Elementary Logic

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

November 4, 2019

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Contents

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Information Update

Figure: The information content of a formula φ is the set $\mathrm{Mod}(\varphi)$ of its models. An update with new information ψ reduces the current set of models $\mathrm{Mod}(\varphi)$ to the overlap of $\mathrm{Mod}(\varphi)$ and $\mathrm{Mod}(\psi)$.

Three Cards Problem

- Three cards ‘red’, ‘white’, ‘blue’ are given to three children: 1, 2, 3.
- The children can only see their own cards.
- 2 asks 1: “Do you have the blue card?”
- 1 answers: “No”.

Unfaithful Husband Puzzle

Problem (大女子主义村出轨问题)

1. 大女子主义村规定：每个发现其老公出轨的女子必须当天枪杀之！
2. 村里住着 100 对夫妇。
3. 男人全都出轨了。
4. 虽然每个女子都知道别人的老公是否出轨，但不知道自己老公是否出轨。村里生活宁静幸福。
5. 直到某日，女王来访，并提醒："村里有男人出轨了"。
6. 宁静幸福的生活还会一直持续下去吗？

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

Test

测试

从 $0 \sim 100$ 之间选一个数字。谁的数字最接近平均数的 $\frac{2}{3}$ 谁赢。

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。
- 你只有向其中一人提问一个“是/否”问题的机会。
- 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

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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. A. Hausman, H. Kahane, P. Tidman: Logic and Philosophy. — *B*
3. M. V. Lawson: A First Course in Logic. — *P*
4. P. Smith: An Introduction to Formal Logic. — *P*
5. *P. Smith: Teach Yourself Logic.* — *P*
6. H. de Swart: Philosophical and Mathematical Logic — *P*
7. T. Sider: Logic for Philosophy. — *P*
8. J. van Benthem: Logic in Action. — *P*
9. Open Logic Project. — *P*
10. **H. Enderton: A Mathematical Introduction to Logic.** — **L**
11. J. L. Bell, M. Machover: A Course in Mathematical Logic. — *L*
12. E. Mendelson: Introduction to Mathematical Logic. — *L*
13. G. S. Boolos, J. P. Burgess, R. C. Jeffrey: Computability and Logic. — *L*
14. H. Ebbinghaus, J. Flum, W. Thomas: Mathematical Logic. — *L*
15. A. Nerode, R. A. Shore: Logic for Applications. — *C*
16. J. H. Gallier: Logic for Computer Science. — *C*
17. Yu. I. Manin: A Course in Mathematical Logic for Mathematicians. — *M*
18. R. Smullyan / I. Chiswell & W. Hodges / P. G. Hinman / A. G. Hamilton / U. Schöning / W. Rautenberg / J. R. Shoenfield / S. M. Srivastava / S. Hedman / D. van Dalen / R. S. Wolf / M. Ben-Ari / R. Cori & D. Lascar

Advanced Readings

- Modal Logic
  - P. Blackburn, M. de Rijke, Y. Venema: Modal Logic
  - J. van Benthem: Modal Logic for Open Minds
- 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

Readings, Movies and More

- D. Hofstadter: Gödel, Escher, Bach
- Dangerous Knowledge
- The Imitation Game
- Philosophical Logic
- Philosophy of Logic
- Philosophy of Mathematics

libgen
sci-hub
XX-Net

Hofstadter's Law

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

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

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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。

Example

- 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

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

- 我认为性教育导致怀孕。
- 是的，正如驾驶教育导致交通事故。 ◎$\hat{o}$◎

Example

庄子《齐物论》

不知周之梦为蝴蝶与，蝴蝶之梦为周与？

庄子《秋水》

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。

身是菩提树，心如明镜台，时时勤拂拭，勿使惹尘埃。

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

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?

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。

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

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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。

Joint Method of Agreement and Difference

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

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

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

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

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Informal Fallacies

ⓘ 形式谬误
ⓘⓘ 非形式谬误
  ❶ 言辞谬误
  ❷ 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。

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

- 告子：性犹湍水也，决诸东方则东流，决诸西方则西流。人性之无分于善不善也，犹水之无分于东西也。
- 孟子：水信无分于东西，无分于上下乎？人性之善也，犹水之就下也。人无有不善，水无有不下。

孟子《生于忧患，死于安乐》

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

三秀才赶考，途遇算命先生，问几人中举？先生竖起一指。

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。**”

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。

原子没有知觉，所以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.

Newton's Apple

If an apple falls, does the moon also fall?

- What is "rest/motion"?
- What is "state of rest/motion"?
- What is "change/tends to change"?
- What is "body"?
- What is "force"?
- What is "definition"?

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

Einstein's Train Thought Experiment

- What is "simultaneity"?
- How to measure "simultaneity"?
- How to measure "time"?

Einstein's Elevator Thought Experiment

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

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 precisely and succinctly?

The glory of the human spirit!

What are the extent and limits of reason?

Contents

1. Introduction
   - Logic Puzzle
   - Textbook and Homework
   - Analogical Argument
   - Mill's Five Methods
   - Fallacy and Bullshit
   - Logic and other Disciplines
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Why Study Logic?

- 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 Mathematical Foundations.
  Logicism / Formalism / Intuitionism / Constructivism / Finitism / Structuralism / Homotopy Type Theory
- Logic vs Computer Science.

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

- ...

Logic vs CS

- Computer Architecture.
  Gates and digital circuit design $\approx$ Propositional Logic
- Programming Languages.
  Semantics of programming languages via methods of logic
  LISP $\approx$ λ-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
- 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
- Hardware and Software Verification.
  Extensive use of formal methods based on logic
  Temporal Logic, Dynamic Logic and Automata, Hoare Logic, Model Checking
- Agents.
  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
- Type Theory
- Lambda Calculus
- Categorical Logic
- 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

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Contents

1 Introduction

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

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Aristotle(384-322 BC) — Term Logic

- 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.
- Any person in the present day who wishes to learn logic will be wasting his time if he reads Aristotle.

— *Russell*

Sophistic vs Valid Argument

1. 没有东西存在；
2. 就算有东西存在，也无法认识它；
3. 就算能认识它，也无法与他人谈论它；
4. 就算能谈论它，也无法互相理解。

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

A: All S are P.

E: No S are P.

I: Some S are P.

O: Some S are not P.

Syllogism

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

- 大项：结论的谓项。
- 小项：结论的主项。
- 中项：第三个项。
- 大前提：含大项的前提。
- 小前提：含小项的前提。

- 4 格，$4^3 \times 4 = 256$ 式。
- 15 布尔有效式。
- 24 亚里士多德有效式。（存在预设）
- 如何断定三段论的有效性？
  1. Venn Diagrams
  2. Rules
  3. Boolean Algebra
  4. Axiomatization

Venn Diagram — Boolean Standpoint

$$\frac{\begin{array}{c}\text{No } P \text{ are } M \\ \text{Some } S \text{ are not } M\end{array}}{\text{Some } S \text{ are } P}$$

1. 在三个圆的图上标记三段论的三个项；
2. 把两个前提在图上表示出来，如果一个前提是全称、另一个是特称，先表示全称；
3. 如果特称前提没有明确表明把 × 画在哪一部分，就把它画在交叉线上；
4. 检查图示是否支持结论。

Venn Diagram — Aristotelean Standpoint

$$\frac{\begin{array}{c}\text{No } M \text{ are } P\\ \text{All } M \text{ are } S\end{array}}{\text{Some } S \text{ are not } P}$$

1. 如果一个含全称前提和特称结论的三段论形式不是布尔有效的，看看是否有一个圆其中除了一个区域外全是阴影，如果有，在那个区域画 ⊗ 。
2. 如果该三段论是条件有效的，检查 ⊗ 是否表示某个存在物，如果是，则该三段论是亚里士多德有效的。

三段论有效性的判定规则

S 周延

P 不周延	**A**: All S are P.	**E**: No S are P.
	I: Some S are P.	**O**: Some S are not P.

P 周延

S 不周延

1. 中项至少周延一次。
2. 结论中周延的项在前提中必周延。
3. 前提与结论中否定命题的数目必相同。
4. 特称结论需要特称前提。（存在谬误）

$\left.\begin{array}{l}1\\2\\3\end{array}\right\}$ *Aristotle*

$\left.\begin{array}{l}1\\2\\3\\4\end{array}\right\}$ *Boole*

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 own 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. *Universal Characteristic and Rational Calculus.*
   - i encyclopedia — arranged in a logical order according to a demonstrative method, beginning with definitions of all the simple and primitive terms (which form the alphabet of human thoughts).
   - ii a universal ideal language that is purged of ambiguity and vagueness. — *the language of creation, the language before the Tower of Babel, the language that God used in creating the universe, the language whose rules of composition directly expresses the structure of the universe, the language in which concepts are expressed in their direct, original format.*

$$\textit{sign} \rightleftarrows \textit{idea}$$

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

   - iii the arrangement of all true propositions in an axiomatic system.
   - iv decision procedure. A calculus of manipulating the knowledge in a computational fashion, so as to reveal its logical interrelations and consequences. — replace reasoning by computation.
   - v a proof that the rational calculus is consistent.
   - vi a procedure for the rapid enlargement of knowledge. — the art of invention. free mind from intuition.

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.*

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

$$P = |\langle \boldsymbol{q}_2, t_2 | \boldsymbol{q}_1, t_1 \rangle|^2 \quad \langle \boldsymbol{q}_2, t_2 | \boldsymbol{q}_1, t_1 \rangle = \int_{\boldsymbol{q}_1}^{\boldsymbol{q}_2} \varphi[\boldsymbol{q}] \mathcal{D}\boldsymbol{q}$$

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

- 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

1 Introduction

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

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

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)

Logicism Mathematics $\rightsquigarrow$ Logic.[2]

- 本书把算术规律归结为分析判断、从而是先验的。算术不过是逻辑的延伸。在科学中应用数学就是在观察事实中应用逻辑；计算就是推理。
- 如果哲学的任务是破除语词对人类精神的支配，揭开由于语言的表达方式而造成的概念关系的假象，把思想从日常语言的负担中解放出来，那么，我的概念文字将成为哲学家的有用工具。

[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]

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

Dem.

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

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

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

- 公理是初始概念的隐定义。
- 我们完全可以用桌子、椅子、啤酒瓶来代替点、线、面。
- 数学是根据某些简单规则使用毫无意义的符号在纸上进行的游戏，是制造快乐的游戏。
- 我们的内心响起了永恒的召唤：那里有一个问题，去找出它的答案！你可以通过纯粹理性找到它，因为，数学里没有不可知！
- 我们必须知道；我们必将知道！

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*

现在正在发生的一切——计算机接管世界、人类社会数字化、信息化，都是 20 世纪初希尔伯特提出的哲学问题的结果。

— *Gregory Chaitin*

It may well be doubted wheter human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve.

— *Edgar Allan Poe*

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.

Philosophy of Math: Logicism/Intuitionism/Formalism

Logicism	Intuitionism	Formalism
$\frac{Mathematics}{Logic}$	$\frac{\frac{Logic}{Mathematics}}{Mind}$	$\frac{Mathematics}{Game}$
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

Contents

1 Introduction

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

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

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.

[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

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Contents

1 Introduction

2 History

3 Propositional Logic
- What is Logic?
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

What is Logic?

- Arithmetic — the study of numbers.
- Geometry — the study of figures.
- Algebra — the study of mathematical symbols.
- Logic — the study of logical notions.
- Set Theory — the study of sets.

- 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 Programm

What is Geometry?

The study of *invariants* under *a group of transformations*.

Figure: Felix Klein

What is Geometry? — Klein's Erlangen Programm

	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?[7]

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

what follows from what

The art of thinking and reasoning in strict accordance with the limitations and incapacities of the human misunderstanding. $^{\circledcirc}\hat{o}^{\circledcirc}$

— *The Devil's Dictionary*

The study of invariants under all automorphisms (symmetries).

[7] Tarski: What are logical notions?

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

1. Introduction
2. History
3. Propositional Logic
   - What is Logic?
   - Syntax
   - Semantics
   - Connectives
   - Formal System
   - Meta-Theorems
   - Application
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Propositional Logic

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

Syntax

Language

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

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

Well-Formed Formula WFF

$$\varphi ::= p_i \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid (\varphi \leftrightarrow \varphi)$$

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

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)

$$\mathscr{E}_{\neg}(\varphi) := (\neg\varphi)$$
$$\mathscr{E}_{\wedge}(\varphi,\psi) := (\varphi \wedge \psi)$$
$$\mathscr{E}_{\vee}(\varphi,\psi) := (\varphi \vee \psi)$$
$$\mathscr{E}_{\rightarrow}(\varphi,\psi) := (\varphi \rightarrow \psi)$$
$$\mathscr{E}_{\leftrightarrow}(\varphi,\psi) := (\varphi \leftrightarrow \psi)$$

$$\boxed{\begin{aligned} \mathscr{E}_{\neg}(\varphi) &:= \neg\varphi \\ \mathscr{E}_{\wedge}(\varphi,\psi) &:= \wedge\varphi\psi \\ \mathscr{E}_{\vee}(\varphi,\psi) &:= \vee\varphi\psi \\ \mathscr{E}_{\rightarrow}(\varphi,\psi) &:= \rightarrow \varphi\psi \\ \mathscr{E}_{\leftrightarrow}(\varphi,\psi) &:= \leftrightarrow \varphi\psi \end{aligned}}$$

Well-Formed Formula

Definition (Construction Sequence)

A construction sequence $(\alpha_1, \ldots, \alpha_n)$ is a finite sequence of expressions s.t. for each $i \leq n$ we have at least one of

$$\alpha_i = p_i \quad \text{for some } i$$
$$\alpha_i = \mathscr{E}_\neg(\alpha_j) \quad \text{for some } j$$
$$\alpha_i = \mathscr{E}_\star(\alpha_j, \alpha_k) \quad \text{for some } j < i, k < i$$
$$\text{where } \star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}.$$

Definition (Well-Formed Formula)

A formula φ is a well-formed formula (wff) iff there is some construction sequence $(\alpha_1, \ldots, \alpha_n)$ and $\alpha_n = \varphi$.

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

$$C_0 := B$$

$$C_{n+1} := C_n \cup \bigcup_{f \in \mathcal{F}} \{f(\boldsymbol{x}) : \boldsymbol{x} \in C_n\}$$

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

$$deg(\boldsymbol{x}) := \mu n\, [\boldsymbol{x} \in C_n]$$

Top Down

- A set S is closed under a function f if for all $\boldsymbol{x}$: $\boldsymbol{x} \in S \rightarrow f(\boldsymbol{x}) \in S$.
- 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

10 块钱最多可以喝几瓶啤酒？$^{\circledcirc}\hat{o}^{\circledcirc}$

- 2 块钱买 1 瓶啤酒。
- 2 个空瓶换 1 瓶啤酒。
- 4 个瓶盖换 1 瓶啤酒。

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.
$(C_* \subset C^*)$: for any $(x_1, \ldots, x_n)$, if $x_j \in C^*$ for all $j < i$, then $x_i \in C^*$. So by induction on i, it follows that, $x_i \in C^*$ for all $i \leq n$.

Induction Principle for WFF

Theorem (归纳原理)

令 Ψ 为一个关于合式公式的性质。假设

- Ψ 对所有的命题符号成立；并且
- Ψ 对公式构造运算封闭。

那么，Ψ 对所有的合式公式都成立。

Proof.

$$\mathrm{WFF}_* = \mathrm{WFF}^* \subset \Psi$$

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

$$\Psi(k) := \Psi(\mathrm{WFF}_k)$$

Induction vs Recursion

$\psi(n) \equiv$ "n rings needs $2^n - 1$ moves."

1. Never leave milk on any day without leaving milk the next day as well.
2. Leave milk today.

Leave milk today and read this note again tomorrow.

Subformula

Definition (Subformula)

The set $\mathrm{Sub}(\varphi)$ of subformulas of a wff φ is the smallest set Γ that satisfies

1. $\varphi \in \Gamma$
2. $\neg\psi \in \Gamma \implies \psi \in \Gamma$
3. $\psi \to \chi \in \Gamma \implies \psi, \chi \in \Gamma$

$$\mathrm{Sub}(\varphi) := \begin{cases} \varphi & \text{if } \varphi = p \\ \{\varphi\} \cup \mathrm{Sub}(\psi) & \text{if } \varphi = \neg\psi \\ \{\varphi\} \cup \mathrm{Sub}(\psi) \cup \mathrm{Sub}(\chi) & \text{if } \varphi = \psi \to \chi \end{cases}$$

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: obviously.

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 $\varphi = (\alpha \wedge \beta)$. The proper initial segments of $(\alpha \wedge \beta)$ are the following:

1. $($
2. $(\alpha_0$ [inductive hypothesis]
3. $(\alpha$ [balanced-parentheses]
4. $(\alpha\wedge$ [balanced-parentheses]
5. $(\alpha \wedge \beta_0$ [inductive hypothesis]
6. $(\alpha \wedge \beta$ [balanced-parentheses]

Unique Readability

Theorem (Unique Readability Theorem)

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

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

Proof.

To show $\mathscr{E}_\wedge$ is ono-to-one.

$$(\varphi \wedge \psi) = (\alpha \wedge \beta)$$
$$\Downarrow$$
$$\varphi \wedge \psi) = \alpha \wedge \beta)$$
$$\Downarrow$$
$$\varphi = \alpha \qquad [Lemma]$$

then it follows $\psi = \beta$.
Similarly, we can prove

$$(\varphi \wedge \psi) \neq (\alpha \rightarrow \beta)$$

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

1 Introduction

2 History

3 Propositional Logic
- What is Logic?
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Assignment

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

$$v\colon \mathscr{P} \to \{0,1\}$$

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

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

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 $n = arity(f)$. Then for every function $h\colon B \to V$, there exists a unique function $\overline{h}\colon C \to V$ s.t.

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

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

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

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

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

Truth Table

p	$\neg p$
0	1
1	0

p	q	$p \to q$	$p \wedge q$	$p \vee q$	$p \leftrightarrow q$
0	0	1	0	0	1
0	1	1	0	1	0
1	0	0	0	1	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

翻哪几张卡才能验证“如果一面是偶数，另一面肯定是红色”？

未满 18 岁禁止饮酒！

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.

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

p	q	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

What is Propositional Logic?

The study of invariants under all permutations in truth space $\{0,1\}^*$.

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, 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. $p \vee q \to r \vDash (p \to r) \wedge (q \to r)$
12. $p \wedge q \to r \vDash (p \to r) \vee (q \to r)$

Example

$^{\circledcirc}\hat{o}^{\circledcirc}$

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.

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

- programmer.

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

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

1. $\Gamma, \varphi \vDash \psi \iff \Gamma \vDash \varphi \to \psi$
2. $\varphi \mathrel{\vDash\!\dashv} \psi \iff \vDash \varphi \leftrightarrow \psi$
3. $\varphi \vee \psi, \neg\varphi \vee \chi \vDash \psi \vee \chi$

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

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

$$\frac{\begin{array}{c} \text{美女是老王或大黄杀的} \\ \text{老王是凶手} \end{array}}{\text{大黄是无辜的}}$$

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

— *Socrates*

Example

好货不贱，贱货不好。

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。

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。
- 你只有向其中一人提问一个“是/否”问题的机会。
- 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
0	0	1	0
0	1	0	1
1	0	0	0
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 $N := \prod_{i=1}^{k} p_i$.

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

Semantic Equivalence

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

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

$$\left.\begin{array}{l}\varphi \vDash\!\!\!\!\dashv \varphi' \\ \psi \vDash\!\!\!\!\dashv \psi'\end{array}\right\} \implies \varphi \star \psi \vDash\!\!\!\!\dashv \varphi' \star \psi'$$

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

- Equivalence relation + Compatible with Operators = Congruence relation

Substitution

$$p[\alpha_1/p_1, \ldots, \alpha_n/p_n] := \begin{cases} \alpha_i & \text{if } p = p_i \text{ for some } 1 \leq i \leq n \\ p & \text{otherwise} \end{cases}$$

$$(\neg\varphi)[\alpha_1/p_1, \ldots, \alpha_n/p_n] := \neg\varphi[\alpha_1/p_1, \ldots, \alpha_n/p_n]$$

$$(\varphi \to \psi)[\alpha_1/p_1, \ldots, \alpha_n/p_n] := \varphi[\alpha_1/p_1, \ldots, \alpha_n/p_n] \to \psi[\alpha_1/p_1, \ldots, \alpha_n/p_n]$$

Theorem

Consider a wff φ and a sequence $\alpha_1, \ldots, \alpha_n$ of wffs.

1. *Let ν be a truth assignment for the set of all propositional symbols. Define ρ to be the truth assignment for which $\rho(p_i) = \overline{\nu}(\alpha_i)$. Then $\overline{\rho}(\varphi) = \overline{\nu}(\varphi[\alpha_1/p_1, \ldots, \alpha_n/p_n])$.*
2. $\vDash \varphi \implies \vDash \varphi[\alpha_1/p_1, \ldots, \alpha_n/p_n]$

Example

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

Duality

Theorem

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

Proof.

Prove by induction.

- $\varphi = p_i$
- $\varphi = \neg\alpha$
- $\varphi = \alpha \wedge \beta$
- $\varphi = \alpha \vee \beta$

Contents

1 Introduction

2 History

3 Propositional Logic
- What is Logic?
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Connectives

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

Example (Exclusive Disjunction)

$$\nu(p \dot{\vee} q) = |\nu(p) - \nu(q)|$$
$$\Downarrow$$
$$\begin{aligned} p \dot{\vee} q &\vDash\!\!\!\dashv (p \wedge \neg q) \vee (\neg p \wedge q) \\ &\vDash\!\!\!\dashv (p \vee q) \wedge \neg(p \wedge q) \\ &\vDash\!\!\!\dashv \neg(p \leftrightarrow q) \end{aligned}$$

p	q	$p \dot{\vee} q$
0	0	0
0	1	1
1	0	1
1	1	0

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

Example

Example

Let $\#$ be a three-place proposition connective.
The interpretation of $\#$ is given by

$$\nu(\#(p,q,r)) = \left\lfloor \frac{\nu(p)+\nu(q)+\nu(r)}{2} \right\rfloor$$

then

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

Boolean Function

A n-place Boolean function is a function $B\colon \{0,1\}^n \to \{0,1\}$.

p	$\neg p$
0	1
1	0

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

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

Definition

Suppose φ is a wff whose propositional symbols are $p_1, \ldots, p_n$. A Boolean function B realized by φ is

$$B_\varphi(\nu(p_1), \ldots, \nu(p_n)) = \overline{\nu}(\varphi)$$

Theorem (Post1921)

Every Boolean function can be realized 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: $B(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in \{0,1\}^n$.
Let $\varphi = p \wedge \neg p$.
Case2:

$$\varphi = \bigvee_{\boldsymbol{x}:B(\boldsymbol{x})=1} \bigwedge_{i=1}^{n} p_i^{x_i}$$

Case1: $B(\boldsymbol{x}) = 1$ for all $\boldsymbol{x} \in \{0,1\}^n$.
Let $\psi = p \vee \neg p$.
Case2:

$$\psi = \bigwedge_{\boldsymbol{x}:B(\boldsymbol{x})=0} \bigvee_{i=1}^{n} p_i^{1-x_i}$$

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):

$$\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} \pm p_{ij}$$

CNF Transformation

$$
\begin{aligned}
\varphi \leftrightarrow \psi &\implies (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi) \\
\varphi \rightarrow \psi &\implies \neg\varphi \vee \psi \\
\neg(\varphi \wedge \psi) &\implies \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) &\implies \neg\varphi \wedge \neg\psi \\
\neg\neg\varphi &\implies \varphi \\
(\varphi_1 \wedge \cdots \wedge \varphi_n) \vee \psi &\implies (\varphi_1 \vee \psi) \wedge \cdots \wedge (\varphi_n \vee \psi)
\end{aligned}
$$

Adequate Sets of Connectives

Definition

An adequate set of connectives is a set s.t. 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

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

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

Contents

1 Introduction

2 History

3 Propositional Logic
- What is Logic?
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

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. $\varphi \to \psi \to \varphi$
2. $(\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to \varphi \to \chi$
3. $(\neg\varphi \to \neg\psi) \to (\neg\varphi \to \psi) \to \varphi$

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\text{MP}]$$

Deduction / Proof

这个句子永远不能被证明

什么是“证明”？

Definition (Deduction)

A deduction from Γ is a sequence of wff $(\varphi_1, \ldots, \varphi_n)$ s.t. for $k \leq n$, either

1. φ_k is an axiom, or
2. $\varphi_k \in \Gamma$, or
3. for some $i < k$ and $j < k$, $\varphi_i = \varphi_j \to \varphi_k$.

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

房子着火了，数学家的妻子拿起灭火器把火灭了；
煤气泄漏了，数学家把房子点了。

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◎

如果这句话是真的那么上帝存在。

If this sentence is true, then I am God.

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

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。

这句话是假的并且上帝不存在。

Curry's Paradox — Kiss-Kiss ♡◎♡

Smullyan 实力撩妹 ♡◎♡

1. Smullyan: "我说一句话，如果它是真的，可以给我你的签名吗？"
2. 美女："可以。"
3. Smullyan: "不过如果我说的不是真的，那就不要给我签名了。"
4. 美女："好的。"
5. 然后 Smullyan 说了一句话。
6. 美女想了一下，发现她必须给他一个吻！

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

Hi 美女，问你个问题呗 ~v~

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 — “搬运工”

Theorem (Deduction Theorem)

$$\Gamma, \varphi \vdash \psi \iff \Gamma \vdash \varphi \to \psi$$

Proof.

Prove by induction on the length of the deduction sequence $(\alpha_1, \ldots, \alpha_n)$ of ψ from $\Gamma \cup \{\varphi\}$.

Base step $n = 1$:

case1. ψ is an axiom. (use Axiom1.)

case2. $\psi \in \Gamma$.

case3. $\psi = \varphi$.

Inductive step $n > 1$:

case1. ψ is either an axiom, or $\psi \in \Gamma$, or $\psi = \varphi$.

case2. $\alpha_i = \alpha_j \to \psi$

$\Gamma, \varphi \vdash \alpha_j \implies \Gamma \vdash \varphi \to \alpha_j$

$\Gamma, \varphi \vdash \alpha_j \to \psi \implies \Gamma \vdash \varphi \to \alpha_j \to \psi$

Equivalent Replacement

Theorem

Suppose $\psi \in \mathrm{Sub}(\varphi)$, and φ^* arises from the wff φ by replacing one or more occurrences of ψ in φ by χ. Then

$$\psi \leftrightarrow \chi \vdash \varphi \leftrightarrow \varphi^*$$

Proof.

Prove by induction on the number of connective of φ.

Example

$^{\circledcirc}\hat{o}^{\circledcirc}$

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. $\varphi \to \psi \to \varphi$
2. $(\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to \varphi \to \chi$
3. $\varphi \wedge \psi \to \varphi$
4. $\varphi \wedge \psi \to \psi$
5. $(\varphi \to \psi) \to (\varphi \to \chi) \to \varphi \to \psi \wedge \chi$
6. $\varphi \to \varphi \vee \psi$
7. $\psi \to \varphi \vee \psi$
8. $(\varphi \to \chi) \to (\psi \to \chi) \to \varphi \vee \psi \to \chi$
9. $(\varphi \to \neg\psi) \to (\varphi \to \psi) \to \neg\varphi$
10. $\neg\varphi \to \varphi \to \psi$
11. $\neg\neg\varphi \to \varphi$

Reference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\text{MP}]$$

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

$$(\varphi \star \psi)' := \neg\neg(\varphi' \star \psi')$$

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

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

$$\Gamma \vdash_{\boldsymbol{C}} \varphi \iff \Gamma' \vdash_{\boldsymbol{I}} \varphi'$$

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

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

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

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

✓

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)

$\varphi_1, \ldots, \varphi_n \vdash \psi$ iff there exists a *closed tree* from $\{\varphi_1, \ldots, \varphi_n, \neg\psi\}$.

Theorem (Soundness & Completeness Theorem)

$$\varphi_1, \ldots, \varphi_n \vdash \psi \iff \varphi_1, \ldots, \varphi_n \vDash \psi$$

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

Examples — Tree Method

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

$p \to q$ ✓

$\neg q \vee r$ ✓

$\neg(\neg p \vee r)$ ✓

$\neg\neg p$

$\neg r$

- $\neg p$ ✗
- q
  - $\neg q$ ✗
  - r ✗

An open branch corresponds to a valuation

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

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

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

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

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

1 Introduction

2 History

3 Propositional Logic
- What is Logic?
- Syntax
- Semantics
- Connectives
- Formal System
- Meta-Theorems
- Application

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Independence

Definition (Independence)

An axiom φ in Γ is independent if $\Gamma \setminus \{\varphi\} \nvdash \varphi$.

找一个这个公理没有的性质，证明能从其他公理推出来的命题都有这个性质。 比如对某个特殊语义 $\Vdash$:

- for all ψ, $\Gamma \setminus \{\varphi\} \vdash \psi \implies \Vdash \psi$
- $\nVdash \varphi$

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

Independence

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

Theorem

Peirce's law is independent of Axiom1 and Axiom2.

$\rightarrow$	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 $\nu(p) = 2$ and $\nu(q) = 3$, then $\nu(((p \rightarrow q) \rightarrow p) \rightarrow p) = 2$.

Model & Semantic Consequence

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

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

Consistency & Satisfiability

- Γ is consistent if $\Gamma \nvdash \bot$.
- Γ is Post-consistent if there is some wff φ: $\Gamma \nvdash \varphi$.

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

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

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

Soundness Theorem

Theorem (Soundness Theorem)

$$\Gamma \vdash \varphi \implies \Gamma \vDash \varphi$$

Proof.

Prove by induction on the length of the deduction sequence.
Case1: φ is an axiom. (truth table)
Case2: $\varphi \in \Gamma$
Case3:

$$\left.\begin{array}{l} \Gamma \vDash \alpha_j \\ \Gamma \vDash \alpha_j \to \varphi \end{array}\right\} \implies \Gamma \vDash \varphi$$

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

Corollary

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

Proof.

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

Applications of Compactness ⊙$\underline{\Delta}$⊙

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

Proof.

Take $V \times \{1, \ldots, n\}$ as the set of atoms.
$\Gamma := \{p(v,1) \vee \cdots \vee p(v,n) : v \in V\} \cup \{\neg(p(v,i) \wedge p(v,j)) : v \in V, 1 \leq i < j \leq n\} \cup \{\neg(p(v,i) \wedge p(w,i)) : (v,w) \in E, 1 \leq i \leq n\}$

Proof of Compactness Theorem

Proof.

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

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

$$\Delta_0 := \Gamma$$

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

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

part2. Define a truth assignment that satisfies Γ.

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

"Compactness Theorem"

Theorem ("Compactness Theorem")

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

Proof.

Suppose $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$.
Then there is a deduction sequence $(\alpha_1, \ldots, \alpha_n)$ of φ from Γ, and a deduction sequence $(\beta_1, \ldots, \beta_m)$ of $\neg\varphi$ from Γ.
Let $\Sigma_0 := \{\alpha_i \in \Gamma : 1 \leq i \leq n\}$ and $\Sigma_1 := \{\beta_i \in \Gamma : 1 \leq i \leq m\}$.
The finite set $\Sigma := \Sigma_0 \cup \Sigma_1$ is inconsistent.

Weak Completeness Theorem

Lemma

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

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

then $p_1^\nu, \ldots, p_n^\nu \vdash \varphi^\nu$.

Weak Completeness Theorem $\vDash \varphi \implies \vdash \varphi$

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

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

Completeness Theorem

$$\vDash \varphi \iff \vdash \varphi$$

$$+$$

Compactness

$$\Downarrow$$

$$\Gamma \vDash \varphi \iff \Gamma \vdash \varphi$$

Completeness Theorem — Post1921

Theorem (Completeness Theorem)

$$\Gamma \vDash \varphi \implies \Gamma \vdash \varphi$$

Corollary

Any consistent set of wffs is satisfiable.

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

Corollary (Compactness Theorem)

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

Proof of Completeness Theorem

Proof.

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

$$\Delta_0 := \Gamma$$

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

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

step2. Define a truth assignment that satisfies Γ.

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

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 $\Gamma \cup \{\varphi\}$ of wffs, will decide whether or not $\Gamma \vDash \varphi$.

Theorem

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

Post 1897-1954

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

Theory & Axiomatization

什么是“理论”？

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

Model Checking & Satisfiability Checking & Validity Checking[8]

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

Figure: *Hamiltonian Circle(NP)*

Figure: *Eulerian Circle(P)*

Figure: *Graph Coloring(NPC)*

[8] Aaronson: Why Philosophers Should Care About Computational Complexity.

Contents

1. Introduction
2. History
3. Propositional Logic
   - What is Logic?
   - Syntax
   - Semantics
   - Connectives
   - Formal System
   - Meta-Theorems
   - Application
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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 3×3 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

$$(A \wedge B) \vee ((C \vee A) \wedge \neg B) \mathrel{\vDash\!\dashv} A \vee (C \wedge \neg B)$$

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	$p \dot{\vee} q$
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

c	x_1	x_2	c'	y_1	y_2
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

Figure: transmit the first bit unchanged and swap the last two bits iff the first bit is 1.
$f\colon (c, x_1, x_2) \mapsto (c, \bar{c}x_1 + cx_2, cx_1 + \bar{c}x_2)$

- If $x_2 = 0$, then $y_2 = cx_1$. $\wedge$
- If $x_2 = 1$, then $y_1 = c + x_1$. $\vee$
- If $x_1 = 0$ and $x_2 = 1$, then $y_2 = \bar{c}$. $\neg$

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

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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

$^{\circledcirc}\hat{o}^{\circledcirc}$

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.

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

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

$^{\circledcirc}\hat{o}^{\circledcirc}$

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

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

打破学科鄙视链

Figure: 还原论 ≠ 演生论

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Syntax

Language

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

where

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

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

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

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 $\mathcal{T}$

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

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

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

Well-Formed Formula WFF

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

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

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

Syntax

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

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

Freedom & Bondage

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

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

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

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

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

$$\int_0^t \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{x^2}{2}} \mathrm{d}x$$

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

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

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)

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

Freedom & Bondage

Definition (Bound Variable)

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

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

Example: $c = d$ is clopen.

