

$$\begin{tikzcd}
F(U_i) \arrow[r] & F(U_i \cap U_j) & F(U_j) \arrow[l] \\
& F(U) \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

A presheaf $F$ is a *sheaf* if $\varprojlim_{\mathbf{I}} F \cong F(U)$.

# Etale Bundle

- Consider the slice category $\mathbf{Top}/X$. An *étale bundle* over $X$ is $(Y, f : Y \to X)$ 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 $f\restriction_U : U \to f(U)$ is a homeomorphism.
- The category $\mathbf{Et}(X)$ is the category of étale bundles over $X$ and morphisms are the continous functions between them.
- $\widehat{\mathcal{O}(X)} \underset{\Gamma}{\overset{\Lambda}{\underset{\longleftarrow}{\overset{\longrightarrow}{\perp}}}} \mathbf{Top}/X$

  where $\Gamma : Y \xrightarrow{f} X \mapsto \left\{s : U \to Y : f \circ s = i : U \hookrightarrow X\right\}$, while $\Lambda : F \mapsto \coprod_{x \in X} F_x$ and $F_x := \varinjlim_{U \ni x} FU$. There are natural transformations

  $$\eta_F : F \to \Gamma\Lambda F, \quad \varepsilon_Y : \Lambda\Gamma Y \to Y$$

  for $F$ a presheaf and $Y$ a bundle which are unit and counit.
- If $F$ is a sheaf, $\eta_F$ is an isomorphism, while if $Y$ is étale, $\varepsilon_Y$ is an isomorphism. $\mathbf{Sh}(X) \underset{\longleftarrow}{\overset{\longrightarrow}{\cong}} \mathbf{Et}(X)$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Welcome to Cantor's Paradise

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory
- Axioms of ZFC
- Ordinal Numbers
- Cardinal Numbers
- Axiom of Choice

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

$X$

$X \cap Y$

$X \cup Y$

$\overline{X}$

$X \Delta Y$

$X \setminus Y$

# 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 $Y = \{x : A(x)\}$.
$$R := \{x : x \notin x\} \quad R \in R? \qquad \text{(Russell Paradox)}$$
- **Separation Schema**.
For any formula $A$, for any $X$, there exists a set $Y = \{u \in X : A(x)\}$.
$$\forall X \exists Y \forall u(u \in Y \leftrightarrow u \in X \wedge A(x))$$

# 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 $Y = \mathrm{P}(X) := \{u : u \subset X\}$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \forall z (z \in u \to z \in X))$$

- **Union**. For any $X$ there exists a set $Y = \bigcup X$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \exists z (z \in X \wedge u \in z))$$

$$\bigcup_{i \in I} X_i := \bigcup \{X_i : i \in I\}$$

$$\bigcap X := \{u : \forall z (z \in X \to u \in z)\}$$

# Relation

- ordered pair.

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\}$$
$$(a_1, \ldots, a_{n+1}) \coloneqq ((a_1, \ldots, a_n), a_{n+1})$$

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \to a_i = b_i \quad \text{for} \quad 1 \leq i \leq n$$

$$X \subsetneq Y \quad X \cup Y \quad X \cap Y \quad X \setminus Y \quad X \Delta Y \quad X \times Y \quad \prod_{i=1}^{n} X_i \quad X^n$$

- $n$-ary relation $R$ on $X_1, \ldots, X_n$.

$$R \subset \prod_{i=1}^{n} X_i$$

$$R(x_1, \ldots, x_n) \coloneqq (x_1, \ldots, x_n) \in R$$

# Equivalence Relation, Quotient, Partition

- $x \sim x$ (Reflexivity)
- $x \sim y \to y \sim x$ (Symmetry)
- $x \sim y \wedge y \sim x \to x \sim z$ (Transitivity)
- equivalence class: $[x] := \{y \in X : x \sim y\}$
- quotient set: $X/\!\sim\; := \big\{[x] : x \in X\big\}$

Figure: torus $\mathbb{R}^2/\!\sim$

$$(x, y) \sim (x', y') \;:=\; (x - x', y - y') \in \mathbb{Z}^2$$

- we say $\mathcal{P} \subset \mathrm{P}(X)$ is a partition of $X$ if
  1. $\forall xy \in \mathcal{P} : x \neq y \to x \cap y = \emptyset$
  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
  $R(x, y) \iff \exists A \in \mathcal{P}(x, y \in A)$.

# Function

- A $n$-ary operation $f : \prod_{i=1}^{n} X_i \to Y$ is a function if

$$(\mathbf{x}, y) \in f \wedge (\mathbf{x}, z) \in f \to y = z$$

- injection (one-to-one). $f : X \rightarrowtail Y$

$$f(x) = f(y) \to x = y$$

- surjection (onto). $f : X \twoheadrightarrow Y$.

$$\forall y \in Y \exists x \in X (f(x) = y)$$

- bijection. $f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$
- restriction. composition. image. inverse image. inverse function.

$$f\restriction_A := \{(x, y) \in f : x \in A\} \quad (f \circ g)(x) := f(g(x))$$

$$f(A) := \{f(x) : x \in A\} \quad f^{-1}(A) := \{x : f(x) \in A\}$$

# Exercises

In **Set**,

$$
\begin{aligned}
f : X \rightarrowtail Y \quad & \text{iff} \quad \exists g : Y \to X : gf = 1_X \\
& \text{iff} \quad \forall Z \forall g_1 g_2 : Z \to X : fg_1 = fg_2 \implies g_1 = g_2 \\
f : X \twoheadrightarrow Y \quad & \text{iff} \quad \exists g : Y \to X : fg = 1_Y \\
& \text{iff} \quad \forall Z \forall g_1 g_2 : Y \to Z : g_1 f = g_2 f \implies g_1 = g_2
\end{aligned}
$$

$$
\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "1_X"'] & Y \arrow[d, "g"] \\
& X
\end{tikzcd}
\qquad
\begin{tikzcd}
Y \arrow[r, "g"] \arrow[dr, "1_Y"'] & X \arrow[d, "f"] \\
& Y
\end{tikzcd}
$$

$$
\begin{tikzcd}
Z \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & X \arrow[r, "f"] & Y
\end{tikzcd}
\qquad
\begin{tikzcd}
X \arrow[r, "f"] & Y \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & Z
\end{tikzcd}
$$

$f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$ iff the diagram commutes:

$$
\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "1_X"'] & Y \arrow[d, "g"] \arrow[dr, "1_Y"] & \\
& X \arrow[r, "f"'] & Y
\end{tikzcd}
$$

# Equivalence Relation / Partition / Transformation Group

## Definition (Transformation Group)

A *transformation group* $G$ is a non-empty set of bijections s.t.

1. the identity $1_G \in G$;
2. if $f, g \in G$, then their coposition $g \circ f \in G$;
3. if $f \in G$, then its inverse $f^{-1} \in G$.

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 equivalent relation, then there is a group $G$ s.t. $R(x, y) \iff \exists f \in G : y = f(x)$.

# Order

- partial order: $x \leq x, x \leq y \wedge y \leq x \rightarrow x = y, x \leq y \wedge y \leq z \rightarrow x \leq z$.
- strict partial order: $x \not< x, x < y \wedge y < z \rightarrow x < z$.
- total order: partial order with $x \leq y \vee y \leq x$.
- A total order of $P$ is a *well order* if every nonempty 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 $X$ if $a \in X \wedge \forall x \in X(a \leq x \rightarrow a = x)$;
- $a$ is a *greatest* element of $X$ if $a \in X \wedge \forall x \in X(x \leq a)$;
- $a$ is an *upper bound* of $X$ if $\forall x \in X(x \leq a)$;
- $a$ is the *supremum* of $X$ if $a$ 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.

$$\forall xyz(A(x,y) \wedge A(x,z) \to y = z) \to \forall X \exists Y \forall y(y \in Y \leftrightarrow \exists x \in X A(x,y))$$

- **Axiom of Regularity**. Every nonempty set has an $\in$-minimal element.

$$\forall X(X \neq \emptyset \to \exists x(x \in X \wedge X \cap x = \emptyset))$$

- **Axiom of Infinity**.

$$\exists X(\emptyset \in X \wedge \forall x(x \in X \to x \cup \{x\} \in X))$$

- **Axiom of Choice** (AC). For any set $X$ of nonempty sets, there exists a choice function $f$ defined on $X$.

$$\forall X \left[\emptyset \notin X \to \exists f : X \to \bigcup X \;\; \forall A \in X \, (f(A) \in A)\right]$$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory
- Axioms of ZFC
- Ordinal Numbers
- Cardinal Numbers
- Axiom of Choice

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Ordinal vs Cardinal

- ordinal. ("length") A set is an ordinal if it is transitive and well-ordered by $\in$. or equivalently,

$$\mathrm{Ord}(x) \;:=\; \bigcup x \subset x \wedge \forall yz(y \in x \wedge z \in x \to y \in z \vee y = z \vee z \in y)$$

- cardinal. ("size") $\mathrm{Card}(x) \;:=\; \mathrm{Ord}(x) \wedge \forall y \in x(|y| \neq |x|)$

$$|M| = |N| \;:=\; \exists f : M \rightarrowtail\!\!\!\!\twoheadrightarrow N \qquad |M| \leq |N| \;:=\; \exists f : M \rightarrowtail N$$

$$|M| := \min\{\alpha \in \mathrm{Ord} : |\alpha| = |M|\}$$

The infinite ordinal numbers that are cardinals are called alephs.

# Ordinal

$$\alpha < \beta := \alpha \in \beta$$

- $\emptyset$ is an ordinal.
- If $\alpha$ is an ordinal and $\beta \in \alpha$, then $\beta$ is an ordinal.
- If $\alpha \neq \beta$ are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.
- If $\alpha, \beta$ are ordinals, then either $\alpha \subset \beta$ or $\beta \subset \alpha$.
- $<$ is a linear ordering of the class *Ord*.
- For each $\alpha$, $\alpha = \{\beta : \beta < \alpha\}$.
- If $C$ is a nonempty class of ordinals, then $\bigcap C$ is an ordinal, $\bigcap C \in C$ and $\bigcap C = \inf C$.
- If $X$ is a nonempty set of ordinals, then $\bigcup X$ is an ordinal, $\bigcup X = \sup X$.
- For every $\alpha$, $\alpha \cup \{\alpha\}$ 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"?

$$\alpha + 1 := \alpha \cup \{\alpha\}$$

$$0 := \emptyset, \quad 1 := 0 + 1, \quad 2 := 1 + 1, \quad 3 := 2 + 1, \ldots$$

- A set $A$ is inductive if $\emptyset \in A$ and $\forall x \in A : x + 1 \in A$.
- A natural number is a set that belongs to every inductive set.

$$\mathbb{N} := \big\{n : \forall A\big(\emptyset \in A \wedge \forall x \in A(x + 1 \in A) \rightarrow n \in A\big)\big\}$$

- A set $A$ is finite if $\exists n \in \mathbb{N} : |A| = n$.
- A set $A$ is countable if $|A| \leq |\mathbb{N}|$.

# Integer $\mathbb{Z}$

$$(m,n) \sim (p,q) := m +_{\mathbb{N}} q = p +_{\mathbb{N}} n$$

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim$$

$$\begin{aligned}
0_{\mathbb{Z}} &:= [(0,0)] \\
[(m,n)] \leq_{\mathbb{Z}} [(p,q)] &:= m +_{\mathbb{N}} q \leq_{\mathbb{N}} p +_{\mathbb{N}} n \\
[(m,n)] +_{\mathbb{Z}} [(p,q)] &:= [(m +_{\mathbb{N}} p, n +_{\mathbb{N}} q)] \\
[(m,n)] \cdot_{\mathbb{Z}} [(p,q)] &:= [(m \cdot_{\mathbb{N}} p + n \cdot_{\mathbb{N}} q, m \cdot_{\mathbb{N}} q + n \cdot_{\mathbb{N}} p)] \\
- [(m,n)] &:= [(n,m)]
\end{aligned}$$

$$\mathbb{Z}^+ := \{x \in \mathbb{Z} : x >_{\mathbb{Z}} 0_{\mathbb{Z}}\}$$

$$\exists f : \mathbb{N} \to \mathbb{Z} \quad n \mapsto [(n,0)]$$

# Rational Number $\mathbb{Q}$

$$(m, n) \sim (p, q) \coloneqq m \cdot_{\mathbb{Z}} q = p \cdot_{\mathbb{Z}} n$$

$$\mathbb{Q} \coloneqq \mathbb{Z} \times \mathbb{Z}^{+} / \sim$$

$$0_{\mathbb{Q}} \coloneqq [(0_{\mathbb{Z}}, x)]$$

$$1_{\mathbb{Q}} \coloneqq [(x, x)]$$

$$[(m, n)] \leq_{\mathbb{Q}} [(p, q)] \coloneqq m \cdot_{\mathbb{Z}} q \leq_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n$$

$$[(m, n)] +_{\mathbb{Q}} [(p, q)] \coloneqq [(m \cdot_{\mathbb{Z}} q +_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n, n \cdot_{\mathbb{Z}} q)]$$

$$[(m, n)] \cdot_{\mathbb{Q}} [(p, q)] \coloneqq [(m \cdot_{\mathbb{Z}} p, n \cdot_{\mathbb{Z}} q)]$$

$$- [(m, n)] \coloneqq [(-m, n)]$$

$$\exists f : \mathbb{Z} \to \mathbb{Q} \quad x \mapsto [(x, 1)]$$

# Dedekind Cut and Real Number $\mathbb{R}$

## Definition (Real Number)

$\mathbb{R}$ is the set of all $x \in \mathrm{P}(\mathbb{Q})$ s.t.

- $x \neq \emptyset,\ x \neq \mathbb{Q}$
- $\forall p \in x \exists q \in x : p < q$
- $\forall pq \in x : p \in x \wedge q < p \rightarrow q \in x$

## Theorem (Least-upper-bound)

*Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound.*

$$\exists f : \mathbb{Q} \rightarrow \mathbb{R} \quad x \mapsto \{q \in \mathbb{Q} : q < x\}$$

$$x \leq_{\mathbb{R}} y := x \subset y$$

$$x +_{\mathbb{R}} y := \{p +_{\mathbb{Q}} q : p \in x \ \&\ q \in y\}$$

$$-x := \{q \in \mathbb{Q} : \exists p > q(-p \notin x)\}$$

$$|x| := x \cup -x$$

$$x \cdot_{\mathbb{R}} y := \begin{cases} \{r : r \leq p \cdot_{\mathbb{Q}} q \ \&\ p \in x \ \&\ q \in y\} & \text{if } x > 0, y > 0 \\ 0 & \text{if } x = 0 \text{ or } y = 0 \\ |x| \cdot_{\mathbb{R}} |y| & \text{if } x < 0, y < 0 \\ -(|x| \cdot_{\mathbb{R}} |y|) & \text{if } x < 0, y > 0 \text{ or } x > 0, y < 0 \end{cases}$$

# Ordinal

$0, 1, 2, 3, \ldots$

$\omega, \omega + 1, \omega + 2, \ldots$

$\omega \cdot 2, (\omega \cdot 2) + 1, (\omega \cdot 2) + 2, \ldots$

$\vdots$

$\omega^2, \omega^2 + 1, \omega^2 + 2, \ldots$

$\vdots$

$\omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \ldots$

$\vdots$

$\omega^{\omega^\omega}, \ldots$

$\vdots$

$\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}, \ldots$

$\vdots$

# 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

$$F_n^2 + F_{n+1}^2 = F_{2n+2} \text{ and } F_{n+1}^2 + 2F_nF_{n+1} = F_{2n+3}$$

**Problem**

*For all natural numbers $n$, $n \not< n$.*

# Induction — Example? $^{\circledcirc}\hat{\mathrm{o}}^{\circledcirc}$

## All horses are the same color. $^{\odot}\hat{\nabla}^{\odot}$

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. $^{\&}\hat{\mathrm{o}}^{\&}$

Assume the contrary. Then there is a lowest non-interesting positive integer. But that's pretty interesting!

# Induction — Example? ⊚ô⊚

## Surprise Exam Paradox ⊚Δ̂⊚

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.

$$P(F_1) = P\left(\bigcap_{n=1}^{\infty} E_n\right) = \lim_{n\to\infty} P(E_n) = \prod_{i=1}^{\infty} \frac{9n}{9n+1} = 0$$

$$\forall i : P(F_i) = 0 \implies P\left(\bigcup_{i=1}^{\infty} F_i\right) \leq \sum_{i=1}^{\infty} P(F_i) = 0$$

# 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 $3/4, 4/5, 5/6, 6/7 \ldots$ 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 $G : V \to V$, there exists a unique function $F : \mathrm{Ord} \to V$ s.t.*

$$F(\alpha) = G(F\restriction_\alpha)$$

*for each $\alpha$.*

# Ordinal Arithmetic

## Definition (Addition)

1. $\alpha + 0 = \alpha$
2. $\alpha + (\beta + 1) = \alpha + \beta + 1$
3. $\alpha + \beta = \lim_{\xi \to \beta} (\alpha + \xi)$ for limit $\beta > 0$

## Definition (Multiplication)

1. $\alpha \cdot 0 = 0$
2. $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$
3. $\alpha \cdot \beta = \lim_{\xi \to \beta} \alpha \cdot \xi$ for limit $\beta > 0$

## Definition (Exponentiation)

1. $\alpha^0 = 1$
2. $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$
3. $\alpha^\beta = \lim_{\xi \to \beta} \alpha^\xi$ for limit $\beta > 0$

$$
\begin{aligned}
\omega &= && 0 < 1 < 2 < 3 < \cdots \\
\omega + 1 &= && 0 < 1 < 2 < 3 < \cdots < \omega \\
1 + \omega &= && \bullet < 0 < 1 < 2 < 3 < \cdots
\end{aligned}
$$

- $1 + \omega = \omega \neq \omega + 1$
- $2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega$
- $(\omega + 1) \cdot 2 \neq \omega \cdot 2 + 1 \cdot 2$
- $(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2$
- $\beta < \gamma \to \alpha + \beta < \alpha + \gamma$
- $\alpha < \beta \to \exists \delta (\alpha + \delta = \beta)$
- $\beta < \gamma \wedge \alpha > 0 \to \alpha \cdot \beta < \alpha \cdot \gamma$
- $\beta < \gamma \wedge \alpha > 1 \to \alpha^\beta < \alpha^\gamma$
- $\alpha > 0 \to \forall \gamma \exists! \beta \exists! \rho < \alpha (\gamma = \alpha \cdot \beta + \rho)$
- $\alpha < \beta \to \alpha + \gamma \leq \beta + \gamma$
- $\alpha < \beta \to \alpha \cdot \gamma \leq \beta \cdot \gamma$
- $\alpha < \beta \to \alpha^\gamma \leq \beta^\gamma$
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
- $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
- $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$

# 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 $k_1, \ldots, k_n \in \mathbb{N}^+$.*

# 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 to 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

$(7,6) \quad (\omega \cdot 2 + 1, \omega \cdot 2) \quad (\frac{19}{8}, \frac{39}{16})$

# Well-Founded Relation

- $R \subset A^2$ is *set-like* if $\mathrm{ext}_R(x) := \{y \in A : Ryx\}$ is a set for every $x \in A$.
- $y \in A$ is *$R$-minimal* in $A$ if $\neg\exists z(z \in A \wedge Rzy)$.
- A set-like relation $R$ is *well-founded* on $A$ if every non-empty set $X \subset A$ has a $R$-minimal element.
- $R$ *well-orders* $A$ if $R$ 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.*

$$\forall x \in \min(A)\, P(x) \wedge \forall x \in A\, [\forall y \in A\, (Ryx \to P(y)) \to P(x)] \to \forall x \in A\, P(x)$$

**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 $x \in A$,*

$$F(x) = G(x, F\restriction_{\mathrm{ext}_R(x)})$$

# Perfect Set

- $x$ is a *limit point* of $A$ if 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 $A' = A$.

$$\boxed{\text{Every perfect set has cardinality } 2^{\aleph_0}.}$$

- $\mathrm{rank}(A) := \mu\alpha[A_\alpha = A_{\alpha+1}]$ where

$$\begin{aligned} A_0 &:= A \\ A_{\alpha+1} &:= A'_\alpha \\ A_\alpha &:= \bigcap_{\gamma<\alpha} A_\gamma \quad \text{if } \alpha \text{ is a limit ordinal.} \end{aligned}$$

# 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 $P := A_{\mathrm{rank}(A)}$. Then

$$A \setminus P = \bigcup_{\alpha < \mathrm{rank}(A)} \left(A_\alpha \setminus A'_\alpha\right)$$

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 $\alpha$ s.t. $a$ is an isolated point of $A_\alpha$.
Let $f(a) := \mu k[A_\alpha \cap J_k = \{a\}]$. Then $f : A \setminus P \to \mathbb{N}$ is injective.

