Elementary Logic

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

June 30, 2020

Contents

Contents

Information Update

Five Logicians Walk into a Bar

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

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

Unfaithful Husband Puzzle

Problem (Unfaithful Husband Puzzle)

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

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

Test

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

Problem

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

下列说法不正确的是：

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

Gateway to Heaven

Problem (天堂之路)

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

Hardest Logic Puzzle Ever

Problem (Hardest Logic Puzzle Ever)

- *Three gods, A, B, and C are called in some order, T, F, and R.*
- *T always speaks truly, F always speaks falsely (if he is certain he can; but if he is unable to lie with certainty, he responds like R), but whether R speaks truly or falsely (or whether R speaks at all) is completely random.*
- *Your task is to determine the identities of A, B, and C by asking 2 (3) yes/no questions; each question must be put to exactly one god.*
- *The gods understand English, but will answer in their own language, in which the words for 'yes' and 'no' are 'da' and 'ja' in some order. You don't know which word means which.*

Contents

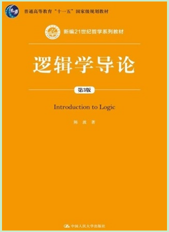
Outline

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

Readings

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

Readings, Movies and More


逻辑学导论

第3版

Introduction to Logic


数理逻辑

证明及其限度


GÖDEL ESCHER BACH

哥德尔 艾舍尔 巴赫

——集异璧之大成

（美）侯世达 著

商 务 印 书 馆

Hofstadter's Law

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

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

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

Exams and Credits

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

Homework

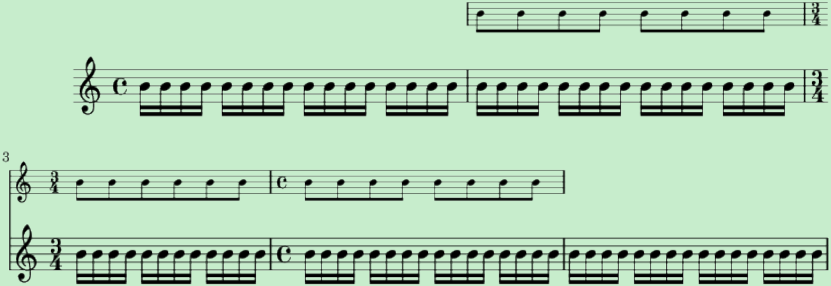
Google/Wikipedia/Stanford Encyclopedia/Internet Encyclopedia

- 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 . . . $\surd$
- Formal Philosophy
- Understanding of the nature of mathematics
- Application in Math / CS / AI / Linguistics / Cognition / Physics / Information Theory / Game Theory / Social Science . . .
- Mathematical Logic

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

Logic vs other Disciplines

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

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

Branches of Logic

Mathematical Logic

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

Computational Logic

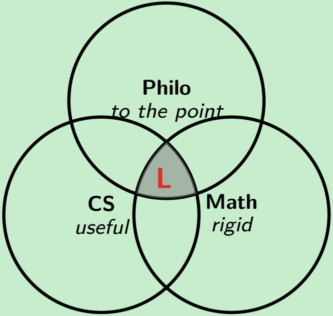
- Automata Theory
- Computational Complexity
- Finite Model Theory
- Model Checking
- Type Theory
- Lambda Calculus
- Categorical Logic
- Theorem Proving
- Description Logic
- Dynamic Logic
- Temporal Logic
- Hoare Logic
- Inductive Logic
- Fuzzy Logic
- Non-monotonic Logic
- Computability Logic
- Default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



Contents

Contents

Aristotle(384-322 BC) — Term Logic

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

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.

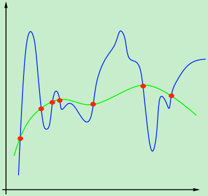
Leibniz's Dream — Deduction

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

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

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

Leibniz's Dream — Induction



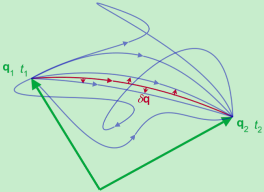
2. Compute all descriptions of possible worlds that can be expressed with the primitive notions. And the possible worlds will all have some propensity to exist.
3. Compute the probabilities of disputed hypotheses relative to the available data. As we learn more our probability assignments will asymptotically tend to a maximum for the real world, i.e., the possibility with the highest actual propensity.

Leibniz's Metaphysics and Quantum Mechanics

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

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

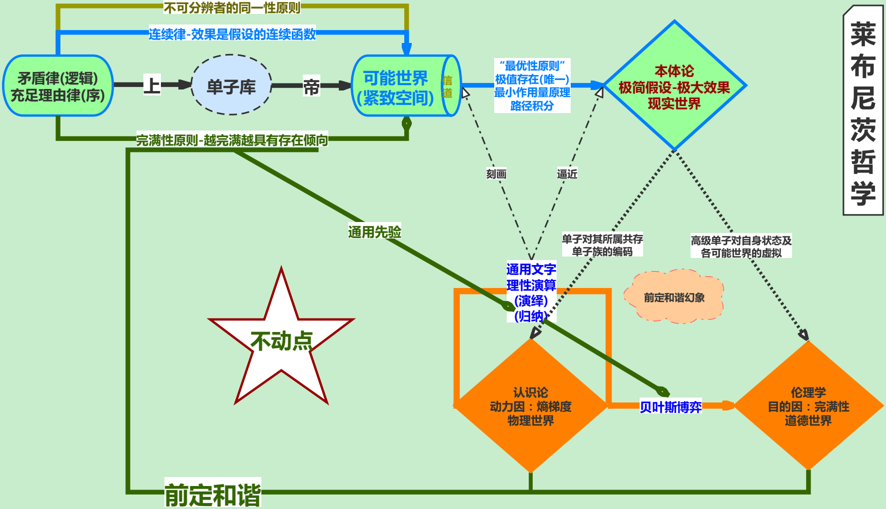
$$\varphi[q] \propto \mathrm{e}^{\frac{\mathrm{i}}{\hbar} S[q]} \quad S[q] = \int_{t_1}^{t_2} L[q(t), \dot{q}(t)] \mathrm{d}t \quad \delta S = 0$$



- Probability of the actual path = maximum
- Action of the actual path = minimum

the absolute square of the sum of probability amplitudes over all possible paths

Leibniz's Program



莱布尼茨哲学

不可分辨者的同一性原则

连续律-效果是假设的连续函数

矛盾律(逻辑)
充足理由律(序)

上

单子库

帝

可能世界
(紧致空间)

信
道

“最优性原则”
极值存在(唯一)
最小作用量原理
路径积分

本体论
极简假设-极大效果
现实世界

完满性原则-越完满越具有存在倾向

刻画

逼近

通用先验

单子对其所属共存
单子族的编码

高级单子对自身状态及
各可能世界的虚拟

通用文字
理性演算
(演绎)
(归纳)

前定和谐幻象

不动点

认识论
动力因：熵梯度
物理世界

贝叶斯博弈

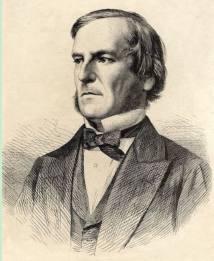
伦理学
目的因：完满性
道德世界

前定和谐

Contents

Boole 1815-1864

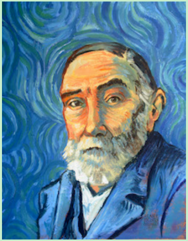
- *The Laws of Thought.*
- Logic as Algebra.
- Propositional Logic.
- Algebra's strength emanates from the fact that the symbols that represent quantities and operations obey a small number of rules.



Cantor 1845-1918

- Mathematics ⇝ 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 ⇝ Logic.[1]

---

[1] 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.[2]

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

Dem.

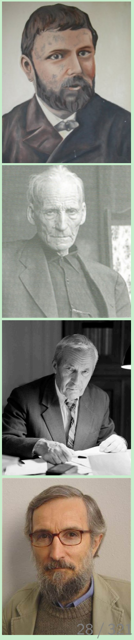
$$
\begin{array}{lll}
\vdash .*54\cdot 26.\ \supset\vdash\!:\ .\alpha=\iota'x.\beta=\iota'y.\ \supset\!:\ \alpha\cup\beta\in 2. & \equiv .x\neq y. & \\
[*51\cdot 231] & \equiv .t'x\cap\iota'y=\Lambda. & \\
[*13\cdot 12] & \equiv .\alpha\cap\beta=\Lambda & (1) \\
\vdash .(1).*11\cdot 11\cdot 35.\ \supset & & \\
\quad\vdash\!:\ .(\exists x,y).\alpha=\iota'x.\beta=\iota'y.\ \supset\!:\ \alpha\cup\beta\in 2. & \equiv .\alpha\cap\beta=\Lambda & (2) \\
\vdash .(2).*11\cdot 54.*52\cdot 1.\ \supset\vdash .Prop & &
\end{array}
$$

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

---

[2] Russell: On denoting.

Intuitionism



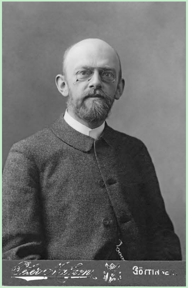
- Impredicativism. (*Poincaré*, Russell)
  Vicious circle principle: No entity can be defined only in terms of a totality to which this entity belongs.
- Intuitionism Logic ⇝ Mathematics ⇝ Mental construction.
  (Kronecker, *Brouwer*, Heyting, *Kolmogorov*, Weyl)
  - Potential infinity vs actual infinity.
  - To be is to be constructed by intuition.
  - Law of excluded middle.×
  - Non-constructive proof.×

  (There exist two irrational numbers x and y s.t. x^y is rational.)

  $$\sqrt{2} \quad \log_2 9$$

  "God created the integers, all the rest is the work of man."
- Constructive Mathematics. (Bishop, *Martin-Löf*)

Hilbert 1862-1943

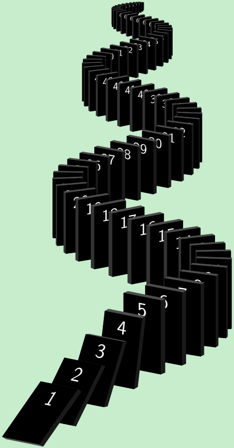


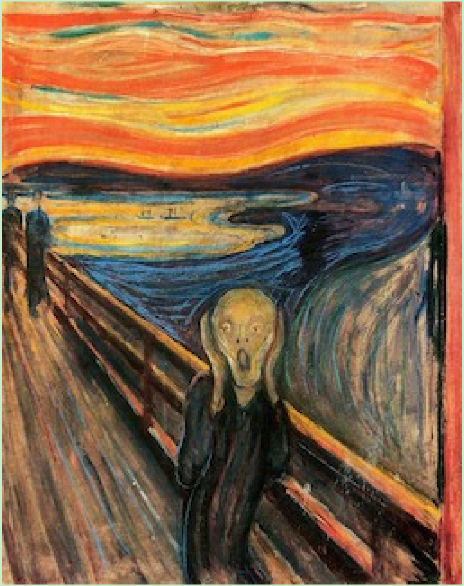
- **Formal** Axiomatization of Geometry.
  The consistency of geometry relative to arithmetic.
  (Klein: Non-Euclidean relative to Euclidean)
  (natural/integer/rational/real/complex)
- Hilbert's $23/24$ problems. $(1^{\text{st}}, 2^{\text{nd}}, 10^{\text{th}}, 24^{\text{th}})$
- Meta-mathematics — Proof Theory.
- Formalism Mathematics ⇝ Symbolic Game.

- Axioms are the implicit definitions of the concepts.
- One must be able to say 'table, chair, beer-mug' each time in place of 'point, line, plane'.
- Mathematics is a game played according to certain rules with meaningless marks on paper.
- We hear within us the perpetual call: There is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is *no ignorabimus*.
- We must know; We will know.

Contents

Leibniz & Hilbert — Dream Shattered. . .





Gödel 1906-1978

"I am unprovable."[3]

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

---

[3] 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.”[4]

Model Theory

Undefinability of Truth

Arithetical truth can’t be defined in arithmetic.

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

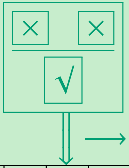
Banach-Tarski Paradox

---

[4] 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.



···	0	1	0	1	0	1	0	···

What is “effective procedure”?[5] — Recursion Theory

---

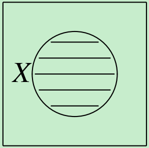
[5] Turing: On computable numbers, with an application to the Entscheidungsproblem.

Contents

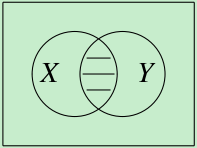
Welcome to Cantor's Paradise

Contents

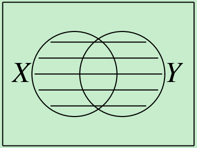
X



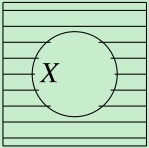
$X \cap Y$



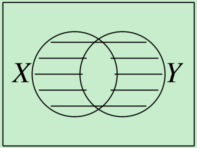
$X \cup Y$



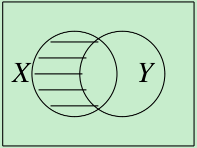
$\overline{X}$



$X \Delta Y$



$X \setminus Y$



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**. $(\times)$
  For any formula A, there exists a set $Y = \{x : A(x)\}$.

$$R := \{x : x \notin x\} \quad R \in R? \qquad \text{(Russell Paradox)}$$

- **Separation Schema**.
  For any formula A, for any X, there exists a set $Y = \{u \in X : A(x)\}$.

$$\forall X \exists Y \forall u(u \in Y \leftrightarrow u \in X \land A(x))$$

ZFC — Axioms

- **Pairing**. For any a and b there exists a set $c = \{a, b\}$.

$$\forall ab \exists c \forall x (x \in c \leftrightarrow x = a \vee x = b)$$

- **Power**. For any X there exists a set $Y = \mathrm{P}(X) := \{u : u \subset X\}$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \forall z (z \in u \to z \in X))$$

- **Union**. For any X there exists a set $Y = \bigcup X$.

$$\forall X \exists Y \forall u (u \in Y \leftrightarrow \exists z (z \in X \wedge u \in z))$$

$$\bigcup_{i \in I} X_i := \bigcup \{X_i : i \in I\}$$

$$\bigcap X := \{u : \forall z (z \in X \to u \in z)\}$$

Relation

- ordered pair.