Translation

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

1. $\boldsymbol{A}$: $\forall x(Sx \to Px)$
2. $\boldsymbol{E}$: $\forall x(Sx \to \neg Px)$
3. $\boldsymbol{I}$: $\exists x(Sx \wedge Px)$
4. $\boldsymbol{O}$: $\exists x(Sx \wedge \neg Px)$
5. Every boy loves some girl. $\forall x\big(Bx \to \exists y(Gy \wedge Lxy)\big)$
6. 有爹就有娘。$\forall x(\exists y Fyx \to \exists y Myx)$
7. 外婆是妈妈的妈妈。
   $\forall xy\big(Gxy \leftrightarrow \exists z(Mxz \wedge Mzy)\big)$
   $\forall xy\big(x = Gy \leftrightarrow \exists z(x = Mz \wedge z = My)\big)$
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. $Cogito(i) \to \exists x(x = i)$ — *Descartes*
2. $\exists x(x = i) \vee \neg\exists x(x = i)$ — *Shakespeare*
3. $\forall x\big(Month(x) \to Crueler(april, x)\big)$ — *Eliot*
4. $\forall x(\neg Weep(x) \to \neg See(x))$ — *Hugo*
5. $\forall x\big(Time(x) \to Better(t, x)\big) \wedge \forall x\big(Time(x) \to Better(x, t)\big)$ — *Dickens*
6. $\exists p\Big(Child(p) \wedge \neg Grow(p) \wedge \forall x\big(Child(x) \wedge x \neq p \to Grow(x)\big)\Big)$ — *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. $\exists t\forall x Fool(x, t) \wedge \exists x\forall t Fool(x, t) \wedge \neg\forall x\forall t Fool(x, t)$ — *Lincoln*
9. $\forall x\big(Problem(x) \wedge Philo(x) \wedge Serious(x) \leftrightarrow x = suicide\big)$ — *Camus*
10. $\forall x\big(Feather(x) \wedge Perch(x, soul) \leftrightarrow x = hope\big)$ — *Dickinson*
11. $\forall x\Big(Enter(x) \to \forall y\big(Hope(y) \to Abandon(x, y)\big)\Big)$ — *Dante*
12. $\exists x\forall y\big(For(y, x) \wedge For(x, y)\big)$? — *Dumas*
13. $\exists x\big(Fear(we, x) \leftrightarrow x = Fear\big)$? — *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. $mother(x, y)$
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

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

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

- 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.

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

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)

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

$$(\forall y\psi)[t_1/x_1, \ldots, t_n/x_n] := \begin{cases} \forall y\psi[t_1/x_1, \ldots, t_n/x_n] & \text{if } y \notin \{x_1, \ldots, x_n\} \\ \forall y\psi[t_1/x_1, \ldots, t_{i-1}/x_{i-1}, t_{i+1}/x_{i+1}, \ldots, t_n/x_n] & \text{if } y = x_i \end{cases}$$

Definition (Substitutable)

t is substitutable for x in φ:

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

$\varphi = \forall y\psi$ iff either

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

避免替换后 t 中的变元被 φ 中的量词约束。

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

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"

什么是"真"？— Are all truths knowable?

1. *formally correct* $\forall x\big(T(x) \leftrightarrow \varphi(x)\big)$
2. *materially adequate* $\varphi(s) \leftrightarrow p$
   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 $\mathcal{A} := (A, I)$, where A is a non-empty set, and I is a mapping which

- assigns to each function symbol f^k a k-ary function $I(f^k)\colon A^k \to A$,
- assigns to each predicate symbol P^k a k-ary relation $I(P^k) \subset A^k$.

We write $\mathcal{A} = \left(A, c^{\mathcal{A}}, f^{\mathcal{A}}, P^{\mathcal{A}}\right)$ 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
疏肝理气
除湿解毒
木
肝
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
金生水
水生木
肾
肺
滋阴壮阳
强筋壮骨
水
金
祛风散寒
止嗽润肺

fire
wood
earth
water
metal

Interpretation

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

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

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

Tarski's Definition of Truth

Definition ($\mathcal{A}, \nu \vDash \varphi$)

- $\mathcal{A}, \nu \vDash t_1 = t_2$ if $\overline{\nu}(t_1) = \overline{\nu}(t_2)$
- $\mathcal{A}, \nu \vDash P(t_1, \ldots, t_n)$ if $(\overline{\nu}(t_1), \ldots, \overline{\nu}(t_n)) \in P^{\mathcal{A}}$
- $\mathcal{A}, \nu \vDash \neg\varphi$ if $\mathcal{A}, \nu \nvDash \varphi$
- $\mathcal{A}, \nu \vDash \varphi \to \psi$ if $\mathcal{A}, \nu \nvDash \varphi$ or $\mathcal{A}, \nu \vDash \psi$
- $\mathcal{A}, \nu \vDash \forall x\varphi$ if for every $a \in A$: $\mathcal{A}, \nu(a/x) \vDash \varphi$
  where
  $$\nu(a/x)(y) := \begin{cases} \nu(y) & \text{if } y \neq x \\ a & \text{otherwise} \end{cases}$$

  or, $\mathcal{A}, \nu \vDash \forall x\varphi$ if for all $\nu' \sim_x \nu$: $\mathcal{A}, \nu' \vDash \varphi$.
  where $\nu' \sim_x \nu$ if for all $y \neq x$: $\nu'(y) = \nu(y)$.

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 formulas to variable assignments $P\big(A^{\mathscr{V}}\big)$.

- $h(t_1 = t_2) = \{v \colon \overline{v}(t_1) = \overline{v}(t_2)\}$
- $h(P(t_1, \ldots, t_k)) = \big\{v \colon (\overline{v}(t_1), \ldots, \overline{v}(t_n)) \in P^{\mathcal{A}}\big\}$

We extend h to $\overline{h} \colon \mathrm{WFF} \to P\big(A^{\mathscr{V}}\big)$ by recursion as follows:

1. $\overline{h}(\varphi) = h(\varphi)$ for atomic φ
2. $\overline{h}(\neg\varphi) = A^{\mathscr{V}} \setminus \overline{h}(\varphi)$
3. $\overline{h}(\varphi \to \psi) = \big(A^{\mathscr{V}} \setminus \overline{h}(\varphi)\big) \cup \overline{h}(\psi)$
4. $\overline{h}(\forall x\varphi) = \bigcap\limits_{a \in A} \big\{v \colon v(a/x) \in \overline{h}(\varphi)\big\}$

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

Tarski's Definition of Truth

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

Example

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

- $c^{\mathcal{A}}$: green point
- $P^{\mathcal{A}}$: blue circles
- $R^{\mathcal{A}}$: arrows

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

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

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

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

Relevance Lemma

Lemma (Relevance Lemma)

Assume $\nu_1, \nu_2 \colon \mathscr{V} \to A$*, and for any* $x \in \mathrm{Fv}(\varphi)\colon \nu_1(x) = \nu_2(x)$*. Then*

$$\mathcal{A}, \nu_1 \vDash \varphi \iff \mathcal{A}, \nu_2 \vDash \varphi$$

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

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

$$\mathscr{L}_A := \mathscr{L} \cup \mathscr{C}_A \quad \text{where} \quad \mathscr{C}_A := \{c_a : a \in A\}$$

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

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

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

Equivalent Replacement

Lemma

Suppose $\psi \in \mathrm{Sub}(\varphi)$, *and* φ^* *arises from* φ *by replacing zero or more occurrences of* ψ *by* χ. *Then*

$$\vDash \psi \leftrightarrow \chi \implies \vDash \varphi \leftrightarrow \varphi^*$$

Alphabetic Variant

Definition (Alphabetic Variant)

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

Theorem

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

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

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

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

Equality and Equivalence

Lemma

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

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

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

Lemma

Suppose $\mathrm{Fv}(\psi) \cup \mathrm{Fv}(\chi) \subset \{x_1, \ldots, x_n\}$, *and* φ^* *arises from the wff* φ *by replacing one occurrence of* ψ *in* φ *by* χ. *Then*

$$\vDash \forall x_1 \ldots x_n (\psi \leftrightarrow \chi) \to (\varphi \leftrightarrow \varphi^*)$$

$$\mathcal{A} \vDash \psi \leftrightarrow \chi \implies \mathcal{A} \vDash \varphi \leftrightarrow \varphi^*$$

Remark

- $\vDash \forall x\big(Px \leftrightarrow Qx\big) \to \big(\forall x Px \leftrightarrow \forall x Qx\big)$
  $\nvDash \big(Px \leftrightarrow Qx\big) \to \big(\forall x Px \leftrightarrow \forall x Qx\big)$
- $\mathcal{A}, v \vDash t = s \;\not\Longrightarrow\; \mathcal{A}, v \vDash \varphi \leftrightarrow \varphi^*$
- $\mathcal{A}, v \vDash \psi \leftrightarrow \chi \;\not\Longrightarrow\; \mathcal{A}, v \vDash \varphi \leftrightarrow \varphi^*$

$$\psi = Px, \quad \chi = Py, \quad \varphi = \forall x Px, \quad \varphi^* = \forall x Py$$

Valid Formulas — Example

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

$\neg\forall x\varphi \leftrightarrow \exists x\neg\varphi$

$\forall x(\varphi \wedge \psi) \leftrightarrow \forall x\varphi \wedge \forall x\psi$

$\exists x(\varphi \vee \psi) \leftrightarrow \exists x\varphi \vee \exists x\psi$

$\forall x(\varphi \to \psi) \to \forall x\varphi \to \forall x\psi$

$\forall xy\varphi \leftrightarrow \forall yx\varphi$

$\exists x\forall y\varphi \to \forall y\exists x\varphi$

$\forall x(\varphi \leftrightarrow \psi) \to (\forall x\varphi \leftrightarrow \forall x\psi)$

$(\forall x\varphi \to \exists x\psi) \leftrightarrow \exists x(\varphi \to \psi)$

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

$\neg\exists x\varphi \leftrightarrow \forall x\neg\varphi$

$\forall x\varphi \vee \forall x\psi \to \forall x(\varphi \vee \psi)$

$\exists x(\varphi \wedge \psi) \to \exists x\varphi \wedge \exists x\psi$

$\forall x(\varphi \to \psi) \to \exists x\varphi \to \exists x\psi$

$\exists xy\varphi \leftrightarrow \exists yx\varphi$

Valid Formulas — Example

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

$$\varphi \leftrightarrow \forall x \varphi$$
$$\forall x(\varphi \vee \psi) \leftrightarrow \varphi \vee \forall x \psi$$
$$\forall x(\varphi \wedge \psi) \leftrightarrow \varphi \wedge \forall x \psi$$
$$\forall x(\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \forall x \psi)$$
$$\forall x(\psi \rightarrow \varphi) \leftrightarrow (\exists x \psi \rightarrow \varphi)$$

$$\varphi \leftrightarrow \exists x \varphi$$
$$\exists x(\varphi \vee \psi) \leftrightarrow \varphi \vee \exists x \psi$$
$$\exists x(\varphi \wedge \psi) \leftrightarrow \varphi \wedge \exists x \psi$$
$$\exists x(\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \exists x \psi)$$
$$\exists x(\psi \rightarrow \varphi) \leftrightarrow (\forall x \psi \rightarrow \varphi)$$
$$\exists x(\varphi \rightarrow \forall x \varphi)$$

Valid Formulas — Example

$$t = t$$

$$t = s \to s = t$$

$$t = s \to s = r \to t = r$$

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

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

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

$$t = s \to \big(\varphi[t/x] \leftrightarrow \varphi[s/x]\big)$$

Valid Formulas — Example

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

$$\exists x(x = t)$$
$$\varphi[t/x] \leftrightarrow \forall x(x = t \rightarrow \varphi)$$
$$\varphi[t/x] \leftrightarrow \exists x(x = t \wedge \varphi)$$

$\{x_1, \ldots, x_n\} \cap \mathrm{Fv}(s) \cap \mathrm{Fv}(t_1) \cap \cdots \cap \mathrm{Fv}(t_n) = \emptyset$:

$$f(t_1, \ldots, t_n) = s$$
$$\updownarrow$$
$$\forall x_1 \ldots x_n \big(t_1 = x_1, \ldots, t_n = x_n \rightarrow f(x_1, \ldots, x_n) = s\big)$$
$$\updownarrow$$
$$\exists x_1 \ldots x_n \big(t_1 = x_1 \wedge t_n = x_n \wedge f(x_1, \ldots, x_n) = s\big)$$

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.

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

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

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Formal Systems

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

Hilbert System = Axiom + Inference Rule

Axiom Schema

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

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\mathrm{MP}]$$

Example

Theorem

$$\varphi \vdash \exists x \varphi$$

Proof.

1	$(\forall x\, \neg\varphi \to \neg\varphi) \to \varphi \to \neg\forall x\, \neg\varphi$	Tautology
2	$\forall x\, \neg\varphi \to \neg\varphi$	A5
3	$\varphi \to \neg\forall x\, \neg\varphi$	1,2 MP
4	φ	Premise
5	$\neg\forall x\, \neg\varphi$	3,4 MP
6	$\exists x\, \varphi$	Definition of $\exists$

Meta-properties

- $\vDash \varphi[\psi_1/p_1, \ldots, \psi_n/p_n]$ where $\varphi \in \mathscr{L}^0$, $\psi_1, \ldots, \psi_n \in \mathscr{L}^1$. tautology
- $\Gamma, \varphi \vdash \psi \iff \Gamma \vdash \varphi \to \psi$ deduction theorem
- $\Gamma, \varphi \vdash \psi \wedge \neg\psi \implies \Gamma \vdash \neg\varphi$ reductio ad absurdum
- $\Gamma, \neg\varphi \vdash \psi \;\&\; \Gamma, \neg\varphi \vdash \neg\psi \implies \Gamma \vdash \varphi$ proof by contradiction
- $\Gamma, \varphi \vdash \neg\psi \iff \Gamma, \psi \vdash \neg\varphi$ contraposition
- $t = s \vdash r[t/x] = r[s/x]$ substitution
- $t = s \vdash \varphi[t/x] \leftrightarrow \varphi[s/x]$ substitution
- $\vdash \psi \leftrightarrow \chi \implies \vdash \varphi \leftrightarrow \varphi^*$ where φ^* arises from φ by replacing one or more occurrences of ψ in φ by χ. equivalent replacement
- $\vdash \forall x\varphi \iff \vdash \forall y\varphi[y/x]$ alphabetic variant

Meta-properties

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

Alphabetic Variant

Theorem (Existence of Alphabetic Variants)

Let φ be a formula, t a term, and x a variable. Then we can find a formula φ^* which differs from φ only in the choice of quantified variables s.t.

1. $\varphi \vdash \varphi^*$
2. *t is substitutable for x in φ^*.*

Strategy

i. $(\rightarrow)$ $\quad \Gamma \vdash \varphi \rightarrow \psi \iff \Gamma, \varphi \vdash \psi$

ii. $(\forall)$

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

iii. $(\neg)$

   1. $(\neg \rightarrow)$ $\quad \Gamma \vdash \neg(\varphi \rightarrow \psi) \iff \Gamma \vdash \varphi \ \& \ \Gamma \vdash \neg\psi$
   2. $(\neg\neg)$ $\quad \Gamma \vdash \neg\neg\varphi \iff \Gamma \vdash \varphi$
   3. $(\neg\forall)$ $\quad \Gamma \vdash \neg\forall x \varphi \iff \Gamma \vdash \neg\varphi[t/x]$
      Unfortunately this is not always possible. Try contraposition, reductio ad absurdum or prove by contradiction...

Tree Method for Propositional Logic

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

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

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

✓

Tree Method for Predicate Logic I

Ground Tree:

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

where t is a ground term.

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

where a is a new constant.

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

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

Tree Method for Predicate Logic II

Tree Method with Unification:

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

where x_i is a new variable.

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

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

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

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

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 σ is a *unifier* for a set Γ of formulas if for every $\varphi, \psi \in \Gamma$: $\varphi\sigma = \psi\sigma$.
- A unifier σ is a *most general unifier* for Γ if for each unifier θ there exists a substitution λ s.t. $\theta = \sigma\lambda$.

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

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

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

Tree Method for Predicate Logic

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

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

Tactics

- Try to apply "non-branching" rules first, in order to reduce the number of branches.
- Try to close off branches as quickly as possible.
- Deal with negated quantifiers first.
- Instantiate existentials before universals.

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)

$\neg P(a)$ ✓

$\neg Q(c)$ ✓

$\neg R(d)$ ✓

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

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

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

$R(d) \vee \neg P(b)$

$P(x_1)$

$x_1 = a$

×

$(R(d) \vee \neg Q(b)) \wedge Q(a)$ ✓

$R(d) \vee \neg Q(b)$ ✓

$Q(a)$

$R(d)$

×

$\neg Q(b)$

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

存在某个人，如果她不孕，则人人不孕。

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

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

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

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

$$\varphi(x_1)$$

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

$$\neg\varphi(a)$$

$$x_1 = a$$

$$\times$$

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

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

$$\varphi(a)$$

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

$$\neg\varphi(b)$$

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

$$\varphi(b)$$

$$\neg\forall x\varphi(x)$$

$$\times$$

Soundness & Completeness

Definition (Deduction)

$\varphi_1, \ldots, \varphi_n \vdash \psi$ iff there exists a closed tree from $\{\varphi_1, \ldots, \varphi_n, \neg\psi\}$.

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.

$$\varphi_1, \ldots, \varphi_n \vdash \psi \iff \varphi_1, \ldots, \varphi_n \vDash \psi$$

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 cannot 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. $\forall x\big(\varphi \vee \psi(x)\big) \to \varphi \vee \forall x \psi(x)$ where $x \notin \mathrm{Fv}(\varphi)$
5. $\exists x\Big(\big(Px \wedge \forall y(Py \to y = x)\big) \wedge Qx\Big) \dashv\vdash \exists x \forall y\Big(\big(Py \leftrightarrow y = x\big) \wedge Qx\Big)$
6. $\exists x\big(Px \wedge \forall y(Py \to y = x)\big) \wedge \exists x\big(Qx \wedge \forall y(Qy \to y = x)\big) \wedge \neg\exists x(Px \wedge Qx) \to \exists xy\big(x \neq y \wedge (Px \vee Qx) \wedge (Py \vee Qy) \wedge \forall z(Pz \vee Qz \to z = x \vee z = y)\big)$

$$1 + 1 = 2$$

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 they know 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.

  $\forall x(contain(x,1) \rightarrow \exists y(adj(x,y) \wedge mine(y) \wedge \forall z(adj(x,z) \wedge mine(z) \rightarrow z = y)))$
- ...

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

$$\psi(\iota_x\varphi) := \exists! x\varphi \wedge \exists x(\varphi \wedge \psi)$$
$$\equiv \exists x \forall y\Big(\big(\varphi(y) \leftrightarrow y = x\big) \wedge \psi(x)\Big)$$

The round square does not exist. $\psi(\iota_x\varphi) \vee (\neg\psi)(\iota_x\varphi)$?

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

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

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

$$\iota_x\varphi = \iota_x\varphi \ ? \qquad \forall x\psi \to \psi(\iota_x\varphi) \ ?$$

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

$$\vdash \forall x\psi \to \psi(\iota_x^y\varphi)$$

- The logical form of a statement may differ from its grammatical form.
- The correct logical analysis of a word or phrase may involve an explanation not of what that word or phrase taken by itself means, but rather of what whole sentences containing the word or phrase mean.
- The method of contextual definition, which the theory of descriptions exemplifies, was inspired by the nineteenth-century rigorization of analysis.

Berkeley: 2nd crisis of the Foundations of Mathematics
For $f(x) = x^2$,

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

$\frac{\mathrm{d}}{\mathrm{d}x}$ 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.

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 PA (proof-theoretical strength of PA)

Natural Deduction

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

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ [\wedge^+] \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ [\wedge^-] \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ [\wedge^-]$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ [\vee^+] \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi}\ [\vee^+] \qquad \frac{\Gamma \vdash \varphi \vee \psi \qquad \Gamma, \varphi \vdash \chi \qquad \Gamma, \psi \vdash \chi}{\Gamma \vdash \chi}\ [\vee^-]$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ [\to^+] \qquad \frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ [\to^-]$$

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

Natural Deduction

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

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

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

Example

Theorem (Proof by Contradiction)

$$\neg\varphi \to \bot \vdash \varphi$$

Proof.

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

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

Example

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(\varphi \to \psi(x)) \vdash \forall x(\varphi \to \psi(x))}\,[\mathsf{I}]}{\forall x(\varphi \to \psi(x)) \vdash \varphi \to \psi(a)}\,[\forall^-]}{\forall x(\varphi \to \psi(x)), \varphi \vdash \psi(a)}\,[\to^-]}{\forall x(\varphi \to \psi(x)), \varphi \vdash \forall x\psi(x)}\,[\forall^+]}{\forall x(\varphi \to \psi(x)) \vdash \varphi \to \forall x\psi(x)}\,[\to^+]}{\vdash \forall x(\varphi \to \psi(x)) \to \varphi \to \forall x\psi(x)}\,[\to^+]$$

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

Natural Deduction — another version

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi}\ [\wedge^+] \qquad \frac{\varphi \wedge \psi}{\varphi}\ [\wedge^-] \qquad \frac{\varphi \wedge \psi}{\psi}\ [\wedge^-]$$

$$\frac{\varphi}{\varphi \vee \psi}\ [\vee^+] \qquad \frac{\psi}{\varphi \vee \psi}\ [\vee^+] \qquad \frac{\varphi \vee \psi \quad \begin{array}{c}[\varphi]^n\\ \vdots \\ \chi\end{array} \quad \begin{array}{c}[\psi]^n\\ \vdots \\ \chi\end{array}}{\chi}\ [\vee^-]^n$$

$$\frac{\begin{array}{c}[\varphi]^n\\ \vdots \\ \psi\end{array}}{\varphi \to \psi}\ [\to^+]^n \qquad \frac{\varphi \to \psi \quad \varphi}{\psi}\ [\to^-]$$

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

Natural Deduction — another version

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

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

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

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

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

Sequent Calculus

Axiom

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

Cut

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

Left structural rules

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

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

$$\frac{\Gamma_1, \varphi, \psi, \Gamma_2 \vdash \Delta}{\Gamma_1, \psi, \varphi, \Gamma_2 \vdash \Delta}\ [\mathrm{PL}]$$

Right structural rules

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

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

$$\frac{\Gamma \vdash \Delta_1, \varphi, \psi, \Delta_2}{\Gamma \vdash \Delta_1, \psi, \varphi, \Delta_2}\ [\mathrm{PR}]$$

Sequent Calculus

Left logical rules:

$$\frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}\ [\wedge L_1]$$

$$\frac{\Gamma, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}\ [\wedge L_2]$$

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

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

Right logical rules:

$$\frac{\Gamma \vdash \varphi, \Delta}{\Gamma \vdash \varphi \vee \psi, \Delta}\ [\vee R_1]$$

$$\frac{\Gamma \vdash \psi, \Delta}{\Gamma \vdash \varphi \vee \psi, \Delta}\ [\vee R_2]$$

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

$$\frac{\Gamma, \varphi \vdash \psi, \Delta}{\Gamma \vdash \varphi \rightarrow \psi, \Delta}\ [\rightarrow R]$$

Sequent Calculus

Left logical rules: Right logical rules:

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

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

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

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

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

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

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

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

Natural Deduction — constant vs variable

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

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

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

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

Natural Deduction — another version — constant vs variable

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

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

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

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

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

where $y \notin \mathrm{Fv}(\exists x\varphi, \psi)$, and y is not free in any assumption which is undischarged in the derivations ending with $\exists x\varphi, \psi$ except in $\varphi[y/x]$.

Sequent Calculus — constant vs variable

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

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

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

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

Cut-Elimination Theorem

Theorem (Cut-Elimination Theorem — Gentzen1934)

If $\Gamma \vdash \Delta$ is provable, then it is provable without use of the Cut Rule.

Corollary (The Subformula Property)

If $\Gamma \vdash \Delta$ is provable, then it has a deduction all of whose formulas are subformulas of Γ and Δ.

Corollary (Consistency)

A contradiction, i.e. the empty sequent $\emptyset \vdash \emptyset$, is not deducible.

Corollary (Conservation)

Predicate logic is conservative over propositional logic.

Theorem (Cut-free Completeness Theorem)

Let Π be a set of sentences. If Π logically implies $\Gamma \vdash \Delta$, then there is a finite subset $\Sigma \subset \Pi$ s.t. $\Sigma, \Gamma \vdash \Delta$ has a cut-free proof.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Definability

什么是“可定义”？

Berry Paradox

The smallest positive integer not definable in fewer than twelve words.

Definition (Definability)

- $X \subset A^n$ is Y-definable $(X \in \mathrm{Def}(\mathcal{A}, Y))$ over $\mathcal{A}$ if there is a wff φ and $b_1, \ldots, b_m \in Y^m$ s.t.
$$X = \{(a_1, \ldots, a_n) \colon \mathcal{A} \vDash \varphi[a_1, \ldots, a_n, b_1, \ldots, b_m]\}$$
- X is definable in $\mathcal{A}$ if it is $\emptyset$-definable in $\mathcal{A}$.

A definition is acceptable only on condition that it implies no contradiction. — *Poincaré*

Representability

什么是“可表示”？

Definition (Representable Functions)

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

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

Definition (Representable Relations)

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

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

A function/relation is representable in Robinson Q iff it is computable.

Example

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

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

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

Homomorphism & Isomorphism

Definition (Homomorphism)

A homomorphism h of $\mathcal{A}$ into $\mathcal{B}$ is a function $h\colon A \to B$ s.t.

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

- An isomorphism (monomorphism/epimorphism) is a bijective (injective/surjective) homomorphism. $\mathcal{A} \cong \mathcal{B}$
- An automorphism (endomorphism) is an isomorphism (homomorphism) from $\mathcal{A}$ to itself.
- A structure $\mathcal{A}$ is rigid if it has no automorphisms other than 1_A.

Homomorphism Theorem

Theorem (Homomorphism Theorem)

Let h be a homomorphism of $\mathcal{A}$ into $\mathcal{B}$, and $v\colon \mathscr{V} \to A$.

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

Definition (Elementary Equivalence)

$$\mathcal{A} \equiv \mathcal{B} \text{ if for any sentence } \varphi\colon \mathcal{A} \vDash \varphi \iff \mathcal{B} \vDash \varphi$$

$$\mathcal{A} \cong \mathcal{B} \implies \mathcal{A} \equiv \mathcal{B}$$

Theorem

$\mathcal{A} \equiv \mathcal{B} \ \ \& \ \ |A| < \infty \implies \mathcal{A} \cong \mathcal{B}$

Proof.

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

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

Since $\mathcal{A} \equiv \mathcal{B}$, then $\mathcal{B} \vDash \exists x_1 \ldots x_n \bigwedge_{i=1}^{m} \varphi_i(x_1, \ldots, x_n)$, and
$\mathcal{B} \vDash \bigwedge_{i=1}^{m} \varphi_i(b_1, \ldots, b_n)$ for some $b_1, \ldots, b_n \in B$.
Let $f_j \colon a_i \mapsto b_i$. But $\mathcal{B} \nvDash \varphi_j(b_1, \ldots, b_n)$.

Substructure

Definition (Substructure)

$\mathcal{A}$ is called a substructure of $\mathcal{B}$ ($\mathcal{A} \subset \mathcal{B}$) iff

- $A \subset B$
- 1. $P^{\mathcal{A}} = P^{\mathcal{B}} \cap A^n$ for any n-ary predicate symbol P.
  2. $f^{\mathcal{A}} = f^{\mathcal{B}} \restriction_{A^n}$ for any n-ary function symbol f.

Suppose $\mathcal{A} \subset \mathcal{B}$. Then

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

$$t^{\mathcal{A}}[a_1, \ldots, a_n] = t^{\mathcal{B}}[a_1, \ldots, a_n]$$

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

$$\mathcal{A} \vDash \varphi[a_1, \ldots, a_n] \iff \mathcal{B} \vDash \varphi[a_1, \ldots, a_n]$$

Example

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

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

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

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

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

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

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

Example

$a \mapsto 1$

$b \mapsto 6$

$c \mapsto 8$

$d \mapsto 3$

$g \mapsto 5$

$h \mapsto 2$

$i \mapsto 4$

$j \mapsto 7$

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

A Story

"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 $h\colon A \to A$, and $R \subset A^n$ definable in $\mathcal{A}$. Then for any $a_1, \ldots, a_n \in A$,

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

Remark: This corollary is sometimes useful in showing that a given relation is not definable.

Example (The set $\mathbb{N}$ is not definable in $(\mathbb{R}, <)$ where $\mathscr{L} = \{<\}$.)

$h\colon a \mapsto a^3$ 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 $\mathcal{A} := \big(\{a, b, c\}, \{(a, b), (a, c)\}\big)$
where the language is $\mathscr{L} = \{E\}$.

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

- $\{b, c\}$ is definable in $\mathcal{A}$: $\exists y E(y, x)$
- $\{b\}$ is not definable in $\mathcal{A}$.

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.

- $U := \{\boldsymbol{x} \in E : |\boldsymbol{x}| = 1\}$ is not definable in $\mathcal{E}$.
- $h : \boldsymbol{x} \mapsto 2\boldsymbol{x}$ is an automorphism but it does not preserve U.

Ehrenfeucht-Fraïssé Game (EF Game)

Spoiler and *Duplicator*, played on two structures $\mathcal{A}$ and $\mathcal{B}$.
Each run of the game has n moves. In each move,

- *Spoiler* picks an element from $\mathcal{A}$ or from $\mathcal{B}$.
- *Duplicator* picks an element from $\mathcal{B}$ or from $\mathcal{A}$.
- *Duplicator* wins the run if $(a_i, b_i)_{i=1}^n$ is a partial isomorphism from $\mathcal{A}$ to $\mathcal{B}$.
- *Spoler* wins the run otherwise.
- $\mathcal{A} \sim_n \mathcal{B}$ if *Duplicator* has a winning strategy in the n-move game.
- $\mathcal{A} \equiv_n \mathcal{B}$ if $\mathcal{A} \vDash \varphi \iff \mathcal{B} \vDash \varphi$ for all sentences up to *quantifier depth* n.

Theorem

$$\mathcal{A} \sim_n \mathcal{B} \iff \mathcal{A} \equiv_n \mathcal{B}$$

Ehrenfeucht-Fraïssé Game (EF Game)

$$\mathcal{A} \sim_2 \mathcal{B} \qquad \mathcal{A} \nsim_3 \mathcal{B}$$

$$\mathcal{A} \vDash \varphi \qquad \mathcal{B} \vDash \neg\varphi$$

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

Isomorphic Embedding, Elementary Embedding

Definition

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

Example

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

$$f\colon \mathcal{A} \prec \mathcal{B} \iff \exists C\big(f\colon \mathcal{A} \cong C \prec \mathcal{B}\big) \iff \exists C\big(\mathcal{A} \prec C \cong \mathcal{B}\big)$$

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 $f : \mathcal{A} \cong \mathcal{B}$, then for any term $t(x_1, \ldots, x_n)$, any wff $\varphi(x_1, \ldots, x_n)$, and any $a_1, \ldots, a_n \in A$,

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

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

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

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

Isomorphic Embedding, Elementary Embedding

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

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

- $f\colon \mathcal{A} \subset \mathcal{B} \iff (\mathcal{B}, f(a))_{a \in A} \vDash \mathrm{diag}(\mathcal{A})$
- $f\colon \mathcal{A} \prec \mathcal{B} \iff (\mathcal{B}, f(a))_{a \in A} \vDash \mathrm{Th}(\mathcal{A}_A)$

$$\mathcal{A} \prec \mathcal{B} \iff \mathcal{A} \subset \mathcal{B} \ \& \ \forall X \in \mathrm{Def}(\mathcal{B}, A)\colon X \cap A \neq \emptyset$$

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

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

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

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: $\varphi_1 \vee \varphi_2 \vee \cdots \vee \varphi_n$, where $n \geq 1$ and $\varphi_1, \varphi_2, \ldots, \varphi_n$ 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
$\varphi \leftrightarrow \psi$	$(\neg\varphi \vee \psi) \wedge (\varphi \vee \neg\psi)$
$\varphi \rightarrow \psi$	$\neg\varphi \vee \psi$
$\neg\neg\varphi$	φ
$\neg(\varphi \vee \psi)$	$\neg\varphi \wedge \neg\psi$
$\neg(\varphi \wedge \psi)$	$\neg\varphi \vee \neg\psi$
$\neg\forall x\varphi$	$\exists x\neg\varphi$
$\neg\exists x\varphi$	$\forall x\neg\varphi$

subformula	replaced by
$(\varphi \wedge \psi) \vee \chi$	$(\varphi \vee \chi) \wedge (\psi \vee \chi)$
$\chi \vee (\varphi \wedge \psi)$	$(\chi \vee \varphi) \wedge (\chi \vee \psi)$

subformula	replaced by
$(\varphi \vee \psi) \wedge \chi$	$(\varphi \wedge \chi) \vee (\psi \wedge \chi)$
$\chi \wedge (\varphi \vee \psi)$	$(\chi \wedge \varphi) \vee (\chi \wedge \psi)$

- 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	
$\neg\forall x\varphi$	$\exists x\neg\varphi$	
$\neg\exists x\varphi$	$\forall x\neg\varphi$	
$\forall x\varphi(x) \wedge \forall x\psi(x)$	$\forall x(\varphi(x) \wedge \psi(x))$	
$\exists x\varphi(x) \vee \exists x\psi(x)$	$\exists x(\varphi(x) \vee \psi(x))$	
$\forall x\varphi(x)$	$\forall y\varphi[y/x]$	where $y \notin \mathrm{Fv}(\varphi) \cup \mathrm{Bv}(\varphi)$
$\varphi \vee Qx\psi$	$Qx(\varphi \vee \psi)$	where $x \notin \mathrm{Fv}(\varphi)$
$\varphi \wedge Qx\psi$	$Qx(\varphi \wedge \psi)$	where $x \notin \mathrm{Fv}(\varphi)$
$\varphi \rightarrow \forall x\psi$	$\forall x(\varphi \rightarrow \psi)$	where $x \notin \mathrm{Fv}(\varphi)$
$\varphi \rightarrow \exists x\psi$	$\exists x(\varphi \rightarrow \psi)$	where $x \notin \mathrm{Fv}(\varphi)$
$\forall x\varphi \rightarrow \psi$	$\exists x(\varphi \rightarrow \psi)$	where $x \notin \mathrm{Fv}(\varphi)$
$\exists x\varphi \rightarrow \psi$	$\forall x(\varphi \rightarrow \psi)$	where $x \notin \mathrm{Fv}(\varphi)$

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 $\forall x_1 \ldots \forall x_n \exists y \varphi$ by $\forall x_1 \ldots \forall x_n \varphi[f(x_1, \ldots, x_n)/y]$, where f is a new function symbol. If there are no universal quantifiers preceding $\exists$, replace $\exists x \varphi$ by $\varphi[c/x]$, where c is a new constant. Given φ, in finitely many steps we can obtain its *Skolem normal form* φ^{SNF} without existential quantifiers.
- Any formula can be *equisatisfiably* transformed into SNF.