# Trigonometric Expansion

## Definition (Trigonometric Expansion)

A function $f : \mathbb{R} \to \mathbb{C}$ *admits a trigonometric expansion* if

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos nx + b_n \sin nx\right)$$

For example, a continuously differentiable function admits a trigonometric expansion, where $a_n, b_n$ can be computed by Fourier formulae

$$a_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \cos nt \, \mathrm{d}t$$

$$b_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \sin nt \, \mathrm{d}t$$

# 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 $A_{\mathrm{rank}(A)} = \emptyset$, then*

$$\forall x \in \mathbb{R} \backslash A \left( \frac{a_0}{2} + \sum_{n=1}^{\infty} \left( a_n \cos nx + b_n \sin nx \right) = 0 \right) \implies \forall n \in \mathbb{N} \left( a_n = b_n = 0 \right)$$

If $f$ is continuous at all but countable points, then it admits an unique trigonometric expansion.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory
- Axioms of ZFC
- Ordinal Numbers
- Cardinal Numbers
- Axiom of Choice

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# How do we count a finite set?

$$M := \{\text{apple}, \text{orange}, \text{banana}, \text{grape}\}$$

What does $|M| = 4$ mean?
There is a bijection between $M$ and $N := \{1, 2, 3, 4\}$.

$$\begin{array}{lcl} \text{apple} & \longleftrightarrow & 1 \\ \text{orange} & \longleftrightarrow & 2 \\ \text{banana} & \longleftrightarrow & 3 \\ \text{grape} & \longleftrightarrow & 4 \end{array}$$

$$|M| = |N| \;:=\; \exists f : M \rightarrowtail\!\!\!\!\twoheadrightarrow N$$

A set $A$ is finite if $\exists n \in \mathbb{N} : |A| = n$.

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?

$$M := \{\text{apple}, \text{orange}, \text{banana}, \text{grape}\}$$

$$N := \{\text{John}, \text{Peter}, \text{Bell}, \text{Emma}, \text{Sam}\}$$

What does $|M| \leq |N|$ mean?

$$\begin{array}{lcccr} \text{apple} & \longleftrightarrow & 1 & \longleftrightarrow & \text{John} \\ \text{orange} & \longleftrightarrow & 2 & \longleftrightarrow & \text{Peter} \\ \text{banana} & \longleftrightarrow & 3 & \longleftrightarrow & \text{Bell} \\ \text{grape} & \longleftrightarrow & 4 & \longleftrightarrow & \text{Emma} \\ & & 5 & \longleftrightarrow & \text{Sam} \end{array}$$

$$\begin{array}{lcr} \text{apple} & \longrightarrow & \text{John} \\ \text{orange} & \longrightarrow & \text{Peter} \\ \text{banana} & \longrightarrow & \text{Bell} \\ \text{grape} & \longrightarrow & \text{Emma} \\ & & \text{Sam} \end{array}$$

$$|M| \leq |N| \;:=\; \exists f : M \rightarrowtail N$$

$$|M| \leq |N| \;:=\; \exists f : N \twoheadrightarrow M$$

$$\begin{array}{lcr} \text{apple} & \longleftarrow & \text{John} \\ \text{orange} & \longleftarrow & \text{Peter} \\ \text{banana} & \longleftarrow & \text{Bell} \\ \text{grape} & \longleftarrow & \text{Emma} \\ & \nwarrow & \text{Sam} \end{array}$$

# The way of comparing the size of finite sets generalizes to infinite sets!

$$|\mathbb{N}| = |\mathbb{Z}|$$

$$\begin{array}{ccr} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 1 \\ 2 & \longleftrightarrow & -1 \\ 3 & \longleftrightarrow & 2 \\ 4 & \longleftrightarrow & -2 \\ 5 & \longleftrightarrow & 3 \\ 6 & \longleftrightarrow & -3 \\ 7 & \longleftrightarrow & 4 \\ 8 & \longleftrightarrow & -4 \\ \vdots & & \vdots \end{array}$$

**Dedekind-Infinite**

A set $A$ is Dedeking-infinite if some proper subset $B \subsetneq A$ is equinumerous to $A$.

Figure: Dedekind

# Countable?

$$\{0, 1, 2, 3, 4, \dots\}$$

$$\{1, 3, 5, 7, 9, \dots\}$$

$$\{0, 2, 4, 6, 8, \dots\}$$

$$\{0, 1, 4, 9, 16, \dots\}$$

$$\{2, 3, 5, 7, 11, \dots\}$$

- A set $A$ is countable iff $|A| \leq |\mathbb{N}|$.
- Is it possible that $A$ is infinite, but $|A| < |\mathbb{N}|$?
- A set $A$ is countably infinite iff $|A| = |\mathbb{N}|$.

$$|\mathbb{N}| = |2^{<\omega}|$$

$$\begin{array}{ccr}
0 & \longleftrightarrow & \epsilon \\
1 & \longleftrightarrow & 0 \\
2 & \longleftrightarrow & 1 \\
3 & \longleftrightarrow & 00 \\
4 & \longleftrightarrow & 01 \\
5 & \longleftrightarrow & 10 \\
6 & \longleftrightarrow & 11 \\
7 & \longleftrightarrow & 000 \\
8 & \longleftrightarrow & 001 \\
\vdots & & \vdots
\end{array}$$

# Countable?

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$$

# Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{N}|$$

# Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$$

# $|\mathbb{N}| = |\mathbb{Q}|$

$$
\begin{tikzcd}
-\frac{2}{1} \arrow[d] & -\frac{1}{1} & \frac{0}{1} \arrow[r] & \frac{1}{1} \arrow[d] & \frac{2}{1} & \frac{3}{1} \arrow[r] & \frac{3}{1} \arrow[d] \\
-\cancel{\frac{2}{2}} \arrow[d] & -\frac{1}{2} \arrow[u] & \cancel{\frac{0}{2}} \arrow[l] & \frac{1}{2} \arrow[l] & \cancel{\frac{2}{2}} \arrow[u] & & \frac{3}{2} \arrow[d] \\
-\frac{2}{3} \arrow[r] & -\frac{1}{3} \arrow[r] & \cancel{\frac{0}{3}} \arrow[r] & \frac{1}{3} \arrow[r] & \frac{2}{3} \arrow[u] & & \cancel{\frac{3}{3}} \arrow[d] \\
-\cancel{\frac{2}{4}} & -\frac{1}{4} \arrow[l] & \cancel{\frac{0}{4}} \arrow[l] & \frac{1}{4} \arrow[l] & \cancel{\frac{2}{4}} \arrow[l] & & \frac{3}{4} \arrow[l]
\end{tikzcd}
$$

$$|\mathbb{N}| = |\mathbb{Z}| = |2^{<\omega}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Q}|$$

# $|\mathbb{N}| = |\mathbb{Q}^+|$

$$
\begin{tikzcd}
\frac{1}{1} \arrow[r] & \frac{1}{2} \arrow[dl] & \frac{1}{3} \arrow[r] & \frac{1}{4} \arrow[dl] & \cdots \\
\frac{2}{1} \arrow[d] & \frac{2}{2} \arrow[ur] & \frac{2}{3} \arrow[dl] & \frac{2}{4} & \cdots \\
\frac{3}{1} \arrow[ur] & \frac{3}{2} \arrow[dl] & \frac{3}{3} & \frac{3}{4} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{tikzcd}
$$

$$x \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

# 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.**

$$f : A \rightarrowtail \mathbb{N} \implies \exists g : \bigcup_{n \in \mathbb{N}} A^{n+1} \rightarrowtail \mathbb{N} \quad (a_1, \ldots, a_n) \mapsto \prod_{i=1}^{n} p_i^{f(a_i)+1}$$

# The set of real numbers is uncountable

Is every set countable?

## Theorem (Cantor)

$$|\mathbb{R}| > |\mathbb{N}|$$

## Proof.

$$\begin{array}{cccccc} 0\,. & r_{11} & r_{12} & r_{13} & r_{14} & \dots \\ 0\,. & r_{21} & r_{22} & r_{23} & r_{24} & \dots \\ 0\,. & r_{31} & r_{32} & r_{33} & r_{34} & \dots \\ 0\,. & r_{41} & r_{42} & r_{43} & r_{44} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Let $d = 0.d_1 d_2 \dots$ 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, $\alpha = \lim_{n\to\infty} a_n$ 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

$$f : (0,1] \rightarrowtail\!\!\!\!\twoheadrightarrow (0,1)$$

$$f(x) := \begin{cases} \frac{3}{2} - x & \text{for } \frac{1}{2} < x \leq 1 \\ \frac{3}{4} - x & \text{for } \frac{1}{4} < x \leq \frac{1}{2} \\ \frac{3}{8} - x & \text{for } \frac{1}{8} < x \leq \frac{1}{4} \\ \vdots & \end{cases}$$

$$f(x) := \begin{cases} \frac{x}{x+1} & \text{if } \exists n \in \mathbb{N} : x = \frac{1}{n} \\ x & \text{otherwise} \end{cases}$$

# Continuum

# Continuum

**Theorem**

$$|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$$

**Proof.**

$$\begin{array}{rlllll} x = & 0.3 & 01 & 2 & 007 & 08\ldots \\ y = & 0.009 & 2 & 05 & 1 & 0003\ldots \end{array}$$

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0003\ \ldots$$

# 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)

$$|X| < |\mathrm{P}(X)|$$

## Proof.

If $f : X \to \mathrm{P}(X)$, 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

$1, 2, \ldots, \aleph_0, \aleph_1, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots, \aleph_{\omega\cdot 2}, \ldots, \aleph_{\omega^2}, \ldots, \aleph_{\omega^\omega}, \ldots, \aleph_{\varepsilon_0}, \ldots, \aleph_{\aleph_0}, \ldots, \aleph_{\aleph_{\aleph_0}}, \ldots$
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!

$$\forall d \in I: \ |S_d| \leq \left|\bigcup_{c \in I} S_c\right| < \left|\mathrm{P}\left(\bigcup_{c \in I} S_c\right)\right|$$

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)

$$\left.\begin{array}{l} |M| \leq |N| \\ |N| \leq |M| \end{array}\right\} \Longrightarrow |M| = |N|$$

1. Finite cycles on $2k+2$ distinct elements $(k \geq 0)$
   $m_0 \longrightarrow n_0 \longrightarrow m_1 \longrightarrow \cdots \longrightarrow m_k \longrightarrow n_k$
2. Two-way infinite chains of distinct elements
   $\cdots \longrightarrow m_0 \longrightarrow n_0 \longrightarrow m_1 \longrightarrow n_1 \longrightarrow \cdots$
3. The one-way infinite chains of distinct elements that start at the elements $m_0 \in M \setminus g(N)$
   $m_0 \longrightarrow n_0 \longrightarrow m_1 \longrightarrow n_1 \longrightarrow m_2 \longrightarrow \cdots$
4. The one-way infinite chains of distinct elements that start at the elements $n_0 \in N \setminus f(M)$
   $n_0 \longrightarrow m_0 \longrightarrow n_1 \longrightarrow m_1 \longrightarrow n_2 \longrightarrow \cdots$

$m_i \mapsto n_i$

# Cantor-Schröder-Bernstein Theorem — another proof

- A complete lattice is a partially ordered set in which every nonempty subset has both a supremum and an infimum.

## Theorem (Tarski's Fixpoint Theorem)

*For a complete lattice $(L, \leq)$ and an order-preserving function $f : L \to L$, the set of fixpoints of $f$ is also a complete lattice, with greatest fixpoint $\bigvee\{x : x \leq f(x)\}$ and least fixpoint $\bigwedge\{x : x \geq f(x)\}$.*

## Proof.

$(\mathrm{P}(M), \subset)$ 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 $M \setminus C = g(N \setminus f(C))$.

$$f\restriction_C \cup g^{-1}\restriction_{M\setminus C}$$

# Cantor-Schröder-Bernstein Theorem — another proof

**Proof.**

$$C_0 := M \setminus g(N)$$
$$D_0 := f(C_0)$$
$$C_{n+1} := g(D_n)$$
$$D_{n+1} := f(C_n)$$
$$C := \bigcup_{n\in\mathbb{N}} C_n$$
$$f\restriction_C \cup g^{-1}\restriction_{g(N)\setminus C}$$

$$h : S \mapsto (M \setminus g(N)) \cup g(f(S))$$
$$C = \bigcup_{n\to\infty} h^n(\emptyset)$$
$$= \bigcap \left\{ S : (M \setminus g(N)) \cup g(f(S)) \subset S \right\}$$

# 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 $(\alpha, \beta) < (\gamma, \delta)$ if ether

- $\max\{\alpha, \beta\} < \max\{\gamma, \delta\}$, 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 $\mathrm{Ord} \times \mathrm{Ord}$ and $\alpha \times \alpha = \big\{(\xi, \eta) : (\xi, \eta) < (0, \alpha)\big\}$.

Let $\Gamma(\alpha, \beta) \coloneqq \mathrm{otp}\big\{(\xi, \eta) : (\xi, \eta) < (\alpha, \beta)\big\}$. Then $(\alpha, \beta) < (\gamma, \delta) \iff \Gamma(\alpha, \beta) < \Gamma(\gamma, \delta)$, and $\Gamma(\omega, \omega) = \omega$, $\Gamma(\alpha, \alpha) \geq \alpha$. Assume $\alpha$ 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

$$C_0 := [0,1]$$

$$C_{k+1} := \frac{C_k}{3} \cup \left(\frac{2}{3} + \frac{C_k}{3}\right)$$

$$\mathcal{C} := \bigcap_{k=0}^{\infty} C_k = \bigcap_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\left[\frac{3k+0}{3^n}, \frac{3k+1}{3^n}\right] \cup \left[\frac{3k+2}{3^n}, \frac{3k+3}{3^n}\right]\right)$$

$$= [0,1] \setminus \bigcup_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\frac{3k+1}{3^n}, \frac{3k+2}{3^n}\right)$$

$$\mathcal{C} = \left\{\sum_{n=1}^{\infty} \frac{x_n}{3^n} : x_n = 0 \vee x_n = 2\right\} \implies |\mathcal{C}| = 2^{\aleph_0}$$

# Banach's Fixpoint Theorem

**Theorem (Banach's Fixpoint Theorem)**

*Let $(M, d)$ be a complete metric space and $T : M \to M$ be a contraction mapping, with Lipschitz constant $\gamma < 1$. Then $T$ has a unique fixpoint $x \in M$. Further, for each $x_0 \in M$, $\lim_{n\to\infty} T^n(x_0) = x$, 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 nonempty 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

$$d_H(A, B) := \inf \{\varepsilon : A \subset N_\varepsilon(B) \ \& \ B \subset N_\varepsilon(A)\}$$

  Then $(\mathcal{M}, d_H)$ is a complete metric space.
- Let $T_i : M \to M, i = 1, \ldots, n$ be a set of contractions. Let $\mathcal{M}'$ be the set of all compact sets of $\mathcal{M}$. Define the map $S : \mathcal{M}' \to \mathcal{M}'$ by $S(X) = \bigcup_{i=1}^{n} T_i(X)$. Then $S$ 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 $\mathcal{C}$ is the fixpoint of $x \mapsto \frac{x}{3} \cup \left(\frac{x}{3} + \frac{2}{3}\right)$.

# Cantor Set

Figure: Torricelli trumpet

- $|\mathcal{C}| = 2^{\aleph_0}$
- $\mathcal{C}$ is perfect.
- $\mathcal{C}$ is *nowhere dense* in $[0, 1]$.
- Lebesgue measure: $0$
- Hausdorff dimension: $\log_3 2$
- compact metric space

(a) Cantor dust(3D)

(b) Menger sponge: infinite surface area but $0$ volume

# Fractal, Hausdorff Dimension, Topological Dimension

$$\boxed{\text{A set } A \text{ is a } \textit{fractal} \text{ if } \dim_H(A) > \dim_T(A).}$$

$$H_{d,\varepsilon}(A) := \inf\left\{\sum_{k=1}^{\infty} \operatorname{diam}(B_k)^d : A \subset \bigcup_{k=1}^{\infty} B_k \ \ \& \ \ \operatorname{diam}(B_k) \leq \varepsilon\right\}$$

$$\dim_H(A) := \inf\left\{d : \lim_{\varepsilon \to 0} H_{d,\varepsilon}(A) = 0\right\}$$

## Definition (Topological Dimension)

The *topological dimension* of a space $X$ is defined by induction as

$$\dim_T(\emptyset) := -1$$

$$\dim_T(X) := \inf\left\{d : X \text{ has a basis } \mathcal{U} \text{ s.t. } \forall U \in \mathcal{U} : \dim_T(\partial U) \leq d - 1\right\}.$$

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 $h_1, h_2 \ldots$ s.t. $h(x) = \lim_{n\to\infty} h_n(x)$.
- 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 $\lim_{n\to\infty} 2^{\frac{1}{2}-n} = 0$. So $h$ fills space!
- Definition. A curve is a continuous map from unit interval $L$ to unit square $S$.
- For a pont $p \in S$ 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 $\varepsilon$. 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 $\mathbb{N}$ — $|\operatorname{Aut}(\mathbb{N})|$

Proof1. Diagonal method: For any countable sequence $(\sigma_n)_{n\in\mathbb{N}}$ of permutations, let $f : 2n \mapsto \min\big(2\mathbb{N} \setminus \{\sigma_0(0), \sigma_1(2), \ldots, \sigma_n(2n)\}\big)$, and $f : 2n+1 \mapsto$ the $n^{\text{th}}$ 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. $|\operatorname{Aut}(\mathbb{N})| > \aleph_0$.

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 $n$. $|\operatorname{Aut}(\mathbb{N})| \geq 2^{\aleph_0}$.

Proof3. Riemann rearrangement $\left(e.g. \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}\right) \implies \mathbb{R} \rightarrowtail \operatorname{Aut}(\mathbb{N})$.

**Theorem (Riemann Rearrangement Theorem)**

*Any conditionally convergent series can be rearranged in a permutation to*

1. *converge to any real number;*
2. *diverge to $\infty$ 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?

$$\sum_{n=1}^{\infty} \frac{1}{2^n} \frac{(-1)^{n+1}2^n}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} = \ln 2 \qquad \sum_{n=1}^{\infty} \left| \frac{(-1)^{n+1}}{n} \right| = \infty$$

# Cofinality and Inaccessible Cardinal

- $\mathrm{cf}(\alpha) :=$ the least limit ordinal $\beta$ s.t. there is an increasing $\beta$-sequence $\langle \alpha_\xi : \xi < \beta \rangle$ with $\lim\limits_{\xi \to \beta} \alpha_\xi = \alpha$.
- An infinite cardinal $\kappa$ is *regular* if $\mathrm{cf}(\kappa) = \kappa$. It is *singular* if $\mathrm{cf}(\kappa) < \kappa$.
- A cardinal $\kappa$ is a *strong limit* cardinal if $\forall \lambda < \kappa \big(2^\lambda < \kappa\big)$.
- A cardinal $\kappa$ is *inaccessible* if it is a regular strong limit uncountable cardinal.