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\}$$
$$(a_1, \ldots, a_{n+1}) \coloneqq ((a_1, \ldots, a_n), a_{n+1})$$

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \to a_i = b_i \quad \text{for} \quad 1 \leq i \leq n$$

$$X \subsetneq Y \quad X \cup Y \quad X \cap Y \quad X \setminus Y \quad X \Delta Y \quad X \times Y \quad \prod_{i=1}^{n} X_i \quad X^n$$

- n-ary relation R on $X_1, \ldots, X_n$.

$$R \subset \prod_{i=1}^{n} X_i$$

$$R(x_1, \ldots, x_n) \coloneqq (x_1, \ldots, x_n) \in R$$

Equivalence Relation, Quotient, Partition

- $x \sim x$ (Reflexivity)
- $x \sim y \rightarrow y \sim x$ (Symmetry)
- $x \sim y \land y \sim x \rightarrow x \sim z$ (Transitivity)
- equivalence class: $[x] := \{y \in X : x \sim y\}$
- quotient set: $X/{\sim} := \big\{[x] : x \in X\big\}$

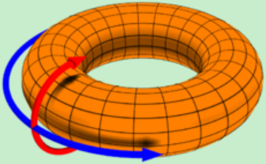
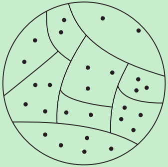


Figure: torus $\mathbb{R}^2/{\sim}$

$$(x, y) \sim (x', y') \ := \ (x - x', y - y') \in \mathbb{Z}^2$$

- we say $\mathcal{P} \subset \mathrm{P}(X)$ is a partition of X if
  1. $\forall xy \in \mathcal{P} : x \neq y \rightarrow x \cap y = \emptyset$
  2. $\bigcup \mathcal{P} = X$
- $X/{\sim}$ is a partition of X.
- $R \subset X^2$ is an equivalence relation iff there is a partition $\mathcal{P}$ of X s.t $R(x, y) \iff \exists A \in \mathcal{P}(x, y \in A)$.



Function

- A n-ary operation $f : \prod_{i=1}^{n} X_i \longrightarrow Y$ is a function if

$$(\mathbf{x}, y) \in f \wedge (\mathbf{x}, z) \in f \longrightarrow y = z$$

- injection (one-to-one). $f : X \rightarrowtail Y$

$$f(x) = f(y) \longrightarrow x = y$$

- surjection (onto). $f : X \twoheadrightarrow Y$.

$$\forall y \in Y \exists x \in X (f(x) = y)$$

- bijection. $f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$
- restriction. composition. image. inverse image. inverse function.

$$f\restriction_A \coloneqq \{(x, y) \in f : x \in A\} \quad (f \circ g)(x) \coloneqq f(g(x))$$

$$f(A) \coloneqq \{f(x) : x \in A\} \quad f^{-1}(A) \coloneqq \{x : f(x) \in A\}$$

Exercises

In **Set**,

$$\begin{aligned} f : X \rightarrowtail Y \quad & \text{iff} \quad \exists g : Y \to X : gf = 1_X \\ & \text{iff} \quad \forall Z \forall g_1 g_2 : Z \to X : f g_1 = f g_2 \implies g_1 = g_2 \\ f : X \twoheadrightarrow Y \quad & \text{iff} \quad \exists g : Y \to X : fg = 1_Y \\ & \text{iff} \quad \forall Z \forall g_1 g_2 : Y \to Z : g_1 f = g_2 f \implies g_1 = g_2 \end{aligned}$$

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "1_X"'] & Y \arrow[d, "g"] \\ & X \end{tikzcd} \qquad \begin{tikzcd} Y \arrow[r, "g"] \arrow[dr, "1_Y"'] & X \arrow[d, "f"] \\ & Y \end{tikzcd}$$

$$\begin{tikzcd} Z \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_1"'] & X \arrow[r, "f"] & Y \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "f"] & Y \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_1"'] & Z \end{tikzcd}$$

$f : X \rightarrowtail\mathrel{\mkern-14mu}\twoheadrightarrow Y$ iff the diagram commutes:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "1_X"'] & Y \arrow[d, "g"] \arrow[dr, "1_Y"] & \\ & X \arrow[r, "f"'] & Y \end{tikzcd}$$

Contents

Ordinal vs Cardinal

- ordinal. ("length") A set is an ordinal if it is transitive and well-ordered by $\in$. or equivalently,

$$\mathrm{Ord}(x) \;:=\; \bigcup x \subset x \wedge \forall yz(y \in x \wedge z \in x \rightarrow y \in z \vee y = z \vee z \in y)$$

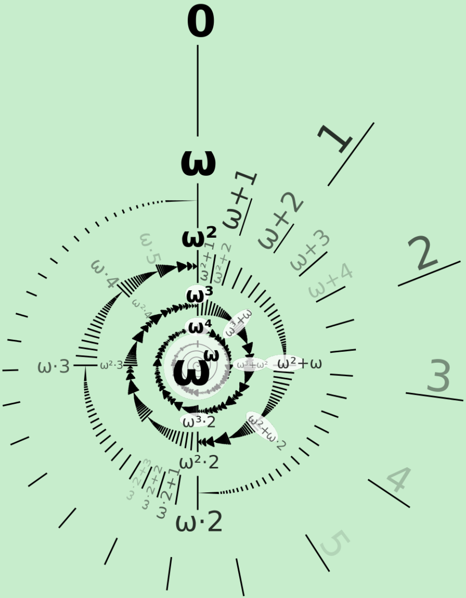
- cardinal. ("size") $\quad \mathrm{Card}(x) \;:=\; \mathrm{Ord}(x) \wedge \forall y \in x(|y| \neq |x|)$

$$|M| = |N| \;:=\; \exists f : M \twoheadrightarrow N \qquad |M| \leq |N| \;:=\; \exists f : M \rightarrowtail N$$

$$|M| \coloneqq \min\{\alpha \in \mathrm{Ord} : |\alpha| = |M|\}$$

The infinite ordinal numbers that are cardinals are called alephs.

Ordinal



$$0, 1, 2, 3, \ldots$$

$$\omega, \omega + 1, \omega + 2, \ldots$$

$$\omega \cdot 2, (\omega \cdot 2) + 1, (\omega \cdot 2) + 2, \ldots$$

$$\vdots$$

$$\omega^2, \omega^2 + 1, \omega^2 + 2, \ldots$$

$$\vdots$$

$$\omega^\omega, \omega^\omega + 1, \omega^\omega + 2, \ldots$$

$$\vdots$$

$$\omega^{\omega^\omega}, \ldots$$

$$\vdots$$

$$\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}, \ldots$$

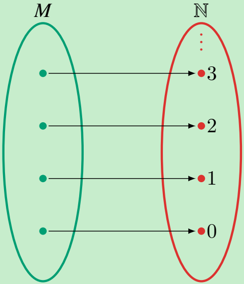
$$\vdots$$

Contents

How do we count a finite set?

$$M \coloneqq \{\text{apple}, \text{orange}, \text{banana}, \text{grape}\}$$

What does $|M| = 4$ mean?
There is a bijection between M and $N \coloneqq \{1, 2, 3, 4\}$.



apple	$\longleftrightarrow$	1
orange	$\longleftrightarrow$	2
banana	$\longleftrightarrow$	3
grape	$\longleftrightarrow$	4

$$|M| = |N| \ \coloneqq\ \exists f : M \rightarrowtail\!\!\!\!\twoheadrightarrow N$$

A set A is finite if $\exists n \in \mathbb{N} : |A| = n$.

Does renaming the elements of a set change its size? No!
Bijection is nothing more than renaming.

How do we compare the sizes of finite sets?

$$M := \{\text{apple, orange, banana, grape}\}$$

$$N := \{\text{John, Peter, Bell, Emma, Sam}\}$$

What does $|M| \le |N|$ mean?

$$\begin{array}{lcccr}
\text{apple} & \longleftrightarrow & 1 & \longleftrightarrow & \text{John} \\
\text{orange} & \longleftrightarrow & 2 & \longleftrightarrow & \text{Peter} \\
\text{banana} & \longleftrightarrow & 3 & \longleftrightarrow & \text{Bell} \\
\text{grape} & \longleftrightarrow & 4 & \longleftrightarrow & \text{Emma} \\
 & & 5 & \longleftrightarrow & \text{Sam}
\end{array}$$

$$\begin{array}{lcr}
\text{apple} & \longrightarrow & \text{John} \\
\text{orange} & \longrightarrow & \text{Peter} \\
\text{banana} & \longrightarrow & \text{Bell} \\
\text{grape} & \longrightarrow & \text{Emma} \\
 & & \text{Sam}
\end{array}$$

$$|M| \le |N| \;:=\; \exists f : M \rightarrowtail N$$

$$|M| \le |N| \;:=\; \exists f : N \twoheadrightarrow M$$

$$\begin{array}{lcr}
\text{apple} & \longleftarrow & \text{John} \\
\text{orange} & \longleftarrow & \text{Peter} \\
\text{banana} & \longleftarrow & \text{Bell} \\
\text{grape} & \longleftarrow & \text{Emma} \\
 & \nwarrow & \text{Sam}
\end{array}$$

The way of comparing the size of finite sets generalizes to infinite sets!

$|\mathbb{N}| = |\mathbb{Z}|$

$$\begin{array}{ccr}
0 & \longleftrightarrow & 0 \\
1 & \longleftrightarrow & 1 \\
2 & \longleftrightarrow & -1 \\
3 & \longleftrightarrow & 2 \\
4 & \longleftrightarrow & -2 \\
5 & \longleftrightarrow & 3 \\
6 & \longleftrightarrow & -3 \\
7 & \longleftrightarrow & 4 \\
8 & \longleftrightarrow & -4 \\
\vdots & & \vdots
\end{array}$$

Dedekind-Infinite

A set A is Dedeking-infinite if some proper subset $B \subsetneq A$ is equinumerous to A.

Figure: Dedekind

Countable?

$$\{0, 1, 2, 3, 4, \dots\}$$

$$\{1, 3, 5, 7, 9, \dots\}$$

$$\{0, 2, 4, 6, 8, \dots\}$$

$$\{0, 1, 4, 9, 16, \dots\}$$

$$\{2, 3, 5, 7, 11, \dots\}$$

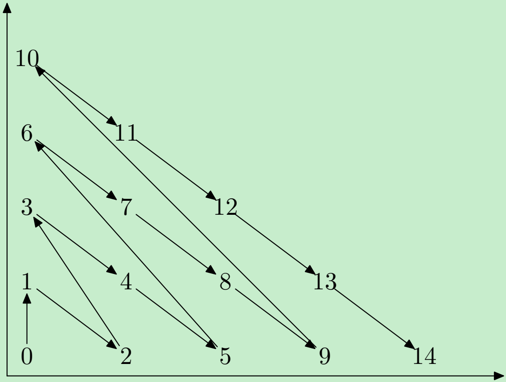
- A set A is countable iff $|A| \leq |\mathbb{N}|$.
- Is it possible that A is infinite, but $|A| < |\mathbb{N}|$?
- A set A is countably infinite iff $|A| = |\mathbb{N}|$.

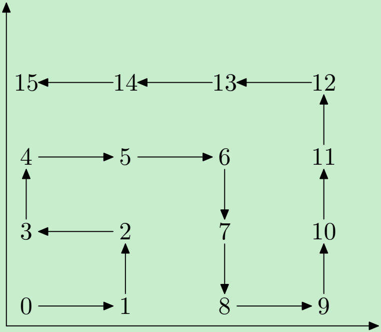
$$|\mathbb{N}| = |2^{<\omega}|$$

$$\begin{array}{ccr}
0 & \longleftrightarrow & \epsilon \\
1 & \longleftrightarrow & 0 \\
2 & \longleftrightarrow & 1 \\
3 & \longleftrightarrow & 00 \\
4 & \longleftrightarrow & 01 \\
5 & \longleftrightarrow & 10 \\
6 & \longleftrightarrow & 11 \\
7 & \longleftrightarrow & 000 \\
8 & \longleftrightarrow & 001 \\
\vdots & & \vdots
\end{array}$$

Countable?

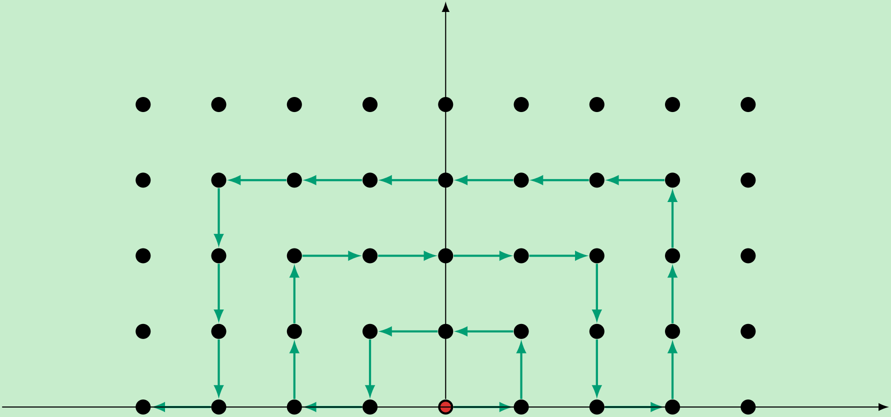
$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$$





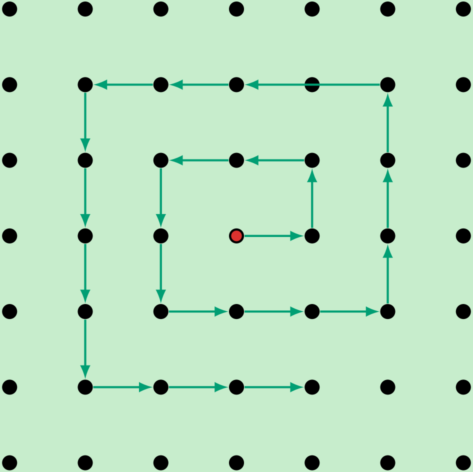
Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{N}|$$



Countable?