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

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

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

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

Example:

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

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

Herbrand Universe

Definition (Herbrand Universe)

Given a sentence φ in Skolem normal form,

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

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 φ is satisfiable iff there is a Herbrand structure satisfying it.

Proof.

Assume φ is in Skolem normal form, and it is satisfied by some structure (A, I). Then Herbrand structure $(H_\varphi, J) \vDash \varphi$, where for each ground term t: $J(t) = t$, and for each predicate symbol P,
$J(P) = \{(t_1, \ldots, t_n) \in H_\varphi : A, I \vDash P(t_1, \ldots, t_n)\}$.

Herbrand's Theorem

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

Definition (Herbrand's Theorem)

A sentence $\forall \boldsymbol{x} \varphi(\boldsymbol{x})$ in Skolem normal form is unsatisfiable iff some finite subset $K \subset \mathcal{E}(\varphi, H_\varphi)$ is unsatisfiable.

Theorem (Herbrand's Theorem)

Suppose φ is a sentence. Then

$$\vdash \varphi \iff \vdash \bigvee_{k=1}^{m} \varphi'(t_{k1}, \ldots, t_{kn})$$

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 φ' is obtained from φ^{HNF} by dropping the quantifiers.

Resolution — Example

Given clauses $A = \varphi(f(x)) \vee \psi(x)$ and $B = \neg\varphi(x) \vee \neg\varphi(y)$.

1. Separate their variables by standard substitutions $\{x_1/x\}$ and $\{y_1/x, y_2/y\}$.

$$A' = \{\varphi(f(x_1)), \psi(x_1)\} \quad B' = \{\neg\varphi(y_1), \neg\varphi(y_2)\}$$

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.

$$C = \{\varphi(f(x_1))\} \quad D = \{\neg\varphi(y_1), \neg\varphi(y_2)\}$$

$$|C \cup D| = \{\varphi(f(x_1)), \varphi(y_1), \varphi(y_2)\}$$

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:

$$R = (A'\sigma \setminus C\sigma) \cup (B'\sigma \setminus D\sigma) = \{\psi(x_1)\}$$

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 φ, $\mathcal{R}(\varphi)$ is φ extended with all resolvents to clauses of φ.
- The successive application of the resolution rule yields a complete proof procedure.

Theorem (Completeness)

If φ is unsatisfiable, then $\mathcal{R}^n(\varphi)$ will contain the empty clause for some n.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic
- Syntax
- Semantics
- Formal Systems
- Definability & Isomorphism
- Normal Forms
- Meta-Theorems

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Model & Semantic Consequence

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

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

Galois Correspondence

Definition (Galois Correspondence)

The function $X \mapsto X^*$ from $P(A)$ to $P(B)$ and the function $Y \mapsto Y^\dagger$ from $P(B)$ to $P(A)$ 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

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

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

Consistency & Satisfiability

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

Soundness Theorem

Theorem (Soundness Theorem)

$$\Gamma \vdash \varphi \implies \Gamma \vDash \varphi$$

Proof.

by induction on derivation lengths.

Truth in a model is preserved under making deductions.

Completeness Theorem

Theorem (Completeness Theorem — Gödel1930)

$$\Gamma \vDash \varphi \implies \Gamma \vdash \varphi$$

Corollary

Any consistent set of wffs is satisfiable.

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

Proof of Completeness Theorem — step1

Lemma (Lindenbaum Lemma)

Any consistent set Θ of sentences can be extended to a maximal consistent set Δ of sentences of the same language.

Proof.

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

$$\Theta_0 := \Theta$$

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

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

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

Proof of Completeness Theorem — step2

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

Lemma (Closure Lemma)

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

Proof.

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

$$\Gamma_0 := \Gamma$$

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

where c_β is the first new constant not occurring in $\Gamma_\xi \cup \{\varphi_\xi\}$.

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

Then $\Theta := \bigcup_{\xi<\kappa} \Gamma_\xi$ is consistent, and we can extend Θ to a maximal consistent set $\Delta \supset \Theta$ by Lindenbaum lemma.

Proof of Completeness Theorem — step3

Lemma (Term Models Lemma)

If Δ is maximal consistent, then there is an interpretation $\mathcal{A}, \nu$ s.t.

$$\mathcal{A}, \nu \vDash \varphi \iff \varphi \in \Delta$$

Proof.

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

Stone Space of Lindenbaum Algebra

$$
\begin{tikzcd}
\mathrm{Str} \arrow[r, leftrightarrow, squiggly, "\models"] \arrow[d, two heads, "\mathcal{A}\mapsto\mathrm{Th}(\mathcal{A})"'] & \mathrm{Sen} \arrow[d, two heads, "\varphi\mapsto[\varphi]"] \\
\mathrm{S}_0 \arrow[r, leftrightarrow, squiggly] \arrow[d, tail] & \mathrm{Lin}_0 \arrow[ul, squiggly, "\ni"] \\
\mathrm{Sto}(\mathrm{Lin}_0) \arrow[ur, squiggly, "\ni"] &
\end{tikzcd}
$$

- Str: the class of structures.
- Sen: the set of sentences.
- S_0: the set of complete theories.
- $\mathrm{Lin}_0 = \mathrm{Sen}/{\sim}$
- $\mathrm{Sto}(A)$: the set of ultrafilters of A.

1. The closed subsets of Sen are precisely the theories.
2. The closed subsets of S_0 compose a Hausdorff topology.
3. $\mathcal{A} \mapsto \mathrm{Th}(\mathcal{A}) \colon \mathrm{Str} \to \mathrm{S}_0$ is continuous, and $[\mathcal{A}] \mapsto \mathrm{Th}(\mathcal{A})$ is a homomorphism, S_0 is a Kolmogorov quotient $\mathrm{Str}/{\equiv}$.
4. For every theory T, $T/{\sim}$ is a filter of Lin_0.
5. For every complete theory T, $T/{\sim}$ is an ultrafilter of Lin_0.
6. $T \mapsto T/{\sim} \colon \mathrm{S}_0 \rightarrowtail \mathrm{Sto}(\mathrm{Lin}_0)$ 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. $T \mapsto T/{\sim} \colon \mathrm{S}_0 \rightarrowtail\!\!\!\!\rightarrow \mathrm{Sto}(\mathrm{Lin}_0)$ iff the topology on S_0 is compact.

Compactness Theorem

Theorem (Compactness Theorem)

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

Corollary

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

Corollary

If a set Γ 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 $\{\mathcal{A}_i : i \in I\}$ is a set of structures, and U is an ultrafilter on I. Define $\mathcal{B} := \prod_{i \in I} \mathcal{A}_i / U$ as follows:

- $B := \prod_{i \in I} A_i / \sim = \left\{ [f] : f \in \prod_{i \in I} A_i \right\}$ where
  $f \sim g := \left\{ i \in I : f(i) = g(i) \right\} \in U$
- $P^{\mathcal{B}}\big([f_1], \ldots, [f_n]\big) := \left\{ i \in I : P^{\mathcal{A}_i}(f_1(i), \ldots, f_n(i)) \right\} \in U$
- $F^{\mathcal{B}}\big([f_1], \ldots, [f_n]\big) := [f]$ where $f(i) := F^{\mathcal{A}_i}\big(f_1(i), \ldots, f_n(i)\big)$

Theorem (Łoś Theorem)

$$\prod_{i \in I} \mathcal{A}_i / U \vDash \varphi\left([f_1], \ldots, [f_n]\right) \iff \left\{ i \in I : \mathcal{A}_i \vDash \varphi\big(f_1(i), \ldots, f_n(i)\big) \right\} \in U$$

Ultrapower

Let $j : a \mapsto [f_a]$, where $f_a(i) = a$ for $i \in I$. Then

$$j : \mathcal{A} \prec \prod_{i \in I} \mathcal{A}/U$$

Theorem (Kiesler-Shelah)

$\mathcal{A} \equiv \mathcal{B}$ iff for some I and an ultrafilter U on I, $\prod_{i \in I} \mathcal{A}/U \cong \prod_{i \in I} \mathcal{B}/U$.

Compactness Theorem

Corollary (Compactness Theorem)

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

Proof.

Let $I := \{\Delta \subset \Gamma : |\Delta| < \infty\}$.
Then $\forall \Delta \in I \; \exists \mathcal{A}_\Delta : \mathcal{A}_\Delta \vDash \Delta$.
Let $\hat{\varphi} := \{\Delta \in I : \varphi \in \Delta\}$.
Then $F := \{\hat{\varphi} : \varphi \in \Gamma\}$ has the finite intersection property because

$$\{\varphi_1, \ldots, \varphi_n\} \in \hat{\varphi}_1 \cap \cdots \cap \hat{\varphi}_n$$

By the ultrafilter theorem, F can be extended to an ultrafilter U on I.
For $\varphi \in \Gamma$,

$$\begin{aligned} \hat{\varphi} \in U \;\; \& \;\; \hat{\varphi} \subset \{\Delta \in I : \mathcal{A}_\Delta \vDash \varphi\} &\implies \{\Delta \in I : \mathcal{A}_\Delta \vDash \varphi\} \in U \\ &\implies \prod_{\Delta \in I} \mathcal{A}_\Delta / U \;\vDash \varphi \end{aligned}$$

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

$$\text{finite} \implies \text{infinite}$$
$$\text{local} \implies \text{global}$$

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_Δ iff $\mathcal{K}$ is closed under ultraproducts and elementary equivalence.*
- *$\mathcal{K}$ is EC iff both $\mathcal{K}$ and the complement of $\mathcal{K}$ are closed under ultraproducts and elementary equivalence.*

Applications of Compactness

- The class of all finite structures is not EC_Δ. (Model finiteness is undefinable even by a set of formulas.)
- The class of all infinite structures is EC_Δ but not EC. (Model infiniteness is definable by a set of formulas but undefinable by a single formula.)
- The class of graphs / groups / rings / fields / ordered fields / n-dimensional vector spaces / fields of characteristic p is EC; the class of infinite groups / divisible groups / torsion-free groups / infinite rings / infinite-dimensional vector spaces / fields of characteristic 0 is EC_Δ but not EC; the class of all connected graphs / finite graphs / finite groups / finite rings / finite fields / algebraically closed fields / torsion groups / finite-dimensional vector spaces / noetherian commutative rings is not EC_Δ.

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

$$\forall k \geq 2\colon R(k,k) \geq 2^{\frac{k}{2}}$$

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 $(X, \mathscr{B}, \mu, T)$ be a measure-preserving system and $A \in \mathscr{B}$ with $\mu(A) > 0$. Then,

$$\forall k \in \mathbb{N}\colon \quad \liminf_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu\left(\bigcap_{j=0}^{k} T^{-jn} A\right) > 0$$

Szemerédi Theorem $\iff$ Furstenberg Multiple Recurrence Theorem

Complete Disorder is Impossible!

Theorem (Poincaré Recurrence Theorem)

Let $(X, \mathscr{B}, \mu, T)$ be a measure-preserving system and $A \in \mathscr{B}$ with $\mu(A) > 0$. Then almost every $x \in A$ returns infinitely often to A.

$$\mu\left(\{x \in A \colon \exists N \forall n > N \colon T^n x \notin A\}\right) = 0$$

Lemma (Kac's Lemma)

Let $(X, \mathscr{B}, \mu, T)$ be a measure-preserving system and $A \in \mathscr{B}$ with $\mu(A) > 0$. Then the recurrence time $\tau_A(x) := \min\left\{k \geq 1 \colon T^k x \in A\right\}$ 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 cannot 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 realises 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 λ has a model of cardinality $\leq \lambda$.

Theorem (Upward Löwenheim-Skolem Theorem)

If a set of sentences in a language of cardinality λ has an infinite model, then it has models of every cardinality $\geq \lambda$.

Skolem Paradox? — Models and Reality

- Cantor: $P(\mathbb{N})$ is uncountable.
- There is a countable model $\mathcal{M} \vDash \mathrm{ZF} \vdash$"$P(\mathbb{N})$ is uncountable".
- The statement "$P(\mathbb{N})$ is uncountable" is interpreted in $\mathcal{M}$ as — within $\mathcal{M}$, there is a set M_1 that looks like $P(\mathbb{N})$ and M_2 that looks like $\mathbb{N}$, but there is no set corresponding to the set of pairs of members of M_1 and M_2."
- Outside of $\mathcal{M}$, we can see that all $\mathcal{M}$-sets are really only countable. The $\mathcal{M}$-set M_1 that $\mathcal{M}$ says is $P(\mathbb{N})$ really isn't — outside $\mathcal{M}$, M_1 and $\mathbb{N}$ can be paired, but this requires the existence of a "pairing" set that isn't in $\mathcal{M}$.
- What we think are uncountable sets in our hierarchy may really be countable $\mathcal{M}'$-sets in the larger hierarchy.
- There is no absolute notion of countability. A set can only be said to be countable or uncountable relative to an interpretation of ZF.

Skolem Paradox? — Models and Reality

Skolem paradox: How can an uncountable set way up *here* in the Hierarchy be thought of as a countable set M way down *here*?

The Interpolation Theorem

Theorem (Craig's Interpolation Theorem)

If $\vDash \varphi \to \psi$*, then there is a sentence* χ *s.t.* $\vDash \varphi \to \chi$ *and* $\vDash \chi \to \psi$*, and* χ *contains no non-logical symbols except such as are both in* φ *and in* ψ*.*

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* $\mathbb{T}_i$ *be a theory in* $\mathscr{L}_i$ *for* $i = 1, 2$*. If* $\mathbb{T}_1$ *and* $\mathbb{T}_2$ *are consistent and if there is no formula* φ *of* $\mathscr{L}_0$ *s.t.* $\mathbb{T}_1 \vdash \varphi$ *and* $\mathbb{T}_2 \vdash \neg\varphi$*, then the union* $\mathbb{T}_1 \cup \mathbb{T}_2$ *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 $\varphi(x_1, \ldots, x_n)$ of $\mathscr{L}$ s.t.

$$\Sigma(P) \vDash \forall x_1 \ldots \forall x_n (P(x_1, \ldots, x_n) \leftrightarrow \varphi(x_1, \ldots, x_n))$$

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 $\mathcal{S}\colon\ signatures \to sets$ assigns to signature τ a set $\mathcal{S}(\tau)$ of sentences, and $\vDash_{\mathcal{L}}$ is a relation between τ-$structures$ and elements of $\mathcal{S}(\tau)$ s.t.

1. (*Monotony*) $\tau \subset \tau' \implies \mathcal{S}(\tau) \subset \mathcal{S}(\tau')$
2. (*Isomorphism*) $\mathcal{A} \vDash_{\mathcal{L}} \varphi \;\&\; \mathcal{A} \cong \mathcal{B} \implies \mathcal{B} \vDash_{\mathcal{L}} \varphi$
3. (*Expansion*) If $\tau \subset \tau', \varphi \in \mathcal{S}(\tau)$, and $\mathcal{A}$ is an τ'-structure, then $\mathcal{A} \vDash_{\mathcal{L}} \varphi \iff \mathcal{A}\restriction_{\tau} \vDash_{\mathcal{L}} \varphi$

$$\mathrm{Mod}^{\tau}_{\mathcal{L}}(\varphi) := \left\{\mathcal{A} \in \tau\text{-}structures\colon \mathcal{A} \vDash_{\mathcal{L}} \varphi\right\}$$

Example — $\mathcal{L}_{\kappa\lambda}$

For $\kappa \geq \lambda$, define the $\mathcal{L}_{\kappa\lambda}$ formulas as for first order logic, plus:

- Given a set of formulas $\{\varphi_i : i \in A\}, |A| < \kappa$, then $\bigwedge_{i \in A} \varphi_i$ and $\bigvee_{i \in A} \varphi_i$ are formulas.
- Given a set of variables $\{x_i : i \in B\}, |B| < \lambda$ and a formula φ, then $\exists(x_i : i \in B)\varphi$ and $\forall(x_i : i \in B)\varphi$ are formulas.

Satisfaction relation:

- $\mathcal{A} \vDash_{\mathcal{L}_{\kappa\lambda}} \bigwedge_{i \in A} \varphi_i$ if $\mathcal{A} \vDash_{\mathcal{L}_{\kappa\lambda}} \varphi_i$ for all $i \in A$.
- $\mathcal{A} \vDash_{\mathcal{L}_{\kappa\lambda}} \exists(x_i : i \in B)\varphi$ if $\mathcal{A} \vDash_{\mathcal{L}_{\kappa\lambda}} \varphi[a_i : i \in B]$ for some $\{a_i : i \in B\} \subset A$.

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 $\varphi \in \mathcal{S}(\tau)$ there is $\psi \in \mathcal{S}(\tau)$ s.t. $\mathcal{A} \vDash_{\mathcal{L}} \psi \iff \mathcal{A} \nvDash_{\mathcal{L}} \varphi$; and $\forall \varphi, \psi \in \mathcal{S}(\tau)\ \exists \chi \in \mathcal{S}(\tau) \colon \mathcal{A} \vDash_{\mathcal{L}} \chi \iff \mathcal{A} \vDash_{\mathcal{L}} \varphi \ \&\ \mathcal{A} \vDash_{\mathcal{L}} \psi$.
2. (*Quantifier*) $\forall c \in \tau \forall \varphi \in \mathcal{S}(\tau)\ \exists \psi \in \mathcal{S}(\tau) \colon$
$$\mathrm{Mod}_{\mathcal{L}}^{\tau \setminus \{c\}}(\psi) = \left\{ \mathcal{A} \colon (\mathcal{A}, a) \in \mathrm{Mod}_{\mathcal{L}}^{\tau}(\varphi) \text{ for some } a \in A \right\}$$
where $(\mathcal{A}, a)$ is the expansion of $\mathcal{A}$ to τ assigning a to c.
3. (*Renaming*) Let $\pi \colon \tau \to \tau'$ be a bijection which respects arity, and we extend π in a canonical way to $\hat{\pi} \colon \tau$-structures $\to \tau'$-structures. Then
$$\forall \varphi \in \mathcal{S}(\tau)\ \exists \varphi' \in \mathcal{S}(\tau) \colon \mathcal{A} \vDash_{\mathcal{L}} \varphi \iff \hat{\pi}(\mathcal{A}) \vDash_{\mathcal{L}} \varphi'$$
4. (*Relativization*) Given $\varphi \in \mathcal{S}(\tau)$ and symbols R, $c_1, \ldots, c_n \notin \tau$, there is $\psi \in \mathcal{S}(\tau \cup \{R, c_1, \ldots, c_n\})$ called the *relativization* of φ to $R(x, c_1, \ldots c_n)$, s.t. for $\mathcal{A} \colon (\mathcal{A}, X, b_1, \ldots, b_n) \vDash_{\mathcal{L}} \psi \iff \mathcal{B} \vDash_{\mathcal{L}} \varphi$ where $\mathcal{B} \subset \mathcal{A}$ with $B = \left\{ a \in A \colon R^{\mathcal{A}}(a, b_1, \ldots, b_n) \right\}$, and $(\mathcal{A}, X, b_1, \ldots, b_n)$ is the expansion of $\mathcal{A}$ interpreting R, $c_1, \ldots, c_n$ by X, $b_1, , \ldots, b_n$ (with $X \subset A^{n+1}$).

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 τ and $\varphi \in \mathcal{S}_1(\tau)$ there is $\psi \in \mathcal{S}_2(\tau)$ s.t.

$$\mathrm{Mod}^{\tau}_{\mathcal{L}_1}(\varphi) = \mathrm{Mod}^{\tau}_{\mathcal{L}_2}(\psi)$$

$$\mathcal{L}_1 \sim \mathcal{L}_2 := \mathcal{L}_1 \leq \mathcal{L}_2 \ \& \ \mathcal{L}_2 \leq \mathcal{L}_1$$

Theorem (Lindström's Theorem)

If a regular abstract logic $\mathcal{L}$ has the Countable Compactness and the Downward Löwenheim-Skolem Properties, then $\mathcal{L} \sim \mathcal{L}_{\omega\omega}$.

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.

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

- Least Number Principle.

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

Dense Linear Ordering without Endpoints

1. $x \not< x$
2. $x < y \rightarrow y < z \rightarrow x < z$
3. $x < y \vee x = y \vee y < x$
4. $x < y \rightarrow \exists z(x < z < y)$
5. $\exists yz(y < x < z)$

Definition (κ-categoricity)

A theory is κ-categorical if it has a unique model of cardinality κ.

Theorem (Cantor)

- *The theory of dense linear orderings without endpoints is $\aleph_0$-categorical.*
- $(\mathbb{R}, <)$ *is the unique complete linear ordering that has a countable dense subset isomorphic to* $(\mathbb{Q}, <)$.

Theorem (Łoś-Vaught Test)

If a theory with no finite model is κ-categorical, then it is complete.

Theorem

The theory ACF_p of algebraically closed fields of characteristic p (for p prime or 0) is κ-categorical for all uncountable cardinals κ.

Corollary

For $p \in \mathbb{P}$ or $p = 0$, ACF_p is complete and decidable.

Theorem (Morley's Categoricity Theorem)

If a theory is κ-categorical for some $\kappa \geq |\mathscr{L}|$, then it is categorical in all cardinalities $\geq |\mathscr{L}|$.

Lefschetz's Transfer Principle

Theorem (Lefschetz's Transfer Principle)

For a sentence φ in the language of fields, the following are equivalent:

1. $\mathbb{C} \vDash \varphi$
2. $\mathrm{ACF}_0 \vDash \varphi$
3. $\mathrm{ACF}_p \vDash \varphi$ *for all sufficiently large primes* p.
4. $\mathrm{ACF}_p \vDash \varphi$ *for infinitely many primes* p.

Proof.

$(1 \leftrightarrow 2)$ follows from the completeness of ACF_0.
$(2 \to 3)$ assume $\mathrm{ACF}_0 \vDash \varphi$, since the deduction $\mathrm{ACF}_0 \vdash \varphi$ only use finitely many instances of $\overbrace{1+1+\cdots+1}^{n \text{ times}} \neq 0$, then for some finite $\Delta \subset \mathrm{ACF}_0$: $\Delta \vdash \varphi$, and $\mathrm{ACF}_p \vDash \Delta$ for all sufficiently large primes p.
$(3 \to 4)$ is trivial.
$(4 \to 2)$ $\mathrm{ACF}_0 \nvdash \varphi \implies \mathrm{ACF}_0 \vdash \neg\varphi \implies \mathrm{ACF}_p \vdash \neg\varphi$ for all sufficiently large primes p.

Ax-Grothendieck Theorem

- An *affine variety* is a set $V \subset \mathbb{C}^n$ s.t. $V = \{(x_1, \ldots, x_n) \colon f_i(x_1, \ldots, x_n) = 0, 1 \leq i \leq k\}$ with $f_i \in \mathbb{C}[x_1, \ldots, x_n]$.
- For any field K a map $f \colon K^n \to K^n$ 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 $f \colon V \to V$ 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 $\mathrm{f}\colon \mathbb{C}^n \to \mathbb{C}^n$ is surjective.

Let $\varphi :=$"Every injective polynomial map f of degree d is surjective". By Lefschetz's transfer principle, we just have to show for all primes p, $\mathrm{ACF}_p \vdash \varphi$.
Moreover, for each p, by completeness of ACF_p, we only need to show φ is true in *some* model of 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 $f\colon F^n \to F^n$.
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 $\exists N\colon K \subset \bigcup_{n=1}^{N} \mathbb{F}_{p^n}$, hence it is finite. So $f\restriction_{K^n}\colon K^n \to K^n$ that is injective must be surjective. Hence $f\colon F^n \to F^n$ is surjective.

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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

$$\mathscr{L}^{=} := \{=, (,)\} \cup \mathscr{V} \cup \overbrace{\mathscr{F}}^{signature}$$

where

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

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

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

Term & Formula

Term $\mathcal{T}$

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

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

Well-Formed Formula WFF

$$\varphi ::= s = t$$

where $s, t \in \mathcal{T}$.

Semantics

A structure is a pair $\mathcal{A} := (A, I)$, where A is a non-empty set, and I is a mapping which assigns to each function symbol f^k a k-ary function $I(f^k)\colon A^k \to A$.
We write $\mathcal{A} = \left(A, c^{\mathcal{A}}, f^{\mathcal{A}}\right)$ for convinence.
An interpretation $(\mathcal{A}, \nu)$ is a structure $\mathcal{A}$ together with a variable assignment $\nu\colon \mathcal{V} \to A$.
We extend ν to $\overline{\nu}\colon \mathcal{T} \to A$ by recursion as follows:

Assignment over Terms

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

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

Semantics

- $\mathcal{A}, \nu \vDash s = t$ if $\overline{\nu}(s) = \overline{\nu}(t)$. (Satisfaction)
- $\mathcal{A} \vDash s = t$ if for all ν: $\mathcal{A}, \nu \vDash s = t$. (True)
- $\mathcal{A} \vDash \mathbb{T}$ if for all $\varphi \in \mathbb{T}$: $\mathcal{A} \vDash \varphi$. (Model)
- $\mathbb{T} \vDash s = t$ if for all $\mathcal{A}$: $\mathcal{A} \vDash \mathbb{T} \implies \mathcal{A} \vDash s = t$.
- $\vDash s = t$ 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.

$\mathbb{T} \vdash s = t$: An equation $s = t$ is a *theorem* of a theory $\mathbb{T}$ if $s = t$ is the last member of some deduction from $\mathbb{T}$.

Meta-Theorems

Theorem (Soundness & Completeness)

$$\mathbb{T} \vdash s = t \iff \mathbb{T} \vDash s = t$$

- Determining Validity? Undecidable!

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
   - Boolean Algebra
   - Lambda Calculus and Combinatory Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Semigroup/Monoid/Group

Group $\mathscr{L} = \{e, \cdot, ^{-1}\}$

1. $\forall xyz\colon x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x\colon e \cdot x = x$
3. $\forall x\colon x \cdot e = x$
4. $\forall x\colon x^{-1} \cdot x = e$
5. $\forall x\colon x \cdot x^{-1} = e$

Group $\mathscr{L} = \{\cdot\}$

1. $\forall xyz\colon x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall xy \exists z\colon xz = y$
3. $\forall xy \exists z\colon zx = y$

Group $\mathscr{L} = \{e, \cdot\}$

1. $\forall xyz\colon x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x\colon e \cdot x = x \cdot e = x$
3. $\forall x \exists y\colon x \cdot y = y \cdot x = e$

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's Theorem

Theorem (Cayley Theorem)

Every group G is isomorphic to a subgroup of the symmetric group on G.

Proof.

Let $\lambda_g : x \mapsto g \cdot x$, and $T : g \mapsto \lambda_g$ for $g \in G$.
For every group $(G, e, \cdot)$, the function T embeds $(G, e, \cdot)$ in the group $(\mathrm{Sym}(G), 1_G, \circ)$ 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 $\mathscr{BR}$

Ring $\mathscr{L} = \{0, 1, \oplus, \odot, -\}$

1. $\forall xyz\colon x \oplus (y \oplus z) = (x \oplus y) \oplus z$
2. $\forall xy\colon x \oplus y = y \oplus x$
3. $\forall x\colon x \oplus (-x) = 0$
4. $\forall x\colon x \oplus 0 = x$
5. $\forall xyz\colon x \odot (y \odot z) = (x \odot y) \odot z$
6. $\forall xyz\colon x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$
7. $\forall xyz\colon (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z)$
8. $\forall x\colon x \odot 1 = 1 \odot x = x$
9. $0 \neq 1$

A ***Boolean ring*** is a ring for which

$$\forall x\colon x \odot x = x$$

Field $\mathscr{L} = \{0, 1, \oplus, -, \odot, {}^{-1}\}$

- $\forall xy\colon x \odot y = y \odot x$
- $\forall x \neq 0\colon x \odot x^{-1} = x^{-1} \odot x = 1$

Logic as Algebra — Boolean Algebra $\mathcal{BA}$

Boolean Algebra $\mathscr{L} = \{0, 1, +, \cdot, ^{-}\}$

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

$$\begin{tikzcd}
 & \text{Logic} & \\
\text{proposition} \arrow[rr, "\text{deduce}"] \arrow[d, "\text{translate}"'] & & \text{proposition} \\
\text{equation} \arrow[rr, "\text{calculate}"] & & \text{equation} \arrow[u, "\text{translate}"'] \\
 & \text{Algebra} &
\end{tikzcd}$$

Power Set Algebra

$$(P(A), \emptyset, A, \cup, \cap, \overline{})$$

$$x \oplus y := (x \cdot \overline{y}) + (\overline{x} \cdot y)$$

$$x = y \iff x \oplus y = 0$$

Boolean Ring $\mathcal{BR}$ vs Boolean Algebra $\mathcal{BA}$

$\mathcal{BR} \implies \mathcal{BA}$

$$x \cdot y = x \odot y$$
$$x + y = x \oplus y \oplus (x \odot y)$$
$$\overline{x} = 1 \oplus x$$

$\mathcal{BA} \implies \mathcal{BR}$

$$x \odot y = x \cdot y$$
$$x \oplus y = (x \cdot \overline{y}) + (\overline{x} \cdot y)$$
$$-x = x$$

Boole's Four Main Theorems

$$\boldsymbol{x}^{\sigma} := x_1^{\sigma_1} \cdots x_n^{\sigma_n} \qquad x_i^{\sigma_i} := \begin{cases} x_i & \text{if } \sigma_i = 1 \\ \overline{x}_i & \text{if } \sigma_i = 0 \end{cases} \qquad \sigma \colon \{1, \ldots, n\} \to \{0, 1\}$$

1. Expansion
$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{\sigma} f(\sigma, \boldsymbol{y}) \cdot \boldsymbol{x}^{\sigma}$$

2. Reduction
$$\bigwedge_i \big(f_i(\boldsymbol{x}) = 0\big) \iff \sum_i f_i(\boldsymbol{x}) = 0$$

3. Elimination
$$\exists \boldsymbol{x} \big(f(\boldsymbol{x}, \boldsymbol{y})\big) = 0 \iff \prod_{\sigma} f(\sigma, \boldsymbol{y}) = 0$$

4. Solution
$$q(\boldsymbol{y}) \cdot x = p(\boldsymbol{y})$$

$$\Updownarrow$$

$$p(\boldsymbol{y}) \cdot \big(p(\boldsymbol{y}) - q(\boldsymbol{y})\big) = 0 \quad \& \quad \exists v \colon x = \sum_{\tau \colon p(\tau) = q(\tau) \neq 0} \boldsymbol{y}^{\tau} + v \cdot \sum_{\tau \colon p(\tau) = q(\tau) = 0} \boldsymbol{y}^{\tau}$$

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.

$$f_1(\boldsymbol{x}) = 0, \ldots, f_k(\boldsymbol{x}) = 0 \iff \sum_{i=1}^{k} f_i(\boldsymbol{x}) = 0$$

3. Elimination. Given the single premise $\sum_{i=1}^{k} f_i(\boldsymbol{y}, \boldsymbol{z}) = 0$, the most general conclution involving only $\boldsymbol{z}$ is $f(\boldsymbol{z}) = 0$, where

$$f(\boldsymbol{z}) := \left(\sum_{i=1}^{k} f_i(1, \ldots, 1, \boldsymbol{z})\right) \cdot \ldots \cdot \left(\sum_{i=1}^{k} f_i(0, \ldots, 0, \boldsymbol{z})\right)$$

4. Expansion. $f(\boldsymbol{z}) = f(1, \ldots, 1) \cdot z_1 \cdot \ldots \cdot z_n + \ldots + f(0, \ldots, 0) \cdot \overline{z}_1 \cdot \ldots \cdot \overline{z}_n$
5. Translation. Interpret the conclusion-equations as propositions.