# von Neumann Universe

## Definition (von Neumann Universe)

$$V_0 := \emptyset$$
$$V_{\alpha+1} := \mathrm{P}(V_\alpha)$$
$$V_\alpha := \bigcup_{\beta<\alpha} V_\beta \quad \text{for limit } \alpha.$$

$$V := \{x : x = x\}$$

$$\boxed{V = \bigcup_{\alpha \in \mathrm{Ord}} V_\alpha}$$

$\mathrm{rank}(x) :=$ the least $\alpha$ s.t. $x \subset V_\alpha$

# Constructable Universe

$$\mathrm{Def}(M) := \{X \subset M : X \text{ is } M\text{-definable over } (M, \in)\}$$

## Definition (Constructable Universe)

$$\begin{aligned} L_0 &:= \emptyset \\ L_{\alpha+1} &:= \mathrm{Def}(L_\alpha) \\ L_\alpha &:= \bigcup_{\beta<\alpha} L_\beta \quad \text{for limit } \alpha. \\ L &:= \bigcup_{\alpha\in\mathrm{Ord}} L_\alpha \end{aligned}$$

## Axiom of Constructibility

$$V = L$$

$$L \vDash \mathrm{ZF}$$

$$L \vDash V = L$$

$$\mathrm{ZF} + \mathrm{V} = \mathrm{L} \vdash \mathrm{AC} + \mathrm{GCH}$$

An inner model is a transitive class model of $\mathrm{ZF}$ that contains all ordinals.
$L$ is the smallest inner model of $\mathrm{ZF}$.

# 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. $x \in U \implies \mathrm{P}(x) \in U$
4. $I \in U \ \& \ x : I \to U \implies \bigcup_{i \in I} x_i \in U$
5. $\omega \in U$

## Universe Axiom

For every set $x$, there exists a Grothendieck universe $U$ s.t. $x \in U$.

$$\boxed{U \text{ is a Grothendieck universe iff } U = V_\kappa \text{ for some inaccessible } \kappa.}$$

The Universe Axiom is equivalent to the "inaccessible cardinal axiom" that "there exist arbitrarily large inaccessible cardinals."

$$U \vDash \mathrm{ZFC}$$

$$\frac{\text{super-infinite}}{\text{infinite}} \approx \frac{\text{infinite}}{\text{finite}}$$

| | | |
|---|---|---|
| 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 $\lambda$, $V_\lambda$ is super-infinite.*

# Shelf

## Definition (Shelf)

A left (right) *shelf* is a set $S$ with an operation $*$ satisfying

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(left self-distributive)}$$

$$(x * y) * z = (x * z) * (y * z) \qquad \text{(right self-distributive)}$$

**Example:**

- $S$ set, $f : S \to S$, 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 $x * y := \overline{x} + y$

Under the logical interpretation, $*$ corresponds to implication $\to$.

# Laver Tables

**Theorem (Laver)**

1. *For every $N$, there exists a unique binary operation $*$ on $\{1, \ldots, N\}$ s.t.*

$$x * 1 = x + 1 \mod N$$

$$x * (y * 1) = (x * y) * (x * 1)$$

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 $(\{1, \ldots, 2^n\}, *)$ satisfying

$$x * 1 = x + 1 \mod 2^n$$

| $A_0$ | 1 |
|---|---|
| 1 | 1 |

| $A_1$ | 1 | 2 |
|---|---|---|
| 1 | 2 | 2 |
| 2 | 1 | 2 |

| $A_2$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 4 | 2 | 4 |
| 2 | 3 | 4 | 3 | 4 |
| 3 | 4 | 4 | 4 | 4 |
| 4 | 1 | 2 | 3 | 4 |

$x \mapsto x \mod 2^{n-1}$ 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 $p+1 \mod 2^n$ 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 | $\cdots$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_n(1)$ | 1 | 1 | 2 | 4 | 4 | 8 | 8 | 8 | 8 | 16 | 16 | 16 | $\cdots$ |
| $\pi_n(2)$ | – | 2 | 2 | 4 | 4 | 8 | 8 | 16 | 16 | 16 | 16 | 16 | $\cdots$ |

$\mu n[\pi_n(1) = 32] \geq A(9, A(8, A(8, 254)))$ where $A$ is the Ackermann Function

**Theorem (Laver)**

1. $\mathrm{ZFC} + \mathrm{I3} \vdash \forall n\big(\pi_n(2) \geq \pi_n(1)\big)$
2. $\mathrm{ZFC} + \mathrm{I3} \vdash \lim\limits_{n\to\infty} \pi_n(1) = \infty$

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 $\infty$), then pass them to the mathematician for a formal proof.

$$\mathrm{crit}(j) \coloneqq \mu\alpha[j(\alpha) > \alpha]$$

The critical ordinal $\mathrm{crit}(j)$ of the elementary embedding $j$ is the least ordinal that is not invariant under $j$.

$$\mathcal{E}_\lambda \coloneqq \{j : V_\lambda \prec V_\lambda \ \ \& \ \ j \text{ is non-surjective}\}$$

$$i[j] \coloneqq \bigcup_{\alpha<\lambda} i(j \cap V_\alpha^2)$$

$(\mathcal{E}_\lambda, [])$ is a left-shelf: $i[j[k]] = i[j][i[k]]$

$$\mathrm{crit}(j \circ j) = \mathrm{crit}(j) \quad \text{but} \quad \mathrm{crit}(j[j]) = j(\mathrm{crit}(j)) > \mathrm{crit}(j)$$

$$j_{[n]} \coloneqq \underbrace{j[j][j]\cdots[j]}_{n \text{ times}}$$

$$\mathrm{Iter}(j) \coloneqq \left\{ j_{[n]} : n \in \mathbb{N}^+ \right\}$$

$$\boxed{\big(\mathrm{Iter}(j), []\big) \text{ is a left-shelf.}}$$

For $k, k' \in \mathrm{Iter}(j)$, declare $k \equiv_n k' \coloneqq \forall x \in V_\gamma \big(k(x) \cap V_\gamma = k'(x) \cap V_\gamma\big)$ with $\gamma \coloneqq \mathrm{crit}(j_{[2^n]})$. Then

$$\boxed{\mathrm{Iter}(j)/{\equiv_n} \text{ is (isomorphic to) the Laver table } A_n.}$$

# Ordinal

$0, 1, 2, 3, \ldots$

$\omega, \omega + 1, \omega + 2, \ldots$

$\omega \cdot 2, (\omega \cdot 2) + 1, (\omega \cdot 2) + 2, \ldots$

$\omega^2, \omega^2 + 1, \omega^2 + 2, \ldots$

$\omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \ldots$

$\omega^{\omega^\omega}, \ldots$

$\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}} = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots\}$

$\varepsilon_1 = \sup\{\varepsilon_0 + 1, \omega^{\varepsilon_0+1}, \omega^{\omega^{\varepsilon_0+1}}, \omega^{\omega^{\omega^{\varepsilon_0+1}}}, \ldots\} = \sup\{0, 1, \varepsilon_0, {\varepsilon_0}^{\varepsilon_0}, {\varepsilon_0}^{{\varepsilon_0}^{\varepsilon_0}}, \ldots\}$

$\varepsilon_{\alpha+1} = \sup\{\varepsilon_\alpha + 1, \omega^{\varepsilon_\alpha+1}, \omega^{\omega^{\varepsilon_\alpha+1}}, \ldots\} = \sup\{0, 1, \varepsilon_\alpha, \varepsilon_\alpha^{\varepsilon_\alpha}, \varepsilon_\alpha^{\varepsilon_\alpha^{\varepsilon_\alpha}}, \ldots\}$

$\varepsilon_\alpha = \sup\{\varepsilon_\beta : \beta < \alpha\}$ if $\alpha$ 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

$$\varphi_0(\alpha) \coloneqq \omega^\alpha$$

$$\varphi_{\gamma+1}(\alpha) \coloneqq \alpha^{\text{th}} \text{ ordinal s.t. } \varphi_\gamma(\beta) = \beta$$

$$\varphi_\delta(\alpha) \coloneqq \alpha^{\text{th}} \text{ common fixpoint of } \varphi_\gamma \text{ for all } \gamma < \delta$$

$$\Gamma_\alpha \coloneqq \alpha^{\text{th}} \text{ ordinal s.t. } \varphi_\alpha(0) = \alpha$$

$$\boxed{\varepsilon_\alpha = \varphi_1(\alpha)}$$

"inaccessible" cardinals
(ZF axioms cannot be used to
prove the existence of these sets)
$\kappa = \aleph_\kappa$
First cardinal that can only be named
by the ordinal that is as big as itself
$\aleph_\omega$
First cardinal to be preceded
by infinitely many cardinals
All sets here and
above are
uncountable
$\aleph_1$
Second infinite cardinal
(first uncountable ordinal)
$\varepsilon_0$
$\omega = \aleph_0$
First infinite cardinal/ordinal (ℕ)
All sets here are
countable (same
size as ℕ)
6
All sets here
are finite
5
65,536 sets
below Stage 5!
The number of
sets here has
20,000 digits!
empty set ∅

$$
\begin{tikzcd}
0 = 1 \arrow[r] & \text{I0-I3} \arrow[r] & n\text{-huge} \arrow[d] \\
 & & \text{superhuge} \arrow[dl] \\
 & \text{huge} \arrow[d] & \\
 & \text{almost huge} \arrow[dl] & \\
\text{Vopěnka's Principle} \arrow[d] & & \\
\text{extendible} \arrow[r] & \text{supercompact} \arrow[dl] \arrow[dr] & \\
\text{superstrong} \arrow[dr] & & \text{strongly compact} \arrow[dl] \\
 & \text{Woodin} \arrow[d] & \\
 & \text{strong} \arrow[d] & \\
 & 0^{\dagger} \text{ exists} \arrow[d] & \\
 & \text{measurable} \arrow[d] & \\
 & \text{Ramsey} \arrow[dl] \arrow[dr] & \\
\kappa \longrightarrow (\omega_1)_2^{<\omega} \arrow[dr] & & \text{Rowbottom} \arrow[dl] \\
 & \text{Jónsson} \arrow[d] & \\
 & \forall a \in {}^{\omega}\omega (a^{\#} \text{ exists}) \arrow[d] & \\
 & 0^{\#} \text{ exists} \arrow[r] & \kappa \longrightarrow (\omega)_2^{<\omega} \arrow[d] \\
 & & \text{indescribable} \arrow[dl] \\
 & \text{weakly compact} \arrow[dl] & \\
\alpha\text{-Mahlo} \arrow[dr] & & \\
 & \text{Mahlo} \arrow[dr] & \\
 & & \alpha\text{-inaccessible} \arrow[dl] \\
 & \text{inaccessible} \arrow[d] & \\
 & \text{weakly inaccessible} &
\end{tikzcd}
$$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory
- Axioms of ZFC
- Ordinal Numbers
- Cardinal Numbers
- Axiom of Choice

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 nonempty 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

$$n_0, n_1, n_2, \ldots$$

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.

$$\forall A \subset \omega^\omega : \Big(\forall n_0 \exists n_1 \forall n_2 \exists n_3 \ldots \big[(n_i)_{i \in \omega} \in A\big]\Big) \vee \Big(\exists n_0 \forall n_1 \exists n_2 \forall n_3 \ldots \big[(n_i)_{i \in \omega} \notin A\big]\Big)$$

- AD is inconsistent with AC.
- AD implies countable axiom of choice.
- AD implies that every subset of reals is Lebesgue measurable.
- AD $\implies$ CH. Since GCH $\implies$ AC, AD is inconsistent with GCH.

# Equivalents of AC

- Well-ordering theorem: Every set can be well-ordered.
- Trichotomy: For any two cardinals $\kappa$ and $\lambda : \kappa < \lambda \vee \kappa = \lambda \vee \kappa > \lambda$.
- For any infinite cardinal $\kappa : \kappa^2 = \kappa$.
- The Cartesian product of any family of nonempty sets is nonempty.
- 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 $\Gamma$ of formulae with $|\mathscr{L}| = \kappa$ is finitely satisfiable, then it has a model with cardinality $\leq \kappa + \aleph_0$.

# AC

## Theorem (Well-Ordering Theorem)

*Every set can be well-ordered.*

## Proof.

Assume $f$ is a choice function for $\mathrm{P}(A) \setminus \{\emptyset\}$. Let

$$a_\alpha = f\left(A \setminus \left\{a_\xi : \xi < \alpha\right\}\right)$$

$$\theta \coloneqq \mu\alpha\left[A = \left\{a_\xi : \xi < \alpha\right\}\right]$$

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 (Gödel1938)**

$$\mathrm{Con}(\mathrm{ZF}) \to \mathrm{Con}(\mathrm{ZFC} + \mathrm{GCH})$$

**Theorem (Cohen1963)**

- $\mathrm{Con}(\mathrm{ZF}) \to \mathrm{Con}(\mathrm{ZF} + \neg\mathrm{AC})$
- $\mathrm{Con}(\mathrm{ZF}) \to \mathrm{Con}(\mathrm{ZFC} + \neg\mathrm{GCH})$

Figure: Cohen

$\theta_1 + \theta_2 + \theta_3 > 180°$

Spherical (positive curvature)

$\theta_1 + \theta_2 + \theta_3 = 180°$

Euclidean (zero curvature)

$\theta_1 + \theta_2 + \theta_3 < 180°$

Hyperbolic (negative curvature)

# GCH vs Weak GCH

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \qquad \text{(GCH)}$$

$$\Downarrow$$

$$2^\kappa < 2^{\kappa^+} \qquad \text{(WGCH)}$$

$$\Updownarrow$$

$$\kappa < \lambda \implies 2^\kappa < 2^\lambda$$

$$\boxed{\text{“}|X| < |Y| \implies |\mathrm{P}(X)| < |\mathrm{P}(Y)|\text{” is independent of ZFC.}}$$

# Freiling's Axiom of Symmetry

## Freiling's Axiom of Symmetry (AX)

$$\forall f : \mathbb{R} \to \mathbb{R}_{\aleph_0} \exists xy \big[ x \notin f(y) \wedge y \notin f(x) \big]$$

## Theorem

$$\mathrm{ZFC} \vdash \mathrm{AX} \leftrightarrow \neg \mathrm{CH}$$

## Proof.

$(\to)$: Let $<$ be a well ordering of $\mathbb{R}$ of length $\aleph_1$. Let $f(x) := \{y : y \leq x\}$. Then $f : \mathbb{R} \to \mathbb{R}_{\aleph_0}$. So $\exists xy \big(x < y \wedge y < x\big)$. Contradiction.

$(\leftarrow)$: Assume $2^{\aleph_0} > \aleph_1$. Let $x_1, x_2, \ldots$ be an $\aleph_1$-sequence of distinct reals.

Let $f : \mathbb{R} \to \mathbb{R}_{\aleph_0}$. Then $\left| \bigcup_{\alpha < \aleph_1} f(x_\alpha) \right| = \aleph_1$. So $\exists y \in \mathbb{R} \forall \alpha < \aleph_1 \big(y \notin f(x_\alpha)\big)$.

Since $f(y)$ is countable, $\exists \alpha \big(x_\alpha \notin f(y)\big)$. Therefore $y \notin f(x_\alpha) \wedge x_\alpha \notin f(y)$.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Presburger/Robinson/Peano Arithmetic

- $x + 0 = x$
- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- $x + z = y + z \rightarrow x = y$
- $x \cdot 0 = 0$
- $x \cdot 1 = x$
- $x \cdot y = y \cdot x$
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $P(0) \wedge \forall x(P(x) \rightarrow P(x + 1)) \rightarrow \forall x P(x)$

$$\left.\begin{array}{ll} 1. & S(x) \neq 0 \\ 2. & S(x) = S(y) \rightarrow x = y \\ 3. & y = 0 \vee \exists x(S(x) = y) \\ 4. & x + 0 = x \\ 5. & x + S(y) = S(x + y) \\ 6. & x \cdot 0 = 0 \\ 7. & x \cdot S(y) = (x \cdot y) + x \end{array}\right\} Q$$

8. $P(0) \wedge \forall x(P(x) \rightarrow P(S(x))) \rightarrow \forall x P(x)$

# Exponentiation is definable in $\mathcal{N}$/representable in $\mathrm{Q}$

$$\pi(x,y) := (x+y)^2 + x + 1$$
$$\pi_1(z) := \mu x[\exists y \leq z : \pi(x,y) = z]$$
$$\pi_2(z) := \mu y[\exists x \leq z : \pi(x,y) = z]$$
$$\beta(s,i) := \mu x < s\big[\pi_1(s) \equiv x \mod 1 + (i+1)\cdot\pi_2(s)\big]$$
$$\beta^*(s,i) := \mu x < s\,[\exists y < s\,\exists z < s : s = \pi(y,z) \;\wedge\; (1 + (\pi(x,i)+1)\cdot z) \mid y]$$

**Lemma**

*For every $a_0, \ldots, a_n$, there is an $s \in \mathbb{N}$ s.t. $\forall i \leq n : \beta(s,i) = a_i$.*

**Proof.**

$$b := \max\{n, a_0, \ldots, a_n\} \quad d := b! \quad d_i := 1 + (i+1)\cdot d$$
$$c := \mu x\,\big[\forall i \leq n\big(x \equiv a_i \mod d_i\big)\big]$$
$$s := \pi(c,d)$$

$$x^y := \beta\Big(\mu s\big[\beta(s,0) = 1 \;\wedge\; \forall i < y : \beta(s,i+1) = \beta(s,i)\cdot x\big], y\Big)$$

# Chinese Remainder Theorem

## Theorem (Chinese Remainder Theorem)

*Suppose $m_0, \ldots, m_n$ are pairwise relatively prime. Let $a_0, \ldots, a_n$ be arbitrary integers. Then there is $x \in \mathbb{Z}$ s.t. for $i \leq n$ :*

$$x \equiv a_i \mod m_i$$

## Proof.

$$m := \prod_{i=1}^{n} m_i \qquad m_i^* := \frac{m}{m_i}$$

$$m_i' := \mu x \left[ x \cdot m_i^* \equiv 1 \mod m_i \right]$$

$$x \equiv \sum_{i=1}^{n} m_i' \cdot m_i^* \cdot a_i \mod m$$

# Arithmetization of Syntax

| $\zeta$ | $\forall$ | $0$ | $S$ | $+$ | $\times$ | $($ | $)$ | $\neg$ | $\rightarrow$ | $=$ | $x_0$ | $\ldots$ | $x_k$ | $\ldots$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\ulcorner\zeta\urcorner$ | $1$ | $3$ | $5$ | $7$ | $9$ | $11$ | $13$ | $15$ | $17$ | $19$ | $21$ | $\ldots$ | $2k+21$ | $\ldots$ |

$$\langle a_1, \ldots, a_n\rangle \coloneqq \mu x\big[\beta(x,0) = n \wedge \beta(x,1) = a_1 \wedge \cdots \wedge \beta(x,n) = a_n\big]$$

$$\textit{or} \quad \langle a_1, \ldots, a_n\rangle \coloneqq \prod_{i=1}^{n} p_i^{a_i+1}$$

$$\ulcorner\zeta_0 \cdots \zeta_n\urcorner \coloneqq \langle \ulcorner\zeta_0\urcorner, \ldots, \ulcorner\zeta_n\urcorner\rangle$$

$\mathrm{prf}_{\mathrm{T}}(y,x) \coloneqq$ "$y$ is the code of a proof in $\mathrm{T}$ of the formula with code $x$."

$$\mathrm{prov}_{\mathrm{T}}(x) \coloneqq \exists y\, \mathrm{prf}_{\mathrm{T}}(y,x)$$

$$\Box_{\mathrm{T}} A \coloneqq \mathrm{prov}_{\mathrm{T}}(\ulcorner A\urcorner)$$

Is there a wff $A$ s.t. $\mathrm{T} \vdash A \leftrightarrow \neg\Box_{\mathrm{T}} A$?