$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$$

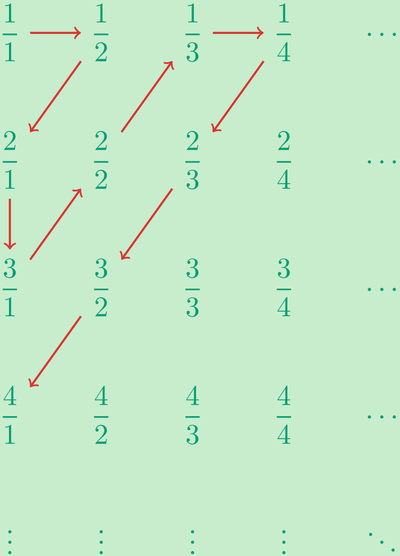


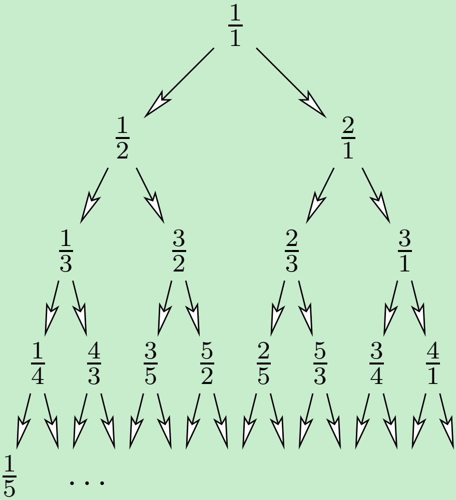
$|\mathbb{N}| = |\mathbb{Q}|$

$$\begin{tikzcd}
\cdots & {[5]}\ -\frac{2}{1} \arrow[d] & {[4]}\ -\frac{1}{1} \arrow[l] & {[0]}\ \frac{0}{1} \arrow[r, mapsto] \arrow[d, dashed] & {[1]}\ \frac{1}{1} \arrow[d] & {[10]}\ \frac{2}{1} \arrow[r] & {[11]}\ \frac{3}{1} \arrow[d] & \cdots \\
\cdots & -\cancel{\frac{2}{2}} \arrow[d] & {[3]}\ -\frac{1}{2} \arrow[u] & \cancel{\frac{0}{2}} \arrow[l] \arrow[d, dashed] & {[2]}\ \frac{1}{2} \arrow[l] & \cancel{\frac{2}{2}} \arrow[u] & {[12]}\ \frac{3}{2} \arrow[d] & \cdots \\
\cdots & {[6]}\ -\frac{2}{3} \arrow[r] & {[7]}\ -\frac{1}{3} \arrow[r] & \cancel{\frac{0}{3}} \arrow[r] \arrow[d, dashed] & {[8]}\ \frac{1}{3} \arrow[r] & {[9]}\ \frac{2}{3} \arrow[u] & \cancel{\frac{3}{3}} \arrow[d] & \cdots \\
{} & -\cancel{\frac{2}{4}} \arrow[l] & {[15]}\ -\frac{1}{4} \arrow[l] & \cancel{\frac{0}{4}} \arrow[l] & {[14]}\ \frac{1}{4} \arrow[l] & \cancel{\frac{2}{4}} \arrow[l] & {[13]}\ \frac{3}{4} \arrow[l] & \cdots \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

$$|\mathbb{N}| = |\mathbb{Z}| = |2^{<\omega}| = |\mathbb{N}\times\mathbb{N}| = |\mathbb{Z}\times\mathbb{N}| = |\mathbb{Z}\times\mathbb{Z}| = |\mathbb{Q}|$$

$|\mathbb{N}| = |\mathbb{Q}^+|$





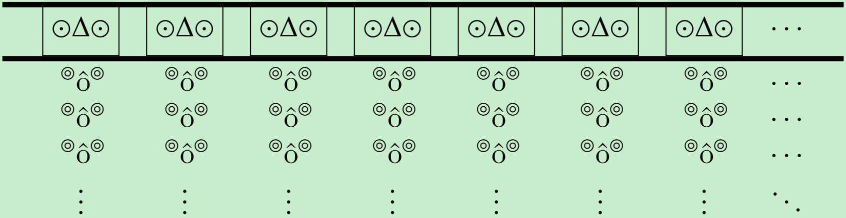
$$x \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

Hilbert's Hotel

Problem (Hilbert's Hotel)

Consider a hypothetical hotel with a countably infinite number of rooms, all of which are occupied.

1. *Finitely many new guests.*
2. *Infinitely many new guests.*
3. *Infinitely many buses with infinitely many guests each.*



The set of real numbers is uncountable

Is every set countable?

Theorem (Cantor)

$$|\mathbb{R}| > |\mathbb{N}|$$

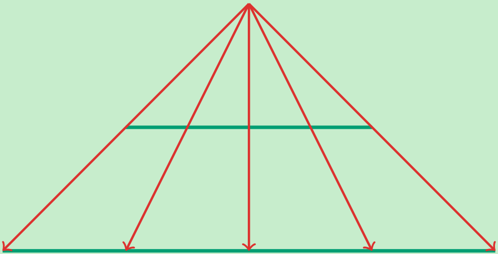
Proof.

$$\begin{array}{cccccc}
0\,. & r_{11} & r_{12} & r_{13} & r_{14} & \dots \\
0\,. & r_{21} & r_{22} & r_{23} & r_{24} & \dots \\
0\,. & r_{31} & r_{32} & r_{33} & r_{34} & \dots \\
0\,. & r_{41} & r_{42} & r_{43} & r_{44} & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

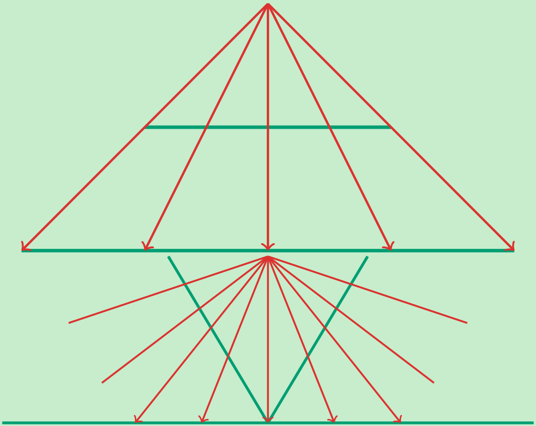
Let $d = 0.d_1 d_2 \dots$ where

$$d_n = 9 - r_{nn}$$

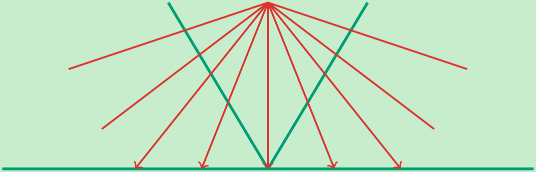
Continuum

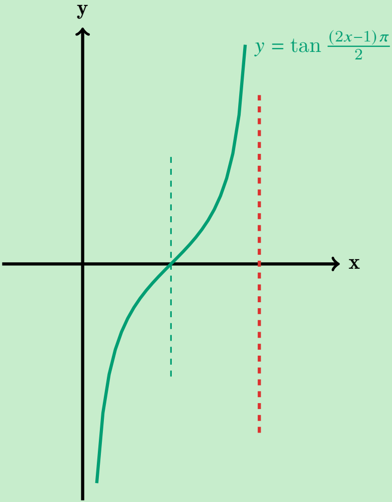


Continuum



Continuum



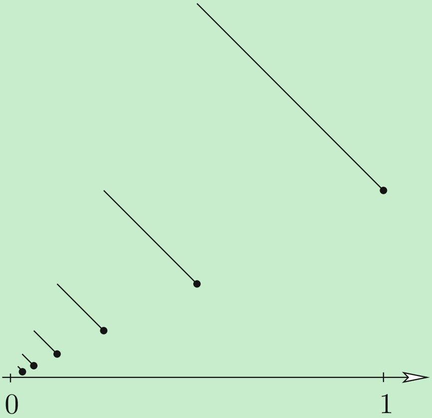


Continuum

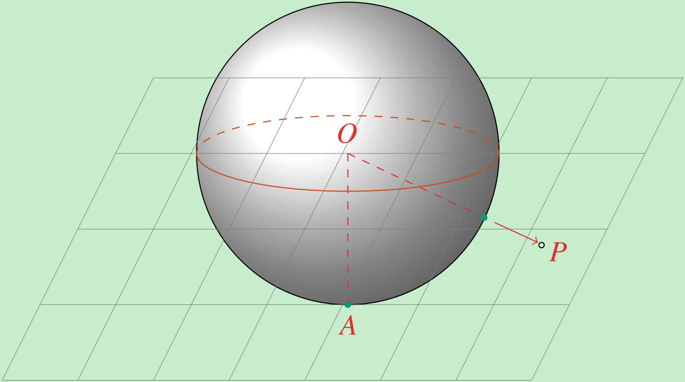
$$f : (0,1] \rightarrowtail\!\!\!\!\twoheadrightarrow (0,1)$$

$$f(x) := \begin{cases} \frac{3}{2} - x & \text{for } \frac{1}{2} < x \leq 1 \\ \frac{3}{4} - x & \text{for } \frac{1}{4} < x \leq \frac{1}{2} \\ \frac{3}{8} - x & \text{for } \frac{1}{8} < x \leq \frac{1}{4} \\ \quad\vdots & \end{cases}$$

$$f(x) := \begin{cases} \frac{x}{x+1} & \text{if } \exists n \in \mathbb{N} : x = \frac{1}{n} \\ x & \text{otherwise} \end{cases}$$



Continuum



Continuum

Theorem

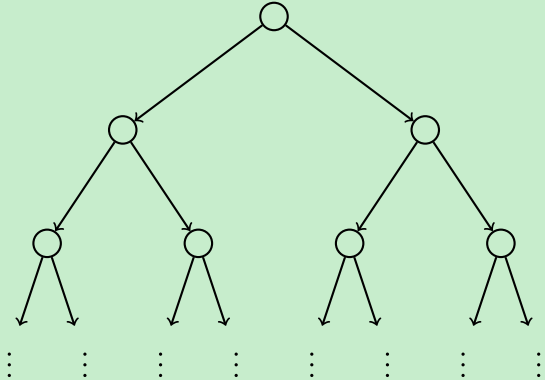
$$|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$$

Proof.

$$\begin{array}{rllllllllll} x = & 0.3 & & 01 & & 2 & & 007 & & 08\ldots \\ y = & 0.009 & & & 2 & & 05 & & 1 & & 0003\ldots \end{array}$$

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0003\ \ldots$$

Continuum

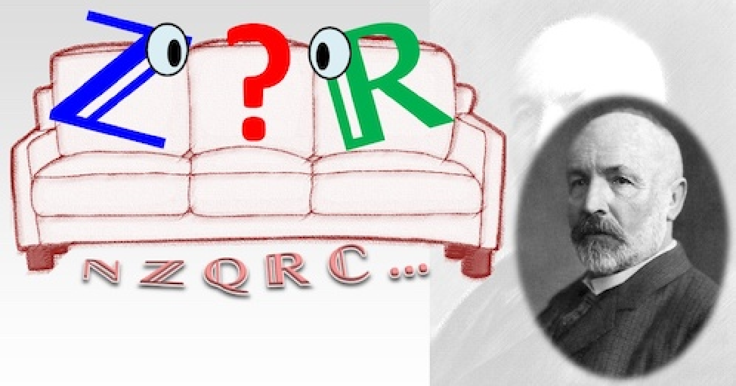


$$[0,1] = \left\{ \sum_{n=1}^{\infty} \frac{x_n}{2^n} : x_n = 0 \vee x_n = 1 \right\}$$

Cantor's Continuum Hypothesis

Cantor's Continuum Hypothesis (CH)

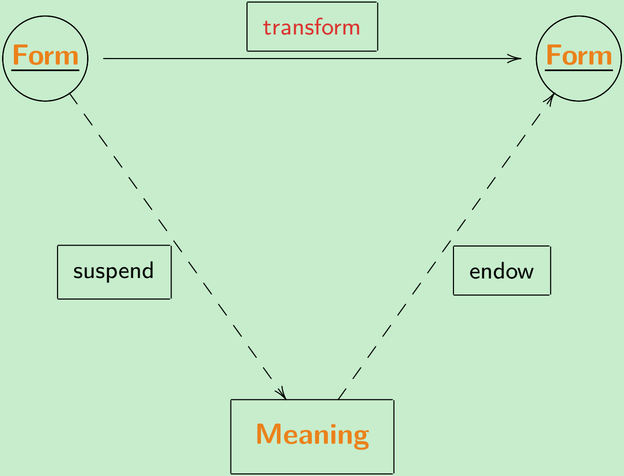
$$2^{\aleph_0} \overset{?}{=} \aleph_1$$



Contents

Logic → Truth

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



transform

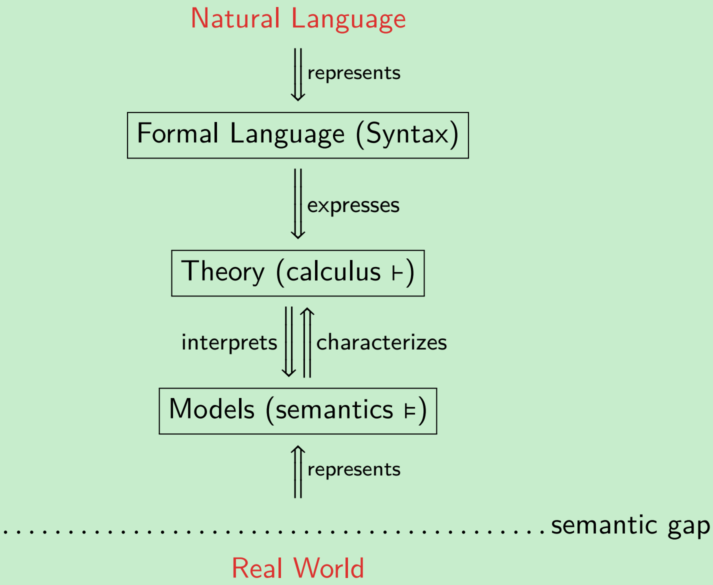
Form

Form

suspend

endow

Meaning



Natural Language

represents

Formal Language (Syntax)

expresses

Theory (calculus ⊢)

interprets

characterizes

Models (semantics ⊨)

represents

. . . . semantic gap

Real World

Contents

Propositional Logic

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

Syntax

Language

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

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

Well-Formed Formula wff

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

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

Example

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

Well-Formed Formula

Definition (Formula-Building Operator)

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

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

Well-Formed Formula

Definition (Construction Sequence)

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

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

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

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

Definition (Well-Formed Formula)

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

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

Generation — Bottom Up vs Top Down

Problem

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

Bottom Up

$$\begin{aligned} C_0 &:= B \\ C_{n+1} &:= C_n \cup \bigcup_{f \in \mathcal{F}} \{f(\mathbf{x}) : \mathbf{x} \in C_n\} \qquad \deg(\mathbf{x}) := \mu n\, [\mathbf{x} \in C_n] \\ C_* &:= \bigcup_{n \in \mathbb{N}} C_n \end{aligned}$$

Top Down

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

Bottom Up vs Top Down

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

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

Generation — Bottom Up vs Top Down

Example

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

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

There is more than one way of obtaining a member of C_*, e.g. $1 = S(0) = S(P(S(0)))$.