Boole's Method — Syllogism

$$\begin{array}{c} MAP \\ SAM \\ \hline SAP \end{array}$$

$$\underbrace{m \cdot \overline{p} = 0 \qquad s \cdot \overline{m} = 0}$$

$$\Big\Downarrow \textit{Reduction}$$

$$m \cdot \overline{p} + s \cdot \overline{m} = 0$$

$$\Big\Downarrow \textit{Elimination}$$

$$(1 \cdot \overline{p} + s \cdot 0) \cdot (0 \cdot \overline{p} + s \cdot 1) = 0$$

$$\Big\Downarrow \textit{Expansion}$$

$$(1 \cdot 0 + 1 \cdot 0) \cdot (0 \cdot 1 + 1 \cdot 1) \cdot s \cdot p + \ldots + (1 \cdot 1 + 0 \cdot 0) \cdot (0 \cdot 1 + 0 \cdot 1) \cdot \overline{s} \cdot \overline{p} = 0$$

$$\Big\Downarrow$$

$$s \cdot \overline{p} = 0$$

$$s \cdot \overline{p} = s \cdot 1 \cdot \overline{p} = s \cdot (m + \overline{m}) \cdot \overline{p} = s \cdot m \cdot \overline{p} + s \cdot \overline{m} \cdot \overline{p} = 0 + 0 = 0$$

Boole's Method — Syllogism

A : $x \cdot \overline{y} = 0$; **E** : $x \cdot y = 0$; **I** : $x \cdot y \neq 0$; **O** : $x \cdot \overline{y} \neq 0$.

$$\begin{array}{c} PAM \\ SOM \\ \hline SOP \end{array}$$

$$p \cdot \overline{m} = s \cdot \overline{m} \cdot p + \overline{s} \cdot \overline{m} \cdot p = 0$$

$$s \cdot \overline{m} = s \cdot \overline{m} \cdot p + s \cdot \overline{m} \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$p \cdot \overline{m} + s \cdot \overline{m} = s \cdot \overline{m} \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$s \cdot \overline{m} \cdot \overline{p} + s \cdot m \cdot \overline{p} = s \cdot \overline{p} \neq 0$$

$$\begin{array}{c} MEP \\ MIS \\ \hline SOP \end{array}$$

$$m \cdot p = s \cdot m \cdot p + \overline{s} \cdot m \cdot p = 0$$

$$m \cdot s = s \cdot m \cdot p + s \cdot m \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$m \cdot p + m \cdot s = s \cdot m \cdot \overline{p} \neq 0$$

$$\Downarrow$$

$$s \cdot m \cdot \overline{p} + s \cdot \overline{m} \cdot \overline{p} = s \cdot \overline{p} \neq 0$$

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.

$$\vDash (\neg h \to h) \land (h \to s) \land (s \leftrightarrow \neg h) \to \neg h \land \neg s$$

$$x =? \implies \vDash (\neg x \to h) \land (x \to s) \land (s \leftrightarrow \neg h) \to \neg h \land \neg s$$

Problem (General Solution?)

$$x =? \implies \vDash \varphi(x)$$

[9] Brown: Boolean Reasoning.

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 — Kiss-Kiss ♡◎♡

Smullyan 实力撩妹 ♡◎♡

1. Smullyan: “我说一句话，如果它是真的，可以给我你的签名吗？”
2. 美女：“可以。”
3. Smullyan: “不过如果我说的不是真的，那就不要给我签名了。”
4. 美女：“好的。”
5. 然后 Smullyan 说了一句话。
6. 美女想了一下，发现她必须给他一个吻！

Application — Kiss-Kiss ♡◎♡

Smullyan 实力撩妹 ♡◎♡

1. Smullyan: “我说一句话，如果它是真的，可以给我你的签名吗？”
2. 美女：“可以。”
3. Smullyan: “不过如果我说的不是真的，那就不要给我签名了。”
4. 美女：“好的。”
5. 然后 Smullyan 说了一句话。
6. 美女想了一下，发现她必须给他一个吻！

Solution

$$(s \cdot x + \overline{s} \cdot \overline{x}) \cdot \overline{k} = 0$$

$$x = \overline{s} \cdot \overline{k} + \theta \cdot (\overline{s} + k)$$

$$\vDash (s \leftrightarrow \neg s \wedge \neg k) \rightarrow k$$

$$\vDash (s \leftrightarrow (s \rightarrow k)) \rightarrow k$$

General Solution of Boolean Equation

Theorem (General Solution of Boolean Equation)

Given the Boolean funciton $f\colon \{0,1\}^n \to \{0,1\}$, *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*

$$\begin{aligned} f_n &:= f \\ f_{i-1}(x_1,\ldots,x_{i-1}) &:= f_i(x_1,\ldots,x_{i-1},0)\cdot f_i(x_1,\ldots,x_{i-1},1) \end{aligned}$$

then

$$\begin{aligned} f_0 &= 0 \\ f_i(x_1,\ldots,x_{i-1},0) \le x_i &\le \overline{f_i(x_1,\ldots,x_{i-1},1)} \qquad (i=1,\ldots,n) \end{aligned}$$

is a genereal solution of $f(x_1,\ldots,x_n)=0$.

Propositional Logic vs Boolean Algebra

$$
\begin{aligned}
(\bot)^* &:= 0 \\
(\top)^* &:= 1 \\
(p)^* &:= p \\
(\neg\varphi)^* &:= \overline{\varphi^*} \\
(\varphi \vee \psi)^* &:= \varphi^* + \psi^* \\
(\varphi \wedge \psi)^* &:= \varphi^* \cdot \psi^*
\end{aligned}
$$

$$
\begin{aligned}
(0)' &:= \bot \\
(1)' &:= \top \\
(p)' &:= p \\
(\overline{\varphi})' &:= \neg\varphi' \\
(\varphi + \psi)' &:= \varphi' \vee \psi' \\
(\varphi \cdot \psi)' &:= \varphi' \wedge \psi'
\end{aligned}
$$

$$\varphi \vdash \psi \iff \mathcal{BA} \vdash \varphi^* \leq \psi^*$$

$$\mathcal{BA} \vdash \varphi \leq \psi \iff \varphi' \vdash \psi'$$

where $x \leq y := x \cdot \overline{y} = 0$

Homomorphism

- Let $\mathcal{A}$ and $\mathcal{B}$ be Boolean algebras. A (Boolean) homomorphism is a mapping $h\colon A \to B$ s.t. for all $a, b \in A$:
  1. $h(0) = 0$
  2. $h(1) = 1$
  3. $h(\overline{a}) = \overline{h(a)}$
  4. $h(a + b) = h(a) + h(b)$
  5. $h(a \cdot b) = h(a) \cdot h(b)$
- If $h\colon A \rightarrowtail B$, it is an isomorphic embedding of $\mathcal{A}$ into $\mathcal{B}$.
- If $h\colon A \rightarrowtail\!\!\!\!\twoheadrightarrow B$, then $\mathcal{A}$ and $\mathcal{B}$ are isomorphic ($\mathcal{A} \cong \mathcal{B}$).

Example — Lindenbaum Algebra of Propositional Logic

Lindenbaum Algebra of Propositional Logic

$$\mathrm{Lin} := \left(\mathrm{WFF}/{\sim}, 0, 1, +, \cdot, {}^{-}\right)$$

where

$$\begin{aligned}
\sim &:= \vdash \\
[\varphi] &:= \{\psi \in \mathrm{WFF} \colon \varphi \sim \psi\} \\
\mathrm{WFF}/{\sim} &:= \{[\varphi] \colon \varphi \in \mathrm{WFF}\} \\
0 &:= [\bot] \\
1 &:= [\top] \\
\overline{[\varphi]} &:= [\neg\varphi] \\
[\varphi] + [\psi] &:= [\varphi \vee \psi] \\
[\varphi] \cdot [\psi] &:= [\varphi \wedge \psi]
\end{aligned}$$

$$2 := \left(\{0,1\}, 0, 1, \max, \min, 1 - \right)$$

$$\mathrm{Lin} \overset{?}{\cong} 2$$

If ν is a truth assignment, then $h \colon [\varphi] \mapsto \nu(\varphi)$ is a homomorphism.

If $h \colon \mathrm{Lin} \to 2$ is a homomorphism, then $\nu \colon \varphi \mapsto h([\varphi])$ is a truth assignment.

Ultrafilter

- A partial order R over A is a binary relation which is reflexive, antisymmetric, and transitive, i.e., for all a, b, and c in A:
  1. Raa
  2. $Rab \wedge Rba \rightarrow a = b$
  3. $Rab \wedge Rbc \rightarrow Rac$
- $\leq$ is a partial order.
- Let $\mathcal{B} = (B, 0, 1, +, \cdot, \overline{})$ be a Boolean algebra. A subset $F \subset B$ is a filter if
  1. $1 \in F$
  2. $a \in F \wedge a \leq b \rightarrow b \in F$
  3. $a \in F \wedge b \in F \rightarrow a \cdot b \in F$
- A filter F is proper if $0 \notin F$.
- A proper filter F is an ultrafilter if either $a \in F$ or $\overline{a} \in F$.
- 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.

Arrow's Impossibility Theorem

Let N be a set of voters, and C a set of candidates. A social welfare function (SWF) is $f\colon \mathcal{S}_C^N \to \mathcal{S}_C$, 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 $\boldsymbol{\pi} \in \mathcal{S}_C^N$, $N^{\boldsymbol{\pi}}_{a \succ b} := \{i \in N \colon a \succ_i b \text{ under } \boldsymbol{\pi}\}$.

- Unanimity ($\boldsymbol{U}$): If all voters rank a above b, then so does society: $N^{\boldsymbol{\pi}}_{a \succ b} = N \implies a \succ_{f(\boldsymbol{\pi})} b$.
- Irrelevant Alternatives ($\boldsymbol{IA}$): the relative social ranking of two candidates only depends on their relative individual rankings: $N^{\boldsymbol{\pi}}_{a \succ b} = N^{\boldsymbol{\pi}'}_{a \succ b} \implies \Big(a \succ_{f(\boldsymbol{\pi})} b \iff a \succ_{f(\boldsymbol{\pi}')} b\Big)$.
- Nondictatorship ($\boldsymbol{ND}$): There is no $i \in N$ s.t. $\pi_i = f(\boldsymbol{\pi})$.

Theorem (Arrow's Impossibility Theorem)

If N is finite and $|C| \geq 3$, then any SWF that satisfy $\boldsymbol{U}$ and $\boldsymbol{IA}$ 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 π with the property that $\{i \in N : \pi_i = \pi\} \in \mathcal{F}$.

Theorem (Arrow's Theorem)

Assume $|C| \geq 3$. There is a $1-1$ correspondence between ultrafilters on N and SWF that satisfy $\boldsymbol{U}$ and $\boldsymbol{IA}$. 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

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 $h : B \to P(\mathrm{Sto}(B))$ by

$$x \mapsto \{w \in \mathrm{Sto}(B) : x \in w\}$$

Then

$$\mathcal{B} \cong (h(B), \emptyset, \mathrm{Sto}(B), \cup, \cap, \setminus)$$

$\boxed{\vDash \varphi \implies \vdash \varphi}$

$$\nvdash \varphi$$
$$\Downarrow$$
$$[\varphi] \neq [\top]$$
$$\Downarrow$$
$$[\neg\varphi] \neq [\bot]$$
$$\Downarrow$$
$$h([\neg\varphi]) \neq \emptyset$$
$$\Downarrow$$
$$\exists w \in \mathrm{Sto}(B)\big([\neg\varphi] \in w\big)$$
$$\Downarrow$$
$$\chi_w([\neg\varphi]) = 1$$

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

Let $2 := \{0,1\}$ be the discrete topology, and $2^{\mathscr{P}}$ be the product topology.
By Tychonoff Theorem, $2^{\mathscr{P}}$ is a compact, Hausdorff space.
For any wff φ, let $\mathrm{Mod}(\varphi) := \left\{\nu \in 2^{\mathscr{P}} : \overline{\nu}(\varphi) = 1\right\}$.
It can be shown that $\mathrm{Mod}(\varphi)$ is clopen in $2^{\mathscr{P}}$.
By hypothesis, for each finite $\Gamma_0 \subset \Gamma$, there is a truth assignment making Γ_0 true, i.e. $\mathrm{Mod}(\Gamma_0) \neq \emptyset$. That is to say, $\{\mathrm{Mod}(\varphi) : \varphi \in \Gamma\}$ has the Finite Intersection Property. By the compactness of $2^{\mathscr{P}}$, $\mathrm{Mod}(\Gamma) \neq \emptyset$.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

Boolean Algebra

Lambda Calculus and Combinatory Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic

9 Logic vs Game Theory

Church 1903-1995

- Lambda Calculus
- Church-Turing Thesis
- Undecidability
- Church-Rosser Theorem
- Frege-Church Ontology

Lambda Calculus

$\mathscr{L} = \{\lambda, .\}$

Definition (λ-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

$$\lambda x.M \stackrel{\alpha}{=} \lambda y.M[y/x] \quad \text{if } y \text{ does not occur in } M.$$

$$(\lambda x.M)N \stackrel{\beta}{=} M[N/x]$$

$$\lambda x.Mx \stackrel{\eta}{=} M \quad \text{if } x \notin \mathrm{Fv}(M)$$

λ-definability

$$\underline{n} := \lambda f x.f^n x$$
$$f^0 x := x$$
$$f^{n+1} x := f(f^n x)$$

Definition (λ-definability)

An n-ary function $f(x_1, \ldots, x_n)$ is λ-definable if there is a λ-term F s.t. for all $a_1, \ldots, a_n$,

$$F\underline{a_1} \ldots \underline{a_n} \overset{\beta}{=} \underline{f(a_1, \ldots, a_n)}$$

$\boxed{\text{A function } f \text{ is computable iff it is } \lambda\text{-definable.}}$

$$add := \lambda mnfx.mf(nfx)$$
$$mult := \lambda mnfx.m(nf)x$$
$$exp := \lambda mn.nm$$

$$\begin{tikzcd}
\mathbb{N}^* \arrow[r, "f"] \arrow[d, "-"'] & \mathbb{N} \arrow[d, "-"] \\
\Lambda^* \arrow[r, "F"] & \Lambda
\end{tikzcd}$$

Combinator

Definition (Combinator)

A λ-term M is called a combinator if $\mathrm{Fv}(M) = \emptyset$.

$$\boldsymbol{K} = \lambda xy.x$$
$$\boldsymbol{S} = \lambda xyz.xz(yz)$$
$$\boldsymbol{I} = \lambda x.x$$
$$\omega = \lambda x.xx$$
$$\Omega = \omega\omega$$
$$Y = \lambda f.(\omega(\lambda x.f(xx)))$$

$$\boldsymbol{F} = \lambda xy.y$$
$$\boldsymbol{T} = \boldsymbol{K}$$
$$\boldsymbol{B} = \boldsymbol{S}(\boldsymbol{KS})\boldsymbol{K}$$
$$\boldsymbol{C} = \boldsymbol{S}(\boldsymbol{BBS})(\boldsymbol{KK})$$
$$\boldsymbol{W} = \boldsymbol{SS}(\boldsymbol{SK})$$
$$\boldsymbol{D} = \boldsymbol{SII}$$
$$\boldsymbol{L} = \boldsymbol{D}(\boldsymbol{BDD})$$
$$\boldsymbol{neg} = \lambda x.x\boldsymbol{FT}$$
$$\boldsymbol{zero} = \lambda x.x(\lambda y.\boldsymbol{F})\boldsymbol{T}$$

$$\iota = \lambda x.x\boldsymbol{SK}$$

$$\boldsymbol{K} = \iota(\iota(\iota\iota))$$
$$\boldsymbol{S} = \iota(\iota(\iota(\iota\iota)))$$

$$\iota\iota x = \boldsymbol{SK}(\boldsymbol{KK})x = x = \boldsymbol{I}x$$

Exercises

- $\boldsymbol{B}xyz = x(yz)$ (composition)
- $\boldsymbol{C}xyz = xzy$ (swap)
- $\boldsymbol{W}xy = xyy$ (duplicate)
- $\boldsymbol{D}x = xx$ (doubling)
- $\boldsymbol{L} = \boldsymbol{L}\boldsymbol{L}$ (self-doubling)

Fixpoint in Lambda Calculus

Theorem (Fixpoint in Lambda Calculus)

For every λ-term F there is a λ-term X s.t. $F\ulcorner X\urcorner = X$.

Proof.

Let $W := \lambda x.F(xx)$ and $X := WW$.

$$Y = \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$$

$$\boldsymbol{O} := Y\boldsymbol{K} \implies \boldsymbol{O}x = \boldsymbol{O} \qquad \boldsymbol{L} := Y\boldsymbol{D} \implies \boldsymbol{L} = \boldsymbol{L}\boldsymbol{L}$$

Corollary

For any λ-term $C(f, \vec{x})$, there exists a λ-term M s.t. for all λ-terms $\vec{N}$

$$M\vec{N} = C(M, \vec{N})$$

Proof.

Let $M := Y(\lambda f\vec{x}.C(f, \vec{x}))$.

Fixpoint Combinator

$$Y = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx)) \qquad \text{Curry}$$

$$\Theta = (\lambda xy.y(xxy))(\lambda xy.y(xxy)) \qquad \text{Turing}$$

$$\text{fac } n = \text{if_then_else (zero } n\text{) (1) (mult } n \text{ (fac (pred } n\text{)))}$$

$$\text{fac} = \lambda n.\text{if_then_else (zero } n\text{) (1) (mult } n \text{ (fac (pred } n\text{)))}$$

$$\text{fac} = (\lambda f.\lambda n.\text{if_then_else (zero } n\text{) (1) (mult } n \text{ (} f \text{ (pred } n\text{)))) fac}$$

$$F := \lambda f.\lambda n.\text{if_then_else (zero } n\text{) (1) (mult } n \text{ (} f \text{ (pred } n\text{)))}$$

$$\text{fac} := YF$$

$$YF = F(YF)$$

$$\text{fac} = F \text{ fac}$$

Church-Rosser Theorem

We write $M \twoheadrightarrow_\beta N$ if M β-reduces to N in zero or more steps.

Definition (β-nf)

A term is in β normal form if it cannot be β-reduced.
A term M has a β normal form if it β reduces to some N that is in β-nf.

Theorem (Church-Rosser Theorem)

Let $\twoheadrightarrow$ denote either $\twoheadrightarrow_\beta$ or $\twoheadrightarrow_{\beta\eta}$. Suppose M, P, Q are λ-terms s.t. $M \twoheadrightarrow P$ and $M \twoheadrightarrow Q$. Then there exists a λ-term N s.t. $P \twoheadrightarrow N$ and $Q \twoheadrightarrow N$.

$$\begin{tikzcd}
 & M \arrow[dl, two heads] \arrow[dr, two heads] & \\
P \arrow[dr, dotted, two heads] & & Q \arrow[dl, dotted, two heads] \\
 & N &
\end{tikzcd}$$

Fixpoint Theorem in Lambda Calculus

We write $\ulcorner M \urcorner$ to denote the λ-term representing the Gödel number of M.

Theorem (Fixpoint Theorem in Lambda Calculus)

For every λ-term F there is a λ-term X s.t. $F\ulcorner X \urcorner = X$.

Proof.

By Church-Turing thesis, there is a term D s.t. $D\ulcorner M \urcorner = \ulcorner\ulcorner M \urcorner\urcorner$.
Furthermore, there is a term A s.t. $A\ulcorner M \urcorner\ulcorner N \urcorner = \ulcorner MN \urcorner$.
Take $G := \lambda n.F(An(Dn))$. Then let $X := G\ulcorner G \urcorner$.

$$\begin{aligned} X &= G\ulcorner G \urcorner \\ &= F(A\ulcorner G \urcorner(D\ulcorner G \urcorner)) \\ &= F(A\ulcorner G \urcorner(\ulcorner\ulcorner G \urcorner\urcorner)) \\ &= F\ulcorner G\ulcorner G \urcorner\urcorner \\ &= F\ulcorner X \urcorner \end{aligned}$$

Undecidability

Theorem (Church1936)

There is no term that will decide whether two terms have the same normal form.

Theorem (Church1936)

There is no λ-term D s.t. for all $\underline{n}$,

$$D\underline{n} = \begin{cases} \underline{0} & \textit{if term with Gödel number } n \textit{ has a } \beta\textit{-nf} \\ \underline{1} & \textit{otherwise} \end{cases}$$

Proof.

Suppose there was such a D. Then define $G := \lambda n.\boldsymbol{zero}(Dn)\Omega\boldsymbol{I}$.
By the fixpoint theorem, there is X s.t. $G(\ulcorner X \urcorner) = X$.
X has a β-nf $\implies D\ulcorner X \urcorner = \underline{0} \implies G\ulcorner X \urcorner = \Omega \implies X$ has no β-nf
X has no β-nf $\implies D\ulcorner X \urcorner = \underline{1} \implies G\ulcorner X \urcorner = \boldsymbol{I} \implies X$ has a β-nf

Undecidability

Theorem (Church1936)

There is no D s.t. for all M,

$$DM = \begin{cases} \boldsymbol{T} & \text{if } M \text{ has a normal form} \\ \boldsymbol{F} & \text{otherwise} \end{cases}$$

Proof.

let $G := \boldsymbol{C}(\boldsymbol{C}(\boldsymbol{B}D(\boldsymbol{SII}))\Omega)\boldsymbol{I}$ and $X := GG$. Then

$$X = D(X)\Omega\boldsymbol{I}$$

If X has a normal form, then $D(X)\Omega\boldsymbol{I} = \Omega$, but Ω has no normal form.
If X has no normal form, then $D(X)\Omega\boldsymbol{I} = \boldsymbol{I}$, but $\boldsymbol{I}$ 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 $Q \in \Lambda \setminus A$.

$$G := \lambda n.\boldsymbol{zero}(Dn)QP$$

$$G \in B \iff D\ulcorner G\urcorner = \underline{0} \implies G\ulcorner G\urcorner = Q \implies G\ulcorner G\urcorner \notin A \implies G \notin B$$
$$G \notin B \iff D\ulcorner G\urcorner = \underline{1} \implies G\ulcorner G\urcorner = P \implies G\ulcorner G\urcorner \in A \implies G \in B$$

Combinatory Logic

Definition (Combinatory Terms)

$$C ::= x \mid \boldsymbol{K} \mid \boldsymbol{S} \mid (CC)$$

Reduction

$$\boldsymbol{K}MN = M$$
$$\boldsymbol{S}MNL = ML(NL)$$

- $\varphi_k(x, y) = x$
- $\varphi_s(x, y, z) = \varphi_{\varphi_x(z)}(\varphi_y(z))$

Combinatory Completeness

Proposition (Combinatory Completeness)

For every λ-term P and variable x, there is a combinator $\lambda^* x.P$ s.t.

$$(\lambda^* x.P)Q = P[Q/x]$$

Proof.

$$\lambda^* x.P := \begin{cases} \boldsymbol{I} & \text{if } P \equiv x \\ \boldsymbol{K}P & \text{if } x \notin \mathrm{Fv}(P) \\ \boldsymbol{S}(\lambda^* x.M)(\lambda^* x.N) & \text{if } P \equiv MN \end{cases}$$

Lambda Calculus subsumes Combinatory Logic

M	$(M)_\lambda$
$\boldsymbol{I}$	$\lambda x.x$
$\boldsymbol{K}$	$\lambda xy.x$
$\boldsymbol{S}$	$\lambda xyz.xz(yz)$
PQ	$(P)_\lambda(Q)_\lambda$

Table: translation: $()_\lambda : \boldsymbol{CL} \to \Lambda$

$$\vdash_{\boldsymbol{CL}} M = N \implies \vdash_\lambda (M)_\lambda = (N)_\lambda$$

But not the other way around:
$\nvdash_{\boldsymbol{CL}} \boldsymbol{SKI} = \boldsymbol{I}$, $\vdash_\lambda (\boldsymbol{SKI})_\lambda = (\boldsymbol{I})_\lambda$.

Combinatory Logic subsumes Lambda Calculus

M	$(M)_{\boldsymbol{C}}$
x	x
$\lambda x.P$	$\lambda^* x.(P)_{\boldsymbol{C}}$
PQ	$(P)_{\boldsymbol{C}}(Q)_{\boldsymbol{C}}$

Table: translation: $()_{\boldsymbol{C}} : \Lambda \to \boldsymbol{CL}$

$$\vdash_{\lambda} M = N \iff \vdash_{\boldsymbol{CL}} (M)_{\boldsymbol{C}} = (N)_{\boldsymbol{C}}$$

Simply-Typed Lambda Calculus (STLC)

- Type

$$T ::= 1 \mid T \times T \mid T \to T$$

- Term

$$\Lambda ::= x \mid * \mid \Lambda\Lambda \mid \lambda x.\Lambda \mid \langle \Lambda, \Lambda \rangle \mid \pi_1 \Lambda \mid \pi_2 \Lambda$$

- Judgement

$$x_1 : T_1, \ldots, x_n : T_n \vdash t : T$$

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 β/η-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

$$
\dfrac{\dfrac{\dfrac{\dfrac{[x : A \to B \to C]^3 \qquad [z : A]^1}{xz : B \to C} \qquad \dfrac{[y : A \to B]^2 \qquad [z : A]^1}{yz : B}}{xz(yz) : C}}{\lambda z.xz(yz) : A \to C}\,[\to^+]^1}{\lambda y.\lambda z.xz(yz) : (A \to B) \to A \to C}\,[\to^+]^2}{\lambda x.\lambda y.\lambda z.xz(yz) : (A \to B \to C) \to (A \to B) \to A \to C}\,[\to^+]^3
$$

- $\boldsymbol{I} := \lambda x.x : A \to A$
- $\boldsymbol{K} := \lambda x.\lambda y.x : A \to B \to A$
- $\boldsymbol{S} := \lambda x.\lambda y.\lambda z.xz(yz) : (A \to B \to C) \to (A \to B) \to A \to C$

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* $\Gamma \vdash w : A$.

Category

Definition (Category)

A category $\mathcal{C}$ consists of a class of objects $\mathrm{Ob}(\mathcal{C})$ and a class of arrows $\mathcal{C}(A, B) := \{f \colon A \to B\}$ for $A, B \in \mathrm{Ob}(\mathcal{C})$ with the following properties:

- for $A \in \mathrm{Ob}(\mathcal{C})$, there exists the identity $1_A \in \mathcal{C}(A, A)$;
- for $A, B, C \in \mathrm{Ob}(\mathcal{C})$, there exists the composition $\circ \colon \mathcal{C}(A, B) \times \mathcal{C}(B, C) \to \mathcal{C}(A, C)$ such that
  - $\forall AB \in \mathrm{Ob}(\mathcal{C}) \forall f \colon A \to B \left[f \circ 1_A = f \ \& \ 1_B \circ f = f \right]$
  - $\forall ABCD \in \mathrm{Ob}(\mathcal{C}) \forall fgh \colon A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \left[h \circ (g \circ f) = (h \circ g) \circ f \right]$

- **Set** sets and functions.
- **Rel** sets and relations.
- **Type** types and computable functions.
- **Grp** groups and homomorphisms.
- **Ab** abelian groups and homomorphisms.
- **Rng** rings and ring homomorphisms.
- **Vec** vector spaces and linear maps.
- **Top** topological spaces and continuous functions.

Initial/Terminal Object & Product/Coproduct

- A *initial* object in $\mathcal{C}$ is an object 0 s.t. for every object A, there is a unique arrow $0 \to A$.
- A *terminal* object in $\mathcal{C}$ is an object 1 s.t. for every object A, there is a unique arrow $A \to 1$.
- A *product* of A and B is an object $A \times B$ together with a pair of arrows $A \xleftarrow{\pi_1} A \times B \xrightarrow{\pi_2} B$ s.t
$$\forall C \forall f g \colon A \xleftarrow{f} C \xrightarrow{g} B \; \exists! h \colon C \to A \times B \big[f = \pi_1 \circ h \;\; \& \;\; g = \pi_2 \circ h \big]$$
- A *coproduct* of A and B is an object $A + B$ together with a pair of arrows $A \xrightarrow{\iota_1} A + B \xleftarrow{\iota_2} B$ s.t
$$\forall C \forall f g \colon A \xrightarrow{f} C \xleftarrow{g} B \; \exists! h \colon A + B \to C \big[f = h \circ \iota_1 \;\; \& \;\; g = h \circ \iota_2 \big]$$

$$\begin{tikzcd}
A & A \times B \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & B \\
& C \arrow[ul, "f"] \arrow[u, dashed, "!h"] \arrow[ur, "g"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\iota_1"] \arrow[dr, "f"'] & A + B \arrow[d, dashed, "!h"] & B \arrow[l, "\iota_2"'] \arrow[dl, "g"] \\
& C &
\end{tikzcd}$$

Exponential & Cartesian Closed Category (CCC)

- An *exponential* of objects A, B is an object B^A together with an arrow $\varepsilon\colon B^A \times A \to B$ s.t.

$$\forall C \forall f\colon C \times A \to B\ \exists! \lambda f\colon C \to B^A \left[\varepsilon \circ (\lambda f \times 1_A) = f\right]$$

$$\begin{tikzcd}
B^A & B^A \times A \arrow[r, "\varepsilon"] & B \\
C \arrow[u, dashed, "\lambda f"] & C \times A \arrow[u, dashed, "\lambda f \times 1_A"] \arrow[ur, "f"'] &
\end{tikzcd}$$

- **Cartesian Closed Category (CCC)** is a category with a terminal object, products and exponentials.

Curry-Howard-Lambek Isomorphism

- **Objects** types/formulas $\top \mid A \times B \mid A \to B$
- **Arrows** terms/proofs $1_A \mid * \mid \varepsilon \mid \pi_1 \mid \pi_2 \mid \lambda f \mid \langle f, g \rangle \mid g \circ f$
  $f : A \to B \iff A \vdash B$

$$\frac{}{1_A : A \vdash A} \qquad \frac{}{* : A \vdash \top} \qquad \frac{f : A \vdash B \qquad g : B \vdash C}{g \circ f : A \vdash C}$$

$$\frac{f : A \vdash B \qquad g : A \vdash C}{\langle f, g \rangle : A \vdash B \times C} \qquad \frac{}{\pi_1 : A \times B \vdash A} \qquad \frac{}{\pi_2 : A \times B \vdash B}$$

$$\frac{f : A \times B \vdash C}{\lambda f : A \vdash B \to C} \qquad \frac{}{\varepsilon : (A \to B) \times A \vdash B}$$

Curry-Howard-Lambek Isomorphism

Logic	**Type Theory**	**Categories**
Formula	Type	Object
Proof	Term/Program	Arrow
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	β-reduction	composition $\circ$
modus ponens	application app	evaluation ε

Curry-Howard-Lambek Isomorphism

$$\begin{tikzcd}
\mathit{Logic} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \mathit{Computation} \arrow[dl, leftrightarrow] \\
& \mathit{Categories} &
\end{tikzcd}$$

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

Functor

Definition (Functor)

A functor $F\colon \mathcal{C} \to \mathcal{D}$ between categories $\mathcal{C}$ and $\mathcal{D}$ is a mapping of objects to objects and arrows to arrows, in such a way that:

- $F(f\colon A \to B) = Ff\colon FA \to FB$
- $F(1_A) = 1_{FA}$
- $F(g \circ f) = Fg \circ Ff$

identity functor $1_{\mathcal{C}}$ and composition of functors

$$1_{\mathcal{C}} \quad \begin{tikzcd} A \arrow[d, "f"] \\ B \end{tikzcd} \quad = \quad \begin{tikzcd} A \arrow[d, "f"] \\ B \end{tikzcd} \qquad\qquad G \circ F \quad \begin{tikzcd} A \arrow[d, "f"] \\ B \end{tikzcd} \quad = \quad \begin{tikzcd} G(FA) \arrow[d, "G(Ff)"] \\ G(FB) \end{tikzcd}$$

Natural Transformation

Definition (Natural Transformation)

Given categories and functors $F, G \colon \mathcal{C} \to \mathcal{D}$, a natural transformation $\eta \colon F \to G$ is a family of $\mathcal{D}$-arrows $\{\eta_A \colon FA \to GA\}_{A \in \mathrm{ob}(\mathcal{C})}$, such that for all $\mathcal{C}$-arrows $f \colon A \to B$, the diagram commutes:

$$\begin{tikzcd}
FA \arrow[r, "Ff"] \arrow[d, "\eta_A"'] & FB \arrow[d, "\eta_B"] \\
GA \arrow[r, "Gf"'] & GB
\end{tikzcd}$$

Equivalence of Categories

Definition (Natural Isomorphism)

A natural transformation $\eta\colon F \to G$ is a natural isomorphism ($F \cong G$) if each arrow $\eta_A\colon FA \to GA$ is an isomorphism.

Definition (Equivalence of Categories)

The categories $\mathcal{C}$ and $\mathcal{D}$ are equivalent ($\mathcal{C} \simeq \mathcal{D}$) if there are functors $\mathcal{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{D}$ and natural isomorphisms $G \circ F \cong 1_{\mathcal{C}}, F \circ G \cong 1_{\mathcal{D}}$.

- The categories $\mathcal{C}$ and $\mathcal{D}$ are isomorphic ($\mathcal{C} \cong \mathcal{D}$) if there are functors $\mathcal{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{D}$ satisfying $G \circ F = 1_{\mathcal{C}}, F \circ G = 1_{\mathcal{D}}$.
- Equivalence of categories is a generalization of isomorphism. It can be seen as "isomorphism up to isomorphism".

Product Category

Definition (Product Category)

Given categories $\mathcal{C}$ and $\mathcal{D}$, the product category $\mathcal{C} \times \mathcal{D}$ has

- objects (A, B) for $A \in \mathrm{ob}(\mathcal{C})$ and $B \in \mathrm{ob}(\mathcal{D})$.
- arrows $(f, g) \colon (A, B) \to (A', B')$ for $f \in \mathcal{C}(A, A')$ and $g \in \mathcal{D}(B, B')$.
- identity $1_{(A,B)} := (1_A, 1_B)$.
- composition $(f', g') \circ (f, g) := (f' \circ f, g' \circ g)$.

Functor Category

Definition (Functor Category)

Given categories $\mathcal{C}$ and $\mathcal{D}$, the functor category $\mathcal{D}^{\mathcal{C}}$ has

- objects: functors $F\colon \mathcal{C} \to \mathcal{D}$
- arrows: natural transformations $\eta\colon F \to G$
- identity natural transformation $(1_F)_A := 1_{FA}$
  given a functor $F\colon \mathcal{C} \to \mathcal{D}$, define $1_F : F \to F$ with
  $(1_F)_A := FA \xrightarrow{1_{FA}} FA$.
- composition of natural transformations $(\theta \circ \eta)_A := \theta_A \circ \eta_A$
  given functors $F, G, H\colon \mathcal{C} \to \mathcal{D}$ and natural transformations
  $F \xrightarrow{\eta} G \xrightarrow{\theta} H$, define $\theta \circ \eta\colon F \to H$ with

$$(\theta \circ \eta)_A := FA \xrightarrow{\eta_A} GA \xrightarrow{\theta_A} HA$$

The Category of Small Categories **Cat**

- Assume there is an infinite sequence $U_0 \in U_1 \in U_2 \in \dots$ of bigger and bigger Grothendieck universes.
- $\mathbf{Set}_n$ = category whose objects are the sets in U_n and with $\mathbf{Set}_n(A, B) = B^A$ = the functions from A to B.
- A category $\mathcal{C}$ is locally small if $\forall AB \in \mathcal{C} \colon \mathcal{C}(A, B) \in \mathbf{Set}_0$.
- A category $\mathcal{C}$ is small if it is both locally small and $\mathrm{ob}(\mathcal{C}) \in \mathbf{Set}_0$.