- $\mathrm{Con}(\mathrm{T}) \coloneqq \neg\Box_{\mathrm{T}}\bot$
- $\omega$-consistent: $\forall x \Box_{\mathrm{T}} \neg A(x) \to \neg\Box_{\mathrm{T}} \exists x A(x)$ for any formula $A$
- 1-consistent: $\forall x \Box_{\mathrm{T}} \neg A(x) \to \neg\Box_{\mathrm{T}} \exists x A(x)$ for $A \in \Delta_0$
- $\mathrm{Rfn}_{\Gamma}(\mathrm{T}) : \Box_{\mathrm{T}} A \to A$ for any sentence $A \in \Gamma$
- $\mathrm{RFN}_{\Gamma}(\mathrm{T}) : \forall x \big(\Box_{\mathrm{T}} A(x) \to A(x)\big)$ for any wff $A \in \Gamma$
- arithmetically sound: $\mathrm{Rfn}_{\Sigma_{<\omega}}(\mathrm{T})$
- 1-consistent $\iff \mathrm{Rfn}_{\Sigma_1}(\mathrm{T})$
- $\mathrm{Rfn}_{\Pi_1}(\mathrm{T}) \iff \mathrm{RFN}_{\Pi_1}(\mathrm{T}) \iff \mathrm{Con}(\mathrm{T})$

**Definition (Gödelian Theory)**

A theory is Gödelian if it is

1. consistent
2. axiomatizable
3. rich enough to represent elementary arithmetic (able to represent primitive recursive functions)

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Primitive Recursive Function & Recursive Function

- initial functions:
  1. projection: $I_i^m(n_1, \ldots, n_m) = n_i$ for $1 \leq i \leq m$
  2. successor: $S(n) = n + 1$
  3. zero: $Z(n) = 0$
- composition: given $g, h_1, \ldots, h_k$,

$$f(\mathbf{x}) = g\left(h_1(\mathbf{x}), \ldots, h_k(\mathbf{x})\right)$$

- primitive recursion: given $g, h$,

$$f(\mathbf{x}, 0) = g(\mathbf{x})$$
$$f(\mathbf{x}, n+1) = h\left(\mathbf{x}, n, f(\mathbf{x}, n)\right)$$

- regular $\mu$-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

- $\mu$-operation: given $g$,

$$f(\mathbf{x}) = \mu y\,[g(\mathbf{x}, y) = 0]$$

where

$$\mu y\,[g(\mathbf{x}, y) = 0] = n \iff g(\mathbf{x}, n) = 0 \;\wedge\; \forall z < n\big(g(\mathbf{x}, z)\downarrow \neq\; 0\big)$$

bounded $\mu$-operation: $\mu x < n[A(x)] \coloneqq \mu x[A(x) \vee x = n]$

**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 $\mu$-operation, $\mu$-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.*

$$a \uparrow^n b := \begin{cases} ab & \text{if } n = 0 \\ (a \uparrow^{n-1})^b 1 & \text{if } n \geq 1 \end{cases}$$

$$a \uparrow b = a^b \qquad a \uparrow\uparrow b = \underbrace{a \uparrow (a \uparrow (\cdots \uparrow a))}_{b \text{ copies of } a} 1 = \underbrace{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}_{b \text{ copies of } a}$$

$$A(m,n) = 2 \uparrow^{m-2} (n+3) - 3$$

## Thesis (Church-Turing Thesis)

*effective calculable* = *recursive* = *Turing Computable*

||

*representable in* $\mathrm{Q}$ = $\lambda$*-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?

# Computability vs Representability

A function/relation is representable in Robinson $\mathrm{Q}$ 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 $\mu$-operation and primitive recursion.
最后一步证明对原始递归封闭的困难在于，一个公式不能通过自身来定义自己，而必须借助一些编码技巧（Gödel $\beta$ 函数）。

$$f(\mathbf{x}, 0) = g(\mathbf{x})$$
$$f(\mathbf{x}, n+1) = h(\mathbf{x}, n, f(\mathbf{x}, n))$$

we can code the sequence of values of $f$ from $0$ to $y$ by using $\beta$:

$$F(\mathbf{x}, y) = \mu z\big[\beta(z, 0) = g(\mathbf{x}) \ \wedge \ \forall i < y : \beta(z, i+1) = h\big(\mathbf{x}, i, \beta(z, i)\big)\big]$$

$$f(\mathbf{x}, y) = \beta\big(F(\mathbf{x}, y), y\big)$$

# 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

$\varphi_e$ is the $e^{\text{th}}$ partial recursive function:

$$\varphi_e(\mathbf{x}) := U(\mu y T(e, \mathbf{x}, y))$$

# Incompleteness Theorem

- The function $\bar{f}$ is a *completion* of a partial function $f$ if $\bar{f}$ is total and $\forall n : f(n)\downarrow \implies f(n) = \bar{f}(n)$.
- A partial function $f$ is *potentially recursive* if it has a completion which is recursive.

**Not every partial recursive function is potentially recursive.**

$$f(n) \coloneqq \varphi_n(n) + 1$$

**Theorem (Incompleteness Theorem)**

*Any $\omega$-consistent Gödelian $\mathrm{T}$ is incomplete.*

**Proof.**

Suppose $T$ is represented in $\mathrm{T}$ by $\gamma$.

$$\bar{\varphi}_e(n) \coloneqq \begin{cases} U(\mu y T(e,n,y)) & \text{if } \exists y T(e,n,y) \\ 0 & \text{if } \mathrm{T} \vdash \forall y \neg\gamma(e,n,y) \end{cases}$$

# 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 $e$, $\varphi_e^n$ is a partial recursive function of $n$ variables.*
- *if $\psi$ is a partial recursive function of $n$ variables, then there is $e$ s.t. $\psi = \varphi_e^n$.*
- *there is a partial recursive function $\varphi$ of $n+1$ variables s.t. $\varphi(e, \mathbf{x}) = \varphi_e(\mathbf{x})$.*

## Theorem ($smn$ 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*

$$\varphi_{s_n^m(e,x_1,\ldots,x_m)} = \lambda y_1 \ldots y_n . \varphi_e(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

# Acceptable Numbering

## Definition (Acceptable Numbering)

A numbering $\psi$ is acceptable if 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)

*$\psi$ is an acceptable numbering iff there is a recursive permutation $h$ s.t.,*

$$\psi_e = \varphi_{h(e)}$$

## Theorem (Blum)

*If $\psi$ is an acceptable numbering, then there is a recursive permutation $h$ s.t.*

$$h(\psi_e(x)) = \varphi_{h(e)}(h(x))$$

# 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

$$\exists e : \varphi_e(y) = \varphi_{s(e)}(y) = f(e, y)$$

# Kleene's Relativized Fixpoint Theorem (with Parameters)

**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. $\varphi^A_{e(y)} = \varphi^A_{f(e(y),y)}$ for all $y$. Moreover, $e$ does not depend on $A$.*

**Proof.**

Let the index $e$ code the function

$$\varphi^A_e(x, y, z) = \begin{cases} \varphi^A_{\varphi_x(x,y)}(z) & \text{if } \varphi_x(x, y) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

By the relativized $smn$ theorem there is a computable function $s(x, y)$ s.t.

$$\varphi^A_{s(x,y)} = \varphi^A_e(x, y, z)$$

We know $\exists v : \varphi^A_v(x, y) = f(s(x, y), y)$. Let $e(y) := s(v, y)$.

$$\varphi^A_{e(y)} = \varphi^A_{s(v,y)} = \varphi^A_{\varphi^A_v(v,y)} = \varphi^A_{f(s(v,y),y)} = \varphi^A_{f(e(y),y)}$$

# 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.*

$$\varphi_e(y) = f(e, y)$$

$$\boxed{\text{Kleene's Fixpoint Theorem} \iff \text{Second Recursion Theorem}}$$

## Theorem (First Recursion Theorem)

*Every partial recursive functional $F(\alpha, x)$ admits a least fixpoint. In other words, there is a partial recursive function $\alpha$ s.t.,*

1. $\forall x \big(\alpha(x) = F(\alpha, x)\big)$
2. $\forall x \big(\beta(x) = F(\beta, x)\big) \implies \alpha \subset \beta$

# Gödel's Speed-Up Theorem

## Theorem (Gödel's Speed-Up Theorem)

*Let $\mathrm{T}' \supset \mathrm{T}$ be formal systems (with recursive sets of axioms and of recursive rules) such that $\mathrm{T}' \setminus \mathrm{T}$ is not r.e. Given a recursive function $h$, there is a theorem $A$ of $\mathrm{T}$ and a number $n$ such that $A$ admits a proof of length $\leq n$ in $\mathrm{T}'$, but no proof of length $\leq h(n)$ in $\mathrm{T}$.*

## Proposition

*If $\mathrm{T}$ is an essentially undecidable formal system, and $\mathrm{T} \nvdash A$, then $\mathrm{T} \cup \{A\} \setminus \mathrm{T}$ is not r.e.*

**Remark:** Adding an unprovable sentence to an essentially undecidable formal system $\mathrm{T}$ radically shortens some proof of some theorem of $\mathrm{T}$.

# Blum's Speed-Up Theorem

## Theorem (Blum's Speed-Up Theorem)

*Given a complexity measure $(\varphi, \Phi)$ 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.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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.
- $\cdots$

## 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.

## 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?

## 自我实现/自我修复?

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

# 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...

# 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”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 from 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"。

# Diagonalization[13]

## Definition (Point-Surjective)

A morphism $f : X \to Y$ is *point-surjective* if for every $y : 1 \to Y$, there is an $x : 1 \to X$ such that $y = f \circ x$.

## Theorem (Lawvere's Fixpoint Theorem)

*In a cartesian closed category, if there is a point-surjective morphism $f : X \to Y^X$, then every morphism $\alpha : Y \to Y$ has a fixpoint $y : 1 \to Y$.*

[13] 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 $g : X \to Y$ is *representable* by $f : X \times X \to Y$ iff

$$\exists y \forall x : g(x) = f(x, y)$$

**Theorem (Lawvere's Fixpoint Theorem)**

*For sets $X, Y$, functions $f : X \times X \to Y$, $\alpha : Y \to Y$, let $g := \alpha \circ f \circ \Delta$.*

1. *If $\alpha$ has no fixpoint, then $g$ is not representable by $f$.*
2. *If $g$ is representable by $f$, then $\alpha$ has a fixpoint.*

$$\begin{tikzcd}
X \times X \arrow[r, "f"] & Y \arrow[d, "\alpha"] \\
X \arrow[u, "\Delta"] \arrow[r, "g"'] & Y
\end{tikzcd}$$

$$\alpha\big(f(\ulcorner g \urcorner, \ulcorner g \urcorner)\big) = g(\ulcorner g \urcorner) = f(\ulcorner g \urcorner, \ulcorner g \urcorner)$$

- $\Delta : x \mapsto (x, x)$ diagonal
- $f$ evaluation
- $\alpha$ "negation"
- $g$ ($\ulcorner g \urcorner$) fixpoint-(free) transcendence
- $f(\ulcorner g \urcorner, \ulcorner g \urcorner)$ self-reference "I have property $\alpha$."

# Diagonalization

- A function $g : X \to Z$ is *representable* by $f : X \times Y \to Z$ 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 $\beta : X \to Y, f : X \times Y \to Z, \alpha : Z \to Z$, let $g := \alpha \circ f \circ \langle 1_X, \beta \rangle$. Assume $\beta$ is surjective.*

1. *If $\alpha$ has no fixpoint, then $g$ is not representable by $f$.*
2. *If $g$ is representable by $f$, then $\alpha$ has a fixpoint.*

$$\begin{tikzcd}
X \times Y \arrow[r, "f"] & Z \arrow[d, "\alpha"] \\
X \arrow[u, "\langle 1_X, \beta \rangle"] \arrow[r, "g"'] & Z
\end{tikzcd}$$

# Example — Grelling/Liar/Quine. . . Paradox

$$\begin{tikzcd} X \times X \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\ X \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2} \end{tikzcd}$$

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

$$\begin{tikzcd} X \times X \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\ X \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2} \end{tikzcd}$$

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 — Yablo Paradox in Linear Temporal Logic(LTL)

$$
\begin{aligned}
n \Vdash A \wedge B &\iff n \Vdash A \;\&\; n \Vdash B \\
n \Vdash \neg A &\iff n \nVdash A \\
n \Vdash \bigcirc A &\iff n+1 \Vdash A \\
n \Vdash \Box A &\iff \forall m \geq n \implies m \Vdash A
\end{aligned}
$$

$$
\begin{tikzcd}
\mathrm{Sen} \times \mathrm{Sen} \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\
\mathrm{Sen} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}
$$

$f : (X, Y) \mapsto [\![ X \nleftrightarrow \bigcirc\Box\neg Y ]\!]$ and $\alpha : x \mapsto 1 - x$

**Theorem**

*For any wff $A$, $\mathrm{LTL} \nvdash A \leftrightarrow \bigcirc\Box\neg A$.*

# Example — Euclid's Theorem

**Theorem (Euclid's Theorem)**

*There are infinitely many prime numbers.*

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}$$

where

$$f(m,n) = \begin{cases} 1 & \forall p \in \mathbb{P} : p|(m!+1) \to p < n \\ 0 & \text{otherwise} \end{cases}$$

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 $\alpha$. Contradiction!

# Example — The set of real numbers is uncountable

**Theorem (Cantor)**

*$\mathbb{R}$ is uncountable.*

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & \mathbf{10} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{10}
\end{tikzcd}$$

where $f : (m, n) \mapsto r_{mn} :=$ "the $n^{\text{th}}$ digit of the $m^{\text{th}}$ 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):

$f : (m, n) \mapsto r_{mn} :=$ "the $n^{\text{th}}$ digit of the real named by the $m^{\text{th}}$ sentence"

# Example — Cantor's Theorem

**Theorem (Cantor's Theorem)**

$$|X| < |\mathrm{P}(X)|$$

$$\begin{tikzcd}
X \times \mathrm{P}(X) \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\
X \arrow[u, "\langle 1_X, \beta \rangle"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}$$

where $f : (x, y) \mapsto [\![ x \in y ]\!]$ and $\alpha : x \mapsto 1 - x$.

$\beta$ is not surjective.

another proof: assume $h : \mathrm{P}(X) \rightarrowtail X$.

$$\begin{tikzcd}
\mathrm{P}(X) \times \mathrm{P}(X) \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\
\mathrm{P}(X) \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}$$

where $f : (x, y) \mapsto [\![ h(x) \in y ]\!]$, and $\alpha : x \mapsto 1 - x$.

$g$ is representable by $y \coloneqq \{ h(x) : x \subset X \ \& \ h(x) \notin x \}$.

# Example — Cantor's Theorem — another proof

If $|X| \geq |\mathrm{P}(X)|$, then there exists some enumeration $\{S_i\}_{i \in X}$ of $\mathrm{P}(X)$.

$$\begin{tikzcd}
X \times \{S_i\}_{i \in X} \arrow[r, "f"] & \mathbf{2} \arrow[d, "\alpha"] \\
X \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}$$

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 $\mathrm{P}(X)$, 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

**Theorem (Cantor's Theorem)**

*For* $|Y| \geq 2$,

$$|X| < |Y^X|$$

$$\begin{tikzcd}
X \times X \arrow[r, "f"] & Y \arrow[d, "\alpha"] \\
X \arrow[u, "\Delta"] \arrow[r, "g"'] & Y
\end{tikzcd}$$

where $\alpha$ is the cyclic permutation.

Every $g : X \to Y$ is representable by some $f : X \times X \to Y$ iff $\exists f : X \twoheadrightarrow Y^X$.

$\boxed{\textit{If there exists } f : X \twoheadrightarrow Y^X\textit{, then every } \alpha : Y \to Y \textit{ has a fixpoint.}}$

# 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 $\|f\|_\infty = \sup_{x\in\mathbb{R}} |f(x)|$.

$$\begin{tikzcd}
\mathbb{R} \times C(\mathbb{R},\mathbb{R}) \arrow[r, "\mathcal{F}"] & \mathbb{R} \arrow[d, "\alpha"] \\
\mathbb{R} \arrow[u, "\langle 1_{\mathbb{R}},\beta\rangle"] \arrow[r, "g"'] & \mathbb{R}
\end{tikzcd}$$

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, $f : I \to X^I$.

# Example — total recursive but not primitive recursive

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & \mathbb{N} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbb{N}
\end{tikzcd}$$

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

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathcal{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathcal{E}_\varphi : (m,n) \mapsto \varphi_n(m)$, and $\alpha : \varphi_n(m) \mapsto \min\left(\mathbb{N} \setminus \{\varphi_k(m) : k \leq n\}\right)$

$$g(m) = \min\left(\mathbb{N} \setminus \{\varphi_k(m) : k \leq m\}\right) = \mu n\,[K(n|m) > m]$$

$g$ 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

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathcal{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathcal{E}_\varphi : (m,n) \mapsto \varphi_n(m)$, and $\alpha : x \mapsto x+1$

$$g : m \mapsto \varphi_m(m) + 1$$

$$g \text{ partial recursive} \implies g \text{ representable} \implies \alpha(g(\ulcorner g \urcorner)) = g(\ulcorner g \urcorner) \uparrow$$

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 (Turing1936)**

*The Halting problem is unsolvable.*

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "H"] & \mathbf{2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{2}
\end{tikzcd}$$

where $H : (x, y) \mapsto [\![\varphi_y(x) \downarrow]\!]$, and $\alpha(x) = \begin{cases} 1 & \text{if } x = 0 \\ \uparrow & \text{otherwise} \end{cases}$.

$$H(\ulcorner g \urcorner, \ulcorner g \urcorner) \uparrow$$

$\boxed{\text{There is no perfect anti-virus software.}}$

# Example — Turing's Halting Problem — another proof

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathcal{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathcal{E}_\varphi : (m,n) \mapsto \varphi_n(m)$, 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 computable, then $g$ is computable. $\times$

# Example — Kleene's Fixpoint Theorem

## Theorem (Kleene's Fixpoint Theorem)

*Given a recursive function $h$, there is an index $e$ s.t.*

$$\varphi_e = \varphi_{h(e)}$$

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & \{\varphi_n\}_{n \in \mathbb{N}} \arrow[d, "\mathcal{E}_h"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n\}_{n \in \mathbb{N}}
\end{tikzcd}$$

where $f : (m, n) \mapsto \varphi_{\varphi_n(m)}$, and $\mathcal{E}_h : \varphi_n \mapsto \varphi_{h(n)}$.
The function $g : m \mapsto \varphi_{h(\varphi_m(m))}$ is a recursive sequence of partial recursive functions, and thus is representable by $f$. Explicitly,

$$g(m) = \varphi_{h(\varphi_m(m))} = \varphi_{s(m)} = \varphi_{\varphi_t(m)} = f(m, t)$$
$$e \coloneqq \varphi_t(t)$$

# Example — $\mathbf{Y}$ Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\mathcal{E}_y"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

where $f : (x, y) \mapsto yx$, and $\mathcal{E}_y : x \mapsto yx$.

$$g = \lambda x.y(xx)$$

$$gg = \mathcal{E}_y(gg)$$

$$\mathbf{Y} \coloneqq \lambda y.gg = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx))$$

$$\mathbf{Y}h = h(\mathbf{Y}h) = h(h(\mathbf{Y}h)) = \cdots$$

# Example — $\mathbf{Z}$ Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\mathcal{E}_y"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

where $f : (x, y) \mapsto \lambda v.yxv$, and $\mathcal{E}_y : x \mapsto yx$.

$$g = \lambda x.y(\lambda v.xxv)$$

$$gg = \mathcal{E}_y(gg)$$

$$\mathbf{Z} := \lambda y.gg = \lambda y.(\lambda x.y(\lambda v.xxv))(\lambda x.y(\lambda v.xxv))$$

$$\mathbf{Z}hv = h(\mathbf{Z}h)v$$

$$e := \mathbf{Z}h \implies ev = hev$$ (Kleene's fixpoint)

# Example — $\Theta$ Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\alpha"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

where $f : (x, y) \mapsto yx$, and $\alpha : x \mapsto \lambda y.y(xy)$.

$$g = \lambda xy.y(xxy)$$

$$gg = \alpha(gg)$$

$$\Theta := gg = (\lambda xy.y(xxy))(\lambda xy.y(xxy))$$

$$\Theta h = h(\Theta h) = h(h(\Theta h)) = \cdots$$

Generally, let $\gamma := \lambda x_1 \ldots x_{n-1} y.y(wy)$ where $w$ is an arbitrary word of length $n$ over the alphabet $\{x_1, \ldots, x_{n-1}\}$. Then $\Gamma := \gamma^n$ is a fixpoint combinator.