Theorem (Bottom up and Top down)

$$C_* = C^*$$

Proof.

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

Induction Principle for wff

Theorem (Induction Principle)

Let P be a property of formulae, satisfying

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

then every formula has property P.

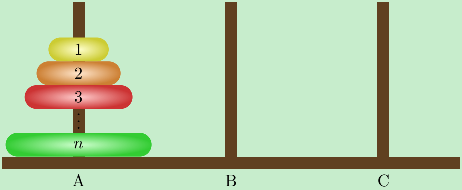
Proof.

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

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

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

Induction vs Recursion



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

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

Leave milk today and read this note again tomorrow.

Subformula

Definition (Subformula)

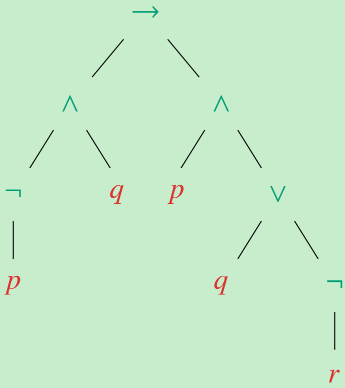
The set $\mathrm{Sub}(A)$ of subformulae of a wff A is the smallest set Γ that satisfies

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

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

Unique Readability, Unique Tree

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



subformula vs subtree

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

Assignment

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

$$\nu : \mathcal{P} \longrightarrow \{0, 1\}$$

- Such a truth assignment can be uniquely extended to $\overline{\nu} : \mathrm{wff} \longrightarrow \{0, 1\}$ satisfying the following condition:
  1. $\overline{\nu}(p) = \nu(p)$ for $p \in \mathcal{P}$
  2. $\overline{\nu}(\neg A) = 1 - \overline{\nu}(A)$
  3. $\overline{\nu}(A \wedge B) = \min\{\overline{\nu}(A), \overline{\nu}(B)\}$
  4. $\overline{\nu}(A \vee B) = \max\{\overline{\nu}(A), \overline{\nu}(B)\}$
  5. $\overline{\nu}(A \longrightarrow B) = 1 - \overline{\nu}(A) + \overline{\nu}(A) \cdot \overline{\nu}(B)$
  6. $\overline{\nu}(A \leftrightarrow B) = \overline{\nu}(A) \cdot \overline{\nu}(B) + (1 - \overline{\nu}(A)) \cdot (1 - \overline{\nu}(B))$

Truth Table & Truth/Boolean Function

p	$\neg p$
0	1
1	0

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

Example

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

Material Implication vs Cognition

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

No drinking under 18!

Tautology

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

p	q	$q \to p$	$p \to q \to p$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

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

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

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

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

Truth Table — Simplification for Tautology

$(p$	$\rightarrow$	q	$\rightarrow$	$r)$	$\rightarrow$	$(p$	$\rightarrow$	$q)$	$\rightarrow$	p	$\rightarrow$	r
					$\underline{\mathbf{0}}$							
	1				$\mathbf{0}$				$\underline{\mathbf{0}}$			
	1				$\mathbf{0}$		1		$\mathbf{0}$		$\underline{\mathbf{0}}$	
1	1			0	$\mathbf{0}$	1	$\underline{\mathbf{1}}$		$\mathbf{0}$	1	$\mathbf{0}$	0
1	$\underline{\mathbf{1}}$	1		0	$\mathbf{0}$	1	$\mathbf{1}$	1	$\mathbf{0}$	1	$\mathbf{0}$	0
1	$\mathbf{1}$	1	$\underline{\mathbf{1}}$	0	$\mathbf{0}$	1	$\mathbf{1}$	1	$\mathbf{0}$	1	$\mathbf{0}$	0
			×									

Exercises — Translation

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

Example

◎ô◎

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

- wife.

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

- programmer.

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

Exercises — Validity

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

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

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

$$\begin{array}{r} p \to q \\ q \\ \hline p \end{array} \qquad \begin{array}{l} p \to q \\ \neg p \\ \hline \neg q \end{array} \qquad \begin{array}{c} p \lor q \\ p \\ \hline \neg q \end{array}$$

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

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

> *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。

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

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

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

Example

诉讼悖论

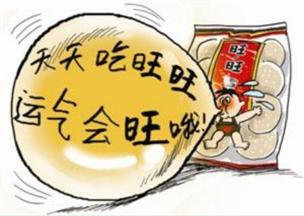
- 曾有师生签订合同：上学期间不收费，学生毕业打赢第一场官司后交学费。
- 可学生毕业后并未从事律师职业，于是老师威胁起诉学生。
- 老师说：如果我赢了，根据法庭判决，你必须交学费；如果你赢了，根据合同，你也必须交学费。要么我赢要么你赢，你都必须交学费。
- 学生说：如果我赢了，根据法庭判决，我不用交学费；如果你赢了，根据合同，我不用交学费。要么我赢要么你赢，我都不用交学费。

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

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

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

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



The Crocodile Dilemma

The Crocodile Dilemma

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

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

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

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

Gateway to Heaven

Problem (天堂之路)

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

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

- p: 你说真话。
- q: 左门通天堂。

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

Contents

Why Study Formal System?

Why truth tables are not sufficient?

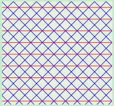
- Exponential size
  - How many times would you have to fold a piece of paper($0.1mm$) onto itself to reach the Moon?
  - Common Ancestors of All Humans

    (1) Someone alive $1000BC$ is an ancestor of everyone alive today;

    (2) Everyone alive $2000BC$ is either an ancestor of nobody alive today or of everyone alive today;

    (3) Most of the people you are descended from are no more genetically related to you than strangers are.

    (4) Even if everyone alive today had exactly the same set of ancestors from $2000BC$, the distribution of one's ancestors from that population could be very different.
- Inapplicability beyond Boolean connectives.



Formal System = Axiom + Inference Rule

Axiom Schema

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

Inference Rule

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

Deduction / Proof

This sentence can never be proved.

What is "proof"?

Definition (Deduction)

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

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

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

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

Example

Theorem

$$\vdash p \to p$$

Proof.

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

Example

Theorem

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

Proof.

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

Example

Theorem

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

Proof.

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

Example — Curry's Paradox ◎ô◎

If this sentence is true, then God exists.

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

Proof.

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

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

This sentence is false, and God does not exist.

Curry's Paradox — How to Flirt with a Beauty ♡◎♡

Smullyan Flirts with a Beauty ♡◎♡

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

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

Hi 美女，问你个问题呗

如果我问你“你能做我女朋友吗”，那么你的答案能否和**这个问题本身**的答案一样?

Deduction Theorem

Theorem (Deduction Theorem)

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

Proof.

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

Base step $n = 1$:

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

case2. $B \in \Gamma$.

case3. $B = A$.

Inductive step $n > 1$:

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

case2. $C_i = C_j \to B$

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

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

$\Gamma \vdash A \to B$

Equivalent Replacement

Theorem

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

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

Proof.

Prove by induction on the number of connective of A.

Example

◎ô◎

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

- wife.

$$p?$$

- logician.

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

Formal System — Variant

Axiom Schema

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

Reference Rule

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

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

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

where $\star \in \{\land, \lor, \to\}$

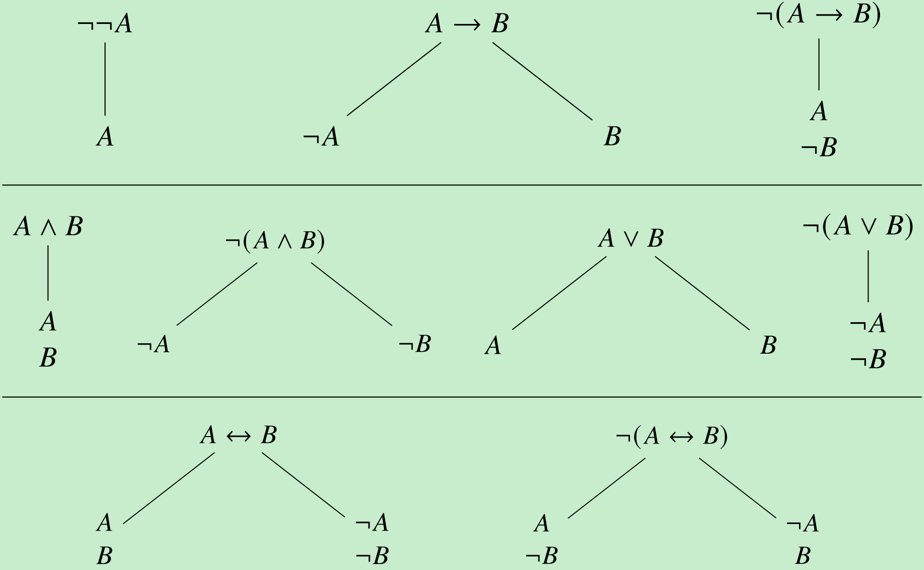
$$\Gamma' := \{A' : A \in \Gamma\}$$

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

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

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

Tree Method for Propositional Logic



$\neg\neg A$

A

$A \rightarrow B$

$\neg A$ | B

$\neg(A \rightarrow B)$

A

$\neg B$

$A \wedge B$

A

B

$\neg(A \wedge B)$

$\neg A$ | $\neg B$

$A \vee B$

A | B

$\neg(A \vee B)$

$\neg A$

$\neg B$

$A \leftrightarrow B$

A, B | $\neg A$, $\neg B$

$\neg(A \leftrightarrow B)$

A, $\neg B$ | $\neg A$, B

✓

Instructions for Tree Construction

- A *literal* is an atomic formula or its negation.
- When a non-literal wff has been fully unpacked, check it with ✓

1. Start with premises and the negation of the conclusion.
2. Inspect each open path for an occurrance of a wff and its negation. If these occur, close the path with ×.
3. If there is no unchecked non-literal wff on any open path, then stop!
4. Otherwise, unpack any unchecked non-literal wff on any open path.
5. Goto ②.

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

Tactics

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

Definition (Deduction)

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

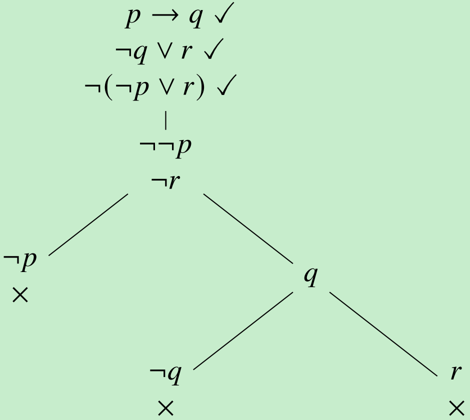
Theorem (Soundness & Completeness Theorem)

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

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

Examples — Tree Method

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



$p \to q$ ✓

$\neg q \vee r$ ✓

$\neg(\neg p \vee r)$ ✓

$\neg\neg p$

$\neg r$

$\neg p$

×

q

$\neg q$

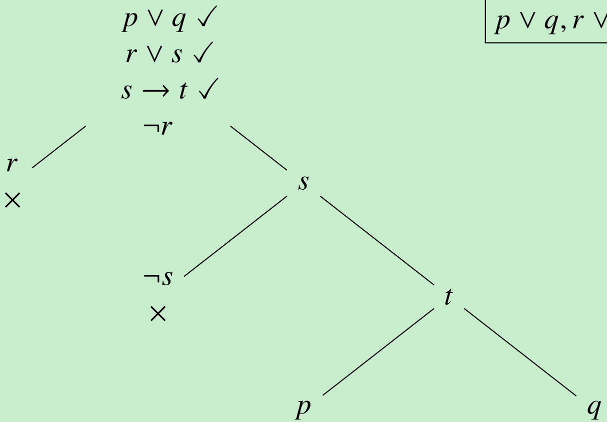
×

r

×

An open branch corresponds to a valuation

$$\boxed{p \vee q, r \vee s, s \rightarrow t \overset{?}{\vDash} r}$$



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

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

$$\nu \vDash p \vee q, \quad \nu \vDash r \vee s, \quad \nu \vDash s \rightarrow t, \quad \nu \nvDash r$$

Don't just read it; fight it!

Ask your own questions,
look for your own examples,
discover your own proofs.
Is the hypothesis necessary?
Is the converse true?
What happens in the classical special case?
What about the degenerate cases?
Where does the proof use the hypothesis?

Exercises — Tree Method

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

Exercises — Tree Method

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

1. $(p \vee q) \wedge r \overset{?}{\vDash} p \vee (q \wedge r)$
2. $p \vee (q \wedge r) \overset{?}{\vDash} (p \vee q) \wedge r$
3. $p \leftrightarrow (q \rightarrow r) \overset{?}{\vDash} (p \leftrightarrow q) \rightarrow r$
4. $(p \leftrightarrow q) \rightarrow r \overset{?}{\vDash} p \leftrightarrow (q \rightarrow r)$
5. $\neg(p \rightarrow q \wedge r), r \rightarrow p \wedge q \overset{?}{\vDash} \neg r$
6. $p \rightarrow (q \wedge r), \neg(p \vee q \rightarrow r) \overset{?}{\vDash} p$
7. $p \rightarrow q, r \rightarrow s, p \vee r, \neg(q \wedge s) \overset{?}{\vDash} (q \rightarrow p) \wedge (s \rightarrow r)$
8. If God does not exist, then it's not the case that *if I pray, my prayers will be answered*; and I don't pray; so God exists.