Definition (The Category of Small Categories Cat)

The category of small categories **Cat** has

- objects: small categories.
- arrows: functors $F \colon \mathcal{C} \to \mathcal{D}$.
- identity and composition as for functors.

Cat is large.

Cat is CCC

- **Cat** has a terminal object $1 := \bullet \circlearrowleft 1_{\bullet}$.
- **Cat** has products.
- There is a functor $\varepsilon \colon \mathcal{D}^{\mathcal{C}} \times \mathcal{C} \to \mathcal{D}$ that makes $\mathcal{D}^{\mathcal{C}}$ the exponential.
- **Cat** is cartesian closed.

Left/Right Adjoint

Definition (Left/Right Adjoint)

Functors $\mathcal{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{D}$ are adjoint if there are natural isomorphisms

$$\mathcal{D}(F(A), B) \cong \mathcal{C}(A, G(B))$$

Then F is left adjoint to G and G is right adjoint to F, notated $F \dashv G$.

Example

Assume $R \subset X \times Y$, and take the projection function $\pi_1 \colon X \times Y \to X$, then the function π_1^{-1} has both a left adjoint $\exists \colon P(X) \to P(Y)$ and a right adjoint $\forall \colon P(X) \to P(Y)$. For $A \subset X, R \subset X \times Y$:

$$\exists(R) \subset A \iff R \subset \pi_1^{-1}(A) \qquad \pi_1^{-1}(A) \subset R \iff A \subset \forall(R)$$

$$\boxed{\text{Quantifiers are Adjoints: } \exists \dashv \pi_1^{-1} \dashv \forall}$$

$$\exists(R) := \{x \in X \colon \exists y \in Y \colon Rxy\} \qquad \forall(R) := \{x \in X \colon \forall y \in Y \colon Rxy\}$$

Galois Connection

Definition (Galois Connection)

- Let $(\mathcal{C}, \prec)$ and $(\mathcal{D}, \sqsubset)$ be two partially ordered sets. A monotone Galois connection between these posets consists of two monotone functions: $F\colon \mathcal{C} \to \mathcal{D}, G\colon \mathcal{D} \to \mathcal{C}$ s.t.,
$$\forall A \in \mathcal{C} \forall B \in \mathcal{D}\colon F(A) \sqsubset B \iff A \prec G(B)$$
- Let $(\mathcal{C}, \prec)$ and $(\mathcal{D}, \sqsubset)$ be two partially ordered sets. An antitone Galois connection between these posets consists of two order-reversing functions: $F\colon \mathcal{C} \to \mathcal{D}, G\colon \mathcal{D} \to \mathcal{C}$ s.t.,
$$\forall A \in \mathcal{C} \forall B \in \mathcal{D}\colon B \sqsubset F(A) \iff A \prec G(B)$$

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 $\mathcal{C}$ and $\mathcal{D}$ is just a monotone Galois connection between $\mathcal{C}$ and the order dual $\mathcal{D}^{\mathrm{op}}$.
- 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

$$F^* := \mathrm{Aut}(L/F) := \left\{\sigma \in \mathrm{Aut}(L) \colon \forall x \in F\big(\sigma(x) = x\big)\right\}$$

$$H^\dagger := \left\{x \in L \colon \forall \sigma \in H\big(\sigma(x) = x\big)\right\}$$

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. $F^* \lhd G \implies \mathrm{Aut}(F/K) \cong G/F^*$.

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Welcome to Cantor's Paradise

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
   - Axioms of ZFC
   - Ordinal Numbers
   - Cardinal Numbers
   - Axiom of Choice
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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 φ, there exists a set $Y = \{x : \varphi(x)\}$.

$$R := \{x : x \notin x\} \quad R \in R? \qquad \text{(Russell Paradox)}$$

- **Separation Schema**.
  For any formula φ, for any X, there exists a set $Y = \{u \in X : \varphi(x)\}$.

$$\forall X \exists Y \forall u(u \in Y \leftrightarrow u \in X \wedge \varphi(x))$$

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 $Y = P(X) := \{u : u \subset X\}$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \forall z (z \in u \to z \in X))$$

- **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.

$$(a, b) := \{\{a\}, \{a, b\}\}$$
$$(a_1, \ldots, a_{n+1}) := ((a_1, \ldots, a_n), a_{n+1})$$

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \to a_i = b_i \quad \text{for} \quad 1 \leq i \leq n$$

$$X \subsetneq Y \quad X \cup Y \quad X \cap Y \quad X \setminus Y \quad X \Delta Y \quad X \times Y \quad \prod_{i=1}^{n} X_i \quad X^n$$

- n-ary relation R on $X_1, \ldots, X_n$.

$$R \subset \prod_{i=1}^{n} X_i$$

$$R(x_1, \ldots, x_n) := (x_1, \ldots, x_n) \in R$$

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 $\mathscr{X} \subset P(X)$ is a partition of X if
  1. $\forall xy \in \mathscr{X} : x \neq y \to x \cap y = \emptyset$
  2. $\bigcup \mathscr{X} = X$
- $X/\!\sim$ is a partition of X.
- $R \subset X^2$ is an equivalence relation iff there is a partition $\mathscr{X}$ of X s.t $R(x, y) \iff \exists A \in \mathscr{X}\,(x, y \in A)$.

Function

- A n-ary operation $f\colon \prod_{i=1}^{n} X_i \to Y$ is a function if

$$(\boldsymbol{x}, y) \in f \wedge (\boldsymbol{x}, z) \in f \to y = z$$

- injection (one-to-one). $f\colon X \rightarrowtail Y$

$$f(x) = f(y) \to x = y$$

- surjection (onto). $f\colon X \twoheadrightarrow Y$.

$$\forall y \in Y \exists x \in X (f(x) = y)$$

- bijection. $f\colon X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$
- 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

$$
\begin{aligned}
f\colon X \rightarrowtail Y \quad & \text{iff} \quad \exists g\colon Y \to X\colon gf = 1_X \\
& \text{iff} \quad \forall Z \forall g_1 g_2\colon Z \to X\colon fg_1 = fg_2 \implies g_1 = g_2 \\
f\colon X \twoheadrightarrow Y \quad & \text{iff} \quad \exists g\colon Y \to X\colon fg = 1_Y \\
& \text{iff} \quad \forall Z \forall g_1 g_2\colon Y \to Z\colon g_1 f = g_2 f \implies g_1 = g_2
\end{aligned}
$$

$$
\begin{tikzcd}
X \arrow[r, "f"] \arrow[rr, bend right, "1_X"'] & Y \arrow[r, "g"] & X
\end{tikzcd}
\qquad
\begin{tikzcd}
Y \arrow[r, "g"] \arrow[rr, bend right, "1_Y"'] & X \arrow[r, "f"] & Y
\end{tikzcd}
$$

$$
\begin{tikzcd}
Z \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_1"'] & X \arrow[r, "f"] & Y
\end{tikzcd}
\qquad
\begin{tikzcd}
X \arrow[r, "f"] & Y \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_1"'] & Z
\end{tikzcd}
$$

$f\colon X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$ iff the diagram commutes:

$$
\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "1_X"'] & Y \arrow[d, "g"] \arrow[dr, "1_Y"] & \\
& X \arrow[r, "f"'] & Y
\end{tikzcd}
$$

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.

$$\forall xyz(\varphi(x,y) \wedge \varphi(x,z) \to y = z) \to \forall X \exists Y \forall y(y \in Y \leftrightarrow \exists x \in X \varphi(x,y))$$

- **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.

$$\forall X \left[\emptyset \notin X \to \exists f \colon X \to \bigcup X \;\; \forall A \in X\, (f(A) \in A)\right]$$

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
   - Axioms of ZFC
   - Ordinal Numbers
   - Cardinal Numbers
   - Axiom of Choice
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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") $\mathrm{Card}(x) \;:=\; \mathrm{Ord}(x) \wedge \forall y \in x(|y| \neq |x|)$

$$|M| = |N| \;:=\; \exists f\colon M \rightarrowtail\!\!\!\!\twoheadrightarrow N \qquad |M| \leq |N| \;:=\; \exists f\colon M \rightarrowtail N$$

$$|M| := \min\{\alpha \in \mathrm{Ord}\colon |\alpha| = |M|\}$$

The infinite ordinal numbers that are cardinals are called alephs.

Ordinal

$$\alpha < \beta := \alpha \in \beta$$

- $\emptyset$ is an ordinal.
- If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.
- If $\alpha \neq \beta$ are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.
- If α, β are ordinals, then either $\alpha \subset \beta$ or $\beta \subset \alpha$.
- $<$ is a linear ordering of the class *Ord*.
- For each α, $\alpha = \{\beta \colon \beta < \alpha\}$.
- 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 α, $\alpha \cup \{\alpha\}$ is an ordinal and $\alpha \cup \{\alpha\} = \inf\{\beta \colon \beta > \alpha\}$.

Natural Number $\mathbb{N}$

什么是“数”？什么是“无穷”？什么是“超穷”？

$$\alpha + 1 := \alpha \cup \{\alpha\}$$

$$0 := \emptyset, \quad 1 := 0 + 1, \quad 2 := 1 + 1, \quad 3 := 2 + 1, \ldots$$

- 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.

$$\mathbb{N} := \left\{ n : \forall A \left(\emptyset \in A \wedge \forall x \in A (x + 1 \in A) \rightarrow n \in A \right) \right\}$$

- A set A is finite if $\exists n \in \mathbb{N} : |A| = n$.
- A set A is countable if $|A| \leq |\mathbb{N}|$.

Integer $\mathbb{Z}$

$$(m,n) \sim (p,q) := m +_{\mathbb{N}} q = p +_{\mathbb{N}} n$$

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim$$

$$\begin{aligned}
0_{\mathbb{Z}} &:= [(0,0)] \\
[(m,n)] \leq_{\mathbb{Z}} [(p,q)] &:= m +_{\mathbb{N}} q \leq_{\mathbb{N}} p +_{\mathbb{N}} n \\
[(m,n)] +_{\mathbb{Z}} [(p,q)] &:= [(m +_{\mathbb{N}} p, n +_{\mathbb{N}} q)] \\
[(m,n)] \cdot_{\mathbb{Z}} [(p,q)] &:= [(m \cdot_{\mathbb{N}} p + n \cdot_{\mathbb{N}} q, m \cdot_{\mathbb{N}} q + n \cdot_{\mathbb{N}} p)] \\
- [(m,n)] &:= [(n,m)]
\end{aligned}$$

$$\mathbb{Z}^+ := \{x \in \mathbb{Z} \colon x >_{\mathbb{Z}} 0_{\mathbb{Z}}\}$$

$$\exists f \colon \mathbb{N} \to \mathbb{Z} \quad n \mapsto [(n,0)]$$

Rational Number $\mathbb{Q}$

$$(m,n) \sim (p,q) := m \cdot_{\mathbb{Z}} q = p \cdot_{\mathbb{Z}} n$$

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^{+} / \sim$$

$$0_{\mathbb{Q}} := [(0_{\mathbb{Z}}, x)]$$

$$1_{\mathbb{Q}} := [(x,x)]$$

$$[(m,n)] \leq_{\mathbb{Q}} [(p,q)] := m \cdot_{\mathbb{Z}} q \leq_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n$$

$$[(m,n)] +_{\mathbb{Q}} [(p,q)] := [(m \cdot_{\mathbb{Z}} q +_{\mathbb{Z}} p \cdot_{\mathbb{Z}} n, n \cdot_{\mathbb{Z}} q)]$$

$$[(m,n)] \cdot_{\mathbb{Q}} [(p,q)] := [(m \cdot_{\mathbb{Z}} p, n \cdot_{\mathbb{Z}} q)]$$

$$- [(m,n)] := [(-m,n)]$$

$$\exists f : \mathbb{Z} \to \mathbb{Q} \quad x \mapsto [(x,1)]$$

Dedekind Cut and Real Number $\mathbb{R}$

Definition (Real Number)

$\mathbb{R}$ is the set of all $x \in P(\mathbb{Q})$ s.t.

- $x \neq \emptyset,\ x \neq \mathbb{Q}$
- $\forall p \in x \exists q \in x\colon p < q$
- $\forall pq \in x\colon p \in x \wedge q < p \to q \in x$

Theorem (Least-upper-bound)

Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound.

$$\exists f\colon \mathbb{Q} \to \mathbb{R} \quad x \mapsto \{q \in \mathbb{Q}\colon q < x\}$$

$$x \leq_{\mathbb{R}} y := x \subset y$$

$$x +_{\mathbb{R}} y := \{p +_{\mathbb{Q}} q\colon p \in x \ \&\ q \in y\}$$

$$-x := \{q \in \mathbb{Q}\colon \exists p > q(-p \notin x)\}$$

$$|x| := x \cup -x$$

$$x \cdot_{\mathbb{R}} y := \begin{cases} \{r\colon r \leq p \cdot_{\mathbb{Q}} q \ \&\ p \in x \ \&\ q \in y\} & \text{if } x > 0, y > 0 \\ 0 & \text{if } x = 0 \text{ or } y = 0 \\ |x| \cdot_{\mathbb{R}} |y| & \text{if } x < 0, y < 0 \\ -(|x| \cdot_{\mathbb{R}} |y|) & \text{if } x < 0, y > 0 \text{ or } x > 0, y < 0 \end{cases}$$

Ordinal

$0, 1, 2, 3, \ldots$

$\omega, \omega+1, \omega+2, \ldots$

$\omega \cdot 2, (\omega \cdot 2)+1, (\omega \cdot 2)+2, \ldots$

$\vdots$

$\omega^2, \omega^2+1, \omega^2+2, \ldots$

$\vdots$

$\omega^\omega, \omega^\omega+1, \omega^\omega+2, \ldots$

$\vdots$

$\omega^{\omega^\omega}, \ldots$

$\vdots$

$\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}, \ldots$

$\vdots$

Theorem (Transfinite Induction Theorem)

Given a well ordered set A, let P be a property. Then

$$P(\min(A)) \wedge \forall x \in A[\forall y < x\, P(y) \to P(x)] \to \forall x \in A\, P(x)$$

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

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

$$F_n^2 + F_{n+1}^2 = F_{2n+2} \quad \text{and} \quad F_{n+1}^2 + 2F_nF_{n+1} = F_{2n+3}$$

Problem

For all natural numbers n, $n \not< n$.

Induction — Example? $^{\circledcirc}\hat{o}^{\circledcirc}$

All horses are the same color. $^{\odot}\hat{\nabla}^{\odot}$

假设命题 $P(k)$ 表示 k 匹马的颜色相同；显然，$P(1)$ 成立；给定 $k+1$ 匹马，移除一匹马; 根据假设，剩下的 k 匹马的颜色相同。放回被移除的马并移除另一匹马; 根据假设，k 匹马的颜色相同。重复这个过程，直到穷尽 $k+1$ 个 k 匹马的集合，它们的颜色都相同。因此 $P(k+1)$ 成立。

All positive integers are interesting. $^{\&}\hat{o}^{\&}$

假设有无趣的正整数，那么，无趣的正整数集必有最小元。但最小元很有趣！把这个最小元移到有趣数的集合，剩下的无趣集仍有最小元……

Induction — Example? ◎ô◎

突击考试悖论 ◎Δ̂◎

老师宣布："下周将会有一个突击考试，但你们事先无法知道一周中究竟哪一天考试。"
学生们争辩说这个突击考试不可能进行：

- 首先不可能在最后一天举行，因为否则在考试的前一晚就应该知道第二天将进行考试。
- 由于最后一天已经被排除，所以同样的逻辑适用于最后一天的前一天。
- 同样，所有的日子都可以从列表中删除。
- 所以，老师根本不可能进行一场突击考试。

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.

$$P(F_1) = P\left(\bigcap_{n=1}^{\infty} E_n\right) = \lim_{n\to\infty} P(E_n) = \prod_{i=1}^{\infty} \frac{9n}{9n+1} = 0$$

$$\forall i\colon P(F_i) = 0 \implies P\left(\bigcup_{i=1}^{\infty} F_i\right) \le \sum_{i=1}^{\infty} P(F_i) = 0$$

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 α.

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

$$(7,6) \quad (\omega \cdot 2 + 1, \omega \cdot 2) \quad (\tfrac{19}{8}, \tfrac{39}{16})$$

Well-Founded Relation

- $R \subset A^2$ is *set-like* if $ext_R(x) := \{y \in A \colon Ryx\}$ 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 $x \in A$,

$$F(x) = G(x, F\restriction_{ext_R(x)})$$

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 $A' = A$.

$$\boxed{\text{Every perfect set has cardinality } 2^{\aleph_0}.}$$

- $rank(A) := \mu\alpha[A_\alpha = A_{\alpha+1}]$ 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 $P := A_{rank(A)}$. Then

$$A \setminus P = \bigcup_{\alpha < rank(A)} \left(A_\alpha \setminus A'_\alpha\right)$$

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 α s.t. a is an isolated point of A_α.
Let $f(a) := \mu k[A_\alpha \cap J_k = \{a\}]$. Then $f : A \setminus P \to \mathbb{N}$ 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 formulas

$$a_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \cos nt \, \mathrm{d}t$$
$$b_n := \frac{1}{\pi} \int_0^{2\pi} f(t) \sin nt \, \mathrm{d}t$$

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 $A_{rank(A)} = \emptyset$, 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

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
   - Axioms of ZFC
   - Ordinal Numbers
   - Cardinal Numbers
   - Axiom of Choice
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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 $N := \{1, 2, 3, 4\}$.

$$\begin{array}{lcl} \text{apple} & \longleftrightarrow & 1 \\ \text{orange} & \longleftrightarrow & 2 \\ \text{banana} & \longleftrightarrow & 3 \\ \text{grape} & \longleftrightarrow & 4 \end{array}$$

$$|M| = |N| \;:=\; \exists f \colon M \rightarrowtail\!\!\!\!\twoheadrightarrow N$$

A set A is finite if $\exists n \in \mathbb{N} \colon |A| = n$.

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?

$$\begin{array}{lcccr} \text{apple} & \longleftrightarrow & 1 & \longleftrightarrow & \text{John} \\ \text{orange} & \longleftrightarrow & 2 & \longleftrightarrow & \text{Peter} \\ \text{banana} & \longleftrightarrow & 3 & \longleftrightarrow & \text{Bell} \\ \text{grape} & \longleftrightarrow & 4 & \longleftrightarrow & \text{Emma} \\ & & 5 & \longleftrightarrow & \text{Sam} \end{array}$$

$$\begin{array}{lcr} \text{apple} & \longrightarrow & \text{John} \\ \text{orange} & \longrightarrow & \text{Peter} \\ \text{banana} & \longrightarrow & \text{Bell} \\ \text{grape} & \longrightarrow & \text{Emma} \\ & & \text{Sam} \end{array}$$

$$|M| \leq |N| \;:=\; \exists f \colon M \rightarrowtail N$$

$$|M| \leq |N| \;:=\; \exists f \colon N \twoheadrightarrow M$$

$$\begin{array}{lcr} \text{apple} & \longleftarrow & \text{John} \\ \text{orange} & \longleftarrow & \text{Peter} \\ \text{banana} & \longleftarrow & \text{Bell} \\ \text{grape} & \longleftarrow & \text{Emma} \\ & & \text{Sam} \end{array}$$

$$|\mathbb{N}| = |\mathbb{Z}|$$

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 1 \\ 2 & \longleftrightarrow & -1 \\ 3 & \longleftrightarrow & 2 \\ 4 & \longleftrightarrow & -2 \\ 5 & \longleftrightarrow & 3 \\ 6 & \longleftrightarrow & -3 \\ 7 & \longleftrightarrow & 4 \\ 8 & \longleftrightarrow & -4 \\ \vdots & & \vdots \end{array}$$

Dedekind-Infinite

A set A is Dedeking-infinite if some proper subset $B \subsetneq A$ is equinumerous to A.

Figure: Dedekind

Countable?

$$\{0, 1, 2, 3, 4, \ldots\}$$

$$\{1, 3, 5, 7, 9, \ldots\}$$

$$\{0, 2, 4, 6, 8, \ldots\}$$

$$\{0, 1, 4, 9, 16, \ldots\}$$

$$\{2, 3, 5, 7, 11, \ldots\}$$

- 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?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$$

$|\mathbb{N}| = |\mathbb{Q}|$

$$
\begin{tikzcd}
\cdots & {[5]}\ -\frac{2}{1} \arrow[d] & {[4]}\ -\frac{1}{1} & {[0]}\ \frac{0}{1} \arrow[r, mapsto] \arrow[d, dashed] & {[1]}\ \frac{1}{1} \arrow[d] & {[10]}\ \frac{2}{1} \arrow[r] & {[11]}\ \frac{3}{1} \arrow[d] & \cdots \\
\cdots & -\cancel{\frac{2}{2}} \arrow[d] & {[3]}\ -\frac{1}{2} & \cancel{\frac{0}{2}} \arrow[l] \arrow[d, dashed] & {[2]}\ \frac{1}{2} \arrow[l] & \cancel{\frac{2}{2}} & {[12]}\ \frac{3}{2} \arrow[d] & \cdots \\
\cdots & {[6]}\ -\frac{2}{3} \arrow[r] & {[7]}\ -\frac{1}{3} \arrow[r] & \cancel{\frac{0}{3}} \arrow[r] \arrow[d, dashed] & {[8]}\ \frac{1}{3} \arrow[r] & {[9]}\ \frac{2}{3} & \cancel{\frac{3}{3}} \arrow[d] & \cdots \\
\leftarrow & -\cancel{\frac{2}{4}} \arrow[l] & {[15]}\ -\frac{1}{4} \arrow[l] & \cancel{\frac{0}{4}} \arrow[l] & {[14]}\ \frac{1}{4} \arrow[l] & \cancel{\frac{2}{4}} \arrow[l] & {[13]}\ \frac{3}{4} \arrow[l] & \cdots \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{tikzcd}
$$

$$|\mathbb{N}| = |\mathbb{Z}| = |2^{<\omega}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Q}|$$

$|\mathbb{N}| = |\mathbb{Q}^+|$

$$
\begin{array}{ccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$x \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

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.

$$\begin{array}{cccccc} 0\,. & r_{11} & r_{12} & r_{13} & r_{14} & \cdots \\ 0\,. & r_{21} & r_{22} & r_{23} & r_{24} & \cdots \\ 0\,. & r_{31} & r_{32} & r_{33} & r_{34} & \cdots \\ 0\,. & r_{41} & r_{42} & r_{43} & r_{44} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Let $d = 0.d_1 d_2 \ldots$ 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

$$f\colon (0,1] \rightarrowtail\!\!\!\!\twoheadrightarrow (0,1)$$

$$f(x) := \begin{cases} \frac{3}{2} - x & \text{for } \frac{1}{2} < x \leq 1 \\ \frac{3}{4} - x & \text{for } \frac{1}{4} < x \leq \frac{1}{2} \\ \frac{3}{8} - x & \text{for } \frac{1}{8} < x \leq \frac{1}{4} \\ \quad\vdots & \end{cases}$$

$$f(x) := \begin{cases} \frac{x}{x+1} & \text{if } \exists n \in \mathbb{N}\colon x = \frac{1}{n} \\ x & \text{otherwise} \end{cases}$$

Continuum

Continuum

Theorem

$$|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$$

Proof.

$$\begin{array}{lcccccc} x = & 0.3 & 01 & 2 & 007 & 08\ldots \\ y = & 0.009 & 2 & 05 & 1 & 0003\ldots \end{array}$$

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0003\ \ldots$$

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)

$$|X| < |P(X)|$$

Proof.

If $f : X \to P(X)$, 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 cannot be a set!

$$\forall d \in I\colon\ |S_d| \leq \left|\bigcup_{c \in I} S_c\right| < \left|P\left(\bigcup_{c \in I} S_c\right)\right|$$

where S_c is a representative set that has cardinality c.

Cantor's Continuum Hypothesis

Cantor's Continuum Hypothesis (CH)

$$2^{\aleph_0} \stackrel{?}{=} \aleph_1$$

Cantor-Schröder-Bernstein Theorem

Theorem (Cantor-Schröder-Bernstein Theorem)

$$\left.\begin{array}{l} |M| \leq |N| \\ |N| \leq |M| \end{array}\right\} \Longrightarrow |M| = |N|$$

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 $f\colon L \to L$, the set of fixpoints of f is also a complete lattice, with greatest fixpoint $\bigvee\{x\colon x \leq f(x)\}$ and least fixpoint $\bigwedge\{x\colon x \geq f(x)\}$.

Proof.

$(P(M), \subset)$ is a complete lattice. Since the map

$$\varphi\colon S \mapsto M \setminus g(N \setminus f(S))$$

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.

$$C_0 := M \setminus g(N)$$
$$D_0 := f(C_0)$$
$$C_{n+1} := g(D_n)$$
$$D_{n+1} := f(C_n)$$
$$C := \bigcup_{n\in\mathbb{N}} C_n$$
$$f\restriction_C \cup g^{-1}\restriction_{g(N)\setminus C}$$

$$\varphi\colon S \mapsto (M \setminus g(N)) \cup g(f(S))$$
$$C = \bigcup_{n\to\infty} \varphi^n(\emptyset)$$
$$= \bigcap \left\{ S\colon (M \setminus g(N)) \cup g(f(S)) \subset S \right\}$$

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 $\alpha \times \alpha = \big\{(\xi, \eta) \colon (\xi, \eta) < (0, \alpha)\big\}$.

Let $\Gamma(\alpha, \beta) := otp\big\{(\xi, \eta) \colon (\xi, \eta) < (\alpha, \beta)\big\}$. Then $(\alpha, \beta) < (\gamma, \delta) \iff \Gamma(\alpha, \beta) < \Gamma(\gamma, \delta)$, and $\Gamma(\omega, \omega) = \omega$, $\Gamma(\alpha, \alpha) \geq \alpha$. Assume α is the least ordinal s.t. $\Gamma(\omega_\alpha, \omega_\alpha) \neq \omega_\alpha$. Let $\beta, \gamma < \omega_\alpha$ s.t. $\Gamma(\beta, \gamma) = \omega_\alpha$. Pick $\delta < \omega_\alpha$ s.t. $\delta > \beta, \gamma$. We have $\Gamma(\delta, \delta) \supset \omega_\alpha$ and so $|\delta \times \delta| \geq \aleph_\alpha$. However, $|\delta \times \delta| = |\delta| \cdot |\delta| = |\delta| < \aleph_\alpha$. Contradiction.

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$$

Cantor Set

$$C_0 := [0,1]$$

$$C_{k+1} := \frac{C_k}{3} \cup \left(\frac{2}{3} + \frac{C_k}{3}\right)$$

$$C := \bigcap_{k=0}^{\infty} C_k = \bigcap_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\left[\frac{3k+0}{3^n}, \frac{3k+1}{3^n}\right] \cup \left[\frac{3k+2}{3^n}, \frac{3k+3}{3^n}\right]\right)$$

$$= [0,1] \setminus \bigcup_{n=1}^{\infty} \bigcup_{k=0}^{3^{n-1}-1} \left(\frac{3k+1}{3^n}, \frac{3k+2}{3^n}\right)$$

$$C = \left\{\sum_{n=1}^{\infty} \frac{x_n}{3^n} : x_n = 0 \vee x_n = 2\right\} \implies |C| = 2^{\aleph_0}$$

Banach's Fixpoint Theorem

Theorem (Banach's Fixpoint Theorem)

Let (M, d) be a complete metric space and $T\colon M \to M$ 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 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

$$\boxed{\text{A set } A \text{ is a } \textit{fractal} \text{ if } dim_H(A) > dim_T(A).}$$

$$H_{d,\varepsilon}(A) := \inf\left\{\sum_{k=1}^{\infty} diam(B_k)^d : A \subset \bigcup_{k=1}^{\infty} B_k \ \ \& \ \ diam(B_k) \leq \varepsilon\right\}$$

$$dim_H(A) := \inf\left\{d : \lim_{\varepsilon\to 0} H_{d,\varepsilon}(A) = 0\right\}$$

Definition (Topological Dimension)

The *topological dimension* of a space X is defined by induction as

$$dim_T(\emptyset) := -1$$

$$dim_T(X) := \inf\{d : X \text{ has a basis } \mathcal{U} \text{ s.t. } \forall U \in \mathcal{U} : dim_T(\partial U) \leq d-1\}.$$

The topological dimension of a space X is the smallest integer d such that every open cover $\mathcal{U}$ of X has a refinement $\mathcal{V}$ in which no point of X lies in more than $d+1$ elements of $\mathcal{V}$.

Hilbert's Space-filling Curve

Hilbert's Space-filling Curve

- When we draw h_n, we impose a $2^n \times 2^n$ grids onto the square S. The diagonal of each grid is of length $\sqrt{(2^{-n})^2 + (2^{-n})^2} = 2^{\frac{1}{2}-n}$.
- We define the curve h as the limit of these successive functions $h_1, h_2 \ldots$ 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 ε. let I be the largest open part of L which h_n maps into the relevant grid. Whenever $x \in I$, $h_m(x)$ lies in that same grid, for any $m > n$. So h is continuous.
- Hilbert's curve is continuous everywhere but differentiable nowhere.
- Hausdorff dimension: 2

Cardinality of the Permutations of $\mathbb{N}$ — $|\mathrm{Sym}(\mathbb{N})|$

Proof1. Diagonal method: For any countable sequence $(\sigma_n)_{n\in\mathbb{N}}$ of permutations, let $f\colon 2n \mapsto \min\big(2\mathbb{N} \setminus \{\sigma_0(0), \sigma_1(2), \ldots, \sigma_n(2n)\}\big)$, and $f\colon 2n+1 \mapsto$ the nth element of $\mathbb{N} \setminus f(2\mathbb{N})$. Then $\forall n\colon f \neq \sigma_n$.

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. $|\mathrm{Sym}(\mathbb{N})| > \aleph_0$.

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. $|\mathrm{Sym}(\mathbb{N})| \geq 2^{\aleph_0}$.

Proof3. Riemann rearrangement $\left(e.g. \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}\right) \implies \mathbb{R} \rightarrowtail \mathrm{Sym}(\mathbb{N})$.

Theorem (Riemann Rearrangement Theorem)

Any conditionally convergent series can be rearranged in a permutation to

1. *converge to any real number;*
2. *diverge to ∞ or $-\infty$;*
3. *oscillate finitely or infinitely.*

The Pasadena Paradox

The Pasadena Game

Toss a fair coin until the first head appears. If the first head appears on toss n, the payoff is $\frac{(-1)^{n-1}2^n}{n}$.

How to calculate the expected utility?

$$\sum_{n=1}^{\infty} \frac{1}{2^n} \frac{(-1)^{n-1}2^n}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln 2 \qquad \sum_{n=1}^{\infty} \left| \frac{(-1)^{n-1}}{n} \right| = \infty$$

Cofinality and Inaccessible Cardinal

- $\mathrm{cf}(\alpha)$:= the least limit ordinal β s.t. there is an increasing β-sequence $\langle \alpha_\xi : \xi < \beta \rangle$ with $\lim\limits_{\xi \to \beta} \alpha_\xi = \alpha$.
- An infinite cardinal κ is *regular* if $\mathrm{cf}(\kappa) = \kappa$. It is *singular* if $\mathrm{cf}(\kappa) < \kappa$.
- A cardinal κ is a *strong limit* cardinal if $\forall \lambda < \kappa \big(2^\lambda < \kappa\big)$.
- A cardinal κ is *inaccessible* if it is a regular strong limit uncountable cardinal.

von Neumann Universe

Definition (von Neumann Universe)

$$V_0 := \emptyset$$

$$V_{\alpha+1} := P(V_\alpha)$$

$$V_\alpha := \bigcup_{\beta<\alpha} V_\beta \quad \text{for limit } \alpha.$$

$$V := \{x : x = x\}$$

$$\boxed{V = \bigcup_{\alpha \in \mathrm{Ord}} V_\alpha}$$

$rank(x) :=$ the least α 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)

$$L_0 := \emptyset$$
$$L_{\alpha+1} := \mathrm{Def}(L_\alpha)$$
$$L_\alpha := \bigcup_{\beta<\alpha} L_\beta \quad \text{for limit } \alpha.$$
$$L := \bigcup_{\alpha\in\mathrm{Ord}} L_\alpha$$

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 ZF that contains all ordinals.
L is the smallest inner model of ZF.

Grothendieck Universe

Definition (Grothendieck Universe)

1. $x \in y \in U \implies x \in U$
2. $x \in U \ \& \ y \in U \implies \{x, y\} \in U$
3. $x \in U \implies P(x) \in U$
4. $I \in U \ \& \ x \colon I \to U \implies \bigcup_{i \in I} x_i \in U$
5. $\omega \in U$

Universe Axiom

For every set x, there exists a Grothendieck universe U s.t. $x \in U$.

U is a Grothendieck universe iff $U = V_\kappa$ for some inaccessible κ.

The Universe Axiom is equivalent to the "inaccessible cardinal axiom" that "there exist arbitrarily large inaccessible cardinals."

$$U \vDash \mathrm{ZFC}$$

$$\frac{\text{super-infinite}}{\text{infinite}} \approx \frac{\text{infinite}}{\text{finite}}$$

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 λ, V_λ is super-infinite.