# Example — $\Theta_v$ Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\alpha"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

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 $\lambda$-term $F$ there is a $\lambda$-term $G$ s.t.*

$$F\ulcorner G\urcorner = G$$

$$\begin{tikzcd}
\underline{\Lambda} \times \underline{\Lambda} \arrow[r, "A"] & \Lambda \arrow[d, "\mathcal{E}_F"] \\
\underline{\Lambda} \arrow[u, "\Delta"] \arrow[r, "W"'] & \Lambda
\end{tikzcd}$$

where $\underline{\Lambda} := \{\ulcorner M\urcorner : M \in \Lambda\}$, and $A : (\ulcorner M\urcorner, \ulcorner N\urcorner) \mapsto N\,(\ulcorner M\urcorner)$, and $\mathcal{E}_F : M \mapsto F\ulcorner M\urcorner$.

$$W\ulcorner M\urcorner = F\ulcorner M\ulcorner M\urcorner\urcorner$$

$$G := W\ulcorner W\urcorner$$

# Example — Fixpoint Lemma in Logic

## Theorem (Fixpoint Lemma in Logic)

*For any wff $F(x)$ with one free variable $x$, there exists a sentence $G$ s.t.*

$$\mathrm{Q} \vdash G \leftrightarrow F\left(\ulcorner G \urcorner\right)$$

$$\begin{tikzcd}
\mathrm{Lin}_1 \times \mathrm{Lin}_1 \arrow[r, "f"] & \mathrm{Lin}_0 \arrow[d, "\mathcal{E}_F"] \\
\mathrm{Lin}_1 \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathrm{Lin}_0
\end{tikzcd}$$

where $f : (M(x), N(x)) \mapsto N\left(\ulcorner M(x) \urcorner\right)$, and $\mathcal{E}_F : M \mapsto F(\ulcorner M \urcorner)$.

$$g(M(x)) = F\left(\ulcorner M\left(\ulcorner M(x) \urcorner\right) \urcorner\right)$$

$$W(x) \coloneqq F\left(D(x)\right)$$

where $D : \ulcorner M(x) \urcorner \mapsto \ulcorner M\left(\ulcorner M(x) \urcorner\right) \urcorner$

$$G \coloneqq W\left(\ulcorner W(x) \urcorner\right)$$

# Fixpoint vs Diagonalization

$$\begin{tikzcd} X \times X \arrow[r, "f"] & Y \arrow[d, "\alpha"] \\ X \arrow[u, "\Delta"] \arrow[r, "g"'] & Y \end{tikzcd}$$

| Curry $\mathbf{Y}$ | $\hat{=}$ | $\lambda$-fixpoint | $\hat{=}$ | Gödel | $\hat{=}$ | Kleene | $\hat{=}$ | Russell |
|---|---|---|---|---|---|---|---|---|
| $yx$ | $\hat{=}$ | $N\,(\ulcorner M \urcorner)$ | $\hat{=}$ | $N(\ulcorner M(x) \urcorner)$ | $\hat{=}$ | $\varphi_n(m)$ | $\hat{=}$ | $x \in y$ |
| $xx$ | $\hat{=}$ | $M\,(\ulcorner M \urcorner)$ | $\hat{=}$ | $M(\ulcorner M(x) \urcorner)$ | $\hat{=}$ | $\varphi_n(n)$ | $\hat{=}$ | $x \in x$ |
| $y(xx)$ | $\hat{=}$ | $F\ulcorner M \ulcorner M \urcorner\urcorner$ | $\hat{=}$ | $F(\ulcorner M(\ulcorner M(x) \urcorner) \urcorner)$ | $\hat{=}$ | $h(\varphi_n(n))$ | $\hat{=}$ | $x \notin x$ |
| $\lambda x.y(xx)$ | $\hat{=}$ | $W$ | $\hat{=}$ | $W(x)$ | $\hat{=}$ | $\varphi_t(n)$ | $\hat{=}$ | $x \notin R$ |
| $(\lambda x.y(xx))(\lambda x.y(xx))$ | $\hat{=}$ | $W\,(\ulcorner W \urcorner)$ | $\hat{=}$ | $W(\ulcorner W(x) \urcorner)$ | $\hat{=}$ | $\varphi_t(t)$ | $\hat{=}$ | $R \notin R$ |

$$\boxed{\text{self-reference} \overset{?}{\Longrightarrow} \text{self-improvement}}$$

# Non-operational Self-inspection?

*The information available to the observer regarding his own state could have absolute limitations, by the laws of nature.*

*— von Neumann*

$$\begin{tikzcd}
\mathbf{M} \times \mathbf{M} \arrow[r, "f"] & \mathbf{O} \arrow[d, "\alpha"] \\
\mathbf{M} \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathbf{O}
\end{tikzcd}$$

- $\mathbf{M}$: quantum measurements.
- $\mathbf{O}$: possible outcomes of quantum measurements.

If we assume that it is not possible to measure properties without changing them (observer effect: $\alpha$ is fixpoint-free), then there is a limit to self-inspection.

# 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。

# Self-reproducing Program

There is a program that outputs its own length.

There is a program that outputs its own source code.

## Corollary (Self-reproducing Program)

*There is a recursive function $\varphi_e$ s.t. $\forall x : \varphi_e(x) = e$.*

## Quine in Python

```
s='s=%r; print(s%%s)'; print(s%s)
```

$$(\lambda x.xx)(\lambda x.xx)$$

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

# von Neumann's Self-reproducing Automata

1. A universal constructor $A$.

$$A + \ulcorner X \urcorner \rightsquigarrow X$$

2. A copying machine $B$.

$$B + \ulcorner X \urcorner \rightsquigarrow \ulcorner X \urcorner$$

3. A control machine $C$, which first activates $B$, then $A$.

$$A + B + C + \ulcorner X \urcorner \rightsquigarrow X + \ulcorner X \urcorner$$

4. Let $X := A + B + C$. Then $A + B + C + \ulcorner A + B + C \urcorner$ is self-reproducing.

$$A + B + C + \ulcorner A + B + C \urcorner \rightsquigarrow A + B + C + \ulcorner A + B + C \urcorner$$

5. It is possible to add the description of any machine $D$.

$$A + B + C + \ulcorner A + B + C + D \urcorner \rightsquigarrow A + B + C + D + \ulcorner A + B + C + D \urcorner$$

6. Now allow mutation on the description $\ulcorner A + B + C + D \urcorner$.

$$A + B + C + \ulcorner A + B + C + D' \urcorner \rightsquigarrow A + B + C + D' + \ulcorner A + B + C + D' \urcorner$$

# Introspective Program

## Definition ($\psi$-introspective)

Given a total recursive function $\psi$,

- the *$\psi$-analysis* of $\varphi(x)$ is the code of the computation of $\varphi(x)$ to $\psi(x)$ steps.
- $\varphi$ is *$\psi$-introspective* at $x$ if $\varphi(x)\downarrow$ and outputs its own $\psi$-analysis.
- $\varphi$ is *totally $\psi$-introspective* if it is $\psi$-introspective at all $x$.

## Corollary

*There is a program that is totally $\psi$-introspective.*

## Proof.

Let $f(n,x) :=$ "the $\psi$-analysis of $\varphi_n(x)$".

# Introspective Program

There is a program that is totally introspective.

$$\boxed{\varphi_{\mathbf{e}} = \varphi_{\mathbf{h}(\mathbf{e})}}$$

| **Self-simulating Computer** | **Self-consciousness** |
|---|---|
| Host Machine | Experiencing Self |
| Virtual Machine | Remembering Self |
| Hardware | Body |

# 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 Stange 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 $\mathscr{L} := \{\neg, \wedge, \vee, \rightarrow, \forall, \exists, =, (, ), \ldots, +, -, \cdot, /, <, \ldots\}$
- well-formed formula
- utility function $u(s, e) = \mathbb{E}_\mu \left[ \sum_{t=1}^{T} r_t \middle| s, e \right]$
- target theorem

$$u\big[s(t) \oplus \big(\mathrm{switchbit}(t) = 1\big), e(t)\big] > u\big[s(t) \oplus \big(\mathrm{switchbit}(t) = 0\big), e(t)\big]$$

- theorem prover

hardware, costs, environment, initial state, utility, logic/arithmetic/probability

Figure: Schmidhuber

# Gödel Machine

- GRL
- Universal Search
- Self-Improvement
- Logic

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 |

$$\boxed{\varphi_{\mathbf{e}} = \varphi_{\mathbf{h(e)}}}$$

$$\boxed{\text{self-reference} \overset{?}{\Longrightarrow} \text{self-improvement}}$$

# 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 ≠ exponential iteration

3. *beyond computability*: Kleene's relativized fixpoint theorem

$$\varphi^A_{e(y)} = \varphi^A_{h(e(y),y)}$$

   - Gödel Machine PK AIXI$^{t\ell}$
   - Gödel Machine PK AIXI

# Limitation

1. Gödel's first incompleteness theorem / Rice's theorem
2. Gödel's second incompleteness theorem

$$\mathrm{T} \vdash \Box_{\mathrm{T}'} A \to A \implies \mathrm{T} \vdash \mathrm{Con}(\mathrm{T}')$$

   - Biological Evolution: Darwin PK Lamarch
   - Life3.0
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: $\boxed{\text{Learning is to forget!}}$
5. Physical constraint: If we assume that it is not possible to measure properties without changing them (observer effect: $\alpha$ is fixpoint-free), then there is a limit to self-inspection.

# The Universal program (warm-up): the petulant child

## The Petulant Child

Consider program $e$:

It searches for a proof in $\mathrm{PA}$ 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 $\mathcal{N} \vDash \mathrm{PA}$, the program never halts.
- For any $n$, there is a model $\mathcal{M} \vDash \mathrm{PA}$ 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 $\mathrm{PA}$ of a statement:

"program $e$ does not enumerate the sequence $a_0, \ldots, a_n$ and halt."

When found, enumerate that sequence.

## Theorem (The Universal algorithm: sequence version)

*There is a program $e$ s.t.,*

1. $\mathrm{PA}$ *proves that the set accepted by $e$ is finite.*
2. *For any finite $A \subset \mathbb{N}$, there is a model $\mathcal{M} \vDash \mathrm{PA}$ in which the program $e$ accepts exactly $A$.*
3. *Indeed, for any $A \subset \mathbb{N}$, there is a model $\mathcal{M} \vDash \mathrm{PA}$ 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. $\mathrm{PA}$ *proves that the function computed by $e$ is finite.*
2. *For any finite partial function $f$, there is a model $\mathcal{M} \vDash \mathrm{PA}$ in which the program $e$ computes exactly $f$.*
3. *For any partial function $f$, there is a model $\mathcal{M} \vDash \mathrm{PA}$ in which the program $e$ computes exactly $f$.*

Every function can be computable!. . . in the right universe.

**Proof.**

The statements "the $n^{\text{th}}$ number enumerated by $e$ is $f(n)$" are finitely consistent with $\mathrm{PA}$. 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. $\mathrm{PA}$ *proves that the sequence enumerated by* $e$ *is finite.*
2. *In the standard model* $\mathcal{N} \vDash \mathrm{PA}$*, program* $e$ *enumerates the empty sequence.*
3. *For any model* $\mathcal{M} \vDash \mathrm{PA}$ *in which* $e$ *enumerates a finite (possibly nonstandard) sequence* $s$*, and any finite* $t \in \mathcal{M}$ *extending* $s$*, there is an end-extension of* $\mathcal{M}$ *to a model* $\mathcal{M}' \vDash \mathrm{PA}$ *in which* $e$ *enumerates exactly* $t$*.*

In particular, every finite sequence $s$ is enumerated by $e$ in some model $\mathcal{M} \vDash \mathrm{PA}$.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# 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 (The Infinity of Primes)

*The set of primes is infinite.*

## Proof.

$$n = \prod_{i=1}^{m} p_i^{e_i}$$

For a random $n$,

$$\begin{aligned}
\log n &\leq K(n) \\
&\stackrel{+}{\leq} K(\langle e_1, \ldots, e_m \rangle) \\
&\stackrel{+}{\leq} \sum_{i=1}^{m} K(e_i) \\
&\stackrel{+}{\leq} mK(\log n) \\
&\stackrel{+}{\leq} m(\log\log n + 2\log\log\log n)
\end{aligned}$$

## Proof by Combinatorics.

$$n = \prod_{i=1}^{m} p_i^{e_i} \implies e_i \leq \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor \implies \# \left\{ (e_1, \ldots, e_m) : \prod_{i=1}^{m} p_i^{e_i} \leq n \right\} \leq$$
$$\prod_{i=1}^{m} \left( \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor + 1 \right) \leq (\ln n)^m \ll n$$

## 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 $N \leq \# \left\{ (r, s) : rs^2 \leq N \text{ and } r \text{ is squre-free} \right\} \leq 2^{\#\mathbb{P}} \sqrt{N}$.

## 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 $\varphi(n) := \#\{k : 1 \leq k \leq n \ \ \& \ \ \gcd(n, k) = 1\}$. 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 $\exists m \forall p_i \in \{p_1, \ldots, p_n\} : p_i \nmid m$.

## 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.

$$\ln x \leq \sum_{n \leq x} n^{-1} \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left( \sum_{k \geq 0} p^{-k} \right) = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 - p^{-1}\right)^{-1} = \prod_{n=1}^{\pi(x)} \left(1 + \frac{1}{p_n - 1}\right) \leq$$

$$\prod_{n=1}^{\pi(x)} \left(1 + \frac{1}{n}\right) = \pi(x) + 1.$$

## Proof by Lagrange's Theorem.

Let $p := \max \mathbb{P}$. Let $q$ be a prime dividing $2^p - 1$. We have $2^p \equiv 1 \mod q$. 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 $N_{a,b} := \{a + nb : n \in \mathbb{Z}\}$. 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 nonempty open set is infinite. And $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$ is clopen. Since any $n \in \mathbb{Z} \setminus \{1, -1\}$ has a prime divisor, then $\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}$. If $\mathbb{P}$ were finite, then $\bigcup_{p \in \mathbb{P}} N_{0,p}$ 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 $2 \max\{U(p) : p \in B\}$.

$$\ell(q) \overset{+}{\leq} \log n \lesssim n \implies U(q) \geq 2U(q)$$

# 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 $\mathrm{T}$, $\exists c \forall x : \mathrm{T} \nvdash K(x) > c$.*

"given $n$, find $\mu y\big[\,\mathrm{prf}_{\mathrm{T}}\,(y, K(x) > n)\big]$, ouput $x$" $\implies n < K(x) \leq O(\log n)$

"the least number undefinable in fewer characters than there are in this sentence."

$M_e :=$"find $\mu y\big[\,\mathrm{prf}_{\mathrm{T}}\,(y, K(x) > e)\big]$, ouput $x$" (Berry Paradox)

**Theorem (Chaitin)**

*For any arithmetically sound Gödelian $\mathrm{T}$, $\big|\{x : \mathrm{T} \vdash K(x) > \ell(x)\}\big| < \infty$.*

# Incompressibility vs Incompleteness vs Berry Paradox

## Definition (Kolmogorov Complexity $H$)

$$H(x|y) \coloneqq \mu e[\varphi_e(y) = x]$$
$$H(x) \coloneqq H(x|\epsilon)$$

## Theorem (Chaitin)

*For any arithmetically sound Gödelian* $\mathrm{T}$, $\exists c \forall x : \mathrm{T} \nvdash H(x) > c$.

## Proof.

For any $m$, construct:

$$M_n \coloneqq \text{“find } \mu y\big[\,\mathrm{prf}_{\mathrm{T}}\big(y, H(x) > m\big)\big], \text{output } x\text{”}$$

Then there exists a computable $f : m \mapsto n$.

By Kleene's fixpoint theorem,

$$\exists e : M_e = M_{f(e)} = \text{“find } \mu y\big[\,\mathrm{prf}_{\mathrm{T}}\big(y, H(x) > e\big)\big], \text{output } x\text{”}$$

Take $c \coloneqq e$.

# Incompressibility vs Incompleteness vs Intelligence

- $P(x) := \{p \in \mathcal{X}^* : \exists m \forall n \geq m \, (p(x_{1:n}) = x_{n+1})\}$
- $P(A) := \bigcap_{x \in A} P(x)$
- $P_n := P(\{x : Km(x) \leq n\})$

- $\forall n \exists p \in P_n : K(p) \stackrel{+}{\leq} n + O(\log n)$
- $\forall n : p \in P_n \Longrightarrow K(p) \stackrel{+}{\geq} n$

**Theorem (Legg)**

*For any arithmetically sound Gödelian* $\mathrm{T}$, $\exists n \forall p : \mathrm{T} \nvdash p \in P_n$.

# Halting Probability

## Definition (Halting Probability)

$$
\begin{aligned}
E_t &:= \{p : U(p) \downarrow \text{ in at most } t \text{ steps}\} \\
E &:= E_\infty \\
\Omega^t &:= \sum_{p \in E_t} 2^{-\ell(p)} \\
\Omega &:= \Omega^\infty \\
t(n) &:= \mu t[\Omega^t \geq \Omega_{1:n}]
\end{aligned}
$$

Obviously,

$$\Omega^1 \leq \cdots \leq \Omega^i \leq \Omega^{i+1} \leq \cdots \xrightarrow{i \to \infty} \Omega$$

and

$$\Omega_{1:n} \leq \Omega < \Omega_{1:n} + 2^{-n}$$

and $t(n)$ is computable with Oracle $\Omega$.