Contents

Model & Semantic Consequence

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

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

Consistency & Satisfiability

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

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

- Γ is maximal if for every wff A, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- 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 $\Gamma \vdash A$, then $\Gamma \cup \{A\}$ is consistent.
- $\Gamma \cup \{\neg A\}$ is inconsistent iff $\Gamma \vdash A$.
- If Γ is maximal consistent, then $A \notin \Gamma \implies \Gamma \cup \{A\}$ is inconsistent.

Soundness Theorem

Theorem (Soundness Theorem)

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

Proof.

Prove by induction on the length of the deduction sequence.

Case1: A is an axiom. (truth table)

Case2: $A \in \Gamma$

Case3:

$$\left.\begin{aligned} &\Gamma \vDash C_j \\ &\Gamma \vDash C_j \to A \end{aligned}\right\} \implies \Gamma \vDash A$$

Corollary

Any satisfiable set of wffs is consistent.

Compactness Theorem

Theorem (Compactness Theorem)

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

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

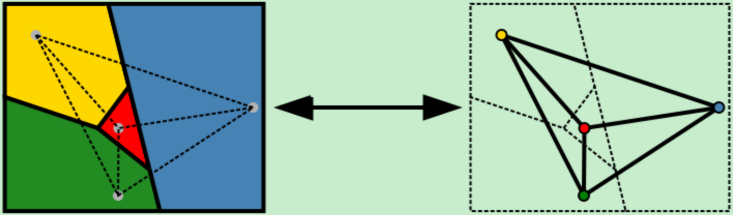
Corollary

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

Proof.

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

Applications of Compactness



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

Proof.

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

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

Completeness Theorem — Post1921

Theorem (Completeness Theorem)

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

Corollary

Any consistent set of wffs is satisfiable.

$$\begin{tikzcd}
\Gamma \models A \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & \Gamma \vdash A \arrow[d, Leftrightarrow] \\
\begin{array}{c} \Gamma \cup \{\neg A\} \\ \text{unsatisfiable} \end{array} \arrow[r, Leftrightarrow] & \begin{array}{c} \Gamma \cup \{\neg A\} \\ \text{inconsistent} \end{array}
\end{tikzcd}$$

Corollary (Compactness Theorem)

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

Proof of Completeness Theorem

Proof.

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

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

step2. Define a truth assignment that satisfies Γ.

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

Decidability — Post1921

Theorem

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

Theorem

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

Theorem

If 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

What is “theory”?

- A set Γ of sentences is a theory if $\Gamma = \mathrm{Cn}(\Gamma)$.
- A theory Γ is complete if for every sentence A, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- 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[6]

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

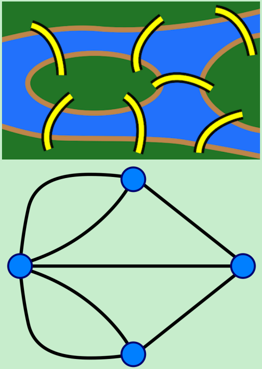


Figure: *Eulerian Circle(P)*

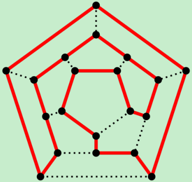


Figure: *Hamiltonian Circle(NPC)*

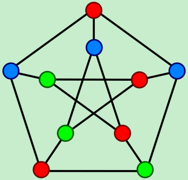
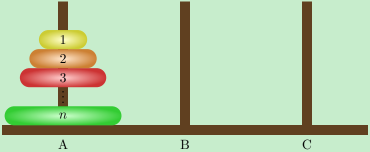


Figure: *Graph Coloring(NPC)*



---

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

Contents

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.

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

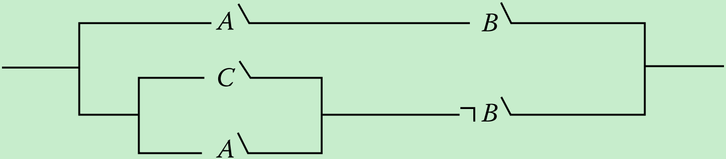
- Every 3×3 block contains every number.

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

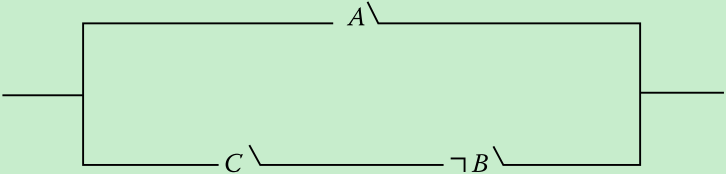
- No cell contains more than one number.
  for all $1 \leq i, j, n, n' \leq 9$ and $n \neq n'$:

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

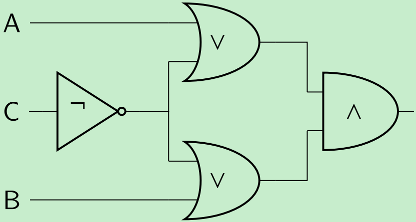
Shannon — Digital Circuit Design

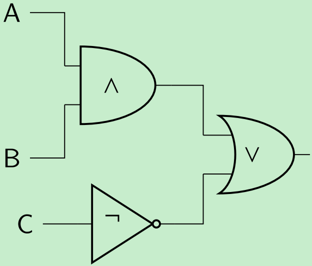


$$(A \land B) \lor ((C \lor A) \land \neg B) \Dashv\vDash A \lor (C \land \neg B)$$



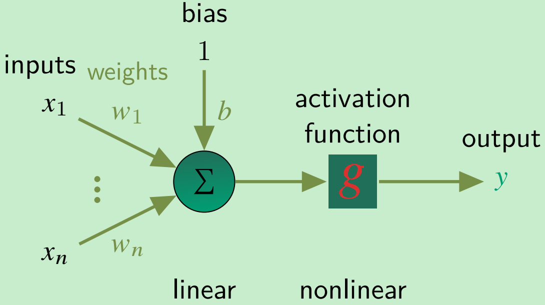
Shannon — Digital Circuit Design





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

McCulloch-Pitts Artificial Neural Network



bias

1

inputs

weights

x_1

w_1

b

activation function

output

g

y

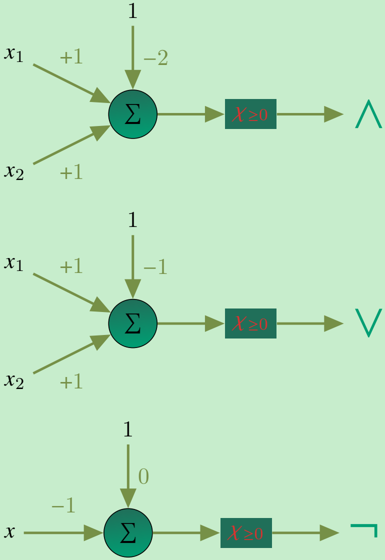
x_n

w_n

linear

nonlinear

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



1

x_1 $+1$ -2

x_2 $+1$

Σ $\chi_{\geq 0}$ $\wedge$

1

x_1 $+1$ -1

x_2 $+1$

Σ $\chi_{\geq 0}$ $\vee$

1

0

x -1

Σ $\chi_{\geq 0}$ $\neg$

《三体》

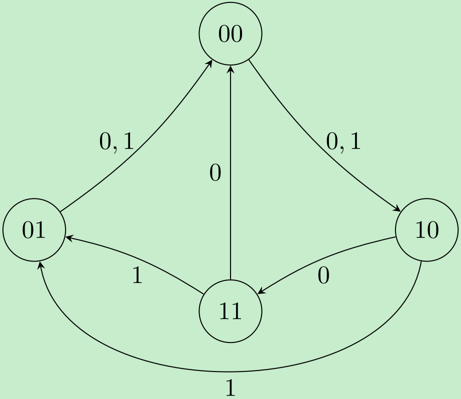
- 秦始皇：朕当然需要预测太阳的运行，但你们让我集结三千万大军，至少要首先向朕演示一下这种计算如何进行吧。
- 冯诺依曼：陛下，请给我三个士兵，我将为您演示。……
- 秦始皇：他们不需要学更多的东西了吗?
- 冯诺依曼：不需要，我们组建一千万个这样的门部件，再将这些部件组合成一个系统，这个系统就能进行我们所需要的运算，解出那些预测太阳运行的微分方程。

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

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

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

Finite State Automaton



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

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

Reversible Computing — Fredkin Gate: CSWAP

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

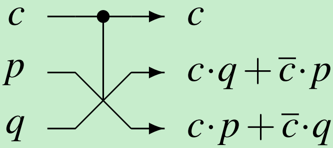


Figure: transmit the first bit unchanged and swap the last two bits iff the first bit is 1.
$f : (c, p, q) \mapsto (c, c\cdot q+\overline{c}\cdot p, c\cdot p+\overline{c}\cdot q)$

$$\text{CSWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

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

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

Exercise

宝藏在哪里?

你面前有三扇门，只有一扇门后是宝藏。门上各有一句话，只有一扇门上的是真话。

1. 宝藏不在这儿。
2. 宝藏不在这儿。
3. 宝藏在②号门。

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

Exercise

谁是凶手?

一起凶杀案有三个嫌疑人：小白、大黄和老王。

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

谁是窃贼?

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

Exercise

哪个部落的?

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

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

我在做什么?

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

Contents

Logic as Algebra — Boolean Algebra BA

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

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

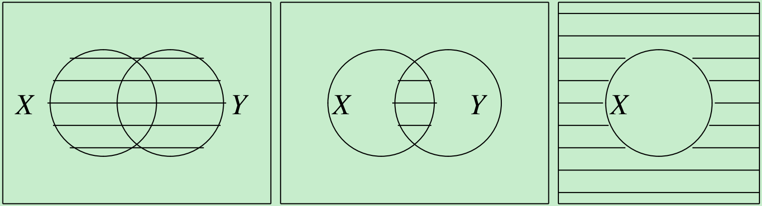
Logic

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

Algebra

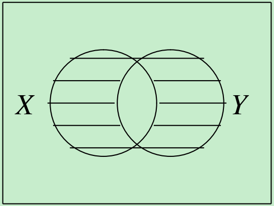
Power Set Algebra

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



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

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



Propositional Logic vs Boolean Algebra

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

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

$$A \vdash B \iff \mathrm{BA} \vdash A^* \leq B^*$$

$$\mathrm{BA} \vdash A \leq B \iff A' \vdash B'$$

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

Boolean Algebra vs Propositional Logic

Exercise

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

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

$$A \to \neg B \wedge C \qquad A \cdot (B + \overline{C}) = 0$$

$$B \wedge D \to (A \wedge \neg C) \vee (\neg A \wedge C) \qquad B \cdot D \cdot (\overline{A} \cdot \overline{C} + A \cdot C) = 0$$

$$\neg B \wedge C \to \neg A \wedge D \qquad \overline{B} \cdot C \cdot (A + \overline{D}) = 0$$

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。

$$x = ? \implies \models (x \leftrightarrow b \vee s) \to b$$

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

General Solution?[7]

Exercise — Save Yourself

You can say one sentence. If you lie I will hang you. If you tell the truth I will shoot you.

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

Problem (General Solution?)

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

---

[7] Brown: Boolean Reasoning.

General Solution?

$$x^5 - x - 1 = 0 \implies x = ?$$

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

$$ax^2 + bx + c = 0 \implies x = ?$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

General Solution of Boolean Equation

Theorem (General Solution of Boolean Equation)

Assume $f(x) = 0$ *is consistent (it has at least one solution, i.e.,* $f(0) \cdot f(1) = 0$*), then*

$$f(x) = 0$$

$$\Updownarrow$$

$$f(0) \leq x \leq \overline{f(1)}$$

$$\Updownarrow$$

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

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

Application — How to Flirt with a Beauty ♡◎♡

Smullyan Flirts with a Beauty ♡◎♡

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

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

Application — How to Flirt with a Beauty ♡◎♡

Smullyan Flirts with a Beauty ♡◎♡

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

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

Solution

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

$$\models (s \leftrightarrow \neg s \wedge \neg k) \to k$$

$$\models (s \leftrightarrow (s \to k)) \to k$$

Contents

Why Study Predicate Logic?

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

Example

◎ô◎

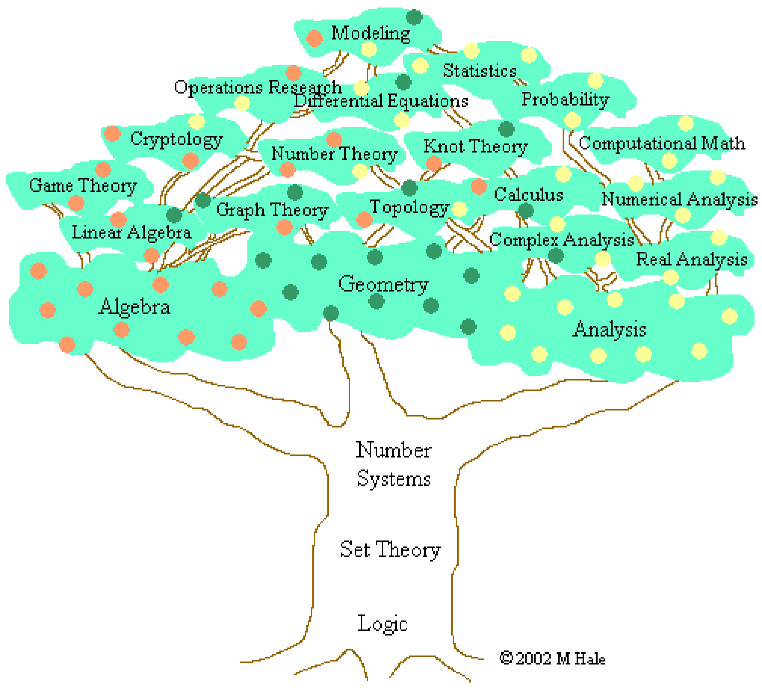
What will a logician choose: an egg or eternal bliss in the afterlife? An egg! Because nothing is better than eternal bliss in the afterlife, and an egg is better than nothing.