Shelf

Definition (Shelf)

A left (right) *shelf* is a set S with an operation $*$ satisfying

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(left self-distributive)}$$

$$(x * y) * z = (x * z) * (y * z) \qquad \text{(right self-distributive)}$$

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 pth 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 ∞), then pass them to the mathematician for a formal proof.

$$crit(j) := \mu\alpha[j(\alpha) > \alpha]$$

The critical ordinal $crit(j)$ of the elementary embedding j is the least ordinal that is not invariant under j.

$$\mathcal{E}_\lambda := \{j : V_\lambda \prec V_\lambda \ \ \& \ \ j \text{ is non-surjective}\}$$

$$i[j] := \bigcup_{\alpha<\lambda} i(j \cap V_\alpha^2)$$

$$(\mathcal{E}_\lambda, [\,]) \text{ is a left-shelf: } i[j[k]] = i[j][i[k]]$$

$$crit(j \circ j) = crit(j) \quad \text{but} \quad crit(j[j]) = j(crit(j)) > crit(j)$$

$$j_{[n]} := \underbrace{j[j][j]\cdots[j]}_{n \text{ times}}$$

$$Iter(j) := \left\{ j_{[n]} : n \in \mathbb{N}^+ \right\}$$

$$\boxed{\big(Iter(j), []\big) \text{ is a left-shelf.}}$$

For $k, k' \in Iter(j)$, declare $k \equiv_n k' := \forall x \in V_\gamma \big(k(x) \cap V_\gamma = k'(x) \cap V_\gamma\big)$ with $\gamma := crit(j_{[2^n]})$. Then

$$\boxed{Iter(j)/{\equiv_n} \text{ is (isomorphic to) the Laver table } A_n.}$$

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 α is a limit ordinal.

$\boxed{\varepsilon_\alpha \text{ is countable iff } \alpha \text{ is countable.}}$

$\boxed{\forall \alpha \geq 1 \colon \varepsilon_{\omega_\alpha} = \omega_\alpha}$

Veblen Hierarchy

$$\varphi_0(\alpha) := \omega^\alpha$$

$$\varphi_{\gamma+1}(\alpha) := \alpha^{th} \text{ ordinal s.t. } \varphi_\gamma(\beta) = \beta$$

$$\varphi_\delta(\alpha) := \alpha^{th} \text{ common fixpoint of } \varphi_\gamma \text{ for all } \gamma < \delta$$

$$\Gamma_\alpha := \alpha^{th} \text{ ordinal s.t. } \varphi_\alpha(0) = \alpha$$

$$\boxed{\varepsilon_\alpha = \varphi_1(\alpha)}$$

$$V_0 = \emptyset$$

$$V_{\alpha+1} = P(V_\alpha)$$

$$V_\alpha = \bigcup_{\beta<\alpha} V_\beta \quad \text{for limit } \alpha.$$

$$V = \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha$$

$0 = 1$

I0-I3

n-huge

superhuge

huge

almost huge

Vopěnka's Principle

extendible

supercompact

strongly compact

superstrong

Woodin

strong

$0^\dagger$ exists

measurable

Ramsey

Rowbottom

Jónsson

$\kappa \longrightarrow (\omega_1)_2^{<\omega}$

$\forall a \in {}^\omega\omega (a^\# \text{ exists})$

$0^\#$ exists

$\kappa \longrightarrow (\omega)_2^{<\omega}$

indescribable

weakly compact

α-Mahlo

Mahlo

α-inaccessible

inaccessible

weakly inaccessible

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
   - Axioms of ZFC
   - Ordinal Numbers
   - Cardinal Numbers
   - Axiom of Choice
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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 $A = \biguplus_{i=1}^{n} A_i, B = \biguplus_{i=1}^{n} B_i$ 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 κ and λ: $\kappa < \lambda \vee \kappa = \lambda \vee \kappa > \lambda$.
- For any infinite cardinal κ: $\kappa^2 = \kappa$.
- The Cartesian product of any family of 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 Γ of formulas with $|\mathscr{L}| = \kappa$ is finitely satisfiable, then it has a model with cardinality $\leq \kappa + \aleph_0$.

Theorem (Well-Wrdering Theorem)

Every set can be well-ordered.

Proof.

Assume f is a choice function for $P(A) \setminus \{\emptyset\}$. Let

$$a_\alpha = f\left(A \setminus \left\{a_\xi : \xi < \alpha\right\}\right)$$

$$\theta := \mu\alpha\left[A = \left\{a_\xi : \xi < \alpha\right\}\right]$$

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)

$$Con(\mathrm{ZF}) \rightarrow Con(\mathrm{ZFC} + \mathrm{GCH})$$

Theorem (Cohen1963)

- $Con(\mathrm{ZF}) \rightarrow Con(\mathrm{ZF} + \neg\mathrm{AC})$
- $Con(\mathrm{ZF}) \rightarrow Con(\mathrm{ZFC} + \neg\mathrm{GCH})$

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

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \qquad \text{(GCH)}$$

$$\Downarrow$$

$$2^\kappa < 2^{\kappa^+} \qquad \text{(WGCH)}$$

$$\Updownarrow$$

$$\kappa < \lambda \implies 2^\kappa < 2^\lambda$$

$$\boxed{\text{“}|X| < |Y| \implies |P(X)| < |P(Y)|\text{” is independent of ZFC.}}$$

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

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Presburger/Robinson/Peano Arithmetic

- $x + 0 = x$
- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- $x + z = y + z \rightarrow x = y$
- $x \cdot 0 = 0$
- $x \cdot 1 = x$
- $x \cdot y = y \cdot x$
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x + 1)) \rightarrow \forall x \varphi$

$$\left.\begin{array}{ll}
1 & S(x) \neq 0 \\
2 & S(x) = S(y) \rightarrow x = y \\
3 & y = 0 \vee \exists x(S(x) = y) \\
4 & x + 0 = x \\
5 & x + S(y) = S(x + y) \\
6 & x \cdot 0 = 0 \\
7 & x \cdot S(y) = (x \cdot y) + x
\end{array}\right\} Q$$

8. $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(S(x))) \rightarrow \forall x \varphi$

Exponentiation is definable in $\mathcal{N}$/representable in Q

$$\pi(x,y) := (x+y)^2 + x + 1$$
$$\pi_1(z) := \mu x[\exists y \leq z \colon \pi(x,y) = z]$$
$$\pi_2(z) := \mu y[\exists x \leq z \colon \pi(x,y) = z]$$
$$\beta(s,i) := \mu x < s\big[\pi_1(s) \equiv x \mod 1 + (i+1)\cdot \pi_2(s)\big]$$
$$\beta^*(s,i) := \mu x < s\,[\exists y < s\, \exists z < s \colon s = \pi(y,z) \ \wedge\ (1 + (\pi(x,i)+1)\cdot z) \mid y]$$

Lemma

For every $a_0, \ldots, a_n$, there is an $s \in \mathbb{N}$ s.t. $\forall i \leq n \colon \beta(s,i) = a_i$.

Proof.

$$b := \max\{n, a_0, \ldots, a_n\} \quad d := b! \quad d_i := 1 + (i+1)\cdot d$$
$$c := \mu x\,\big[\forall i \leq n\big(x \equiv a_i \mod d_i\big)\big]$$
$$s := \pi(c,d)$$

$$x^y := \beta\Big(\mu s\big[\beta(s,0) = 1 \ \wedge\ \forall i < y \colon \beta(s,i+1) = \beta(s,i)\cdot x\big], y\Big)$$

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

ζ	$\forall$	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	$\ldots$	$2k+21$	$\ldots$

$$\langle a_1, \ldots, a_n\rangle := \mu x\big[\beta(x,0) = n \wedge \beta(x,1) = a_1 \wedge \cdots \wedge \beta(x,n) = a_n\big]$$

$$or \quad \langle a_1, \ldots, a_n\rangle := \prod_{i=1}^{n} p_i^{a_i+1}$$

$$\ulcorner\zeta_0 \cdots \zeta_n\urcorner := \langle\ulcorner\zeta_0\urcorner, \ldots, \ulcorner\zeta_n\urcorner\rangle$$

$prf_{\mathbb{T}}(y,x) :=$ "y is the code of a proof in $\mathbb{T}$ of the formula with code x."

$$\Box_{\mathbb{T}} x := \exists y\, prf_{\mathbb{T}}(y,x)$$

$$\Box_{\mathbb{T}}\varphi := \Box_{\mathbb{T}}\ulcorner\varphi\urcorner$$

Is there a φ s.t. $\mathbb{T} \vdash \varphi \leftrightarrow \neg\Box_{\mathbb{T}}\varphi$?

- $Con(\mathbb{T}) := \neg\Box_{\mathbb{T}}\bot$
- ω-consistent: $\forall x \Box_{\mathbb{T}} \neg\varphi(x) \to \neg\Box_{\mathbb{T}}\exists x\varphi(x)$ for any formula φ
- 1-consistent: $\forall x \Box_{\mathbb{T}} \neg\varphi(x) \to \neg\Box_{\mathbb{T}}\exists x\varphi(x)$ for $\varphi \in \Delta_0$
- $\mathrm{Rfn}_\Gamma(\mathbb{T})$: $\Box_{\mathbb{T}}\varphi \to \varphi$ for any sentence $\varphi \in \Gamma$
- $\mathrm{RFN}_\Gamma(\mathbb{T})$: $\forall x\big(\Box_{\mathbb{T}}\varphi(x) \to \varphi(x)\big)$ for any wff $\varphi \in \Gamma$
- arithmetically sound: $\mathrm{Rfn}_{\Sigma_{<\omega}}(\mathbb{T})$
- 1-consistent $\iff$ $\mathrm{Rfn}_{\Sigma_1}(\mathbb{T})$
- $\mathrm{Rfn}_{\Pi_1}(\mathbb{T}) \iff \mathrm{RFN}_{\Pi_1}(\mathbb{T}) \iff Con(\mathbb{T})$

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

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

8 Modal Logic

9 Logic vs Game Theory

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 $g, h_1, \ldots, h_k$,

$$f(\boldsymbol{x}) = g\left(h_1(\boldsymbol{x}), \ldots, h_k(\boldsymbol{x})\right)$$

- primitive recursion: given g, h,

$$f(\boldsymbol{x}, 0) = g(\boldsymbol{x})$$
$$f(\boldsymbol{x}, n+1) = h\left(\boldsymbol{x}, n, f(\boldsymbol{x}, n)\right)$$

- regular μ-operation: given g, and $\forall \boldsymbol{x} \exists y [g(\boldsymbol{x}, y) = 0]$,

$$f(\boldsymbol{x}) = \mu y [g(\boldsymbol{x}, y) = 0]$$

Partial Recursive Function

- μ-operation: given g,

$$f(\boldsymbol{x}) = \mu y\,[g(\boldsymbol{x}, y) = 0]$$

where

$$\mu y\,[g(\boldsymbol{x}, y) = 0] = n \iff g(\boldsymbol{x}, n) = 0 \;\wedge\; \forall z < n\big(g(\boldsymbol{x}, z)\downarrow \neq\; 0\big)$$

bounded μ-operation: $\mu x < n[\varphi(x)] := \mu x[\varphi(x) \vee x = n]$

Definition (Primitive Recursive / Recursive / Partial Recursive)

The class of primitive recursive functions (recursive functions, partial recursive functions) is the smallest class of functions containing the initial functions and closed under composition, primitive recursion (regular μ-operation, μ-operation).

Ackermann Function

Definition (Ackermann Function)

$$A(m,n) := \begin{cases} n+1 & \text{if } m = 0 \\ A(m-1,1) & \text{if } m > 0 \text{ and } n = 0 \\ A(m-1, A(m,n-1)) & \text{if } m > 0 \text{ and } n > 0 \end{cases}$$

Theorem

The Ackermann function is recursive but not primitive recursive.

$$a \uparrow^n b := \begin{cases} ab & \text{if } n = 0 \\ (a \uparrow^{n-1})^b 1 & \text{if } n \geq 1 \end{cases}$$

$$a \uparrow b = a^b \qquad a \uparrow\uparrow b = \underbrace{a \uparrow (a \uparrow (\cdots \uparrow a))}_{b \text{ copies of } a} 1 = \underbrace{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}_{b \text{ copies of } a}$$

$$A(m,n) = 2 \uparrow^{m-2} (n+3) - 3$$

Thesis (Church-Turing Thesis)

effective calculable = *recursive* = *Turing Computable*

||

representable in Q = λ-*definable*

||

finite definable = *Herbrand-Gödel computable*

||

flowchart (or 'while') computable

||

neural network with unbounded tape = *Conway's 'game of life'*

||

Post/Markov/McCarthy/Kolmogorov-Uspensky computable ...

- The behavior of any discrete physical system evolving according to local mechanical laws is computable?
- Any possible discrete physical process is computable?
- Any constructive function is computable?
- The mental functions can be simulated by machines?

Computability vs Representability

A function/relation is representable in Robinson Q iff it is computable.

(proof sketch.) We have to show that all initial functions are representable, and the representable functions are closed under composition, regular μ-operation and primitive recursion.
最后一步证明对原始递归封闭的困难在于，一个公式 φ 不能通过自身来定义自己，而必须借助一些编码技巧（Gödel β 函数）。

$$f(\boldsymbol{x}, 0) = g(\boldsymbol{x})$$
$$f(\boldsymbol{x}, n+1) = h(\boldsymbol{x}, n, f(\boldsymbol{x}, n))$$

we can code the sequence of values of f from 0 to y by using β:

$$F(\boldsymbol{x}, y) = \mu z\big[\beta(z, 0) = g(\boldsymbol{x}) \ \wedge \ \forall i < y : \beta(z, i+1) = h\big(\boldsymbol{x}, i, \beta(z, i)\big)\big]$$

$$f(\boldsymbol{x}, y) = \beta\big(F(\boldsymbol{x}, y), y\big)$$

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.

- $f(\boldsymbol{x})\downarrow \iff \exists y T(e, \boldsymbol{x}, y)$
- $f(\boldsymbol{x}) = U(\mu y T(e, \boldsymbol{x}, y))$

$T(e, \boldsymbol{x}, y)$:= "y is the code number of some computation according to program P_e with input $\boldsymbol{x}$."
$U(y)$:= "the number of 1's in the final configuration of y."

Definition

φ_e is the eth partial recursive function:

$$\varphi_e(\boldsymbol{x}) := U(\mu y T(e, \boldsymbol{x}, y))$$

Incompleteness Theorem

- The function $\bar{f}$ is a *completion* of a partial function f if $\bar{f}$ is total and $\forall n\colon f(n)\downarrow \implies f(n) = \bar{f}(n)$.
- A partial function f is *potentially recursive* if it has a completion which is recursive.

Not every partial recursive function is potentially recursive.

$$f(n) := \varphi_n(n) + 1$$

Theorem (Incompleteness Theorem)

Any ω-consistent Gödelian $\mathbb{T}$ is incomplete.

Proof.

Suppose T is represented in $\mathbb{T}$ by γ.

$$\bar{\varphi}_e(n) := \begin{cases} U(\mu y T(e,n,y)) & \text{if } \exists y T(e,n,y) \\ 0 & \text{if } \mathbb{T} \vdash \forall y \neg\gamma(e,n,y) \end{cases}$$

Enumeration Theorem & smn Theorem

Theorem (Enumeration Theorem)

The sequence $\{\varphi_e^n\}_{e\in\omega}$ is a partial recursive enumeration of the n-ary partial recursive functions, in the sense that:

- *for each e, φ_e^n is a partial recursive function of n variables.*
- *if ψ is a partial recursive function of n variables, then there is e s.t. $\psi = \varphi_e^n$.*
- *there is a partial recursive function φ of $n+1$ variables s.t. $\varphi(e, \boldsymbol{x}) = \varphi_e(\boldsymbol{x})$.*

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 ψ 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)

ψ is an acceptable numbering iff there is a recursive permutation h s.t.,

$$\psi_e = \varphi_{h(e)}$$

Theorem (Blum)

If ψ is an acceptable numbering, then there is a recursive permutation h s.t.

$$h(\psi_e(x)) = \varphi_{h(e)}(h(x))$$

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

$$\exists e \colon \varphi_e(y) = \varphi_{s(e)}(y) = f(e, y)$$

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 $\exists v \colon \varphi^A_v(x, y) = f(s(x, y), y)$. 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 α 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 $\mathbb{T}' \supset \mathbb{T}$ be formal systems (with recursive sets of axioms and of recursive rules) such that $\mathbb{T}' \setminus \mathbb{T}$ is not r.e. Given a recursive function h, there is a theorem φ of $\mathbb{T}$ and a number n such that φ admits a proof of length $\leq n$ in $\mathbb{T}'$, but no proof of length $\leq h(n)$ in $\mathbb{T}$.

Proposition

If $\mathbb{T}$ is an essentially undecidable formal system, and $\mathbb{T} \nvdash \varphi$, then $\mathbb{T} \cup \{\varphi\} \setminus \mathbb{T}$ is not r.e.

Remark: Adding an unprovable sentence to an essentially undecidable formal system $\mathbb{T}$ radically shortens some proof of some theorem of $\mathbb{T}$.

Blum's Speed-Up Theorem

Theorem (Blum's Speed-Up Theorem)

Given a complexity measure (φ, Φ) and a total computable function f with two parameters, there exists a $0,1$-valued total computable function g s.t. for every index i for g, there is another index j for g s.t. for almost all x

$$f(x, \Phi_j(x)) \leq \Phi_i(x)$$

Remark: For any complexity measure there are computable functions that are not optimal with respect to that measure. There is no notion of best complexity for all total recursive functions.

Remark: No computer can be optimal for every purpose: no matter how good a computer is, there are always functions on which such a computer behaves very badly.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

8 Modal Logic

9 Logic vs Game Theory

自指

- 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.

“自指”与“悖论”

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

Print two copies of the following, the second copy in quotes:
“Print two copies of the following, the second copy in quotes:”

“自指”的威力？

Curry’s Paradox

- 如果这句话是真的那么上帝存在。
- 这句话是假的并且上帝不存在。

Hi 美女，问你个问题呗 ~v~

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。

怎么“指”？— 层次

怎么“指”？— 层次

无穷虚拟层？

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

无穷虚拟层？

怎么穿越层次？— 编码

- 国王让 100 个死囚排成一列。
- 每人头戴一顶帽子，帽子分红、蓝两色。
- 每人只能看到前面人的帽子的颜色。
- 国王要求囚犯从最后一个开始报自己头上帽子的颜色，报对可活，报错即杀。
- 囚犯能商量出什么办法让尽可能多的人活下来吗？

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[10]

Theorem (Lawvere's Fixpoint Theorem)

In any Cartesian closed category, given an object Y, if there is an object X and an arrow $f\colon X \times X \to Y$ such that, for every $g\colon X \to Y$ there is a $t\colon 1 \to X$ for all $x\colon 1 \to X$: $g \circ x = f \circ (x, t)$, then every arrow $\alpha\colon Y \to Y$ has a fixpoint $y\colon 1 \to Y$ such that $\alpha \circ y = y$.

[10] 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 $g\colon X \to Y$ is *representable* by $f\colon X \times X \to Y$ iff

$$\exists y \forall x\colon g(x) = f(x, y)$$

Theorem (Lawvere's Fixpoint Theorem)

For sets X, Y, functions $f\colon X \times X \to Y$, $\alpha\colon Y \to Y$, let $g := \alpha \circ f \circ \Delta$.

1. *If α has no fixpoint, then g is not representable by f.*
2. *If g is representable by f, then α has a fixpoint.*

$$\begin{tikzcd}
X \times X \arrow[r, "f"] & Y \arrow[d, "\alpha"] \\
X \arrow[u, "\Delta"] \arrow[r, "g"'] & Y
\end{tikzcd}$$

- $\Delta\colon x \mapsto (x, x)$ diagonal
- f evaluation
- α "negation"
- g ($\ulcorner g \urcorner$) fixpoint-(free) transcendence
- f ($\ulcorner g \urcorner, \ulcorner g \urcorner$) self-reference "I have property α."

$$\alpha\big(f(\ulcorner g \urcorner, \ulcorner g \urcorner)\big) = g(\ulcorner g \urcorner) = f(\ulcorner g \urcorner, \ulcorner g \urcorner)$$

Diagonalization

- A function $g\colon X \to Z$ is *representable* by $f\colon X \times Y \to Z$ iff

$$\exists y \in Y \forall x \in X\colon g(x) = f(x, y)$$

Theorem (Lawvere's Fixpoint Theorem)

For sets X, Y, Z, functions $\beta\colon X \to Y$, $f\colon X \times Y \to Z$, $\alpha\colon Z \to Z$, let $g := \alpha \circ f \circ (1_X, \beta)$. Assume β is surjective.

1. *If α has no fixpoint, then g is not representable by f.*
2. *If g is representable by f, then α has a fixpoint.*

$$\begin{tikzcd}
X \times Y \arrow[r, "f"] & Z \arrow[d, "\alpha"] \\
X \arrow[u, "(1_X,\beta)"] \arrow[r, "g"'] & Z
\end{tikzcd}$$

Example — Grelling/Liar/Quine. . . Paradox

$$\begin{tikzcd} X \times X \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\ X \arrow[u, "\Delta"] \arrow[r, "g"'] & 2 \end{tikzcd}$$

where $f\colon (x, y) \mapsto [\![y \text{ “describes” } x]\!]$ and $\alpha\colon x \mapsto 1 - x$.

- 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

$$\begin{tikzcd} V \times V \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\ V \arrow[u, "\Delta"] \arrow[r, "g"'] & 2 \end{tikzcd}$$

where

$$f\colon (x, y) \mapsto [\![x \in y]\!]$$

and

$$\alpha\colon x \mapsto 1 - x$$

$$R := \{x\colon x \notin x\} \quad \text{exist?}$$

Barber paradox: $f\colon (x, y) \mapsto [\![y \text{ “shaves” } x]\!]$

Let $S \subset V \times V$

$$S_y := \{x\colon Sxy\}$$

$$R := \{x\colon x \notin S_x\}$$

$$\forall x\colon \; R \neq S_x$$

Example — Yablo Paradox in Linear Temporal Logic(LTL)

$$
\begin{array}{lcr}
n \Vdash \varphi \wedge \psi & \Longleftrightarrow & n \Vdash \varphi \;\&\; n \Vdash \psi \\
n \Vdash \neg\varphi & \Longleftrightarrow & n \nVdash \varphi \\
n \Vdash \bigcirc\varphi & \Longleftrightarrow & n+1 \Vdash \varphi \\
n \Vdash \Box\varphi & \Longleftrightarrow & \forall m \geq n \implies m \Vdash \varphi
\end{array}
$$

$$
\begin{tikzcd}
\mathrm{Sen} \times \mathrm{Sen} \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\
\mathrm{Sen} \arrow[u, "\Delta"] \arrow[r, "g"'] & 2
\end{tikzcd}
$$

$f : (X, Y) \mapsto [\![X \nleftrightarrow \bigcirc\Box\neg Y]\!]$ and $\alpha : x \mapsto 1 - x$

Theorem

For any φ, $\mathrm{LTL} \nvdash \varphi \leftrightarrow \bigcirc\Box\neg\varphi$.

Example — Euclid's Theorem

Theorem (Euclid's Theorem)

There are infinitely many prime numbers.

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & 2
\end{tikzcd}$$

where

$$f(m,n) = \begin{cases} 1 & \forall p \in \mathbb{P}\colon p \mid (m!+1) \to p < n \\ 0 & \text{otherwise} \end{cases}$$

and $\alpha\colon x \mapsto 1 - x$.

Obviously, $\forall n\colon f(n,n) = 0$, and $g(n) = \alpha(f(n,n)) = 1$.

If $|\mathbb{P}| < \infty$, let $t := \max \mathbb{P} + 1$, then $\forall n\colon f(n,t) = 1$ and $\forall n\colon g(n) = f(n,t)$.

Therefore, $f(t,t)$ is a fixpoint of α. Contradiction!

Example — The set of real numbers is uncountable

Theorem (Cantor)

$\mathbb{R}$ is uncountable.

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & 10 \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & 10
\end{tikzcd}$$

where $f : (m, n) \mapsto r_{mn} :=$ "the nth digit of the mth real" and $\alpha : x \mapsto 9 - x$.

- There exists uncomputable real $\sum_n g(n) 10^{-n}$, where

$$f : (m, n) \mapsto r_{mn} := \begin{cases} \text{the } n^{th} \text{ digit output by the } m^{th} \text{ Turing machine} \\ 0 \ \text{ if the } m^{th} \text{ Turing machine never outputs a } n^{th} \text{ digit} \end{cases}$$

- Richard paradox(unnameable real):

$f : (m, n) \mapsto r_{mn} :=$ "the nth digit of the real named by the mth sentence"

Example — Cantor's Theorem

Theorem (Cantor's Theorem)

$$|X| < |P(X)|$$

$$\begin{tikzcd}
X \times P(X) \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\
X \arrow[u, "{(1_X, \beta)}"] \arrow[r, "g"'] & 2
\end{tikzcd}$$

where $f\colon (x, y) \mapsto [\![x \in y]\!]$ and $\alpha\colon x \mapsto 1 - x$.

β is not surjective.

another proof: assume $h\colon P(X) \rightarrowtail X$.

$$\begin{tikzcd}
P(X) \times P(X) \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\
P(X) \arrow[u, "\Delta"] \arrow[r, "g"'] & 2
\end{tikzcd}$$

where $f\colon (x, y) \mapsto [\![h(x) \in y]\!]$, and $\alpha\colon x \mapsto 1 - x$.

g is representable by $y := \{h(x) : x \subset X \;\&\; h(x) \notin x\}$.

Example — Cantor's Theorem — another proof

If $|X| \geq |P(X)|$, then there exists some enumeration $\{S_i\}_{i \in X}$ of $P(X)$.

$$\begin{tikzcd}
X \times \{S_i\}_{i \in X} \arrow[r, "f"] & 2 \arrow[d, "\alpha"] \\
X \arrow[u, "\Delta"] \arrow[r, "g"'] & 2
\end{tikzcd}$$

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 $P(X)$, 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 α is the cyclic permutation.

Every $g : X \to Y$ is representable by some $f : X \times X \to Y$ iff $\exists f : X \twoheadrightarrow Y^X$.

If there exists $f : X \twoheadrightarrow Y^X$, *then every* $\alpha : Y \to Y$ *has a fixpoint.*

Example — Continuous Functions

- Since a continuous function on $\mathbb{R}$ is determined by its values at rational points, the set of continuous functions $|C(\mathbb{R},\mathbb{R})| = |\mathbb{R}|$. However, there is no continuous surjection $\mathbb{R} \twoheadrightarrow C(\mathbb{R},\mathbb{R})$ from the real line to the Banach space of continuous real functions, equipped with the $\sup$-norm $\|f\|_\infty = \sup_{x\in\mathbb{R}} |f(x)|$.

$$\begin{tikzcd}
\mathbb{R} \times C(\mathbb{R},\mathbb{R}) \arrow[r, "\mathscr{F}"] & \mathbb{R} \arrow[d, "\alpha"] \\
\mathbb{R} \arrow[u, "(1_{\mathbb{R}},\beta)"] \arrow[r, "g"'] & \mathbb{R}
\end{tikzcd}$$

where $\mathscr{F} : (x, f) \mapsto f(x)$ 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

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathscr{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathscr{E}_\varphi \colon (m,n) \mapsto \varphi_n(m)$, and $\alpha \colon \varphi_n(m) \mapsto \min\big(\mathbb{N} \setminus \{\varphi_k(m) \colon k \leq n\}\big)$

$$g(m) = \min\big(\mathbb{N} \setminus \{\varphi_k(m) \colon k \leq m\}\big) = \mu n\,[K(n|m) > m]$$

$$g \text{ unrepresentable} \implies g \text{ uncomputable} \implies K \text{ uncomputable}$$

$$\Sigma(m) := \max\{\varphi_k(0) \colon k \leq m\} = \max\{n \colon K(n) \leq m\}$$

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathscr{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathscr{E}_\varphi : (m,n) \mapsto \varphi_n(m)$, 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.

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "H"] & 2 \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & 2
\end{tikzcd}$$

where $H\colon (x, y) \mapsto [\![\varphi_y(x)\downarrow]\!]$, 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

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "\mathscr{E}_\varphi"] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2} \arrow[d, "\alpha"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n(m)\}_{(m,n)\in\mathbb{N}^2}
\end{tikzcd}$$

where $\mathscr{E}_\varphi \colon (m,n) \mapsto \varphi_n(m)$, and

$$\alpha \colon \varphi_n(m) \mapsto \begin{cases} 0 & \text{if } H(m,n) = 0 \\ \varphi_n(m) + 1 & \text{if } H(m,n) = 1 \end{cases}$$

or

$$\alpha \colon \varphi_n(m) \mapsto 1 + \sum_{k=0}^{n} H(m,k) \cdot \varphi_k(m)$$

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.

$$\varphi_e = \varphi_{h(e)}$$

$$\begin{tikzcd}
\mathbb{N} \times \mathbb{N} \arrow[r, "f"] & \{\varphi_n\}_{n \in \mathbb{N}} \arrow[d, "\mathscr{E}_h"] \\
\mathbb{N} \arrow[u, "\Delta"] \arrow[r, "g"'] & \{\varphi_n\}_{n \in \mathbb{N}}
\end{tikzcd}$$

where $f : (m, n) \mapsto \varphi_{\varphi_n(m)}$, and $\mathscr{E}_h : \varphi_n \mapsto \varphi_{h(n)}$.
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,

$$g(m) = \varphi_{h(\varphi_m(m))} = \varphi_{s(m)} = \varphi_{\varphi_t(m)} = f(m, t)$$
$$e := \varphi_t(t)$$

Example — Y Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\mathscr{E}_y"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

where $f : (x, y) \mapsto yx$, and $\mathscr{E}_y : x \mapsto yx$.

$$g = \lambda x.y(xx)$$

$$gg = y(gg)$$

$$Y := \lambda y.gg = \lambda y.(\lambda x.y(xx))(\lambda x.y(xx))$$

$$Y\varphi = \varphi(Y\varphi) = \varphi(\varphi(Y\varphi)) = \cdots$$

Example — Z Combinator

$$\begin{tikzcd}
\Lambda \times \Lambda \arrow[r, "f"] & \Lambda \arrow[d, "\mathscr{E}_y"] \\
\Lambda \arrow[u, "\Delta"] \arrow[r, "g"'] & \Lambda
\end{tikzcd}$$

where $f : (x, y) \mapsto \lambda v.yxv$, and $\mathscr{E}_y : x \mapsto yx$.

$$g = \lambda x.y(\lambda v.xxv)$$

$$Z := \lambda y.gg = \lambda y.(\lambda x.y(\lambda v.xxv))(\lambda x.y(\lambda v.xxv))$$

$$Zhv = h(Zh)v$$

$$e := Zh \implies ev = hev \qquad \text{(Kleene's fixpoint)}$$

Example — Θ 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 $\alpha : x \mapsto \lambda y.y(xy)$.

$$g = \lambda xy.y(xxy)$$

$$\Theta := gg = (\lambda xy.y(xxy))(\lambda xy.y(xxy))$$

$$\Theta\varphi = \varphi(\Theta\varphi) = \varphi(\varphi(\Theta\varphi)) = \cdots$$

Example — Θ_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 $\alpha : x \mapsto \lambda y.y(\lambda z.xyz)$.

$$g = \lambda xy.y(\lambda z.xxyz)$$

$$\Theta_v := gg = (\lambda xy.y(\lambda z.xxyz))(\lambda xy.y(\lambda z.xxyz))$$

$$\Theta_v \varphi v = \varphi(\Theta_v \varphi)v$$

Example — Fixpoint Theorem in Lambda Calculus

Theorem (Fixpoint Theorem in Lambda Calculus)

For every λ-term F there is a λ-term X s.t.

$$F\ulcorner X\urcorner = X$$

$$\begin{tikzcd}
\underline{\Lambda} \times \underline{\Lambda} \arrow[r, "A"] & \Lambda \arrow[d, "\mathscr{E}_F"] \\
\underline{\Lambda} \arrow[u, "\Delta"] \arrow[r, "G"'] & \Lambda
\end{tikzcd}$$

where $\underline{\Lambda} := \{\ulcorner M\urcorner : M \in \Lambda\}$, and $A : (\ulcorner M\urcorner, \ulcorner N\urcorner) \mapsto N\,(\ulcorner M\urcorner)$, and $\mathscr{E}_F : M \mapsto F\ulcorner M\urcorner$.

$$G\ulcorner M\urcorner = F\ulcorner M\ulcorner M\urcorner\urcorner$$

$$X := G\ulcorner G\urcorner$$

Example — Fixpoint Lemma in Logic

Theorem (Fixpoint Lemma in Logic)

For any wff $\alpha(x)$ with one free variable x, there exists a sentence β s.t.

$$Q \vdash \beta \leftrightarrow \alpha\left(\ulcorner \beta \urcorner\right)$$

$$\begin{tikzcd}
\mathrm{Lin}_1 \times \mathrm{Lin}_1 \arrow[r, "f"] & \mathrm{Lin}_0 \arrow[d, "\mathscr{E}_\alpha"] \\
\mathrm{Lin}_1 \arrow[u, "\Delta"] \arrow[r, "g"'] & \mathrm{Lin}_0
\end{tikzcd}$$

where $f : (\varphi(x), \psi(x)) \mapsto \psi\left(\ulcorner \varphi(x) \urcorner\right)$, and $\mathscr{E}_\alpha : \varphi \mapsto \alpha(\ulcorner \varphi \urcorner)$.

$$g(\varphi(x)) = \alpha\left(\ulcorner \varphi\left(\ulcorner \varphi(x) \urcorner\right) \urcorner\right)$$

$$\gamma(x) := \alpha\left(D(x)\right)$$

where $D : \ulcorner \varphi(x) \urcorner \mapsto \ulcorner \varphi\left(\ulcorner \varphi(x) \urcorner\right) \urcorner$

$$\beta := \gamma\left(\ulcorner \gamma(x) \urcorner\right)$$

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 Y	$\hat{=}$	Fixpoint	$\hat{=}$	Gödel	$\hat{=}$	Kleene	$\hat{=}$	Russell
yx	$\hat{=}$	$N\,(\ulcorner M \urcorner)$	$\hat{=}$	$\psi(\ulcorner \varphi(x) \urcorner)$	$\hat{=}$	$\varphi_n(m)$	$\hat{=}$	$x \in y$
xx	$\hat{=}$	$M\,(\ulcorner M \urcorner)$	$\hat{=}$	$\varphi(\ulcorner \varphi(x) \urcorner)$	$\hat{=}$	$\varphi_n(n)$	$\hat{=}$	$x \in x$
$y(xx)$	$\hat{=}$	$F \ulcorner M \ulcorner M \urcorner\urcorner$	$\hat{=}$	$\alpha(\ulcorner \varphi(\ulcorner \varphi(x) \urcorner) \urcorner)$	$\hat{=}$	$h(\varphi_n(n))$	$\hat{=}$	$x \notin x$
$\lambda x.y(xx)$	$\hat{=}$	G	$\hat{=}$	$\gamma(x)$	$\hat{=}$	$\varphi_t(n)$	$\hat{=}$	$x \notin R$
$(\lambda x.y(xx))(\lambda x.y(xx))$	$\hat{=}$	$G\,(\ulcorner G \urcorner)$	$\hat{=}$	$\gamma(\ulcorner \gamma(x) \urcorner)$	$\hat{=}$	$\varphi_t(t)$	$\hat{=}$	$R \notin R$

self-reference $\overset{?}{\Longrightarrow}$ 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

$$\begin{tikzcd}
\boldsymbol{M} \times \boldsymbol{M} \arrow[r, "f"] & \boldsymbol{O} \arrow[d, "\alpha"] \\
\boldsymbol{M} \arrow[u, "\Delta"] \arrow[r, "g"'] & \boldsymbol{O}
\end{tikzcd}$$

- $\boldsymbol{M}$: quantum measurements.
- $\boldsymbol{O}$: possible outcomes of quantum measurements.