# 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 $\Omega_{1:n}$.

# Randomness of $\Omega$

**Theorem (Randomness of $\Omega$)**

$$\exists c \forall n : K(\Omega_{1:n}) \geq n - c$$

**Proof.**

$$f(\Omega_{1:n}) := \mu x \left[ 2^{<\omega} \setminus \left\{ U(p) : p \in E_{t(n)} \right\} \right]$$

Obviously, $f$ is computable.

$$n < K(f(\Omega_{1:n})) \overset{+}{\leq} K(\Omega_{1:n}) + K(f) \overset{+}{\leq} K(\Omega_{1:n})$$

## Theorem (Chaitin Diophantine Incompleteness)

*There is an exponential diophantine equation*

$$L(n, x_0, x_1, \ldots, x_m) = R(n, x_0, x_1, \ldots, x_m)$$

*which has finitely many solutions* $x_0, x_1, \ldots, x_m$ *iff* $\Omega_n = 0$.

## Proof.

$A := \left\{\langle n, k\rangle : \Omega_n^k = 1\right\}$ is r.e.
Since a set is r.e. iff it is singlefold exponential Diophantine,
hence there exists $L(y, x_0, x_1, \ldots, x_m) = R(y, x_0, x_1, \ldots, x_m)$ s.t.

$$\langle n, k\rangle \in A \iff \exists!\langle x_1, \ldots, x_m\rangle\big(L(n, k, x_1, \ldots, x_m) = R(n, k, x_1, \ldots, x_m)\big)$$

Thereby, $L(n, k, x_1, \ldots, x_m) = R(n, k, x_1, \ldots, x_m)$ has exactly one solution $x_1, \ldots, x_m$ if $\Omega_n^k = 1$, and it has no solution if $\Omega_n^k = 0$.

## Theorem (Chaitin $\Omega$ Incompleteness)

*For any arithmetically sound Gödelian $\mathrm{T}$, $\mathrm{T}$ can determine at most finitely many (scattered) bits of $\Omega$.*

## Proof.

Assume $\mathrm{T}$ can provide infinitely many bit of $\Omega$.
Any $k$ different bits $i_1, i_2, \ldots, i_k$ of $\Omega$ give us a covering $A_k$ of measure $2^{-k}$ which includes $\Omega$.

$$A_k := \left\{ s_1 \Omega_{i_1} \cdots s_k \Omega_{i_k} 2^\omega : \forall 1 \leq j \leq k \left( s_j \in 2^{<\omega} \ \& \ \ell(s_j) = i_j - i_{j-1} - 1 \right) \right\}$$

$$\mu(A_k) = \frac{2^{i_k - k}}{2^{i_k}} = 2^{-k}$$

Thereby,

$$\forall k \left[ \mu(A_k) \leq 2^{-k} \ \ \& \ \ \Omega \in A_k \right]$$

which contradicts the Martin-Löf randomness of $\Omega$.

## Definition (Busy Beaver)

$$\Sigma(n) := \max\{x : K(x) \leq n\}$$
$$\sigma(n) := \mu t \left[\Omega^t_{1:n} = \Omega_{1:n}\right]$$

## Lemma

$$\Sigma(n - K(n) - O(1)) \leq \sigma(n) \leq \Sigma(n + 2K(n) + O(1))$$

## Proof.

$$\Omega_{1:n} = \Omega^{\sigma(n)}_{1:n} \implies K(\Omega_{1:n}) \leq K(n) + K(\sigma(n)) + O(1)$$

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 $\sigma(n) := \mu t \left[\Omega^t_{1:n} = \Omega_{1:n}\right]$ 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* $f$, $\Sigma \overset{+}{\geq} f$ *and* $\sigma \overset{+}{\geq} f$.

**Proof.**

$$K(f(n)) \overset{+}{\leq} K(n) + K(f) \lesssim n \implies \Sigma \overset{+}{\geq} f$$

**Theorem (Chaitin Busy Beaver Incompleteness)**

*For any arithmetically sound Gödelian* $\mathrm{T}$, $\exists n \forall x : \mathrm{T} \nvdash \sigma(n) \leq x$.

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

1. Formalization & Axiomatization (Richness): Formalize and axiomatize (recursively) the elementary logic $\mathrm{L}$, the "finitistic" mathematics $\mathrm{F}$ (which is concerned with the real world) and the "infinitistic" mathematics $\mathrm{T}$ (which is concerned with 'ideal objects').
2. Independence: the axioms should be "independent" of one another.
3. Completeness: $(1)$ all valid logical statements can be proved in $\mathrm{L}$; $(2)$ all true mathematical statements can be proved in $\mathrm{T}$.
4. **Consistency**: a finitistic proof that no contradiction can be proved in $\mathrm{T}$.
5. Conservation(Consequence of Consistency $\forall A \in \Pi_1 : \mathrm{T} \vdash A \implies \mathrm{F}, \mathrm{Con}(\mathrm{T}) \vdash A$): any statement about 'real objects' provable in $\mathrm{T}$ can be proved in $\mathrm{F}$.
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? $\mathrm{T}$ characterizes exactly one model up to isomorphism.

- 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.*

$$\mathrm{Q} \vdash G \leftrightarrow F(\ulcorner G \urcorner)$$

# 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，欲以观其徼。
- 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* $\mathrm{T} \supset \mathrm{Q}$, $\mathrm{Cn}(\mathrm{T}) \subsetneq \mathrm{Th}(\mathcal{N})$.

## Gödel's First Incompleteness Theorem

$$F(x) := \neg\Box x$$

$$G = \text{“I am not provable.”}$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box G$$

## Proof.

$G \leftrightarrow \neg\Box G \implies \Box G \to \neg G \implies \Box(\Box G \to \neg G) \implies \Box G \to \Box\neg G \implies$
$\Box G \to \Box(G \wedge \neg G) \implies \neg\Box\bot \to \neg\Box G$

For every record player, there are records that it can't play.

(sympathetic vibration)

We now know enough to know that we will never know everything.

# Gödel-Rosser's Incompleteness Theorem

## Rosser's Trick

$$\Box^R x := \exists y \big[ \operatorname{prf}_{\mathrm{T}}(y, x) \wedge \neg \exists z < y \ \operatorname{prf}_{\mathrm{T}}\big(z, N(x)\big) \big]$$

where $N : \ulcorner A \urcorner \mapsto \ulcorner \neg A \urcorner$

$$F(x) := \neg \Box^R x$$

$G$ = "For every proof of me, there is a shorter proof of my negation."

# Tarski's Undefinability Theorem

## Tarski's Undefinability Theorem

suppose $\left\{\ulcorner A \urcorner : \mathcal{N} \vDash A\right\}$ is definable by $B(x)$.

$$F(x) := \neg B(x)$$

$G$ = "I am not true."

# Provability Conditions

## Provability Conditions

For any Gödelian $\mathrm{T} \supset \mathrm{PA}$,

1. $\mathrm{T} \vdash A \implies \mathrm{Q} \vdash \Box_{\mathrm{T}} A$
2. $\mathrm{PA} \vdash \Box_{\mathrm{T}} A \to \Box_{\mathrm{T}} \Box_{\mathrm{T}} A$
3. $\mathrm{PA} \vdash \Box_{\mathrm{T}}(A \to B) \to \Box_{\mathrm{T}} A \to \Box_{\mathrm{T}} B$

# Löb's Theorem

## Theorem (Löb's Theorem)

*For any Gödelian* $\mathrm{T} \supset \mathrm{PA}$, $\mathrm{T} \vdash \Box(\Box A \to A) \to \Box A$.

## Löb's Theorem

$$F(x) := \Box x \to A$$

$G$ = "If I am provable, then $A$."

## Corollary

$$\mathrm{T} \vdash \Box A \to A \implies \mathrm{T} \vdash A$$

## Proof.

$\mathrm{T} \vdash \Box G \to \Box\Box G \wedge \Box(\Box G \to A) \implies \mathrm{T} \vdash \Box G \to \Box A \implies \mathrm{T} \vdash \Box G \to A \implies \mathrm{T} \vdash G \implies \mathrm{T} \vdash \Box G \implies \mathrm{T} \vdash A$

## 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* $\mathrm{T} \supset \mathrm{PA}$, $\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box\,\mathrm{Con}(\mathrm{T})$.

**Proof.**

$$\mathrm{T} \vdash \Box(\Box\bot \to \bot) \to \Box\bot \implies \mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box\,\mathrm{Con}(\mathrm{T})$$

$$\mathrm{PA} \nvdash \neg\Box_{\mathrm{PA}}\,\mathrm{Con}(\mathrm{PA})$$

$$\mathrm{PA} \nvdash \mathrm{Con}(\mathrm{PA})$$

$$\mathrm{PA}^* \vdash \neg\,\mathrm{Con}(\mathrm{PA}^*) \text{ where } \mathrm{PA}^* = \mathrm{PA} + \neg\,\mathrm{Con}(\mathrm{PA})$$

**Remark:** The second incompleteness theorem does not imply that the consistency of a system $\mathrm{T}$ can only be proved in a stronger system.

# Gödel's Second Incompleteness Theorem

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \mathrm{Con}(\mathrm{T} + \neg\,\mathrm{Con}(\mathrm{T}))$$

Proof.

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box\,\mathrm{Con}(\mathrm{T})$$
$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box(\neg\,\mathrm{Con}(\mathrm{T}) \to \bot)$$
$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \mathrm{Con}(\mathrm{T} + \neg\,\mathrm{Con}(\mathrm{T}))$$

*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

$$\mathrm{T} \nvdash \mathrm{Con}(\mathrm{T})$$

$$\boxed{\text{second incompleteness} \implies \text{Löb}}$$

## Proof.

$$\mathrm{T} \vdash G \leftrightarrow \neg\Box G$$

$$\mathrm{T} \vdash G \to (\Box G \to \bot)$$

$$\mathrm{T} \vdash \Box G \to \Box(\Box G \to \bot)$$

$$\mathrm{T} \vdash \Box G \to \Box\bot$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \neg\Box G$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \implies \mathrm{T} \vdash \neg\Box G$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \implies \mathrm{T} \vdash G$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \implies \mathrm{T} \vdash \Box G$$

$$\mathrm{T} \nvdash \mathrm{Con}(\mathrm{T})$$

## Löb's Theorem

$$\mathrm{T} \vdash \Box A \to A \iff \mathrm{T} \vdash A$$

## Proof.

Assume $\mathrm{T} \nvdash A$.

Then $\mathrm{T} + \neg A$ is consistent.

$$\mathrm{T} + \neg A \nvdash \mathrm{Con}(\mathrm{T} + \neg A)$$

$$\mathrm{T} + \neg A \nvdash \neg\Box(\neg A \to \bot)$$

$$\mathrm{T} + \neg A \nvdash \neg\Box A$$

$$\mathrm{T} \nvdash \Box A \to A$$

Let $G$ be the Gödel sentence s.t. $\mathrm{T} \vdash G \leftrightarrow \neg\Box G$. Then

$$\mathrm{T} \vdash G \leftrightarrow \mathrm{Con}(\mathrm{T})$$

**Proof.**

$(\rightarrow)$:

$$\mathrm{T} \vdash \bot \rightarrow G$$
$$\mathrm{T} \vdash \Box\bot \rightarrow \Box G$$
$$\mathrm{T} \vdash \Box\bot \rightarrow \neg G$$
$$\mathrm{T} \vdash G \rightarrow \mathrm{Con}(\mathrm{T})$$

$(\leftarrow)$:

$$\mathrm{T} \vdash \Box G \rightarrow \Box\Box G$$
$$\mathrm{T} \vdash \Box G \rightarrow \Box\neg G$$
$$\mathrm{T} \vdash \Box G \rightarrow \Box(G \wedge \neg G)$$
$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \rightarrow G$$

**Fixpoint**

1. For any Gödelian $\mathrm{T} \supset \mathrm{PA}$, $\mathrm{Con}(\mathrm{T})$ is the only fixpoint of $\neg\Box x$ up to the logical equivalence in $\mathrm{T}$.
2. For any Gödelian $\mathrm{T} \supset \mathrm{PA}$, $\top$ is the only fixpoint of $\Box x$ up to the logical equivalence in $\mathrm{T}$.

# Surprise Exam Paradox vs Second Incompleteness Theorem

$$\boxed{\mathrm{T} \nvdash \mathrm{Con}(\mathrm{T})}$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \to \forall x \neg \Box\big(K(x) > c\big) \qquad \text{(Chaitin)}$$

$$\mathrm{T} \vdash \mathrm{Con}(\mathrm{T}) \implies \mathrm{T} \vdash \forall x \in \mathcal{X}^{c+1} \neg \Box\big(K(x) > c\big)$$

$$\mathrm{T} \vdash \forall x \in \mathcal{X}^{c+1} \big[K(x) \leq c \to \Box\big(K(x) \leq c\big)\big] \qquad (\Sigma_1\text{-complete})$$

$$m \coloneqq \left|\left\{x \in \mathcal{X}^{c+1} : K(x) > c\right\}\right|$$

$$\mathrm{T} \vdash 1 \leq m \leq 2^{c+1}$$

We prove by induction that for $1 \leq i \leq 2^{c+1}$,

$$\mathrm{T} \vdash m \geq i \implies \mathrm{T} \vdash m \geq i + 1$$

$$\mathrm{T} \vdash m \geq i \implies \mathrm{T} \vdash m \geq i+1$$

Proof.

Assume $\mathrm{T} \vdash m \geq i$. Let $r := 2^{c+1} - i$.

$$\mathrm{T} \vdash m = i \to \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^{r} \big(K(y_k) \leq c\big)$$

$$\mathrm{T} \vdash m = i \to \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^{r} \Box\big(K(y_k) \leq c\big)$$

$$\forall x \in \mathcal{X}^{c+1} \setminus \{y_1, \dots, y_r\} : \ \mathrm{T} \vdash m \geq i \to \left( \bigwedge_{k=1}^{r} \big(K(y_k) \leq c\big) \to \big(K(x) > c\big) \right)$$

$$\mathrm{T} \vdash \Box\big(m \geq i\big) \to \left( \bigwedge_{k=1}^{r} \Box\big(K(y_k) \leq c\big) \to \Box\big(K(x) > c\big) \right)$$

$$\mathrm{T} \vdash m = i \wedge \Box\big(m \geq i\big) \to \exists x \in \mathcal{X}^{c+1} \Box\big(K(x) > c\big)$$

$$\mathrm{T} \vdash m \neq i$$

- syntactic completeness: $\Box A \vee \Box \neg A$
- semantic completeness: $A \to \Box A$
- $\omega$-completeness: $\forall x \Box A(x) \to \Box \forall x A(x)$

$$\omega\text{-complete} \implies \omega\text{-consistent} \implies 1\text{-consistent} \implies \text{consistent}$$

**Theorem**

*For any Gödelian $\mathrm{T} \supset \mathrm{PA}$, the following are equivalent in $\mathrm{T}$.*

1. $\neg \operatorname{Con}(\mathrm{T})$
2. $\Box A \vee \Box \neg A$
3. $A \to \Box A$
4. $\forall x \Box A(x) \to \Box \forall x A(x)$

1. consistency
2. effectiveness $\mathrm{Th}(\mathcal{N})$
3. richness Real closed field/Euclidean geometry/Presburger
4. completeness $\mathrm{Q}$ / $\mathrm{PA}$ / $\mathrm{ZFC}$

# 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.

$$\mathrm{prflen}_{\mathrm{T}}(m) := \text{“the length of the proof encoded by } m\text{”}$$

$$\Box^n x := \exists m\big(\mathrm{prf}_{\mathrm{T}}(m, x) \wedge \mathrm{prflen}_{\mathrm{T}}(m) < n\big)$$

$$F(x) := \neg\Box^n x$$

$$G = \text{“I have no proof of myself shorter than } n\text{.”}$$

$$\neg\Box G \implies G \implies \Box G$$

# 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

$$F(x) := \neg \Box^{f(y)} x$$

$G(y)$ = "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 formulae with free variables.

$$\boxed{\text{Gödel's no-short-proof theorem} \implies \mathrm{T} \nvdash \forall x G(x)}$$

# Undecidability

$\boxed{\mathrm{Q} \text{ is incomplete.}}$

**Theorem ($\Sigma_1$-completeness of Robinson Arithmetic $\mathrm{Q}$)**

*For any Gödelian $\mathrm{T} \supset \mathrm{Q}$, and any sentence $A \in \Sigma_1$, $\mathrm{Q} \vdash A \to \Box A$.*

**Theorem (Strong Undecidability of $\mathrm{Q}$)**

*If $\mathrm{T} \cup \mathrm{Q}$ is consistent, then $\mathrm{T}$ is undecidable.*

**Remark:** In fact, the above is true for any countable $\mathscr{L}$ containing a $k$-ary predicate or function symbol, $k \geq 2$, or at least two unary function symbols.

$\boxed{\text{First order logic } \mathcal{L}_{\omega\omega} \text{ is undecidable.}}$

**Theorem (Church1936, Turing1936)**

*The set of valid sentences is recursively enumerable but undecidable.*

# Undecidability

**Theorem (Trakhtenbrot's Theorem)**

*Suppose $\mathscr{L}$ 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:*

$$(w_1, v_1), \ldots, (w_n, v_n)$$

*is there a sequence of indices $(i_1, \ldots, i_k)$ with $k \geq 1$ s.t.*

$$w_{i_1} \ldots w_{i_k} \stackrel{?}{=} v_{i_1} \ldots v_{i_k}$$

## 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 (Post1946)

*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.*

$0 \mapsto$ white

$1 \mapsto$ red

$2 \mapsto$ blue

$3 \mapsto$ 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 $10^{\text{th}}$ Problem is Unsolvable

## Definition (Diophantine Set)

A set $A \subset \mathbb{N}^n$ is diophantine if there exists a polynomial $P(\mathbf{x}, \mathbf{y})$ with integer coefficients s.t.

$$\mathbf{x} \in A \iff \exists \mathbf{y} \in \mathbb{N}^m [P(\mathbf{x}, \mathbf{y}) = 0]$$

## 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

$$\underbrace{\Gamma_r \cup \Gamma_m \cup \Gamma_b \vdash A \qquad \mathcal{M}_r \vDash \Gamma_r}$$

$$\Downarrow ?$$

$$\mathcal{M}_r \vDash A$$

$$\frac{\Gamma_r \cup \Gamma'_r \vdash A \quad \mathcal{M}_r \vDash \Gamma_r \cup \Gamma'_r}{\mathcal{M}_r \vDash A}$$

where $\Gamma'_r \subset \Gamma_m \cup \Gamma_b$

# 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* $\mathrm{PA}$ *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

$$\begin{aligned} m_0 &\coloneqq m \\ m_k &\coloneqq G_{k+1}(m_{k-1}) \\ f_G(m) &\coloneqq \mu k[m_k = 0] \end{aligned}$$

$$\begin{aligned} m_0 &= 266 = 2^{2^{2+1}} + 2^{2+1} + 2^1 \\ m_1 &= G_2(m_0) = 3^{3^{3+1}} + 3^{3+1} + 2 \approx 10^{38} \\ m_2 &= G_3(m_1) = 4^{4^{4+1}} + 4^{4+1} + 1 \approx 10^{616} \\ m_3 &= G_4(m_2) = 5^{5^{5+1}} + 5^{5+1} \approx 10^{10000} \end{aligned}$$

# Fast-growing Hierarchy

## Definition (Wainer Hierarchy)

$$f_0(n) := n+1$$
$$f_{\alpha+1}(n) := f_\alpha^n(n)$$
$$f_\alpha(n) := f_{\alpha[n]}(n) \text{ if } \alpha \text{ is a limit ordinal.}$$

For limit ordinals $\lambda < \varepsilon_0$, written in Cantor normal form,

- if $\lambda = \omega^{\alpha_1} + \cdots + \omega^{\alpha_k}$ for $\alpha_1 \geq \cdots \geq \alpha_k$, then $\lambda[n] := \omega^{\alpha_1} + \cdots + \omega^{\alpha_k}[n]$
- if $\lambda = \omega^{\alpha+1}$, then $\lambda[n] := \omega^\alpha[n]$
- if $\lambda = \omega^\alpha$ for a limit ordinal $\alpha$, 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 $f_\alpha$ with $\alpha < \varepsilon_0$ is computable, and provably total in $\mathrm{PA}$.
- If $f$ is computable and provably total in $\mathrm{PA}$, then $\exists \alpha < \varepsilon_0 : f < f_\alpha$. Hence $f_{\varepsilon_0}$ is not provably total in $\mathrm{PA}$.