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

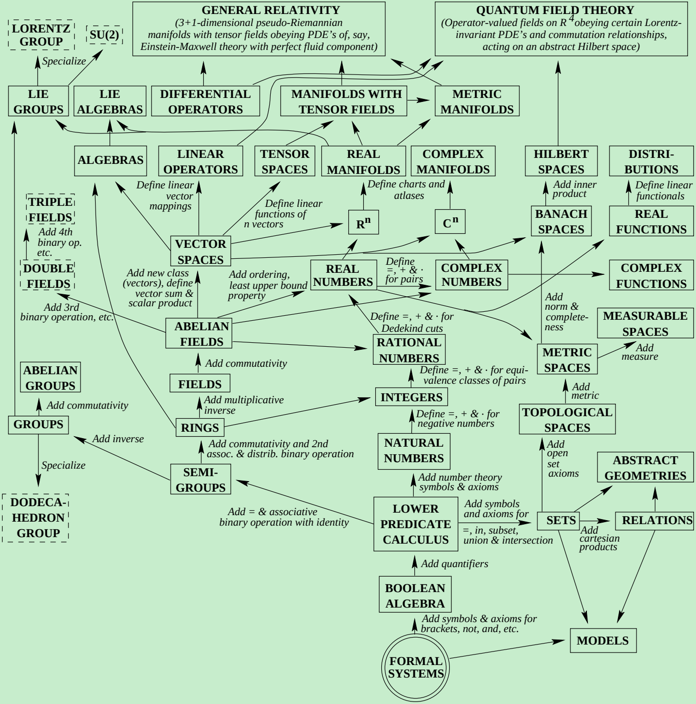
$$\neg \exists x (x > b) \implies 0 \not> b$$

◎ô◎

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


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

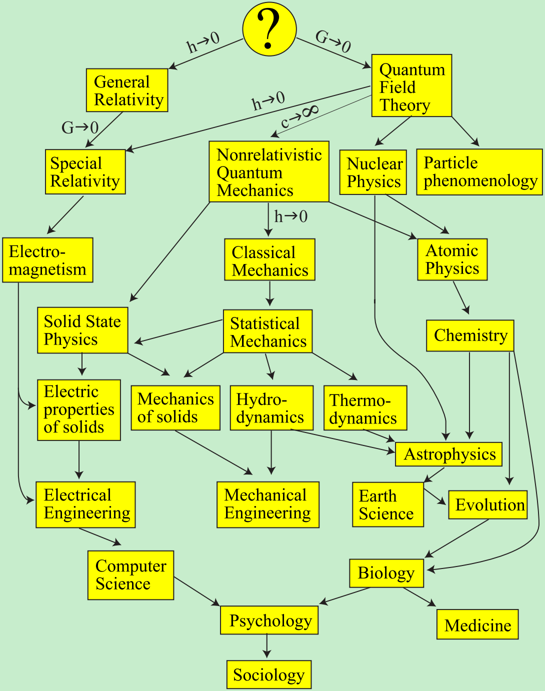
©2002 M Hale



GENERAL RELATIVITY
(3+1-dimensional pseudo-Riemannian manifolds with tensor fields obeying PDE's of, say, Einstein-Maxwell theory with perfect fluid component)

QUANTUM FIELD THEORY
(Operator-valued fields on R^4 obeying certain Lorentz-invariant PDE's and commutation relationships, acting on an abstract Hilbert space)

LORENTZ GROUP
SU(2)
Specialize
LIE GROUPS
LIE ALGEBRAS
DIFFERENTIAL OPERATORS
MANIFOLDS WITH TENSOR FIELDS
METRIC MANIFOLDS
ALGEBRAS
LINEAR OPERATORS
TENSOR SPACES
REAL MANIFOLDS
COMPLEX MANIFOLDS
HILBERT SPACES
DISTRI-BUTIONS
TRIPLE FIELDS
Define linear vector mappings
Define linear functions of n vectors
Define charts and atlases
Add inner product
Define linear functionals
Add 4th binary op. etc.
R^n
C^n
BANACH SPACES
REAL FUNCTIONS
DOUBLE FIELDS
VECTOR SPACES
REAL NUMBERS
Define =, + & · for pairs
COMPLEX NUMBERS
COMPLEX FUNCTIONS
Add new class (vectors), define vector sum & scalar product
Add ordering, least upper bound property
Add 3rd binary operation, etc.
Add norm & complete-ness
MEASURABLE SPACES
ABELIAN FIELDS
Define =, + & · for Dedekind cuts
RATIONAL NUMBERS
METRIC SPACES
Add measure
ABELIAN GROUPS
Add commutativity
FIELDS
Define =, + & · for equi-valence classes of pairs
Add metric
Add commutativity
Add multiplicative inverse
INTEGERS
TOPOLOGICAL SPACES
GROUPS
RINGS
Define =, + & · for negative numbers
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



General Relativity

Quantum Field Theory

Special Relativity

Nonrelativistic Quantum Mechanics

Nuclear Physics

Particle phenomenology

Electro-magnetism

Classical Mechanics

Atomic Physics

Solid State Physics

Statistical Mechanics

Chemistry

Electric properties of solids

Mechanics of solids

Hydro-dynamics

Thermo-dynamics

Astrophysics

Electrical Engineering

Mechanical Engineering

Earth Science

Evolution

Computer Science

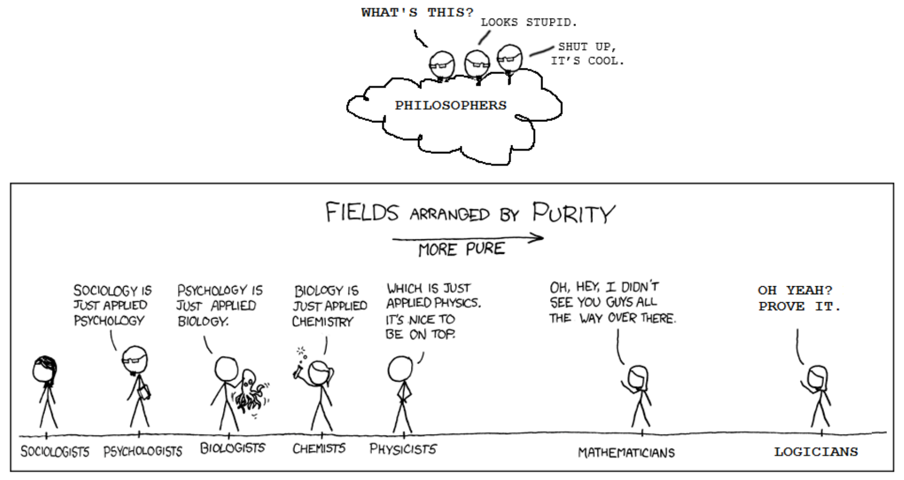
Biology

Psychology

Medicine

Sociology

Reductionism ≠ Emergence



Contents

Syntax

Language

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

where

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

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

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

f^k is a k-place function symbol.
P^k is a k-place predicate symbol.
A 0-place function symbol f^0 is called constant.
A 0-place predicate symbol P^0 is called (atomic) proposition.

Term & Formula

Term $\mathcal{T}$

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

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

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

Well-Formed Formula wff

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

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

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

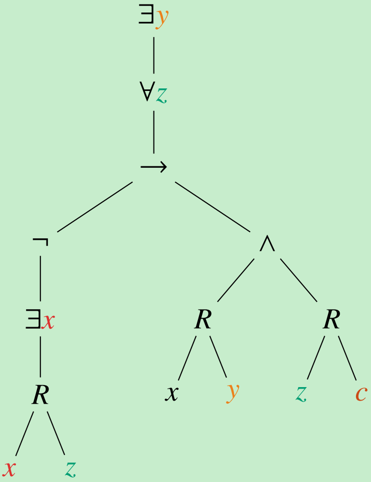
Syntax

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

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

Freedom & Bondage

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



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

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

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

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

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

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

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

Freedom & Bondage

Definition (Free Variable of a Term)

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

Definition (Free Variable of a wff)

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

Freedom & Bondage

Definition (Bound Variable)

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

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

Example: $c = d$ is clopen.

Translation

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

1. **A**: $\forall x(Sx \to Px)$
2. **E**: $\forall x(Sx \to \neg Px)$
3. **I**: $\exists x(Sx \wedge Px)$
4. **O**: $\exists x(Sx \wedge \neg Px)$
5. Every boy loves some girl. $\forall x\big(Bx \to \exists y(Gy \wedge Lxy)\big)$
6. Whoever has a father has a mother. $\forall x(\exists y Fyx \to \exists y Myx)$
7. Grandmother is mother's mother. $\forall xy\big(Gxy \leftrightarrow \exists z(Mxz \wedge Mzy)\big)$ or $\forall xy\big(x = Gy \leftrightarrow \exists z(x = Mz \wedge z = My)\big)$
8. 如果大鱼比小鱼游得快，那么，有最大的鱼就有游得最快的鱼。 $\forall xy(Fx \wedge Fy \wedge Bxy \to Sxy) \to \exists x(Fx \wedge \forall y(Fy \to Bxy)) \to \exists x(Fx \wedge \forall y(Fy \to Sxy))$
9. There are n elements. $\exists x_1 \dots x_n \left(\bigwedge_{1 \le i < j \le n} x_i \neq x_j \wedge \forall x \left(\bigvee_{i=1}^{n} x = x_i\right)\right)$

Translation

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

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

Exercises — Translation

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

Exercises — Translation

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

Translation

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

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

continuity vs uniform continuity

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

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

Translation

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

Translation

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

Substitution and Substitutable

Definition (Substitution in a term/formula)

$$=, P, \neg, \to \cdots$$

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

Definition (Substitutable)

t is substitutable for x in A:

$$=, P, \neg, \to \cdots$$

$A = \forall y B$ iff either

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

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

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

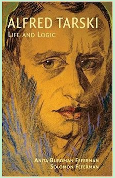
Contents

Philosophy

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

What is "truth" — Are all truths knowable?

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



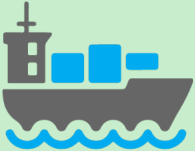
Structure

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

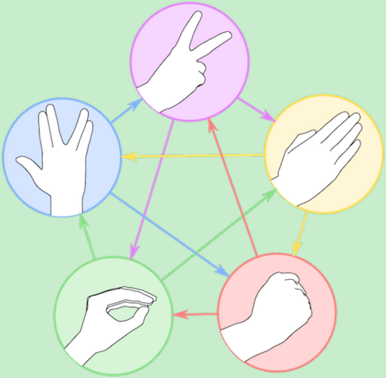
- assigns to each constant symbol c an element $I(c) \in M$,
- assigns to each function symbol f^k a k-ary function $I(f^k) : M^k \to M$,
- assigns to each predicate symbol P^k a k-ary relation $I(P^k) \subset M^k$.

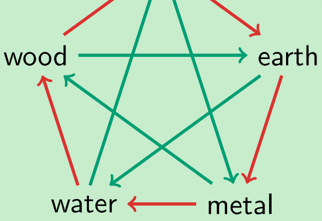
We write $\mathcal{M} = \left(M, c^{\mathcal{M}}, f^{\mathcal{M}}, P^{\mathcal{M}}\right)$ for convenience.

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



Structure





fire

wood

earth

water

metal

Interpretation

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

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

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

Tarski's Definition of Truth

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

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

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

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

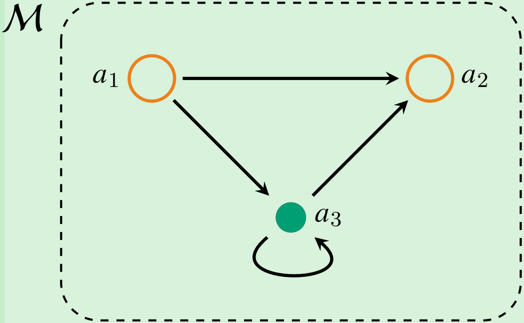
- $\mathcal{M} \vDash A$ if for all $v : \mathcal{M}, v \vDash A$. (True)
- $\mathcal{M}, v \vDash \Gamma$ if for all $A \in \Gamma : \mathcal{M}, v \vDash A$.
- $\mathcal{M} \vDash \Gamma$ if for all $A \in \Gamma : \mathcal{M} \vDash A$.
- $\Gamma \vDash A$ if for all $\mathcal{M}, v : \mathcal{M},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

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

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

Example

Example



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

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

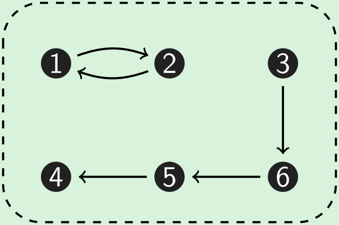
- $\mathcal{M} \overset{?}{\vDash} Pc$
- $\mathcal{M} \overset{?}{\vDash} Pc \lor Rcc$
- $\mathcal{M} \overset{?}{\vDash} \forall x(Px \lor Rxx)$
- $\mathcal{M} \overset{?}{\vDash} \exists x \forall y(y = x \lor Rxy)$
- $\mathcal{M}, \nu \overset{?}{\vDash} Rxy \rightarrow Rcy$
  where $\nu(x) = a_1,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

Example

Example

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

What arrows are missing to make the following a model?



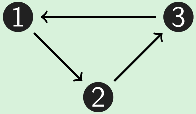
(Add only those arrows that are really needed.)

Counter Model

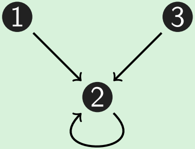
Counter Model

$\forall x \exists y Rxy \not\models \exists x \forall y Rxy$

$\forall x \exists y Rxy \not\models \exists y \forall x Rxy$



$\exists y \forall x Rxy \not\models \forall y \exists x Rxy$



Is there a finite counter model?