If we assume that it is not possible to measure properties without changing them (observer effect: α is fixpoint-free), then there is a limit to self-inspection.

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。

von Neumann's Self-reproducing Automata

There is a program that outputs its own length.

There is a program that outputs its own source code.

Corollary (von Neumann's Self-reproducing Automata)

There is a recursive function φ_e s.t. $\forall x \colon \varphi_e(x) = e$.

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 (ψ-introspective)

Given a total recursive function ψ,

- the *ψ-analysis* of $\varphi(x)$ is the code of the computation of $\varphi(x)$ to $\psi(x)$ steps.
- φ is *ψ-introspective* at x if $\varphi(x)\downarrow$ and outputs its own ψ-analysis.
- φ is *totally ψ-introspective* if it is ψ-introspective at all x.

Corollary

There is a program that is totally ψ-introspective.

Proof.

Let $f(n,x) :=$ "the ψ-analysis of $\varphi_n(x)$".

Introspective Program

There is a program that is totally introspective.

$$\boxed{\varphi_e = \varphi_{h(e)}}$$

Self-simulating Computer	Self-consciousness
Host Machine	Experiencing Self
Virtual Machine	Remembering Self
Hardware	Body

- 裂脑人实验
- 铲雪？
- 铲屎？
- 编纂故事

卡尼曼《思考-快与慢》— 冰手挑战实验

Figure: 短痛不如长痛？

- 冰水 + 温水
- 经验自我
- 记忆自我
- 过程忽视
- 峰终定律

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.

侯士达《“我”是个怪圈》

- 有没有意识取决于在哪个层级上对结构进行观察。在整合度最高的层级上看，大脑是有意识的。下降到微观粒子层面，意识就不见了。
- 意识体是那些在某个描述层级上表现出某种特定类型的循环回路的结构。当一个系统能把外部世界过滤成不同的范畴、并不断向越来越抽象的层级创造新的范畴时，这种循环回路就会逐渐形成。
- 当系统能进行自我表征——对自己讲故事——的时候，这种循环回路就逐渐变成了实体的“我”——一个统一的因果主体。

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** α
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 φ
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** ($\underline{\text{AIXI}^S/\text{AIXI}^{t\ell}}$) interacts with the environment.
- The **Searcher** ($\underline{\text{LSEARCH}/\text{HSEARCH}/\text{OOPS}}$) 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

$$u\big[s(t) \oplus \big(switchbit(t) = 1\big), e(t)\big] > u\big[s(t) \oplus \big(switchbit(t) = 0\big), e(t)\big]$$

- theorem prover

hardware, costs, environment, initial state, utility, logic/arithmetic/probability

ENVIRONMENT
initial software p(1)
storage writable by proof searcher:
proof
switchprog
switchbit
temporary storage of proof technique
currently tested proof technique
initial proof searcher:
proof technique tester
axioms for hard– ware, initial soft– ware, environment, costs & goals
initial problem solver for interaction with environment
temporary storage of solver
output y
input x
time
other hardware variables
writable by proof techniques
writable by switchprog
storage readable by proof techniques
hardware– writable

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. (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

$$\boxed{\varphi_e = \varphi_{h(e)}}$$

$$\boxed{\text{self-reference} \overset{?}{\Longrightarrow} \text{self-improvement}}$$

Gödel Machines

1. 一次自我升级：Kleene's fixpoint theorem

$$\varphi_e = \varphi_{h(e)}$$

   - 全局最优？
   - 目标正交？目标 vs 手段
2. 持续自我升级：Kleene's fixpoint theorem with parameters

$$\varphi_{e(y)} = \varphi_{h(e(y),y)}$$

   - "实时"全局最优？人机交互？
   - 智能爆炸/技术奇点 ??? 持续升级 $\neq$ 指数迭代
3. 超越可计算：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

$$\mathbb{T} \vdash \Box_{\mathbb{T}'}\varphi \to \varphi \implies \mathbb{T} \vdash Con(\mathbb{T}')$$

   - 生物进化：达尔文 PK 拉马克
   - 生命 3.0
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.
   - 心理学："过程忽视"、"峰终定律"
   - 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: α is fixpoint-free), then there is a limit to self-inspection.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

8 Modal Logic

9 Logic vs Game Theory

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.

$$n = \prod_{i=1}^{m} p_i^{e_i} \implies e_i \leq \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor \implies \#\left\{(e_1, \ldots, e_m) \colon \prod_{i=1}^{m} p_i^{e_i} \leq n\right\} \leq$$
$$\prod_{i=1}^{m} \left(\left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor + 1 \right) \leq (\ln n)^m \ll n$$

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 $N \leq \#\left\{(r, s) \colon rs^2 \leq N \text{ and } r \text{ is squre-free}\right\} \leq 2^{\#\mathbb{P}}\sqrt{N}$.

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.

$\forall n \geq 1 \exists p \in \mathbb{P} \colon n < p \leq 2n$.

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 $\exists m \forall p_i \in \{p_1, \ldots, p_n\} \colon p_i \nmid m$.

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 $f(n) := \#\{k \in \mathbb{P} \colon p \mid n\}$, and $P := \prod_{p \in \mathbb{P}} p$. Obviously, $\forall n \colon f(n) = f(n+P)$. 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, $\{k \in \mathbb{N} \colon \gcd(k, P) = 1\} = \{2^i \colon i \in \mathbb{N}\}$. In particular, $\gcd(2, P) = 1$, then $\gcd(P-2, P) = 1$. Therefore, $P - 2 \in \{2^i \colon i \in \mathbb{N}\}$ 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 the following program q:

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 $\mathbb{T}$, $\exists c \forall x \colon \mathbb{T} \nvdash K(x) > c$.

"given n, find $\mu y\big[prf_{\mathbb{T}}\big(y, K(x) > n\big)\big]$, 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 $\mu y\big[prf_{\mathbb{T}}\big(y, K(x) > e\big)\big]$, ouput x" (Berry Paradox)

Theorem (Chaitin)

For any arithmetically sound Gödelian $\mathbb{T}$, $\big|\big\{x \colon \mathbb{T} \vdash K(x) > \ell(x)\big\}\big| < \infty$.

Incompressibility vs Incompleteness vs Berry Paradox

Definition (Kolmogorov Complexity H)

$$H(x|y) := \mu e[\varphi_e(y) = x]$$
$$H(x) := H(x|\epsilon)$$

Theorem (Chaitin)

For any arithmetically sound Gödelian $\mathbb{T}$, $\exists c \forall x : \mathbb{T} \nvdash H(x) > c$.

Proof.

For any m, construct:

$$M_n := \text{“find } \mu y\big[prf_{\mathbb{T}}\big(y, H(x) > m\big)\big], \text{output } x\text{”}$$

Then there exists a computable $f : m \mapsto n$.

By Kleene's fixpoint theorem,

$$\exists e : M_e = M_{f(e)} = \text{“find } \mu y\big[prf_{\mathbb{T}}\big(y, H(x) > e\big)\big], \text{output } x\text{”}$$

Take $c := e$.

Incompressibility vs Incompleteness vs Intelligence

- $P(x) := \{p \in \mathcal{X}^* : \exists m \forall n \geq m \, (p(x_{1:n}) = x_{n+1})\}$
- $P(A) := \bigcap_{x \in A} P(x)$
- $P_n := P(\{x : Km(x) \leq n\})$

- $\forall n \exists p \in P_n : K(p) \overset{+}{\leq} n + O(\log n)$
- $\forall n : p \in P_n \implies K(p) \overset{+}{\geq} n$

Theorem (Legg)

For any arithmetically sound Gödelian $\mathbb{T}$, $\exists n \forall p : \mathbb{T} \nvdash p \in P_n$.

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 Ω.

Halting Probability

Lemma

$$\Omega \equiv_T \chi_E$$

Proof.

If a program p of length $\leq n$ is not in $E_{t(n)}$ then it is not in E at all. Otherwise,

$$\Omega^t + 2^{-n} \leq \Omega^t + 2^{-\ell(p)} < \Omega$$

conflicts with

$$\Omega_{1:n} \leq \Omega^t < \Omega < \Omega_{1:n} + 2^{-n}$$

It follows that $\chi_{E_{1:2^n}}$ can be computed from $\Omega_{1:n}$.

Randomness of Ω

Theorem (Randomness of Ω)

$$\exists c \forall n \colon K(\Omega_{1:n}) \geq n - c$$

Proof.

$$\varphi(\Omega_{1:n}) := \mu x \left[2^{<\omega} \setminus \left\{ U(p) \colon p \in E_{t(n)} \right\} \right]$$

Obviously, φ is computable.

$$n < K(\varphi(\Omega_{1:n})) \overset{+}{\leq} K(\Omega_{1:n}) + K(\varphi) \overset{+}{\leq} K(\Omega_{1:n})$$

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 Ω Incompleteness)

For any arithmetically sound Gödelian $\mathbb{T}$, $\mathbb{T}$ can determine at most finitely many (scattered) bits of Ω.

Proof.

Assume $\mathbb{T}$ can provide infinitely many bit of Ω.
Any k different bits $i_1, i_2, \ldots, i_k$ of Ω give us a covering A_k of measure 2^{-k} which includes Ω.

$$A_k := \left\{ s_1 \Omega_{i_1} \cdots s_k \Omega_{i_k} 2^\omega : \forall 1 \leq j \leq k \left(s_j \in 2^{<\omega} \ \& \ \ell(s_j) = i_j - i_{j-1} - 1 \right) \right\}$$

$$\mu(A_k) = \frac{2^{i_k - k}}{2^{i_k}} = 2^{-k}$$

Thereby,

$$\forall k \left[\mu(A_k) \leq 2^{-k} \ \ \& \ \ \Omega \in A_k \right]$$

which contradicts the Martin-Löf randomness of Ω.

Definition (Busy Beaver)

$$\Sigma(n) := \max\{x \colon K(x) \leq n\}$$
$$\sigma(n) := \mu t \left[\Omega^t_{1:n} = \Omega_{1:n}\right]$$

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 $\exists c \forall n \colon K(\Omega_{1:n}) \geq n - c$, 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 φ, $\Sigma \overset{+}{\geq} \varphi$ and $\sigma \overset{+}{\geq} \varphi$.

Proof.

$$K(\varphi(n)) \overset{+}{\leq} K(n) + K(\varphi) \lesssim n \implies \Sigma \overset{+}{\geq} \varphi$$

Theorem (Chaitin Busy Beaver Incompleteness)

For any arithmetically sound Gödelian $\mathbb{T}$, $\exists n \forall x \colon \mathbb{T} \nvdash \sigma(n) \leq x$.

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory
- Computability
- Diagonal Method
- Incompressibility Method
- Incompleteness

8 Modal Logic

9 Logic vs Game Theory

Fixpoint Lemma

Lemma (Fixpoint Lemma)

For any wff $\alpha(x)$ with one free variable x, there exists a sentence β s.t.

$$Q \vdash \beta \leftrightarrow \alpha(\ulcorner \beta \urcorner)$$

Gödel's First Incompleteness Theorem

Theorem (Gödel's First Incompleteness Theorem)

For any Gödelian $\mathbb{T} \supset Q$, $\mathrm{Cn}(\mathbb{T}) \subsetneq \mathrm{Th}(\mathcal{N})$.

Gödel's First Incompleteness Theorem

$$\alpha(x) := \neg\Box_{\mathbb{T}} x$$

$$\beta = \text{“I am not provable.”}$$

$$\mathcal{N} \vDash \beta \iff \mathbb{T} \nvdash \beta$$

We now know enough to know that we will never know everything.

For every record player, there are records that it can't play.

(sympathetic vibration)

Gödel-Rosser's Incompleteness Theorem

Rosser's Trick

$$\Box^R_{\mathbb{T}} x := \exists y \left[prf_{\mathbb{T}}(y, x) \wedge \neg \exists z < y \; prf_{\mathbb{T}}\big(z, N(x)\big) \right]$$

where $N \colon \ulcorner \varphi \urcorner \mapsto \ulcorner \neg \varphi \urcorner$

$$\alpha(x) := \neg \Box^R_{\mathbb{T}} x$$

$\beta =$ "For every proof of me, there is a shorter proof of my negation."

Tarski's Undefinability Theorem

Tarski's Undefinability Theorem

suppose $\left\{\ulcorner\varphi\urcorner : \mathcal{N} \vDash \varphi\right\}$ is definable by δ.

$$\alpha(x) := \neg\delta(x)$$

$\beta =$ "I am not true."

Provability Conditions

Provability Conditions

For any Gödelian $\mathbb{T} \supset \mathrm{PA}$,

1. $\mathbb{T} \vdash \varphi \implies Q \vdash \Box_{\mathbb{T}}\varphi$
2. $\mathrm{PA} \vdash \Box_{\mathbb{T}}\varphi \to \Box_{\mathbb{T}}\Box_{\mathbb{T}}\varphi$
3. $\mathrm{PA} \vdash \Box_{\mathbb{T}}(\varphi \to \psi) \to \Box_{\mathbb{T}}\varphi \to \Box_{\mathbb{T}}\psi$

Löb's Theorem

Theorem (Löb's Theorem)

For any Gödelian $\mathbb{T} \supset \mathrm{PA}$, $\mathbb{T} \vdash \Box_{\mathbb{T}}(\Box_{\mathbb{T}}\varphi \to \varphi) \to \Box_{\mathbb{T}}\varphi$.

Corollary

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \to \varphi \implies \mathbb{T} \vdash \varphi$$

Löb's Theorem

$$\alpha(x) := \Box_{\mathbb{T}}x \to \varphi$$

β = "If I am provable, then φ."

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 $\mathbb{T} \supset \mathrm{PA}$, $\mathbb{T} \vdash Con(\mathbb{T}) \to \neg\Box_{\mathbb{T}} Con(\mathbb{T})$.

Proof.

$$\mathbb{T} \vdash \Box_{\mathbb{T}}(\Box_{\mathbb{T}}\bot \to \bot) \to \Box_{\mathbb{T}}\bot \implies \mathbb{T} \vdash Con(\mathbb{T}) \to \neg\Box_{\mathbb{T}} Con(\mathbb{T})$$

$$\mathrm{PA} \nvdash \neg\Box_{\mathrm{PA}} Con(\mathrm{PA})$$

$$\mathrm{PA} \nvdash Con(\mathrm{PA})$$

$$\mathrm{PA}^* \vdash \neg Con(\mathrm{PA}^*) \text{ where } \mathrm{PA}^* = \mathrm{PA} + \neg Con(\mathrm{PA})$$

Remark: The second incompleteness theorem does not imply that the consistency of a system $\mathbb{T}$ can only be proved in a stronger system.

Gödel's Second Incompleteness Theorem

$$\mathbb{T} \vdash Con(\mathbb{T}) \rightarrow Con(\mathbb{T} + \neg Con(\mathbb{T}))$$

Proof.

$$\mathbb{T} \vdash Con(\mathbb{T}) \rightarrow \neg \Box_{\mathbb{T}} Con(\mathbb{T})$$
$$\mathbb{T} \vdash Con(\mathbb{T}) \rightarrow \neg \Box_{\mathbb{T}} (\neg Con(\mathbb{T}) \rightarrow \bot)$$
$$\mathbb{T} \vdash Con(\mathbb{T}) \rightarrow Con(\mathbb{T} + \neg Con(\mathbb{T}))$$

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

$$\mathbb{T} \nvdash Con(\mathbb{T})$$

Proof.

$$\mathbb{T} \vdash \varphi \leftrightarrow \neg\Box_{\mathbb{T}}\varphi$$

$$\mathbb{T} \vdash \varphi \to (\Box_{\mathbb{T}}\varphi \to \bot)$$

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \to \Box_{\mathbb{T}}(\Box_{\mathbb{T}}\varphi \to \bot)$$

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \to \Box_{\mathbb{T}}\bot$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \to \neg\Box_{\mathbb{T}}\varphi$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \implies \mathbb{T} \vdash \neg\Box_{\mathbb{T}}\varphi$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \implies \mathbb{T} \vdash \varphi$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \implies \mathbb{T} \vdash \Box_{\mathbb{T}}\varphi$$

$$\mathbb{T} \nvdash Con(\mathbb{T})$$

second incompleteness $\implies$ Löb

Löb's Theorem

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \to \varphi \iff \mathbb{T} \vdash \varphi$$

Proof.

Assume $\mathbb{T} \nvdash \varphi$.

Then $\mathbb{T} + \neg\varphi$ is consistent.

$$\mathbb{T} + \neg\varphi \nvdash Con(\mathbb{T} + \neg\varphi)$$

$$\mathbb{T} + \neg\varphi \nvdash \neg\Box_{\mathbb{T}}(\neg\varphi \to \bot)$$

$$\mathbb{T} + \neg\varphi \nvdash \neg\Box_{\mathbb{T}}\varphi$$

$$\mathbb{T} \nvdash \Box_{\mathbb{T}}\varphi \to \varphi$$

Let φ be the Gödel sentence s.t. $\mathbb{T} \vdash \varphi \leftrightarrow \neg\Box_{\mathbb{T}}\varphi$. Then

$$\mathbb{T} \vdash \varphi \leftrightarrow Con(\mathbb{T})$$

Proof.

$(\rightarrow)$:

$$\mathbb{T} \vdash \bot \rightarrow \varphi$$
$$\mathbb{T} \vdash \Box_{\mathbb{T}}\bot \rightarrow \Box_{\mathbb{T}}\varphi$$
$$\mathbb{T} \vdash \Box_{\mathbb{T}}\bot \rightarrow \neg\varphi$$
$$\mathbb{T} \vdash \varphi \rightarrow Con(\mathbb{T})$$

$(\leftarrow)$:

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \rightarrow \Box_{\mathbb{T}}\Box_{\mathbb{T}}\varphi$$
$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \rightarrow \Box_{\mathbb{T}}\neg\varphi$$
$$\mathbb{T} \vdash \Box_{\mathbb{T}}\varphi \rightarrow \Box_{\mathbb{T}}(\varphi \wedge \neg\varphi)$$
$$\mathbb{T} \vdash Con(\mathbb{T}) \rightarrow \varphi$$

Fixpoint

1. For any Gödelian $\mathbb{T} \supset \mathrm{PA}$, $Con(\mathbb{T})$ is the only fixpoint of $\neg\Box_{\mathbb{T}}x$ up to the logical equivalence in $\mathbb{T}$.
2. For any Gödelian $\mathbb{T} \supset \mathrm{PA}$, $\top$ is the only fixpoint of $\Box_{\mathbb{T}}x$ up to the logical equivalence in $\mathbb{T}$.

Surprise Exam Paradox vs Second Incompleteness Theorem

$$\boxed{\mathbb{T} \nvdash Con(\mathbb{T})}$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \to \forall x \neg \Box_{\mathbb{T}} \big(K(x) > c\big) \qquad \text{(Chaitin)}$$

$$\mathbb{T} \vdash Con(\mathbb{T}) \implies \mathbb{T} \vdash \forall x \in \mathcal{X}^{c+1} \neg \Box_{\mathbb{T}} \big(K(x) > c\big)$$

$$\mathbb{T} \vdash \forall x \in \mathcal{X}^{c+1} \big[K(x) \leq c \to \Box_{\mathbb{T}} \big(K(x) \leq c\big)\big] \qquad (\Sigma_1\text{-complete})$$

$$m := \Big|\big\{x \in \mathcal{X}^{c+1} \colon K(x) > c\big\}\Big|$$

$$\mathbb{T} \vdash 1 \leq m \leq 2^{c+1}$$

We prove by induction that for $1 \leq i \leq 2^{c+1}$,

$$\mathbb{T} \vdash m \geq i \implies \mathbb{T} \vdash m \geq i + 1$$

$$\mathbb{T} \vdash m \geq i \implies \mathbb{T} \vdash m \geq i+1$$

Proof.

Assume $\mathbb{T} \vdash m \geq i$. Let $r := 2^{c+1} - i$.

$$\mathbb{T} \vdash m = i \to \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^{r} \big(K(y_k) \leq c\big)$$

$$\mathbb{T} \vdash m = i \to \exists \text{ different } y_1 \dots y_r \in \mathcal{X}^{c+1} \bigwedge_{k=1}^{r} \Box_{\mathbb{T}}\big(K(y_k) \leq c\big)$$

$$\forall x \in \mathcal{X}^{c+1} \setminus \{y_1, \dots, y_r\}\colon\ \mathbb{T} \vdash m \geq i \to \left(\bigwedge_{k=1}^{r} \big(K(y_k) \leq c\big) \to \big(K(x) > c\big) \right)$$

$$\mathbb{T} \vdash \Box_{\mathbb{T}}\big(m \geq i\big) \to \left(\bigwedge_{k=1}^{r} \Box_{\mathbb{T}}\big(K(y_k) \leq c\big) \to \Box_{\mathbb{T}}\big(K(x) > c\big) \right)$$

$$\mathbb{T} \vdash m = i \wedge \Box_{\mathbb{T}}\big(m \geq i\big) \to \exists x \in \mathcal{X}^{c+1} \Box_{\mathbb{T}}\big(K(x) > c\big)$$

$$\mathbb{T} \vdash m \neq i$$

- syntactic completeness: $\Box_{\mathbb{T}}\varphi \vee \Box_{\mathbb{T}}\neg\varphi$
- semantic completeness: $\varphi \to \Box_{\mathbb{T}}\varphi$
- ω-completeness: $\forall x \Box_{\mathbb{T}}\varphi(x) \to \Box_{\mathbb{T}}\forall x\varphi(x)$

$$\omega\text{-complete} \implies \omega\text{-consistent} \implies 1\text{-consistent} \implies \text{consistent}$$

Theorem

For any Gödelian $\mathbb{T} \supset \mathrm{PA}$, the following are equivalent in $\mathbb{T}$.

1. $\neg Con(\mathbb{T})$
2. $\Box_{\mathbb{T}}\varphi \vee \Box_{\mathbb{T}}\neg\varphi$
3. $\varphi \to \Box_{\mathbb{T}}\varphi$
4. $\forall x \Box_{\mathbb{T}}\varphi(x) \to \Box_{\mathbb{T}}\forall x\varphi(x)$

Incompatibility

1. consistency
2. effectiveness $\mathrm{Th}(\mathcal{N})$
3. richness Real closed field/Euclidean geometry/Presburger
4. completeness Q / PA / ZFC

Parikh Sentences

Parikh Sentences

There are true sentences that have very long proofs, but there are relatively short proof of the fact that the sentences are provable.

$$prflen_{\mathbb{T}}(m) := \text{“the length of the proof encoded by } m\text{”}$$

$$\Box^{n}_{\mathbb{T}} x := \exists m \big(prf_{\mathbb{T}}(m, x) \wedge prflen_{\mathbb{T}}(m) < n \big)$$

$$\alpha(x) := \neg \Box^{n}_{\mathbb{T}} x$$

$\beta =$ “I have no proof of myself shorter than n.”

$$\neg \Box_{\mathbb{T}} \beta \implies \beta \implies \Box_{\mathbb{T}} \beta$$

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 $\beta(x)$ of one free variable such that $\forall x \beta(x)$ is true, but for each n, $\beta(n)$ has no proof with fewer than $f(n)$ steps.

Gödel's No-short-proof Theorem

$$\alpha(x) := \neg \Box_{\mathbb{T}}^{f(y)} x$$

$\beta(y) =$ "I have no proof of myself shorter than $f(y)$."

$$\neg\beta(n) \implies \Box_{\mathbb{T}}^{f(n)} \beta(n) \implies \beta(n)$$

Remark: it is easily seen that the fixpoint lemma applies also to formulas with free variables.

$$\boxed{\text{Gödel's no-short-proof theorem} \implies \mathbb{T} \nvdash \forall x \beta(x)}$$

Undecidability

$\boxed{Q \text{ is incomplete.}}$

Theorem (Σ_1-completeness of Robinson Arithmetic Q)

For any Gödelian $\mathbb{T} \supset Q$, and any sentence $\varphi \in \Sigma_1$, $Q \vdash \varphi \to \Box_{\mathbb{T}}\varphi$.

Theorem (Strong Undecidability of Q)

If $\mathbb{T} \cup Q$ is consistent, then $\mathbb{T}$ 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 φ has a finite model, then it has a model of size at most $f(\varphi)$. 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.

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 10th Problem is Unsolvable

Definition (Diophantine Set)

A set $A \subset \mathbb{N}^n$ is diophantine if there exists a polynomial $P(\boldsymbol{x}, \boldsymbol{y})$ with integer coefficients s.t.

$$\boldsymbol{x} \in A \iff \exists \boldsymbol{y} \in \mathbb{N}^m [P(\boldsymbol{x}, \boldsymbol{y}) = 0]$$

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.

Hilbert's Program

1. Formalization & Axiomatization (Richness): Formalize and axiomatize (recursively) the elementary logic $\mathbb{L}$, the "finitistic" mathematics $\mathbb{F}$ (which is concerned with the real world) and the "infinitistic" mathematics $\mathbb{T}$ (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 $\mathbb{L}$; (2) all true mathematical statements can be proved in $\mathbb{T}$.
4. **Consistency**: a finitistic proof that no contradiction can be proved in $\mathbb{T}$.
5. Conservation(Consequence of Consistency $\forall \varphi \in \Pi_1 : \mathbb{T} \vdash \varphi \implies \mathbb{F}, Con(\mathbb{T}) \vdash \varphi$): any statement about 'real objects' provable in $\mathbb{T}$ can be proved in $\mathbb{F}$.
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? $\mathbb{T}$ characterizes exactly one model up to isomorphism.

Reverse Mathematics

$$\underbrace{\Gamma_r \cup \Gamma_m \cup \Gamma_b \vdash \varphi \qquad\qquad \mathcal{M}_r \vDash \Gamma_r}$$

$$\Downarrow ?$$

$$\mathcal{M}_r \vDash \varphi$$

$$\frac{\Gamma_r \cup \Gamma_r' \vdash \varphi \quad \mathcal{M}_r \vDash \Gamma_r \cup \Gamma_r'}{\mathcal{M}_r \vDash \varphi}$$

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 PA *is consistent.*

Goodstein Function

Definition (Goodstein Function)

Define $G_n(m)$ as follows: if $m = 0$ then $G_n(m) = 0$, if $m \neq 0$ then $G_n(m)$ is a number obtained by replacing every n in the base n representation of m by $n+1$ and then subtracting 1. Let

$$m_0 := m$$
$$m_k := G_{k+1}(m_{k-1})$$
$$f_G(m) := \mu k[m_k = 0]$$

$$m_0 = 266 = 2^{2^{2+1}} + 2^{2+1} + 2^1$$
$$m_1 = G_2(m_0) = 3^{3^{3+1}} + 3^{3+1} + 2 \approx 10^{38}$$
$$m_2 = G_3(m_1) = 4^{4^{4+1}} + 4^{4+1} + 1 \approx 10^{616}$$
$$m_3 = G_4(m_2) = 5^{5^{5+1}} + 5^{5+1} \approx 10^{10000}$$

Fast-growing Hierarchy

Definition (Wainer Hierarchy)

$$f_0(n) := n+1$$
$$f_{\alpha+1}(n) := f_\alpha^n(n)$$
$$f_\alpha(n) := f_{\alpha[n]}(n) \text{ if } \alpha \text{ is a limit ordinal.}$$

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 α, then $\lambda[n] := \omega^{\alpha[n]}$
- if $\lambda = \varepsilon_0$, then $\lambda[0] := 0$ and $\lambda[n+1] := \omega^{\lambda[n]}$

- $\alpha < \beta < \varepsilon_0 \implies f_\alpha < f_\beta$
- For any primitive recursive function f, $\exists \alpha < \omega \colon f < f_\alpha$
- Every f_α with $\alpha < \varepsilon_0$ is computable, and provably total in PA.
- If f is computable and provably total in PA, then $\exists \alpha < \varepsilon_0 \colon f < f_\alpha$. Hence f_{ε_0} is not provably total in PA.

Kirby-Paris Theorem vs Goodstein Theorem

Theorem

$$\forall \alpha < \varepsilon_0 \, (f_\alpha < f_G)$$

$$\mathrm{ZFC} \vdash \forall m \exists k (m_k = 0) \quad \text{but} \quad \mathrm{PA} \nvdash \forall m \exists k (m_k = 0)$$

$$\Sigma(n) := \max\{m \colon K(m) \leq n\}$$

$$\varphi < \Sigma \ \text{ for any computable } \varphi$$

$$\mathrm{PA} \nvdash \forall n \exists m (\Sigma(n) = m)$$

$$\exists n \forall m \colon \mathrm{PA} \nvdash \Sigma(n) \leq m$$

For any arithmetically sound Gödelian $\mathbb{T}$: $\exists n \forall m \colon \mathbb{T} \nvdash \Sigma(n) \leq m$

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)

Platonic
mathematical
world
3
1
2
Mental
world
Physical
world

Mind
Math
Matter

Mind
Math
?
Matter

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

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

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic
- Syntax
- Semantics
- Formal System
- Formal Theory of Knowledge

9 Logic vs Game Theory

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)

Syntax

Language

$$\mathscr{L} := \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \Box, \Diamond, (,)\} \cup \mathscr{P}$$

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

Well-Formed Formula WFF

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid \varphi \leftrightarrow \varphi \mid \Box\varphi \mid \Diamond\varphi$$

- It will always be φ. $G\varphi$
- You ought to do φ. $O\varphi$
- I know φ. $K_i\varphi$
- I believe φ. $B_i\varphi$
- φ is provable in $\mathbb{T}$. $\Box_{\mathbb{T}}\varphi$
- After the execution of the program π, φ holds. $[\pi]\varphi$

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
   - Syntax
   - Semantics
   - Formal System
   - Formal Theory of Knowledge
9. Logic vs Game Theory

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 $V \colon \mathscr{P} \to P(W)$.

- $\mathcal{M}, w \Vdash p$ if $w \in V(p)$
- $\mathcal{M}, w \Vdash \neg\varphi$ if $\mathcal{M} \nVdash \varphi$
- $\mathcal{M}, w \Vdash \varphi \wedge \psi$ if $\mathcal{M}, w \Vdash \varphi$ and $\mathcal{M}, w \Vdash \psi$
- $\mathcal{M}, w \Vdash \Box\varphi$ if $\forall v \in W \colon Rwv \implies \mathcal{M}, v \Vdash \varphi$
- $\mathcal{M}, w \Vdash \Diamond\varphi$ if $\exists v \in W \colon Rwv$ and $\mathcal{M}, v \Vdash \varphi$

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

- φ is satisfiable at $\mathcal{M}, w$ if $\mathcal{M}, w \Vdash \varphi$.
- φ is true in $\mathcal{M}$ ($\mathcal{M} \Vdash \varphi$) if $\forall w \in W\colon \mathcal{M}, w \Vdash \varphi$
- φ is valid in a pointed frame $\mathcal{F}, w$ ($\mathcal{F}, w \Vdash \varphi$) if $\mathcal{M}, w \Vdash \varphi$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- φ is valid in $\mathcal{F}$ ($\mathcal{F} \Vdash \varphi$) if $\mathcal{M} \Vdash \varphi$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- $\Vdash \varphi$ if $\mathcal{F} \Vdash \varphi$ for every $\mathcal{F}$.

Truth is in the eye of the beholder.