# Kirby-Paris Theorem vs Goodstein Theorem

**Theorem**

$$\forall \alpha < \varepsilon_0 \, (f_\alpha < f_G)$$

$$\mathrm{ZFC} \vdash \forall m \exists k (m_k = 0) \quad \text{but} \quad \mathrm{PA} \nvdash \forall m \exists k (m_k = 0)$$

$$\Sigma(n) := \max\{m : K(m) \leq n\}$$

$$f < \Sigma \ \text{ for any computable } f$$

$$\mathrm{PA} \nvdash \forall n \exists m (\Sigma(n) = m)$$

$$\exists n \forall m : \mathrm{PA} \nvdash \Sigma(n) \leq m$$

For any arithmetically sound Gödelian $\mathrm{T} : \exists n \forall m : \mathrm{T} \nvdash \Sigma(n) \leq m$

# Paris-Harrington Theorem vs Ramsey Theorem

$$[A]^n := \{X \subset A : |X| = n\}$$

$$\kappa \to (\lambda)^n_m := \forall F : [\kappa]^n \to m\Big(\exists H \subset \kappa\Big(|H| = \lambda \ \wedge \ \exists i \in m\Big([H]^n \subset F^{-1}(i)\Big)\Big)\Big)$$

Ramsey theorem: $\forall mn \in \omega : \aleph_0 \to (\aleph_0)^n_m$

$$s \to (k_0, \ldots, k_{m-1})^n_m := \forall F : [s]^n \to m\left(\bigvee_{i=0}^{m-1} \exists H \subset s\Big(|H| = k_i \ \wedge \ [H]^n \subset F^{-1}(i)\Big)\right)$$

$$s \underset{*}{\to} (k)^n_m := \forall F : [s]^n \to m\Big(\exists H \subset s\Big(|H| \geq \min(H) \ \wedge \ |H| \geq k \ \wedge \ \exists i \in m\Big([H]^n \subset F^{-1}(i)\Big)\Big)\Big)$$

$$\mathrm{ZFC} \vdash \forall mnk \exists s \left(s \underset{*}{\to} (k)^n_m\right)$$

$$\mathrm{PA} \nvdash \forall mnk \exists s \left(s \underset{*}{\to} (k)^n_m\right)$$

$$\forall \alpha < \varepsilon_0 \, (f_\alpha < f_R) \quad \text{where} \quad f_R(m,n,k) := \mu s \left[s \underset{*}{\to} (k)^n_m\right]$$

# Leibniz — Hilbert — Gödel — Turing $\cdots$

- Either $(a)$ absolutely unsolvable problems exist or $(b)$ the human mind infinitely surpasses any Turing machine or axiomatizable formal system. — *Kurt Gödel*
- Gödel can't consistently assert that this sentence is true.
- 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 N. 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*

# Math-Matter-Mind (Penrose)

$$\begin{tikzcd}
\text{Mind} \arrow[rr, Rightarrow] & & \text{Math} \arrow[dl, Rightarrow] \\
& \text{Matter} \arrow[ul, Rightarrow] &
\end{tikzcd}$$

$$\begin{tikzcd}
\text{Mind} & & \text{Math} \\
& ? \arrow[ul, Rightarrow] \arrow[ur, Rightarrow] \arrow[d, Rightarrow] & \\
& \text{Matter} &
\end{tikzcd}$$

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Pirate Game

## Problem (Pirate Game)

*$5$ rational pirates have a treasure of 100 gold coins.*
*The pirate world's rules of distribution are thus:*

1. *The fiercest pirate proposes how to split the coins, and all pirates (including the proposer) vote for or against it;*
2. *If $50\%$ or more of the pirates vote for it, then the coins will be shared that way. Otherwise, the proposer will be thrown overboard, and the procedure is repeated with the next fiercest pirate;*
3. *As the pirates are bloodthirsty, each pirate would prefer to throw another overboard, if all other results would otherwise be equal.*

# Who Will Survive?

## Problem (Who Will Survive?)

*$5$ rational prisoners are going to take beans from a bag with 100 beans. They will do it one by one. No communication is allowed between them. But they can count the beans left in the bag.*

1. *each must take at least $1$ bean, and the last prisoner need not to take all the rest;*
2. *all prisoners who take the maximum/minimum number will die;*
3. *they will try to survive first and then try to kill more people.*

# Simpson Paradox

| | Group 1 | Group 2 | Total |
|---|---|---|---|
| Lisa | 0% | 75% | 60% |
| Bart | 25% | 100% | 40% |

| | Group 1 | Group 2 | Total |
|---|---|---|---|
| Lisa | 0/1 | 3/4 | 3/5 |
| Bart | 1/4 | 1/1 | 2/5 |

Figure: Something true for different groups is false for the combined group.

# Monty Hall Problem

## Problem (Monty Hall Problem)

*You're given the choice of three doors: Behind one door is a car; behind the others, goats. You pick a door, say No.1, and the host, who knows what's behind the doors, opens another door, say No.3, which has a goat. He then says to you, "Do you want to pick door No.2?"*

# Bertrand's Paradox

## Problem (Bertrand's Paradox)

*Consider an equilateral triangle inscribed in a circle. Suppose a chord of the circle is chosen at random. What is the probability that the chord is longer than a side of the triangle?*

What is "randomness"? a process or a product?

# Confirmation Problem

$$\frac{\begin{array}{c}\neg Rx \wedge \neg Bx \ \text{ confirms } \ \forall x(\neg Bx \rightarrow \neg Rx) \\ \forall x(\neg Bx \rightarrow \neg Rx) \leftrightarrow \forall x(Rx \rightarrow Bx)\end{array}}{\neg Rx \wedge \neg Bx \ \text{ confirms } \ \forall x(Rx \rightarrow Bx)}$$

Figure: Raven Paradox

# Zero-Knowledge Proof

- Alice gave Bob a Sudoku puzzle.
- Bob tried and failed: "Is it an unsolvable one?"
- Alice: "Let me show you that I have a solution. But I will not show you the actual solution."

# Prover vs Verifier

- **Completeness:** $P$ can convince $V$ if $X$ is true.
- **Soundness:** no (efficient) $P$ can convince $V$ if $X$ is not true.
- **Zero Knowledge:** no efficient $V$ learns anything more than the validity of $X$.

**Remark:** The adversary can simulate the proof without knowing the prover's witness.

**Theorem**

*Every NP statement can be proven in zero-knowledge.*

# Logic vs Probability — Cox Theorem

Probability theory extends propositional logic?

## Assumption (Cox's Assumptions for Beliefs)

1. $A \leftrightarrow B \implies b(\cdot|A) = b(\cdot|B)$ & $b(A|\cdot) = b(B|\cdot)$.
2. *there is a continuous binary operation* $\otimes$ *that is strictly increasing in each coordinate s.t.* $b(A \wedge B|C) = b(A|C) \otimes b(B|A \wedge C)$.
3. *for any rational numbers* $r_1, r_2, r_3 \in (0,1)$ *there are* $A, B, C, D \in \Omega$ *s.t.* $r_1 = b(A|D)$, $r_2 = b(B|A \wedge D)$ *and* $r_3 = b(C|A \wedge B \wedge D)$.
4. *thers is a continuous nonnegative nonincreasing function* $N : [0,1] \to [0,1]$ *s.t.* $b(\neg A|C) = N(b(A|C))$.

## Theorem (Cox Theorem)

*A credence function that satisfies Cox's assumptions for beliefs is isomorphic to a probability function.*

# Logic vs Probability — Algorithmic Probability

## Definition (Algorithmic Probability)

$$M(x) := \sum_{p:U(p)=x*} 2^{-\ell(p)}$$

where $U$ is a universal monotone Turing machine.

$$M'(\epsilon) := 1$$

$$M'(x_{1:t}) := M'(x_{<t}) \frac{M(x_{1:t})}{\sum_{x \in \mathcal{X}} M(x_{<t}x)}$$

## Theorem (Completeness Theorem)

*For any computable environment $\mu$,*

$$\sum_{t=1}^{\infty} \sum_{x_{1:t} \in \mathcal{X}^t} \mu(x_{<t}) \big(M'(x_t|x_{<t}) - \mu(x_t|x_{<t})\big)^2 \stackrel{+}{\leq} K(\mu) \ln 2$$

# Game Theory

| | silent | betray |
|---|---|---|
| Silent | $-1, -1$ | $-4, 0$ |
| Betray | $0, -4$ | $-3, -3$ |

Table: Prisoner's Dilemma

| | opera | football |
|---|---|---|
| Opera | $1, 2$ | $0, 0$ |
| Football | $0, 0$ | $2, 1$ |

Table: Battle of the Sexes

| | stop | go |
|---|---|---|
| Stop | $0, 0$ | $0, 1$ |
| Go | $1, 0$ | $-\infty, -\infty$ |

Table: Chicken/Traffic

| | head | tail |
|---|---|---|
| Head | $+1, -1$ | $-1, +1$ |
| Tail | $-1, +1$ | $+1, -1$ |

Table: Matching Pennies

# Preferences Lead to Utility

- A lottery $L = [p_1, x_1; \ldots; p_n, x_n]$ is a probability distribution over outcomes $\mathcal{X}$.
- Preferences of a rational agent must obey constraints.

1. completeness $x_1 \succ x_2 \vee x_1 \sim x_2 \vee x_2 \succ x_1$
2. transitivity $x_1 \succ x_2 \wedge x_2 \succ x_3 \rightarrow x_1 \succ x_3$
3. continuity $x_1 \succ x_2 \succ x_3 \rightarrow \exists p : x_2 \sim [p, x_1; 1-p, x_3]$
4. independence $x_1 \sim x_2 \rightarrow [p, x_1; 1-p, x_3] \sim [p, x_2; 1-p, x_3]$
5. monotonicity $x_1 \succ x_2 \wedge p > q \rightarrow [p, x_1; 1-p, x_2] \succ [q, x_1; 1-q, x_2]$
6. decomposability
$$\big[p, x_1; 1-p, [q, x_2; 1-q, x_3]\big] \sim \big[p, x_1; (1-p)q, x_2; (1-p)(1-q), x_3\big]$$

**Theorem (von Neumann & Morgenstern 1944)**

*If a preference relation $\succeq$ satisfies the above constraints, then there exists a function $u : \mathcal{X} \rightarrow [0, 1]$ such that*

$$x_1 \succeq x_2 \iff u(x_1) \geq u(x_2) \quad \textit{and}$$

$$u\big([p_1, x_1; \ldots; p_n, x_n]\big) = \sum_{i=1}^{n} p_i u(x_i)$$

# Equilibrium

## Definition (Nash Euqilibrium)

- $s^*$ is a *pure Nash equilibrium* if $s^* \in \prod_{i \in N} \operatorname*{argmax}_{s_i \in S_i} u_i(s_i; s_{-i})$.
- $\sigma^*$ is a *mixed Nash equilibrium* if

$$\forall i \in N \forall \sigma_i \in \Delta S_i : u_i(\sigma_i^*; \sigma_{-i}^*) \geq u_i(\sigma_i; \sigma_{-i}^*)$$

## Definition (Correlated Equilibrium)

Let $\Omega$ be the state space, $\mathcal{I}_i$ be the information partition of player $i$, $P(\cdot|\mathcal{I}_i) \in \Delta\Omega$ be the interim belief systems, and $\sigma_i : \Omega \to S_i$ be measurable with regard to $\mathcal{I}_i$. Then $(\sigma_i)_{i \in N}$ is a posteriori equilibrium of the strategic game $(N, S_i, u_i)$ if

$$\forall i \in N \forall s_i \in S_i : \sum_{\omega \in \Omega} P\big(\omega|\mathcal{I}_i(\omega)\big)\Big(u_i\big(\sigma_i(\omega); \sigma_{-i}(\omega)\big) - u_i\big(s_i; \sigma_{-i}(\omega)\big)\Big) \geq 0$$

**Remark:** For every Nash equilibrium there exists a corresponding correlated equilibrium.

# Evolutionarily Stable Strategy

Given a symmetric two-player normal form game, $\sigma^*$ is an ESS iff $\forall \sigma \neq \sigma^* \exists \delta \in (0,1) \forall \varepsilon \in (0,\delta)$ :

$$u\left(\sigma^*, (1-\varepsilon)\sigma^* + \varepsilon\sigma\right) > u\left(\sigma, (1-\varepsilon)\sigma^* + \varepsilon\sigma\right)$$

iff

$$(1-\varepsilon)u\left(\sigma^*, \sigma^*\right) + \varepsilon u\left(\sigma^*, \sigma\right) > (1-\varepsilon)u\left(\sigma, \sigma^*\right) + \varepsilon u\left(\sigma, \sigma\right)$$

iff

- $u\left(\sigma^*, \sigma^*\right) > u\left(\sigma, \sigma^*\right)$ or
- $u\left(\sigma^*, \sigma^*\right) = u\left(\sigma, \sigma^*\right)$ and $u\left(\sigma^*, \sigma\right) > u\left(\sigma, \sigma\right)$

If $\sigma$ is an ESS, then $(\sigma, \sigma)$ is a Nash equilibrium. If $(\sigma, \sigma)$ is a strict Nash equilibrium, then $\sigma$ is an ESS.

| | dove | hawk |
|---|---|---|
| Dove | $\frac{b}{2}, \frac{b}{2}$ | $0, b$ |
| Hawk | $b, 0$ | $\frac{b-c}{2}, \frac{b-c}{2}$ |

$$\frac{b}{2}x + 0(1-x) = bx + \frac{b-c}{2}(1-x)$$

$$c > b \implies (1 - \frac{b}{c}, \frac{b}{c})$$

$$c \leq b \implies (H, h)$$

# Evolutionarily Stable Strategy

- strict Nash Equilibrium: $u(\sigma_i^*; \sigma_{-i}^*) > u(\sigma_i; \sigma_{-i}^*)$
- Nash Equilibrium: $u(\sigma_i^*; \sigma_{-i}^*) \geq u(\sigma_i; \sigma_{-i}^*)$
- ESS:

  - $u(\sigma^*, \sigma^*) > u(\sigma, \sigma^*)$ or
  - $u(\sigma^*, \sigma^*) = u(\sigma, \sigma^*)$ and $u(\sigma^*, \sigma) > u(\sigma, \sigma)$

- weak ESS:

  - $u(\sigma^*, \sigma^*) > u(\sigma, \sigma^*)$ or
  - $u(\sigma^*, \sigma^*) = u(\sigma, \sigma^*)$ and $u(\sigma^*, \sigma) \geq u(\sigma, \sigma)$

- unbeatable strategy: $u(\sigma^*, \sigma^*) > u(\sigma, \sigma^*)$ and $u(\sigma^*, \sigma) > u(\sigma, \sigma)$

unbeatable $\Longrightarrow$ strict Nash $\Longrightarrow$ ESS $\Longrightarrow$ weak ESS $\Longrightarrow$ Nash

# Braess Paradox

*If we all go for the blonde and block each other, not a single one of us is going to get her. So then we go for her friends, but they will all give us the cold shoulder because no one likes to be second choice. But what if none of us goes for the blonde?*

*— A Beautiful Mind*

- The addition of options is not necessarily a good thing.
- A strategy profile is Pareto efficient if no other strategy profile improves the payoff to at least one actor without decreasing the payoff of other actors.
- The Nash equilibrium of a game is not necessarily Pareto efficient.

Figure: $4000$ cars travelling around the lake

# Braess Paradox

Let $L_e(x)$ be the travel time of each car traveling along edge $e$ when $x$ cars take that edge ($L_e(0) := 0$). Suppose there is a traffic graph $G$ with $x_e$ cars along edge $e$. Let $E(e) := \sum_{i=1}^{x_e} L_e(i)$, and $E(G) := \sum_{e \in G} E(e)$. Take a choice of routes that minimizes the total energy $E(G)$. That will be a Nash equilibrium.

# Sperner's Lemma

## Lemma (Sperner's Lemma)

*Suppose that some triangle with vertices $V_1, V_2, V_3$ is triangulated.*
*The vertices in the triangulation get "colors" from $\{1, 2, 3\}$ s.t. vertices on the edge $(V_i, V_j)$ are colored either $i$ or $j$, while the interior vertices are colored $1$, $2$ or $3$.*
*Then in the triangulation there must be an odd number of "tricolored" triangles.*

# Proof of Sperner's Lemma

**Proof.**

Consider the dual graph to the triangulation — but take only those which cross an edge that has endvertices with the colors $1$ and $2$. Thus we get a partial dual graph which has degree $1$ at all vertices that correspond to tricolored triangles, degree $2$ for all triangles in which the two colors $1$ and $2$ appear, and degree $0$ for triangles that do not have both colors $1$ and $2$.

The vertex of the dual graph which corresponds to the outside of the triangulation has odd degree: along the big edge from $V_1$ to $V_2$, there is an odd number of changes between $1$ and $2$. Since the number of odd-degree vertices in any finite graph is even, the number of tricolored triangles is odd.

# Brouwer Fixpoint Theorem

## Theorem (Brouwer Fixpoint Theorem)

*Given a convex compact set $B \subset \mathbb{R}^n$ and continuous function $f : B \to B$, there exists $\mathbf{x}^*$ s.t. $f(\mathbf{x}^*) = \mathbf{x}^*$.*

## Theorem (Kakutani Fixpoint Theorem)

*Given a compact convex set $S \subset \mathbb{R}^n$ and function $f : S \to \mathrm{P}(S)$ for which*

- *for all $x \in S$ the set $f(x)$ is nonempty and convex,*
- *the graph of $f$ is closed (i.e. for all sequences $\{x_n\}$ and $\{y_n\}$ s.t. $y_n \in f(x_n)$ for all $n$, $x_n \to x$, and $y_n \to y$, we have $y \in f(x)$).*

*Then there exists $x^* \in S$ s.t. $x^* \in f(x^*)$.*

## Theorem (Schauder Fixpoint Theorem)

*If $K$ is a nonempty convex subset of a Hausdorff topological vector space $V$ and $T$ is a continuous mapping of $K$ into itself such that $T(K)$ is contained in a compact subset of $K$, then $T$ has a fixpoint.*

# Proof of Brouwer Fixpoint Theorem

**Proof.**

Let $\Delta$ be the triangle in $\mathbb{R}^3$ with vertices $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$, and $\mathbf{e}_3 = (0,0,1)$. We prove that any continuous map $f : \Delta \to \Delta$ has a fixpoint.
Let $\delta(T)$ be the maximal length of an edge in a triangulation $T$.
One can construct an infinite sequence of triangulations $T_1, T_2, \ldots$ of $\Delta$ s.t. $\lim\limits_{k\to\infty} \delta(T_k) = 0$.
Suppose $f$ has no fixpoint. Since $\sum_i \mathbf{v}_i = 1 = \sum_i f(\mathbf{v})_i$, for each of these triangulations, we can define a Sperner coloring of their vertices $\mathbf{v}$ by setting $\lambda(\mathbf{v}) := \min\{i : f(\mathbf{v})_i < \mathbf{v}_i\}$.
Sperner's lemma tells us that in each triangulation $T_k$ there is a tricolored triangle $\left\{\mathbf{v}_1^k, \mathbf{v}_2^k, \mathbf{v}_3^k\right\}$ with $\lambda(\mathbf{v}_i^k) = i$.
Since the simplex $\Delta$ is compact, some subsequence of $\left(\mathbf{v}_1^k\right)_{k\geq 1}$ has a limit point $\mathbf{v}^* \in \Delta$. Since $\lim\limits_{k\to\infty} \delta(T_k) = 0$, the sequences $\mathbf{v}_2^k$ and $\mathbf{v}_3^k$ converge to the same point $\mathbf{v}^*$.
Then $\forall i : f(\mathbf{v}^*)_i \leq \mathbf{v}_i^*$, which contradicts $f(\mathbf{v}^*) \neq \mathbf{v}^*$.