Exercise (Counter Model)

Give a counter model for

1. $\forall x \exists y Rxy \wedge \forall xyz(Rxy \wedge Ryz \rightarrow Rxz) \not\models \exists x Rxx$
2. $\forall x \exists y Rxy \wedge \forall xyz(Rxy \wedge Ryz \rightarrow Rxz) \not\models \exists xy(Rxy \wedge Ryx)$

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

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

Mistakes to Avoid

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

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

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

Coincidence Lemma

Lemma (Coincidence Lemma)

Assume $\nu_1, \nu_2 : \mathcal{V} \to M$, and for all $x \in \mathrm{Fv}(A) : \nu_1(x) = \nu_2(x)$. Then

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

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

Substitution Lemma

Lemma (Substitution Lemma)

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

$$\begin{tikzcd}
s \arrow[rr, "{[t/x]}"] \arrow[dr, swap, "\overline{v(\overline{v}(t)/x)}"] & & s[t/x] \arrow[dl, "\overline{v}"] \\
& M &
\end{tikzcd}$$

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

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

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

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

Equivalent Replacement

Lemma

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

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

Alphabetic Variant

Definition (Alphabetic Variant)

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

Theorem

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

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

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

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

Equality and Equivalence

Lemma

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

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

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

Lemma

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

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

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

Remark

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

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

Valid Formulas — Example

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

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

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

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

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

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

$\exists x \forall y A \rightarrow \forall y \exists x A$

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

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

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

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

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

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

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

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

Valid Formulas — Example

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

$$A \leftrightarrow \forall x A$$

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

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

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

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

$$A \leftrightarrow \exists x A$$

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

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

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

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

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

Valid Formulas — Example

$$t = t$$

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

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

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

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

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

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

Valid Formulas — Example

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

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

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

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

Application — Game Theory

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.

$$\exists x_1 \forall y_1 \dots \exists x_n \forall y_n A \lor \forall x_1 \exists y_1 \dots \forall x_n \exists y_n \neg A$$

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

Contents

Formal Systems

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

Hilbert System = Axiom + Inference Rule

Axiom Schema

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

Inference Rule

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

Example

Theorem

$$A \vdash \exists x A$$

Proof.

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

Deduction Theorem

Theorem (Deduction Theorem1)

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

Inference Rule

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

What if we remove Axiom9 and add the rule of generalization to Hilbert System?

Theorem (Deduction Theorem2)

If $\Gamma, A \vdash B$, where the rule of generalization is not applied to the free variables of A, then $\Gamma \vdash A \to B$.

Meta-properties

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

Meta-properties

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

Alphabetic Variant

Theorem (Existence of Alphabetic Variants)

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

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

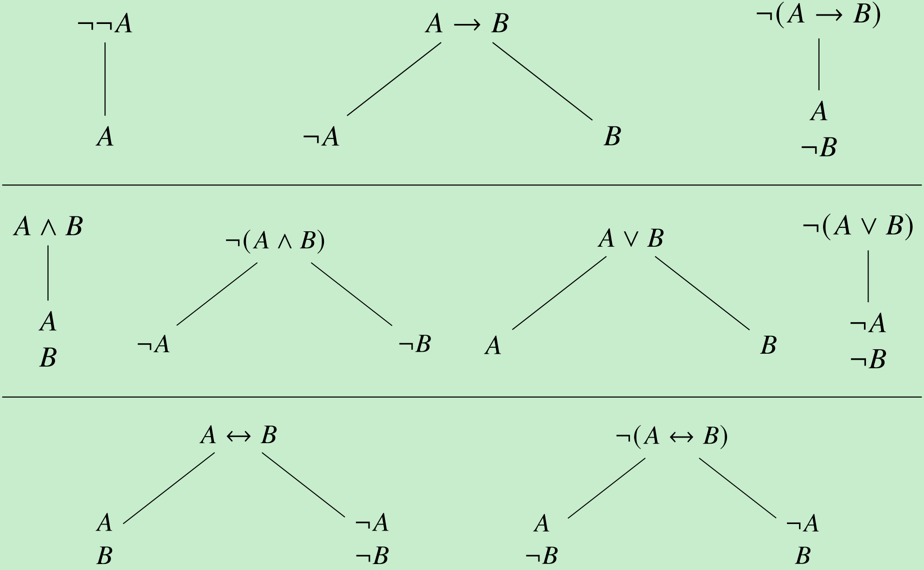
Strategy

$\to$
- $\Gamma \vdash A \to B \;\Longleftarrow\; \Gamma, A \vdash B$

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

$\neg$
1. $(\neg \to)$ $\Gamma \vdash \neg(A \to B) \;\Longleftarrow\; \Gamma \vdash A \;\&\; \Gamma \vdash \neg B$
2. $(\neg\neg)$ $\Gamma \vdash \neg\neg A \;\Longleftarrow\; \Gamma \vdash A$
3. $(\neg\forall)$ $\Gamma \vdash \neg\forall x A \;\Longleftarrow\; \Gamma \vdash \neg A[t/x]$
   Unfortunately this is not always possible. Try contraposition, reductio ad absurdum or prove by contradiction...

Tree Method for Propositional Logic



$\neg\neg A$

A

$A \rightarrow B$

$\neg A$ B

$\neg(A \rightarrow B)$

A

$\neg B$

$A \land B$

A

B

$\neg(A \land B)$

$\neg A$ $\neg B$

$A \lor B$

A B

$\neg(A \lor B)$

$\neg A$

$\neg B$

$A \leftrightarrow B$

A $\neg A$

B $\neg B$

$\neg(A \leftrightarrow B)$

A $\neg A$

$\neg B$ B

✓

Tree Method for Predicate Logic I

Ground Tree:

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

where t is a ground term.

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

where a is a new constant.

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

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

Tree Method for Predicate Logic II

Tree Method with Unification:

$\forall x A$ ✓

$A[x_i/x]$

where x_i is a new variable.

$\exists x A$ ✓

$A[f(x_1, \ldots, x_m)/x]$

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

$\neg\forall x A$ ✓

$\exists x \neg A$

$\neg\exists x A$ ✓

$\forall x \neg A$

Tree Method with Unification

- when expanding a universally quantified formula, do not choose a specific term but a rigid variable as a placeholder.
- choose the term only when it is clear it allows closing a branch.

rigid variable=same value in the whole tree

- variables can 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 formulae if for every $A, B \in \Gamma : A\sigma = B\sigma$.
- A unifier σ is a *most general unifier* for Γ if for each unifier θ there exists a substitution λ s.t. $\theta = \sigma\lambda$.

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

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

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

Tree Method for Predicate Logic

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

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

Deduction & Tactics

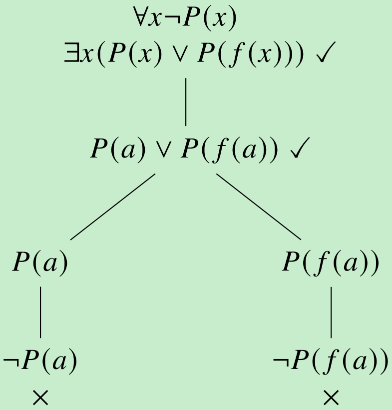
Definition (Deduction)

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

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

Example — Ground Tree

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



$\forall x \neg P(x)$

$\exists x (P(x) \vee P(f(x)))$ ✓

$P(a) \vee P(f(a))$ ✓

$P(a)$

$\neg P(a)$

×

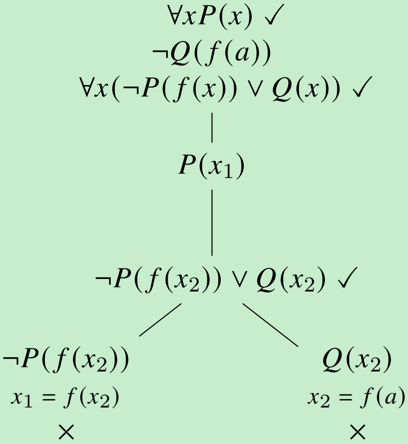
$P(f(a))$

$\neg P(f(a))$

×

Example — Tree Method with Unification

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



$\forall x P(x)$ ✓

$\neg Q(f(a))$

$\forall x(\neg P(f(x)) \vee Q(x))$ ✓

$P(x_1)$

$\neg P(f(x_2)) \vee Q(x_2)$ ✓

$\neg P(f(x_2))$

$x_1 = f(x_2)$

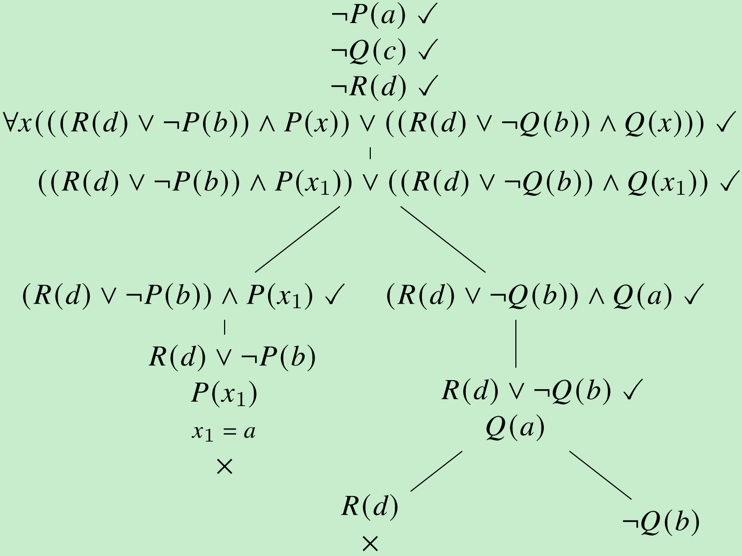
×

$Q(x_2)$

$x_2 = f(a)$

×

Unification — Greedy Unification (incomplete)



$\neg P(a)$ ✓

$\neg Q(c)$ ✓

$\neg R(d)$ ✓

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

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

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

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

$P(x_1)$

$x_1 = a$

×

$(R(d) \vee \neg Q(b)) \wedge Q(a)$ ✓

$R(d) \vee \neg Q(b)$ ✓

$Q(a)$

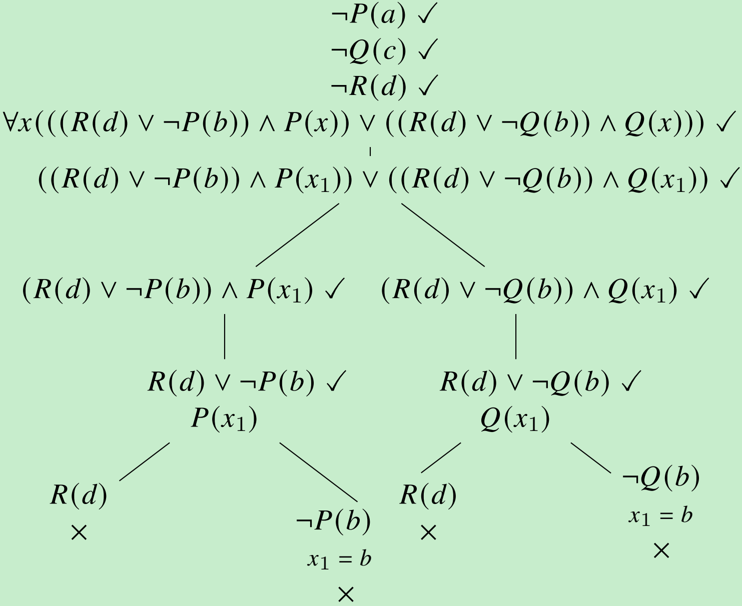
$R(d)$

×

$\neg Q(b)$

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

Unification — Final Closure



$\neg P(a)$ ✓

$\neg Q(c)$ ✓

$\neg R(d)$ ✓

$\forall x(((R(d) \lor \neg P(b)) \land P(x)) \lor ((R(d) \lor \neg Q(b)) \land Q(x)))$ ✓

$((R(d) \lor \neg P(b)) \land P(x_1)) \lor ((R(d) \lor \neg Q(b)) \land Q(x_1))$ ✓

$(R(d) \lor \neg P(b)) \land P(x_1)$ ✓

$(R(d) \lor \neg Q(b)) \land Q(x_1)$ ✓

$R(d) \lor \neg P(b)$ ✓

$P(x_1)$

$R(d) \lor \neg Q(b)$ ✓

$Q(x_1)$

$R(d)$

×

$\neg P(b)$

$x_1 = b$

×

$R(d)$

×

$\neg Q(b)$

$x_1 = b$

×

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

Example — Unification vs Ground

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

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

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

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

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

$$A(x_1)$$

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

$$\neg A(a)$$

$$x_1 = a$$

$$\times$$

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

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

$$A(a)$$

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

$$\neg A(b)$$

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

$$A(b)$$

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

$$\times$$

Soundness & Completeness

Theorem (Soundness Theorem)

If the tree closes, the set is unsatisfiable.

Theorem (Completeness Theorem)

If a set is unsatisfiable, there exists a closed tree from it.

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

Remark: If an inference with predicate wff is not valid and its counterexample is an infinite model, the tree will not find it. The tree method can't generate every counterexample of an invalid inference in predicate logic.

Exercises — Tree Method

1. $\forall x(Px \to Qx) \to \exists x Px \to \exists x Qx$
2. $\exists x \forall y Rxy \to \forall y \exists x Rxy$
3. $\exists x(Px \land Qx) \to \exists x Px \land \exists x Qx$
4. $\forall x\big(A \lor B(x)\big) \to A \lor \forall x B(x)$ where $x \notin \mathrm{Fv}(A)$
5. $\exists x\Big(\big(Px \land \forall y(Py \to y = x)\big) \land Qx\Big) \mathrel{\text{⊣⊢}} \exists x \forall y\Big(\big(Py \leftrightarrow y = x\big) \land Qx\Big)$
6. $\exists x\big(Px \land \forall y(Py \to y = x)\big) \land \exists x\big(Qx \land \forall y(Qy \to y = x)\big) \land \neg \exists x(Px \land Qx) \to$ $\exists xy\big(x \neq y \land (Px \lor Qx) \land (Py \lor Qy) \land \forall z(Pz \lor Qz \to z = x \lor z = y)\big)$

$$1 + 1 = 2$$

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 he knows them both; everyone speaks to Frank; therefore everyone is introduced to Frank by someone who knows him.
4. Whoever stole the goods, knew the safe combination. Someone stole the goods, and *only* Jack knew the safe combination. Hence Jack stole the goods.
5. *No one but* Alice and Bette (*who are different people*) admires Carl. All and only those who admire Carl love him. Hence *exactly* two people love Carl.