Example

$$\Vdash \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$$

Semantic Consequence

- local semantic consequence

$$\Gamma \Vdash_{\mathcal{C}} \varphi \;:=\; \forall \mathcal{M} \in \mathcal{C} \forall w \in W \colon \mathcal{M}, w \Vdash \Gamma \implies \mathcal{M}, w \Vdash \varphi$$

- global semantic consequence

$$\Gamma \Vdash^{g}_{\mathcal{C}} \varphi \;:=\; \forall \mathcal{M} \in \mathcal{C} \colon \mathcal{M} \Vdash \Gamma \implies \mathcal{M} \Vdash \varphi$$

Example

- $p \nVdash_{\mathcal{C}} \Box p$
- $p \Vdash^{g}_{\mathcal{C}} \Box p$

Accessibility

1. $\forall x \exists y : Rxy$	serial
2. $\forall x : Rxx$	reflexive
3. $\forall xy : Rxy \to Ryx$	symmetric
4. $\forall xyz : Rxy \wedge Ryz \to Rxz$	transitive
5. $\forall xyz : Rxy \wedge Rxz \to Ryz$	euclidean
6. $\forall xy : Rxy \vee Ryx$	total
7. $\exists x \forall y : \neg Rxy \wedge \neg Ryx$	isolation
8. $\forall x \exists y : Rxy \wedge Ryy$	successor reflexive
9. $\forall xy : Rxy \to \neg Ryx$	asymmetric
10. $\forall xy : Rxy \wedge Ryx \to x = y$	antisymmetric

Accessibility

Theorem

D	$W, R \Vdash \Box\varphi \to \Diamond\varphi$	$\iff$	R *is serial*
T	$W, R \Vdash \Box\varphi \to \varphi$	$\iff$	R *is reflexive*
B	$W, R \Vdash \varphi \to \Box\Diamond\varphi$	$\iff$	R *is symmetric*
4	$W, R \Vdash \Box\varphi \to \Box\Box\varphi$	$\iff$	R *is transitive*
5	$W, R \Vdash \Diamond\varphi \to \Box\Diamond\varphi$	$\iff$	R *is euclidean*

Counter-model for D,T,B,4,5

Standard Translation

Definition (Standard Translation)

$$T_x(p) = P(x) \qquad T_y(p) = P(y)$$

$$T_x(\neg\varphi) = \neg T_x(\varphi) \qquad T_y(\neg\varphi) = \neg T_y(\varphi)$$

$$T_x(\varphi \wedge \psi) = T_x(\varphi) \wedge T_x(\psi) \qquad T_y(\varphi \wedge \psi) = T_y(\varphi) \wedge T_y(\psi)$$

$$T_x(\Box\varphi) = \forall y(R(x,y) \to T_y(\varphi)) \qquad T_y(\Box\varphi) = \forall x(R(y,x) \to T_x(\varphi))$$

Theorem (Correspondence on Models)

$$\mathcal{M}, w \Vdash \varphi \iff \mathcal{M} \vDash T_x(\varphi)[w]$$

$$\mathcal{M} \Vdash \varphi \iff \mathcal{M} \vDash \forall x T_x(\varphi)$$

$$\mathcal{F}, w \Vdash \varphi \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n T_x(\varphi)[w]$$

$$\mathcal{F} \Vdash \varphi \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n \forall x T_x(\varphi)$$

Tree Method for Modal Logic

$$w \Vdash \Box\varphi$$
$$\Big|$$
$$w' \Vdash \varphi$$

if Rww' is already in the branch.

$$w \nVdash \Box\varphi$$
$$\Big|$$
$$Rww'$$
$$w' \nVdash \varphi$$

where w' is new in the branch.

$$w \Vdash \Diamond\varphi$$
$$\Big|$$
$$Rww'$$
$$w' \Vdash \varphi$$

where w' is new in the branch.

$$w \nVdash \Diamond\varphi$$
$$\Big|$$
$$w' \nVdash \varphi$$

if Rww' is already in the branch.

Example — Tree Method for Modal Logic

$$\boxed{\Vdash \Box p \wedge \Diamond q \rightarrow \Diamond(p \wedge q)}$$

$$w \Vdash \Box p \wedge \Diamond q$$
$$w \Vdash \neg\Diamond(p \wedge q)$$

$$w \Vdash \Box p$$
$$w \Vdash \Diamond q$$

$$Rwv$$
$$v \Vdash q$$

$$v \Vdash p$$

$$v \Vdash \neg(p \wedge q)$$

$$v \Vdash \neg p \qquad\qquad v \Vdash \neg q$$

$\times$ $\times$

Contents

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic
- Syntax
- Semantics
- Formal System
- Formal Theory of Knowledge

9 Logic vs Game Theory

Formal System = Axiom + Inference Rule

Axiom Schema

- tautologies
- $\Diamond\varphi \leftrightarrow \neg\Box\neg\varphi$ Dual
- $\Box(\varphi \to \psi) \to \Box\varphi \to \Box\psi$ K
- $\Box\varphi \to \Diamond\varphi$ D
- $\Box\varphi \to \varphi$ T
- $\varphi \to \Box\Diamond\varphi$ B
- $\Box\varphi \to \Box\Box\varphi$ 4
- $\Diamond\varphi \to \Box\Diamond\varphi$ 5
- $\Box(\Box\varphi \to \varphi) \to \Box\varphi$ L

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\text{MP}] \qquad \frac{\varphi}{\Box\varphi}\ [\text{N}]$$

Intuitionistic Logic vs Modal Logic

$$\boldsymbol{S}4 := K + T + 4$$

$$\boldsymbol{Grz} := \boldsymbol{S}4 + \Box(\Box(\varphi \to \Box\varphi) \to \varphi) \to \varphi$$

$$p^* := \Box p$$
$$(\neg\varphi)^* := \Box\neg\varphi^*$$
$$(\varphi \wedge \psi)^* := \varphi^* \wedge \psi^*$$
$$(\varphi \vee \psi)^* := \varphi^* \vee \psi^*$$
$$(\varphi \to \psi)^* := \Box(\varphi^* \to \psi^*)$$

$$\vdash_{\boldsymbol{I}} \varphi \iff \vdash_{\boldsymbol{S}4} \varphi^* \iff \vdash_{\boldsymbol{Grz}} \varphi^*$$

$$\boldsymbol{GL} := K + L$$

$$p' := p$$
$$(\neg\varphi)' := \neg\varphi'$$
$$(\varphi \wedge \psi)' := \varphi' \wedge \psi'$$
$$(\varphi \vee \psi)' := \varphi' \vee \psi'$$
$$(\varphi \to \psi)' := \varphi' \to \psi'$$
$$(\Box\varphi)' := \varphi' \wedge \Box\varphi'$$

$$\vdash_{\boldsymbol{Grz}} \varphi \iff \vdash_{\boldsymbol{GL}} \varphi'$$
$$\vdash_{\boldsymbol{I}} \varphi \iff \vdash_{\boldsymbol{GL}} (\varphi^*)'$$

Theorem (Craig Interpolation)

If $\boldsymbol{GL} \vdash \varphi \to \psi$*, then there is a* χ *with* $\mathrm{Var}(\chi) \subset \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi)$ *s.t.*

$$\boldsymbol{GL} \vdash \varphi \to \chi \quad \text{and} \quad \boldsymbol{GL} \vdash \chi \to \psi$$

Corollary (Beth Definability)

Assume $\boldsymbol{GL} \vdash \varphi(p) \wedge \varphi(q) \to (p \leftrightarrow q)$ *where* $q \notin \mathrm{Var}(\varphi)$ *and* $\varphi(q)$ *is obtained from* $\varphi(p)$ *by replacing all occurrences of* p *by* q*. Then there exists a formula* ψ *with* $\mathrm{Var}(\psi) \subset \mathrm{Var}(\varphi) \setminus \{p\}$ *s.t.*

$$\boldsymbol{GL} \vdash \varphi(p) \to (p \leftrightarrow \psi)$$

Proof.

Let ψ be an interpolant for $\boldsymbol{GL} \vdash \varphi(p) \wedge p \to (\varphi(q) \to q)$.

Provability Logic

Theorem (Uniqueness of Fixpoint)

If p occurs only boxed in $\varphi(p)$ and $q \notin \mathrm{Var}(\varphi)$, then

$$\boldsymbol{GL} \vdash \boxdot\Big(\big(p \leftrightarrow \varphi(p)\big) \wedge \big(q \leftrightarrow \varphi(q)\big)\Big) \to (p \leftrightarrow q)$$

where $\boxdot\varphi := \varphi \wedge \Box\varphi$.

Corollary

If p occurs only boxed in $\varphi(p)$, then

$$\boldsymbol{GL} \vdash \psi \leftrightarrow \varphi(\psi) \ \& \ \boldsymbol{GL} \vdash \chi \leftrightarrow \varphi(\chi) \implies \boldsymbol{GL} \vdash \psi \leftrightarrow \chi$$

Theorem (Existence of Fixpoint)

If p occurs only boxed in $\varphi(p)$, then there exists a formula ψ with $\mathrm{Var}(\psi) \subset \mathrm{Var}(\varphi) \setminus \{p\}$ s.t.

$$\boldsymbol{GL} \vdash \psi \leftrightarrow \varphi(\psi)$$

$$\boxed{\text{Uniqueness of Fixpoint + Beth Definability} \implies \text{Existence of Fixpoint}}$$

$$\boldsymbol{GL} \vdash \neg\Box\bot \leftrightarrow \neg\Box(\neg\Box\bot) \qquad \boldsymbol{GL} \vdash \top \leftrightarrow \Box\top$$

Soundness & Completeness

Definition (Theorem & Local Syntactic Consequence)

- $\vdash_S \varphi$
- $\Gamma \vdash_S \varphi$ if $\vdash_S \bigwedge_{i=1}^{n} \psi_i \to \varphi$ for some finite subset $\{\psi_1, \ldots, \psi_n\} \subset \Gamma$.

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.

$$\Gamma \vdash_S \varphi \iff \Gamma \Vdash_C \varphi$$

Bisimulation

Definition (Bisimulation)

A bisimulation $Z\colon \mathcal{M} \leftrightarrows \mathcal{M}'$ 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

$$\Box_a(\Diamond_b \top \wedge \Diamond_c \top)$$

反对称性不可模态定义

假设公式 φ 定义反对称性，则对任意框架 $\mathcal{F}$：$\mathcal{F} \vDash \varphi \iff \mathcal{F}$ 是反对称的。考虑如上两个框架（下 $\mathcal{F}$，上 $\mathcal{F}'$）：$\mathcal{F} \vDash \varphi, \mathcal{F}' \nvDash \varphi$，这意味着 $\mathcal{F}'$ 有赋值 V' 和点 v 使得 $\mathcal{F}', V', v \nvDash \varphi$，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 $\mathcal{F}, V, w \nvDash \varphi$，这与 $\mathcal{F} \vDash \varphi$ 矛盾。

Bisimulation

Theorem (van Benthem Characterization Theorem)

Let $\varphi(x)$ be a first order formula. Then $\varphi(x)$ 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

1 Introduction

2 History

3 Propositional Logic

4 Predicate Logic

5 Equational Logic

6 Set Theory

7 Recursion Theory

8 Modal Logic
- Syntax
- Semantics
- Formal System
- Formal Theory of Knowledge

9 Logic vs Game Theory

知识的逻辑

- 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.

$$\exists x KKx \wedge \exists x K\neg Kx \wedge \exists x \neg K \neg Kx$$

- 知之为知之，不知为不知，是知也。

$$K\varphi \to KK\varphi \quad \& \quad \neg K\varphi \to K\neg K\varphi$$

"Real knowledge is to know the extent of one's ignorance." — *Confucius*

- Mutual Knowledge:

  everybody in G knows φ.

- Distributed Knowledge:

  everybody in G would know φ
  if agents in G shared all their information.

- Common Knowledge:

  everybody in G knows φ,
  everybody knows that everybody knows,
  and so on.

Mutual Knowledge

Suppose a group $G \subset \{1 \dots n\}$ of agents, everyone in G knows φ:

$$E_G\varphi \;:=\; \bigwedge_{i \in G} K_i\varphi$$

$$R_E \;:=\; \bigcup_{i \in G} R_i$$

$$\mathcal{M}, w \Vdash E_G\varphi \iff \forall v \in W\colon R_E wv \implies \mathcal{M}, v \Vdash \varphi$$

Distributed Knowledge

$$D_G\varphi \;:=\; \bigvee_{i\in G} K_i\varphi$$

$$R_D \;:=\; \bigcap_{i\in G} R_i$$

$$\mathcal{M}, w \Vdash D_G\varphi \iff \forall v \in W\colon R_D wv \implies \mathcal{M}, v \Vdash \varphi$$

$$w_2 \vDash K_1 p \wedge \neg K_1 q \wedge K_2 q \wedge \neg K_2 p \wedge D_{\{1,2\}}(p \wedge q)$$

Common Knowledge

$$E_G^1\varphi := E_G\varphi$$
$$E_G^{k+1}\varphi := E_G E_G^k\varphi$$
$$C_G\varphi := \bigwedge_{k=1}^{\infty} E_G^k\varphi$$

$$R^1 := R$$
$$R^{k+1} := R \circ R^k$$
$$R \circ S := \{(x, y) \colon \exists z(Rxz \wedge Szy)\}$$
$$R^* := \bigcup_{k=1}^{\infty} R^k$$

$$R_C := \left(\bigcup_{i \in G} R_i\right)^*$$

$$\mathcal{M}, w \Vdash C_G\varphi \iff \forall v \in W \colon R_C wv \implies \mathcal{M}, v \Vdash \varphi$$

A Hierarchy of States of Knowledge

$$C_G\varphi \implies \cdots E_G^k\varphi \implies \cdots E_G\varphi \implies \bigvee_{i \in G} K_i\varphi \implies D_G\varphi \implies \varphi$$

Can we easily have full common knowledge?

$$w_1 \vDash E_{\{1,2\}}p \wedge \neg C_{\{1,2\}}p$$

- 《三体》黑暗森林
- 假设 C 秘密的分别给了 A 和 B 两数字 2 和 3，他只告诉他们俩这两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？

$$(0,1) \overset{B}{\longleftrightarrow} (2,1) \overset{A}{\longleftrightarrow} \underline{(2,3)} \overset{B}{\longleftrightarrow} (4,3) \overset{A}{\longleftrightarrow} (4,5) \overset{B}{\longleftrightarrow} (6,5) \cdots$$

$$(2,3) \Vdash \neg K_B K_A K_B (x + y \leq 10)$$

- Let $p :=$ “every driver must drive on the right.” What kind of knowledge is enough to let people feel safe in driving on the right?

Coordinated Attack

Coordinated Attack

$$C_{Human}\Big(\forall x\Big(Man(x) \wedge Single(x) \wedge Fortune(x)$$

$$\downarrow$$

$$Desire_x\Big(\exists y\big(Woman(y) \wedge Marry(x,y)\big)\Big)\Big)$$

— *Jane Austen*

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新信息）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.
- $K_i \colon P(W) \to P(W)$ is agent i's knowledge operator. $K_i(\varphi) = \{w \colon \mathcal{I}_i(w) \subset \varphi\}$.
- Mutual Knowledge $E_G(\varphi) := \bigcap_{i \in G} K_i(\varphi)$.
- Common knowledge $C_G(\varphi) := \bigcap_{n=1}^{\infty} E_G^n(\varphi)$.

1. $K(W) = W$
2. $\varphi \subset \psi \implies K(\varphi) \subset K(\psi)$
3. $K(\varphi) \cap K(\psi) = K(\varphi \cap \psi)$
4. $K(\varphi) \subset \varphi$
5. $K(\varphi) \subset K(K(\varphi))$
6. $W \setminus K(\varphi) \subset K(W \setminus K(\varphi))$

Aumann's Agreement Theorem

Lemma

If $C_G(\varphi) \neq \emptyset$, *then* $\forall i \in G \exists \mathcal{D}_i \subset \mathcal{I}_i : C_G(\varphi) = \bigcup \mathcal{D}_i$.

Proof.

$w \in C_G(\varphi) \implies \forall i \forall n : w \in K_i E_G^n(\varphi) \implies \forall i \forall n : \mathcal{I}_i(w) \subset E_G^n(\varphi) \implies \forall i : \mathcal{I}_i(w) \subset C_G(\varphi)$

Theorem (Aumann's Agreement Theorem)

Let P *be the common prior belief, and* $A := \bigcap_{i \in G} \{w : P(\varphi | \mathcal{I}_i(w)) = q_i\}$. *If* $P(C_G(A)) > 0$, *then* $\forall i \in G : q_i = P(\varphi | C_G(A))$.

Proof.

$$P(\varphi | C_G(A)) = \frac{P(\varphi \cap \bigcup \mathcal{D}_i)}{\sum_{D \in \mathcal{D}_i} P(D)} = \frac{\sum_{D \in \mathcal{D}_i} P(\varphi | D) P(D)}{\sum_{D \in \mathcal{D}_i} P(D)} = \frac{\sum_{D \in \mathcal{D}_i} q_i P(D)}{\sum_{D \in \mathcal{D}_i} P(D)} = q_i$$

Epistemic Logic

- Knowledge $\boldsymbol{S}5 := K + T + 4 + 5$

$\boxed{\text{知之为知之(4)，不知为不知(5)，是知也}}$

- Belief $K + D + 4 + 5$
- Common Knowledge

$$\boldsymbol{S}5$$
$$+$$
$$C_G\varphi \leftrightarrow (\varphi \wedge E_G C_G \varphi)$$
$$+$$
$$(\varphi \wedge C_G(\varphi \rightarrow E_G\varphi)) \rightarrow C_G\varphi$$

- Distributed Knowledge

$$\boldsymbol{S}5$$
$$+$$
$$D_{\{i\}}\varphi \leftrightarrow K_i\varphi$$
$$+$$
$$D_G\varphi \rightarrow D_{G'}\varphi \ \text{ if } \ G \subset G'$$

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	$\neg B(p \wedge \neg Bp)$	

负自省公理

1. $\neg p \wedge BKp$ 假设你错误的相信你知道 p
2. $\neg Kp$ 知识蕴含真
3. $K\neg Kp$ 负自省公理
4. $B\neg Kp$ 知识至少是信念
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

$$\varphi ::= p \mid \neg\varphi \mid \varphi \wedge \varphi \mid K_i\varphi \mid [\varphi]\varphi$$

$$\mathcal{M}, w \Vdash [\psi]\varphi \;\text{ iff }\; \mathcal{M}, w \Vdash \psi \implies \mathcal{M}{\restriction}_{\psi}, w \Vdash \varphi$$

$$\mathcal{M}, w \Vdash \langle\psi\rangle\varphi \;\text{ iff }\; \mathcal{M}, w \Vdash \psi \;\;\&\;\; \mathcal{M}{\restriction}_{\psi}, w \Vdash \varphi$$

where

$$\mathcal{M}{\restriction}_{\psi} := \big(W', \{R'_i\}_{i\in G}, V'\big)$$

and

$$W' := \{w \in W : \mathcal{M}, w \Vdash \psi\} \quad R'_i := R_i{\restriction}_{W'\times W'} \quad V'(p) := V(p) \cap W'$$

Muddy Children Problem

$\mathcal{M}, mmc \Vdash m_1 \wedge m_2 \wedge \neg m_3$

$\mathcal{M}, mmc \Vdash E_{123}\varphi$

$\mathcal{M}, mmc \Vdash \neg C_{123}\varphi$

$\mathcal{M}, mmc \Vdash \neg K_1 m_1 \wedge K_1 m_2$

$\mathcal{M}, mmc \Vdash K_1 K_3 m_2 \wedge K_1 \neg K_2 m_2$

$\mathcal{M}\restriction_\varphi, mcc \Vdash K_1 m_1$

$\mathcal{M}\restriction_\varphi, mmc \Vdash \langle\chi\rangle\neg\chi$

$\mathcal{M}\restriction_\varphi, mmm \Vdash \langle\chi\rangle\chi$

$\mathcal{M}\restriction_\varphi\restriction_\chi, mmm \Vdash \langle\chi\rangle\neg\chi$

1. "At least one is muddy." $\varphi := m_1 \vee m_2 \vee m_3$
2. "Does anyone...?" $\chi := \neg\psi_1 \wedge \neg\psi_2 \wedge \neg\psi_3$ where $\psi_i := K_i m_i \vee K_i \neg m_i$
3. "Does anyone...?" $\gamma := \psi_1 \wedge \psi_2 \wedge \neg\psi_3$

$$\mathcal{M}, mmc \Vdash [\varphi][\chi][\gamma](K_1 m_1 \wedge K_2 m_2 \wedge K_3 \neg m_3)$$

$$\mathcal{M}, mmm \Vdash [\varphi][\chi][\chi](K_1 m_1 \wedge K_2 m_2 \wedge K_3 m_3)$$

Information Update

一个人口普查员去逻辑学家调查。

- 逻辑学家："我三个小孩的年龄加起来是门牌号，乘起来是 72。"
- 普查员看了一眼门牌号："我还是不知道你孩子多大啊。"
- 逻辑学家："哦，对了，我忘了说我们家老大喜欢咸豆腐脑了。"
- 普查员："那我知道了!"

问：小孩各多大?

大黄和老王都想知道小白的生日，小白列出了十个可能的日期：

$$5.15 \ / \ 5.16 \ / \ 5.19 \ / \ 6.17 \ / \ 6.18 \ / \ 7.14 \ / \ 7.16 \ / \ 8.14 \ / \ 8.15 \ / \ 8.17$$

接着分别告诉大黄和老王她生日的月和日，以下是大黄和老王的对话。

1. 大黄："我不知道小白的生日，但我知道你也不知道。"
2. 老王："一开始我不知道，现在我知道了。"
3. 大黄："那我也知道了。"

小白的生日是哪天？

不是所有被宣告的都会变成公共知识

$$[\psi][\chi]\varphi \Vdash\Dashv [\psi \wedge [\psi]\chi]\varphi$$

$$\Vdash [C_G\varphi]C_G\varphi$$

$$\overset{?}{\Vdash} \varphi \to [\varphi]C_G\varphi$$

$$\mathcal{M}, w \Vdash (p \wedge \neg Kp) \wedge [p \wedge \neg Kp]\, Kp$$

真的被宣告后变成假的!

$$\nVdash \varphi \to [\varphi]K\varphi$$

Remark: If the goal of the announcing person was to "spread the truth of this formula," then this attempt was clearly unsuccessful.

Public Announcement Logic (PAL)

Axiom Schema

1. tautologies
2. $K_i(\varphi \to \psi) \to K_i\varphi \to K_i\psi$
3. $[\psi]p \leftrightarrow (\psi \to p)$
4. $[\psi]\neg\varphi \leftrightarrow (\psi \to \neg[\psi]\varphi)$
5. $[\psi](\varphi \wedge \chi) \leftrightarrow ([\psi]\varphi \wedge [\psi]\chi)$
6. $[\psi]K_i\varphi \leftrightarrow (\psi \to K_i(\psi \to [\psi]\varphi))$
7. $[\psi][\chi]\varphi \leftrightarrow [\psi \wedge [\psi]\chi]\varphi$

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\text{MP}] \qquad\qquad \frac{\varphi}{K_i\varphi}\ [\text{N}]$$

Expressive Power

Theorem

PAL *is equally expressive as basic modal logic.*

Proof.

$$t(\top) = \top$$
$$t(p) = p$$
$$t(\neg\varphi) = \neg t(\varphi)$$
$$t(\varphi \wedge \psi) = t(\varphi) \wedge t(\psi)$$
$$t(K_i\varphi) = K_i t(\varphi)$$

$$t([\psi]\top) = t(\psi \to \top)$$
$$t([\psi]p) = t(\psi \to p)$$
$$t([\psi]\neg\varphi) = t(\psi \to \neg[\psi]\varphi)$$
$$t([\psi](\varphi \wedge \chi)) = t([\psi]\varphi \wedge [\psi]\chi)$$
$$t([\psi]K_i\varphi) = t(\psi \to K_i(\psi \to [\psi]\varphi))$$
$$t([\psi][\chi]\varphi) = t([\psi \wedge [\psi]\chi]\varphi)$$

$$\Vdash \varphi \leftrightarrow t(\varphi)$$

Succinctness

Theorem

PAL *is complete w.r.t. the standard semantics of Public Announcement Logic.*

Proof.

$$\Vdash \varphi \implies \Vdash t(\varphi) \implies \vdash_K t(\varphi) \implies \vdash_{\mathrm{PAL}} t(\varphi) \implies \vdash_{\mathrm{PAL}} \varphi$$

Theorem

PAL *is exponentially more succinct than modal logic on arbitrary models.*

$$\varphi_0 := \top$$

$$\varphi_{n+1} := \langle\langle\varphi_n\rangle\Diamond_1\top\rangle\Diamond_2\top$$

where $\Diamond_i\varphi := \neg K_i\neg\varphi$ and $\langle\psi\rangle\varphi := \neg[\psi]\neg\varphi$.

Propositional Dynamic Logic

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid [\pi]\varphi$$
$$\pi ::= a \mid \varphi? \mid \pi;\pi \mid \pi \cup \pi \mid \pi^*$$

$$\mathcal{M}, w \Vdash [\pi]\varphi \iff \forall v \in W\colon R_\pi wv \implies \mathcal{M}, v \Vdash \varphi$$

where

$$\begin{aligned}
R_{\varphi?} &:= \{(w,w)\colon \mathcal{M}, w \Vdash \varphi\} \\
R_{\pi_1;\pi_2} &:= \big\{(w,v)\colon \exists u\big(R_{\pi_1}wu \wedge R_{\pi_1}uv\big)\big\} \\
R_{\pi_1\cup\pi_2} &:= R_{\pi_1} \cup R_{\pi_2} \\
R_{\pi^*} &:= \bigcup_{n=0}^{\infty} R_{\pi^n}
\end{aligned}$$

Propositional Dynamic Logic (PDL)

Axiom Schema

1. tautologies
2. $[\pi](\varphi \to \psi) \to [\pi]\varphi \to [\pi]\psi$
3. $[\psi?]\varphi \leftrightarrow (\psi \to \varphi)$
4. $[\pi_1;\pi_2]\varphi \leftrightarrow [\pi_1][\pi_2]\varphi$
5. $[\pi_1 \cup \pi_2]\varphi \leftrightarrow [\pi_1]\varphi \cup [\pi_2]\varphi$
6. $[\pi^*]\varphi \leftrightarrow (\varphi \wedge [\pi][\pi^*]\varphi)$
7. $(\varphi \wedge [\pi^*](\varphi \to [\pi]\varphi)) \to [\pi^*]\varphi$

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi}\ [\text{MP}] \qquad\qquad \frac{\varphi}{[\pi]\varphi}\ [\text{N}]$$

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. $\langle x := t \rangle \varphi \leftrightarrow \varphi[t/x]$

Inference Rule

$$\frac{\varphi \quad \varphi \to \psi}{\psi} \text{ [MP]} \qquad \frac{\varphi \to [\pi^n]\psi, \quad n \in \omega}{\varphi \to [\pi^*]\psi} \text{ [IC]}$$

$$\frac{\varphi}{[\pi]\varphi} \text{ [N]} \qquad \frac{\varphi}{\forall x \varphi} \text{ [G]}$$

Application

$$\textbf{skip} := \top?$$

$$\textbf{fail} := \bot?$$

$$\textbf{if } \varphi \textbf{ then } \pi_1 \textbf{ else } \pi_2 := \varphi?; \pi_1 \cup \neg\varphi?; \pi_2$$

$$\textbf{while } \varphi \textbf{ do } \pi := (\varphi?; \pi)^*; \neg\varphi?$$

$$\textbf{repeat } \pi \textbf{ until } \varphi := \pi; (\neg\varphi?; \pi)^*; \varphi?$$

$$\{\varphi\}\pi\{\psi\} := \varphi \to [\pi]\psi$$

$$[(x = m \wedge y = n)?]\left\langle (x \neq y?; (x > y?; x \leftarrow x - y) \cup (x < y?; y \leftarrow y - x))^*; x = y?\right\rangle x = \gcd(m, n)$$

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 φ,

$$\frac{\forall xy\big(K_x\varphi(y) \vee K_x\neg\varphi(y) \to x = y\big) \quad h \neq z \quad z \neq f}{\neg K_z Hf \wedge \neg K_h \neg K_z Hf}$$

Moore's Paradox?

Gödel's Proof of God's Existence

Ax.1 Either a property or its negation is positive, but not both: $\forall\varphi[P(\neg\varphi) \leftrightarrow \neg P(\varphi)]$

Ax.2 A property necessarily implied by a positive property is positive:
$$\forall\varphi\forall\psi\left[\Big(P(\varphi) \wedge \Box\forall x[\varphi(x) \rightarrow \psi(x)]\Big) \rightarrow P(\psi)\right]$$

Th.1 Positive properties are possibly exemplified: $\forall\varphi[P(\varphi) \rightarrow \Diamond\exists x\varphi(x)]$

Df.1 A *God-like* being possesses all positive properties: $G(x) := \forall\varphi[P(\varphi) \rightarrow \varphi(x)]$

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: $\forall\varphi[P(\varphi) \rightarrow \Box P(\varphi)]$

Df.2 An *essence* of an individual is a property necessarily implying any of its properties:
$$E(\varphi, x) := \varphi(x) \wedge \forall\psi(\psi(x) \rightarrow \Box\forall y(\varphi(y) \rightarrow \psi(y)))$$

Th.3 Being God-like is an essence of any God-like being: $\forall x[G(x) \rightarrow E(G, x)]$

Df.3 *Necessary existence* of an individual is the necessary exemplification of all its essences: $N(x) := \forall\varphi[E(\varphi, x) \rightarrow \Box\exists y\varphi(y)]$

Ax.5 Necessary existence is a positive property: $P(N)$

Th.4 Necessarily, God exists: $\Box\exists x G(x)$

Contents

1. Introduction
2. History
3. Propositional Logic
4. Predicate Logic
5. Equational Logic
6. Set Theory
7. Recursion Theory
8. Modal Logic
9. Logic vs Game Theory

Pirate Game

Problem (海盗分金)

5 名海盗抢了 100 个金币。海盗世界的规则如下：

1. 最凶悍的一名海盗提出分配方案，所有海盗就此方案进行表决。
2. 如果至少半数海盗赞同此方案，则此方案通过。
3. 否则，提出方案的海盗将被扔到海里，然后由次凶悍的海盗开始重复上述过程。
4. 海盗都是嗜杀的，同等条件下更愿意看到同伙被扔海里。

Who Will Survive?

Problem (囚犯求生)

5 个囚犯先后从 100 颗绿豆中抓绿豆。他们不能交流，但可以摸出剩下绿豆的数量。

1. 100 颗绿豆不必都分完，但要保证每人至少能抓一颗。
2. 抓的最多和最少的人将被处死。
3. 他们的原则是先求自保、再多杀人。
4. 谁能活命？

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

Problem (零知识证明)

- 小白给小红出了一道非常难的 9×9 数独题。
- 小红怎么也解不出来。
- 小红："这题无解！你在耍我！"
- 小白："我不会直接把解给你，却有办法让你信服我确实有解。"

纸牌密码

纸牌密码

- 玩家 A 和 B 分别从 $0, \ldots, 6$ 中抽取三张牌，剩下一张给 C。
- A 和 B 有没有可能通过公开宣告使得互相都知道对方的牌同时使 C 不知道任何一张不在手里的牌？

- 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.

Logic vs Probability — Cox Theorem

Probability theory extends propositional logic?

Assumption (Cox's Assumptions for Beliefs)

1. $A \equiv B \implies b(\cdot|A) = b(\cdot|B)$ & $b(A|\cdot) = b(B|\cdot)$.
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* $N\colon [0,1] \to [0,1]$ *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 μ,

$$\sum_{t=1}^{\infty} \sum_{x_{1:t} \in \mathcal{X}^t} \mu(x_{<t}) \big(M'(x_t|x_{<t}) - \mu(x_t|x_{<t})\big)^2 \stackrel{+}{\leq} K(\mu) \ln 2$$

	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

Equilibrium

Definition (Nash Euqilibrium)

- s^* is a *pure Nash equilibrium* if $s^* \in \prod_{i \in N} \operatorname*{argmax}_{s_i \in S_i} u_i(s_i; s_{-i})$.
- σ^* 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 Ω 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, σ^* 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 σ is an ESS, then (σ, σ) is a Nash equilibrium. If (σ, σ) is a strict Nash equilibrium, then σ 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 $\implies$ strict Nash $\implies$ ESS $\implies$ weak ESS $\implies$ 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 $f\colon B \to B$, there exists $\boldsymbol{x}^*$ s.t. $f(\boldsymbol{x}^*) = \boldsymbol{x}^*$.

Theorem (Kakutani Fixpoint Theorem)

Given a compact convex set $S \subset \mathbb{R}^n$ and function $f\colon S \to P(S)$ 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 Δ be the triangle in $\mathbb{R}^3$ with vertices $\boldsymbol{e}_1 = (1,0,0)$, $\boldsymbol{e}_2 = (0,1,0)$, and $\boldsymbol{e}_3 = (0,0,1)$. We prove that any continuous map $f\colon \Delta \to \Delta$ 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 Δ s.t. $\lim\limits_{k\to\infty} \delta(T_k) = 0$.
Suppose f has no fixpoint. Since $\sum_i \boldsymbol{v}_i = 1 = \sum_i f(\boldsymbol{v})_i$, for each of these triangulations, we can define a Sperner coloring of their vertices $\boldsymbol{v}$ by setting $\lambda(\boldsymbol{v}) := \min\{i\colon f(\boldsymbol{v})_i < \boldsymbol{v}_i\}$.
Sperner's lemma tells us that in each triangulation T_k there is a tricolored triangle $\left\{\boldsymbol{v}_1^k, \boldsymbol{v}_2^k, \boldsymbol{v}_3^k\right\}$ with $\lambda(\boldsymbol{v}_i^k) = i$.
Since the simplex Δ is compact, some subsequence of $\left(\boldsymbol{v}_1^k\right)_{k\geq 1}$ has a limit point $\boldsymbol{v}^* \in \Delta$. Since $\lim\limits_{k\to\infty} \delta(T_k) = 0$, the sequences $\boldsymbol{v}_2^k$ and $\boldsymbol{v}_3^k$ converge to the same point $\boldsymbol{v}^*$.
Then $\forall i\colon f(\boldsymbol{v}^*)_i \leq \boldsymbol{v}_i^*$, which contradicts $f(\boldsymbol{v}^*) \neq \boldsymbol{v}^*$.

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 $f\colon \prod_{i \in N} \Delta S_i \to \prod_{i \in N} \Delta S_i$ by $f\colon \sigma \mapsto \sigma'$, 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 σ of f. By the linearity of expectation there exists s_i' in the support of σ, for which $u_i(s_i'; \sigma_{-i}) \leq u_i(\sigma)$. Then

$$\varphi_{i,s_i'}(\sigma) = 0 \;\;\&\;\; \sigma_i'(s_i') = \sigma_i(s_i') \implies \forall i \in N \forall s_i \in S_i\colon \varphi_{i,s_i}(\sigma) = 0$$

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 $f_i(p_1^*, \ldots, p_n^*) = 0$.

Thanks