# Nash Equilibrium

## Theorem (Existence of Mixed Nash Equilibrium)

*Every finite strategic game has a mixed Nash equilibrium.*

## Proof.

Given a strategy profile $\sigma \in \prod_{i \in N} \Delta S_i$, define

$$\varphi_{i,s_i}(\sigma) := \max\left\{0, u_i(s_i; \sigma_{-i}) - u_i(\sigma)\right\}$$

Then define a continuous $f : \prod_{i \in N} \Delta S_i \to \prod_{i \in N} \Delta S_i$ by $f : \sigma \mapsto \sigma'$, where

$$\sigma_i'(s_i) := \frac{\sigma_i(s_i) + \varphi_{i,s_i}(\sigma)}{\sum_{s_i \in S_i} \left[\sigma_i(s_i) + \varphi_{i,s_i}(\sigma)\right]} = \frac{\sigma_i(s_i) + \varphi_{i,s_i}(\sigma)}{1 + \sum_{s_i \in S_i} \varphi_{i,s_i}(\sigma)}$$

Since $\prod_{i \in N} \Delta S_i$ is convex and compact, $f$ has a fixpoint.

Consider any fixpoint $\sigma$ of $f$. By the linearity of expectation there exists $s_i'$ in the support of $\sigma$, for which $u_i(s_i'; \sigma_{-i}) \leq u_i(\sigma)$. Then

$$\varphi_{i,s_i'}(\sigma) = 0 \ \ \& \ \ \sigma_i'(s_i') = \sigma_i(s_i') \implies \forall i \in N \forall s_i \in S_i : \varphi_{i,s_i}(\sigma) = 0$$

# Walrasian Equilibrium

## Theorem (Existence of Walrasian Equilibrium)

*Consider an economy with $n$ goods $X_1, \ldots, X_n$ with a price vector $(p_1, \ldots, p_n) \in \Delta_n := \{x \in [0,1]^n : \|x\|_1 = 1\}$, and the prices of at least two goods are not zero. Assume that an excess demand function for each good $f_i(p_1, \ldots, p_n)$ is continuous and satisfies the following condition*

$$\sum_{i=1}^{n} p_i f_i = 0 \qquad \text{(Walras Law)}$$

*Then, there exists an equilibrium price vector $(p_1^*, \ldots, p_n^*)$ s.t.*

$$f_i(p_1^*, \ldots, p_n^*) \leq 0$$

*for all $i = 1, \ldots, n$. And when $p_i > 0$ we have $f_i(p_1^*, \ldots, p_n^*) = 0$.*

# Contents

Introduction

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Metric Space & Topological Space

## Definition (Metric Space)

A *metric space* $(X, d)$ is a set $X$ with a metric $d : X \times X \to \mathbb{R}$ 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 $\mathcal{O}(X) \subset \mathrm{P}(X)$ 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 $F$ is a set $V$ with an element $0 \in V$, addition $+ : V \times V \to V$, and scalar multiplication $\cdot : F \times V \to V$ s.t. for all $a, b \in F$ 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 $F$ with a *norm* $\|\cdot\| : V \to [0, \infty)$ s.t. for all $a \in F$, and $u, v \in V$:

1. $\|av\| = |a|\|v\|$
2. $\|u + v\| \leq \|u\| + \|v\|$
3. $\|v\| = 0 \to v = 0$

- If $\|\cdot\|$ is a norm on $V$, then $d(u, v) = \|u - v\|$ defines a metric on $V$.
- A metric space is *complete* if for every Cauchy sequence $\{x_n\}$, $\lim_{n\to\infty} \|x - x_n\| = 0$.
- 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 $F$ with an *inner product* $\langle\cdot|\cdot\rangle : V \times V \to F$ s.t. for all $a, b \in F$ 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. $\langle v|v\rangle = 0 \to v = 0$

- The vectors $u, v$ are called *orthogonal* if $\langle u|v\rangle = 0$.
- A basis $\{e_1, \ldots, e_n\}$ is called *orthogonal* if $\langle e_i|e_j\rangle = 0$ for all $i \neq j$. It is called *orthonormal* if 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 $\|v\| = \sqrt{\langle v|v\rangle}$.

# Linear Operator

## Definition

A linear operator $A$ is

- *normal* if $AA^\dagger = A^\dagger A$.
- *unitary* if $AA^\dagger = A^\dagger A = I$.
- *self-adjoint* if $A = A^\dagger$.
- a *projection* if $A = A^\dagger$ and $AA = A$.
- *bounded* if $\exists a \geq 0 \forall v : \|Av\| \leq a\|v\|$.

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, $A^\dagger = \overline{A^\mathsf{T}}$.

## Definition (Tensor Product)

Suppose $U$ and $V$ are vector spaces over a field $F$. Then a tensor product of $U$ and $V$ is a vector space $U \otimes V$ over $F$ with a bilinear map $\otimes : U \times V \to U \otimes V :: (u, v) \mapsto u \otimes v$ having the "universal property":

$$\begin{tikzcd} U \times V \arrow[r, "\otimes"] \arrow[dr, "f"'] & U \otimes V \arrow[d, dashed, "\exists! \overline{f}"] \\ & W \end{tikzcd}$$

Given two linear maps $A : U \to X$ and $B : V \to Y$ between vector spaces, the tensor product of the two linear maps $A$ and $B$ is a linear map $A \otimes B : U \otimes V \to X \otimes Y$ defined by

$$(A \otimes B)(u \otimes v) = Au \otimes Bv$$

$W = X \otimes Y \qquad f : (u, v) \mapsto Au \otimes Bv \qquad \overline{f} = A \otimes B$

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{m1}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

# The Postulates of Quantum Mechanics

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.

$$
\begin{aligned}
\langle\phi|\psi\rangle &= \langle\phi|\psi\rangle\langle 0|0\rangle \\
&= \big(\langle\phi|\langle 0|\big)\big(|\psi\rangle|0\rangle\big) \\
&= \big(\langle\phi|\langle 0|\big)U^\dagger U\big(|\psi\rangle|0\rangle\big) \\
&= \big(\langle\phi|\langle\phi|\big)\big(|\psi\rangle\psi\rangle\big) \\
&= \langle\phi|\psi\rangle\langle\phi|\psi\rangle \\
&= \langle\phi|\psi\rangle^2
\end{aligned}
$$

# Quantum Computing

- the standard basis states: $0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \quad 1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$
- 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

$$|\phi\rangle \otimes \psi\rangle = |\phi\rangle|\psi\rangle = |\phi\psi\rangle = \begin{bmatrix}a_0b_0\\a_0b_1\\a_1b_0\\a_1b_1\end{bmatrix}$$

- the conjugate transpose of $|\phi\rangle$ is $\langle\phi| = |\phi\rangle^\dagger = \begin{bmatrix}\overline{a_0} & \overline{a_1}\end{bmatrix}$
- 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: $|\phi\rangle\langle\psi| = \begin{bmatrix}a_0\\a_1\end{bmatrix}\begin{bmatrix}\overline{b_0} & \overline{b_1}\end{bmatrix} = \begin{bmatrix}a_0\overline{b_0} & a_0\overline{b_1}\\a_1\overline{b_0} & a_1\overline{b_1}\end{bmatrix}$

# 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:

$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle \xrightarrow{\text{measurement}} |x\rangle$ 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* if for any unitary matrix $U$ and any $\varepsilon > 0$, there is some circuit $\tilde{U}$ built out of the set of gates such that

$$\left\| U - \tilde{U} \right\| < \varepsilon$$

In other words,

$$\sup_{\|\psi\|=1} \left\| U|\psi\rangle - \tilde{U}|\psi\rangle \right\| < \varepsilon$$

# Quantum Gates

- SWAP Gate

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Hadamard Gate

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|\psi\rangle = a|0\rangle + b|1\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$$

# Quantum Gates

## Pauli Gates

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

## Phase Shift Gate

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{bmatrix}$$

- $H = \frac{X+Z}{\sqrt{2}}$
- $H^2 = X^2 = Y^2 = Z^2 = -\mathrm{i}XYZ = I$
- 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 $x \cdot y := \sum_{i=1}^{n} x_i y_i \mod 2$.

# Bloch Sphere

$$|\psi\rangle = a|0\rangle + b|1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \cos\frac{\theta}{2}|0\rangle + (\cos\phi + i\sin\phi)\sin\frac{\theta}{2}|1\rangle$$

$$x = \sin\theta\cos\phi$$
$$y = \sin\theta\sin\phi$$
$$z = \cos\theta$$

Starting from $|0\rangle$, any state can be reached by first rotating about $y$ by angle $\theta$ and then about $z$ by angle $\phi$.

The density matrix of $|\psi\rangle$ is

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \cos^2\frac{\theta}{2} & e^{-i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+\cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & 1-\cos\theta \end{bmatrix}$$
$$= \frac{1}{2}(I + xX + yY + zZ)$$

# CNOT Gate

## Definition

A quantum state $\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a *product state* if 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*.

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

In general, one can define controlled versions of any unitary gate $U$ as

$$CU = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

$\mathrm{CNOT}(|+\rangle \otimes |0\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}^{\mathsf{T}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ 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.

$$f : (c, p, q) \mapsto (c, c \cdot q + \overline{c} \cdot p, c \cdot p + \overline{c} \cdot q)$$

$$\text{CSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

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

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

# 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.
$f : (c_1, c_2, t) \mapsto \big(c_1, c_2, t \oplus c_1 \cdot c_2\big)$

$$\text{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$\neg \; c_1 = c_2 = 1 \implies x_3 = \bar{t}$

$\wedge \; t = 0 \implies x_3 = c_1 \cdot c_2$

# Universal Quantum Gates

- Fredkin gate $\mathrm{CSWAP}$ is universal for classical computation, but not universal for quantum computation.
- Toffoli gate $\mathrm{CCNOT}$ is universal for classical computation, but not universal for quantum computation.
- $\{\mathrm{CNOT}, H, R_{\frac{\pi}{4}}\}$ is universal for quantum computation.
- Deutsch gate $D(\theta)$ is universal for quantum computation.
- Toffoli gate and Hadamard gate $\{\mathrm{CCNOT}, H\}$ constitute a universal set of quantum gates.

## Deutsch Gate

$$D(\theta) : |a, b, c\rangle \mapsto \begin{cases} \mathrm{i}\cos\theta\,|a, b, c\rangle + \sin\theta\,|a, b, 1-c\rangle & \text{for } a = b = 1 \\ |a, b, c\rangle & \text{otherwise} \end{cases}$$

# Quantum Algorithms

I. 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. Transform $|\psi_i\rangle \to |\psi_f\rangle = \sum_{x\in\{0,1\}^n} b_x|x\rangle$ through a sequence of elementary quantum gates.

III. Extract information by quantum measurement of $|\psi_f\rangle$.

# The "balanced vs constant" Problem

- given a function $f : \{0,1\}^n \to \{0,1\}$ 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 $H^{\otimes n} \otimes H$

$$|\psi_1\rangle = \left(H^{\otimes n} \otimes H\right)|\psi_0\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\right) \otimes |-\rangle$$

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 $H^{\otimes n} \otimes I$

$$|\psi_3\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_2\rangle = \left(\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x\cdot y}|y\rangle\right) \otimes |-\rangle$$

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

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

# Quantum Teleportation

Alice and Bob share $|\Phi^+\rangle$. Alice wants to convey $|\psi\rangle = a|0\rangle + b|1\rangle$ to Bob.
The joint state is
$|\psi\rangle|\Phi^+\rangle = \frac{|\Phi^+\rangle\otimes(a|0\rangle+b|1\rangle)+|\Phi^-\rangle\otimes(a|0\rangle-b|1\rangle)+|\Psi^+\rangle\otimes(a|1\rangle+b|0\rangle)+|\Psi^-\rangle\otimes(a|1\rangle-b|0\rangle)}{2}$.

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.

$$\begin{array}{ccc} a|0\rangle + b|1\rangle & I & a|0\rangle + b|1\rangle \\ a|0\rangle - b|1\rangle & Z & a|0\rangle + b|1\rangle \\ a|1\rangle + b|0\rangle & X & a|0\rangle + b|1\rangle \\ a|1\rangle - b|0\rangle & ZX & a|0\rangle + b|1\rangle \end{array}$$

# 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 $\mathrm{CNOT}$ | After $H$ on $1^{\mathrm{st}}$ 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

$$K^{Q}_{\delta}(x) = \min_{p} \left\{ \ell(p) : \|x - M(p)\|_{\mathrm{tr}} < \delta \right\}$$

and the approximate-scheme quantum Kolmogorov complexity of $|x\rangle$ is

$$K^{Q}(x) = \min_{p} \left\{ \ell(p) : \forall k \in \mathbb{N} : \|x - M(p,k)\|_{\mathrm{tr}} < \frac{1}{k} \right\}$$

where $\|\cdot\|_{\mathrm{tr}}$ is the trace norm, i.e. $\|\rho - \sigma\|_{\mathrm{tr}} := \frac{1}{2}\operatorname{Tr}\left(\sqrt{(\rho-\sigma)^{\dagger}(\rho-\sigma)}\right)$.

# 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. $p \rightarrow q \iff M_p \subset M_q$.
- A trivial true statement $\top$ is represented by the entire Hilbert space $H$. $M_{\top} = H$.
- 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 $\mathbf{FdHilb}$, $U \subset V \implies V \cap (U \oplus W) = U \oplus (V \cap W)$.
- In $\mathbf{Hilb}$, $U \subset V \implies U = V \cap (U \oplus V^\perp)$.

# 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

History

Propositional Logic

Predicate Logic

Modal Logic

Equational Logic

Category Theory

Set Theory

Recursion Theory

Logic vs Game Theory

Quantum Computing

Answers to the Exercises

# Answers to the Exercises — Translation

1. $\forall x\big(\neg Sx \to \exists y(Eyx \land \neg Sy)\big)$
2. $\forall x(Mx \lor Wx \to Ax)$
3. $\forall x\big(\neg(Rx \land Bx) \to \neg Ex\big)$
4. $Hs \land Hp \land \forall x(Hx \to x = s \lor x = p)$
5. $\forall x(x \neq s \land x \neq p \to Hx)$
6. $\forall x\big(Bx \to \exists y\exists z(Gy \land Gz \land y \neq z \land Lxy \land Lxz)\big)$
7. $\neg\forall x(Jx \to Dx)$
8. $\forall x(Jx \to \neg Dx)$
9. $\neg\forall x\big(\mathrm{glitter}(x) \to \mathrm{gold}(x)\big)$
10. $\forall x\forall y(Fx \land Dy \land Oxy \to Hx)$
11. $\forall x\forall y(Fx \land Dy \land Oxy \to Bxy)$
12. $\forall x(Ex \to Dx2) \land \exists x(Ex \land Dx4) \land \exists x(Ex \land \neg Dx4)$

# Answers to the Exercises — Translation

1. $\forall x\big(Bx \to \neg\exists y(Ty \wedge Axy) \vee \forall y(Ty \to Axy)\big)$
2. $\forall x(\neg Hxx \to Hjx)$
3. $\neg\exists x\forall y(Sxy \leftrightarrow \neg Syy)$
4. $\exists x\exists y\exists z(Mxa \wedge Myb \wedge Mzx \wedge Mzy) \wedge \forall u\forall v\forall x\forall y(Mua \wedge Mvb \wedge Mxu \wedge Myv \to x = y)$ $\qquad m(m(a)) = m(m(b))$
5. $\forall x\exists y\exists z(Gy \wedge Gz \wedge y \neq z \wedge Lxy \wedge Lxz \to x = t)$
6. $\exists x\big(Sx \wedge \forall y(Sy \to y = x)\big)$
7. $\forall x\big(L(x, f(w(s))) \to x = m(w(s))\big)$
8. $\forall x(Dx \to Ax) \to \forall x\big(\exists y(Dy \wedge Hxy) \to \exists y(Ay \wedge Hxy)\big)$
9. $\exists x\big(Gx \wedge Lxb \wedge \forall y(Gy \wedge Lyb \to y = x) \wedge \exists y(y \neq x \wedge Sy)\big)$
10. $\exists x(Gx \wedge Lxm \wedge \forall y(Gy \wedge Lym \to y = x) \wedge Lmx \wedge \forall y(Lmy \to y = x))$
11. $\exists x(Lxa \wedge \forall y(Lya \to y = x) \wedge \exists y(Lay \wedge \forall z(Laz \to z = y) \wedge y = x))$
12. $\exists x\Big(Ex \wedge \forall z(Ez \to Tzx) \wedge \exists y\big(Ey \wedge \forall z(Ez \to Tyz) \wedge Lxy\big)\Big)$

1. $\neg\exists x\forall y(Txy \leftrightarrow \neg\exists z(Tyz \wedge Tzy))$
2. $\forall x(Dx \rightarrow Ax) \rightarrow \forall x\big(\exists y(Dx \wedge Hxy) \rightarrow \exists y(Ay \wedge Hxy)\big)$
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. $\neg\exists x\exists y(Gx \wedge Sy \wedge Lxy), Gc \wedge \forall x(Lxc \rightarrow Lcx), Lhc \vdash \neg Sh$
5. $\exists x\forall y\big((Ky \leftrightarrow y = x) \wedge Bx\big), \forall x(Bx \rightarrow Sx) \vdash \forall x(Kx \rightarrow Sx)$
6. $\forall x(Px \rightarrow x = r), Pw \wedge Sw \vdash Sr$
7. $\forall xFxd, \forall x(Fdx \rightarrow x = i) \vdash i = d$
8. $\forall x\forall y\forall z(Lyz \rightarrow Lxy), Lrj \vdash Liu$
9. $\forall x\forall y\forall z(Lyz \rightarrow Lxy) \vdash \exists x\exists yLxy \rightarrow \forall x\forall yLxy$
10. $Pi, \forall x\forall y(Px \wedge Axy \rightarrow Py), \neg\exists x(Px \wedge \neg Ex), Ri, \forall x(Ex \wedge Rx \rightarrow \exists y(Gy \wedge Axy)), \forall x(Ex \rightarrow Cx) \vdash \exists x(Gx \wedge Cx)$
11. $\forall x(Px \rightarrow \exists y(Ly \wedge Axy)), \exists x(Sx \wedge \forall y(Axy \rightarrow Fy)), \neg\exists x(Fx \wedge Lx) \vdash \neg\forall x(Sx \rightarrow Px)$
12. $\forall x\forall y(Sxy \rightarrow \exists zIzxy), \forall x\forall y\forall z(Izxy \rightarrow Kzx \wedge Kzy), \forall xSxf \vdash \forall x\exists y(Iyxf \wedge Kyf)$
13. $\forall x(Sx \rightarrow Kx), \exists xSx, \forall x(Kx \rightarrow x = j) \vdash Sj$
14. $Aac \wedge Abc \wedge a \neq b \wedge \forall x(Axc \rightarrow x = a \vee x = b), \forall x(Axc \leftrightarrow Lxc) \vdash \exists x\exists y(Lxc \wedge Lyc \wedge x \neq y \wedge \forall z(Lzc \rightarrow z = x \vee z = y))$

# Thanks