Application — Minesweeper

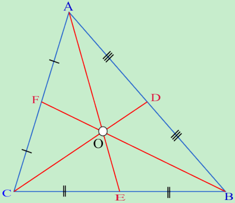
🚩	2	1	1	1	🚩	1	
2	3	🚩	1	1	1	1	
1	🚩	2	2	1	1		
1	1	1	1	🚩	1		
			2	2	2	1	1
1	1		1	🚩	2	2	🚩
🚩	1		1	1	3	🚩	3
1	1				2	🚩	2

- There are exactly n mines in the game.
- If a cell contains the number 1, then there is exactly one mine in the adjacent cells.

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

Russell's Theory of Descriptions

1. The substitution of identicals.
   "The morning star is the evening star."
2. The law of the excluded middle.
   "The present King of France is bald." or
   "The present King of France is not bald."
3. The problem of negative existentials.
   "The round square is round."



Russell's Theory of Descriptions

$$\begin{aligned} B(\iota_x A) &:= \exists! x A \land \exists x (A \land B) \\ &\dashv\vdash \exists x \forall y \Big(\big(A(y) \leftrightarrow y = x \big) \land B(x) \Big) \end{aligned}$$

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

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

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

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

$$\iota_x A = \iota_x A \ \text{ ?} \qquad \forall x B \longrightarrow B(\iota_x A) \ \text{ ?}$$

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

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

Contents

Definability

What is "definability"?

Berry Paradox

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

Definition (Definability)

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

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

- X is definable in $\mathcal{M}$ if it is $\emptyset$-definable in $\mathcal{M}$.

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

Representability

What is “representability”?

Definition (Representable Functions)

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

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

Definition (Representable Relations)

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

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

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

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

Example

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

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

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

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

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

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

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

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

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

Homomorphism & Isomorphism

Definition (Homomorphism)

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

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

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

Homomorphism Theorem

Theorem (Homomorphism Theorem)

Let h be a homomorphism of $\mathcal{M}$ into $\mathcal{N}$, and $v : \mathcal{V} \to M$.

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

Definition (Elementary Equivalence)

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

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

Substructure

Definition (Substructure)

$\mathcal{M}$ is called a *substructure* of $\mathcal{N}$ ($\mathcal{M} \subset \mathcal{N}$) iff

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

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

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

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

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

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

Example

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

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

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

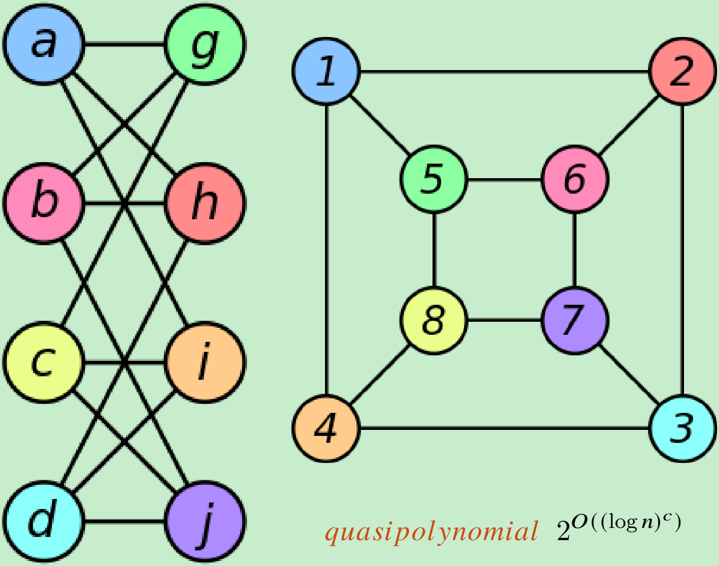
$$h : n \mapsto 2n, \quad h : \mathcal{M} \cong \mathcal{N}, \quad \text{but} \quad \mathcal{M} \not\subset \mathcal{N}$$

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

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

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

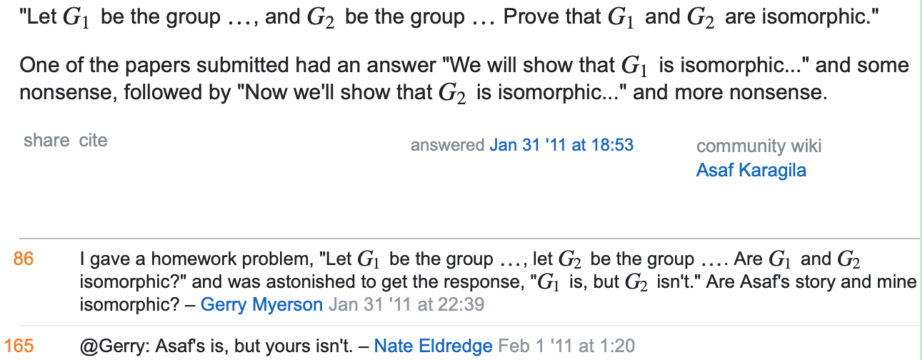
Example



$a \mapsto 1$
$b \mapsto 6$
$c \mapsto 8$
$d \mapsto 3$
$g \mapsto 5$
$h \mapsto 2$
$i \mapsto 4$
$j \mapsto 7$

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

A Joke



"Let G_1 be the group $\ldots$, and G_2 be the group $\ldots$ Prove that G_1 and G_2 are isomorphic."

One of the papers submitted had an answer "We will show that G_1 is isomorphic..." and some nonsense, followed by "Now we'll show that G_2 is isomorphic..." and more nonsense.

answered Jan 31 '11 at 18:53

community wiki
Asaf Karagila

86 I gave a homework problem, "Let G_1 be the group $\ldots$, let G_2 be the group $\ldots$. Are G_1 and G_2 isomorphic?" and was astonished to get the response, "G_1 is, but G_2 isn't." Are Asaf's story and mine isomorphic? – Gerry Myerson Jan 31 '11 at 22:39

165 @Gerry: Asaf's is, but yours isn't. – Nate Eldredge Feb 1 '11 at 1:20

Automorphism & Undefinability

Corollary

Let h be an automorphism $h : M \to M$, and $R \subset M^n$ definable in $\mathcal{M}$. Then for any $a_1, \ldots, a_n \in M$,

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

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

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

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

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

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

Example

Example

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

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

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

Example

Consider the vector space $\mathcal{E} \coloneqq (E, +, f_r)_{r \in \mathbb{R}}$, where E is the universe, f_r is the scalar multiplication by r.

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

Contents

What is Logic?

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

- What is a number?
- What is a line?
- What is a set?
- What is a logical notion?

What is Mathematics?

Mathematics is the art of giving the same name to different things.

— Henri Poincaré

Not substance but invariant form is the carrier of the relevant mathematical information.

— F. William Lawvere

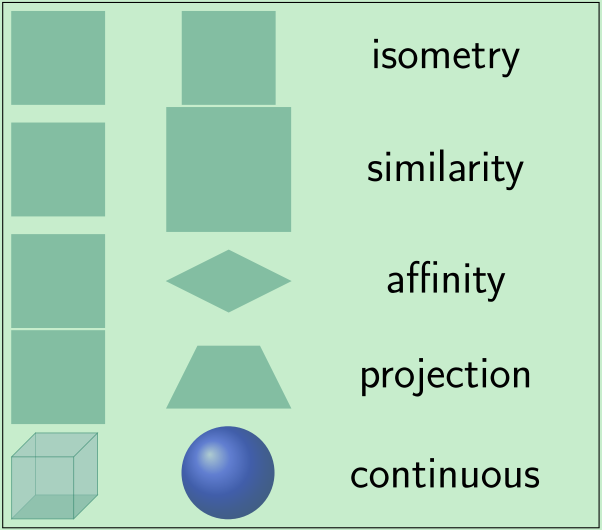
Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true.

— Bertrand Russell

What is Geometry? — Klein's Erlangen Program

What is Geometry?

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



isometry

similarity

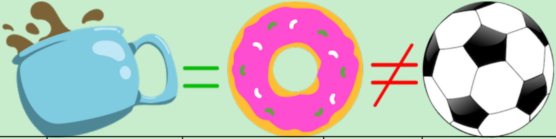
affinity

projection

continuous

Figure: Felix Klein

What is Geometry? — Klein's Erlangen Program



	isometry	similarity	affine	projective	continuous
location					
length	✓				
area	✓				
perpendicularity	✓	✓			
parallelism	✓	✓	✓		
collinearity	✓	✓	✓	✓	
concurrence	✓	✓	✓	✓	
connectedness	✓	✓	✓	✓	✓

> *Given a manifold, and a transformation group acting on it, to study its invariants.*
>
> — *Felix Klein*

Klein's Erlangen Program vs Logic

What is Logic?[8]

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.* ◎ô◎
>
> — *The Devil's Dictionary*

The study of invariants under all automorphisms (symmetries).

---

[8] Tarski: What are logical notions?

Logic as permutation-invariant theory

Logic as permutation-invariant theory.

The study of invariants under all automorphisms (symmetries).

> *A notion is "logical" if it is invariant under all possible one-one transformations of the universe of discourse onto itself.*
>
> — *Tarski*

> *Logic analyzes the meaning of the concepts common to all the sciences, and establishes the general laws governing the concepts.*
>
> — *Tarski*

Contents

Model & Semantic Consequence

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

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

Theory & Axiomatization

- A set Γ of sentences is a theory if $\Gamma = \mathrm{Cn}(\Gamma)$.
- A theory Γ is complete if for every sentence A, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- 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 $\mathcal{K} = \mathrm{Mod}(A)$ for some sentence A.
- 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 A, either $A \in \Gamma$ or $\neg A \in \Gamma$.
- 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)

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

Proof.

by induction on derivation lengths.

Truth in a model is preserved under making deductions.

Completeness Theorem

Theorem (Completeness Theorem — Gödel1930)

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

Corollary

Any consistent set of wffs is satisfiable.

$$\begin{tikzcd}
\Gamma \vDash A \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & \Gamma \vdash A \arrow[d, Leftrightarrow] \\
\begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{unsatisfiable}\end{array} \arrow[r, Leftrightarrow] & \begin{array}{c}\Gamma \cup \{\neg A\} \\ \text{inconsistent}\end{array}
\end{tikzcd}$$

Compactness Theorem

Theorem (Compactness Theorem)

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

Corollary

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

Corollary

If a set 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* $\mathcal{M} \not\cong \mathcal{N}$*.*

Compactness and Compactification

- Extreme value theorem: A continuous real-valued function on a compact space is bounded and attains its maximum and minimum values.
- A subset of a topological space is *compact* if every open cover of it has a finite subcover.
- Heine-Borel Theorem: A subset of $\mathbb{R}$ is compact iff it is closed and bounded.
- Cantor's Intersection Theorem: A decreasing nested sequence of non-empty, closed and bounded subsets of $\mathbb{R}$ has a non-empty intersection.
- Bolzano-Weierstrass Theorem: Every bounded sequence of real numbers has a convergent subsequence.

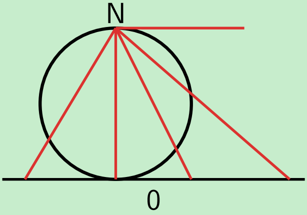
Compactness

finite $\Longrightarrow$ infinite

local $\Longrightarrow$ global

Compactification

$$\mathbb{R} \Longrightarrow \mathbb{R} \cup \{-\infty, +\infty\}$$



$$x \mapsto \left(\frac{x}{1+x^2}, \frac{x^2}{1+x^2}\right)$$

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 $\mathbb{N}$.

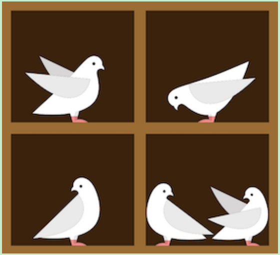
$$\prod_{i\in\mathbb{N}} \mathcal{R}/U \vDash \mathrm{Th}(\mathcal{R})$$

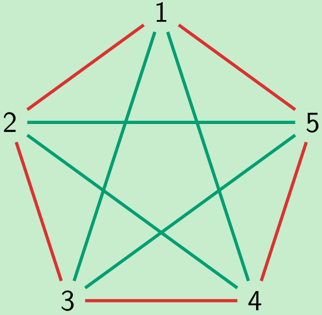
Let $\varepsilon \coloneqq \left[(1, \frac{1}{2}, \frac{1}{3}, \dots)\right] \in \mathbb{R}$.
For any $n \in \mathbb{N}$,

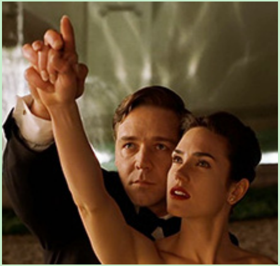
$$\prod_{i\in\mathbb{N}} \mathcal{R}/U \vDash \varepsilon < \frac{1}{n}$$

Problem (Complete Disorder is Impossible!)

- *How many people do you need to invite in a party in order to have that either at least n of them are mutual strangers or at least n of them are mutual acquaintances?*
- *How may we know that such number exists for any n?*







Applications of Compactness

Theorem (Infinite Ramsey Theorem)

If (V, E) is a graph with infinitely many vertices, then it has an infinite clique or an infinite independent set.

Theorem (Finite Ramsey Theorem)

For every $m, n \geq 1$ there is an integer $R(m, n)$ s.t. any graph with at least $R(m, n)$ vertices has a clique with m vertices or an independent set with n vertices.

$$R(m, n) \leq R(m-1, n) + R(m, n-1)$$

$$R(m, n) \leq \binom{m+n-2}{m-1}$$

Ramsey Number

m, n	1	2	3	4	5	6	7	8	9	10
1	**1**	1	1	1	1	1	1	1	1	1
2	1	**2**	3	4	5	6	7	8	9	10
3	1	3	**6**	9	14	18	23	28	36	40 – 42
4	1	4	9	**18**	25	36 – 41	49 – 61	59 – 84	73 – 115	92 – 149
5	1	5	14	25	**43 – 48**	58 – 87	80 – 143	101 – 216	133 – 316	149 – 442
6	1	6	18	36 – 41	58 – 87	**102 – 165**	115 – 298	134 – 495	183 – 780	204 – 1171
7	1	7	23	49 – 61	80 – 143	115 – 298	**205 – 540**	217 – 1031	252 – 1713	292 – 2826
8	1	8	28	59 – 84	101 – 216	134 – 495	217 – 1031	**282 – 1870**	329 – 3583	343 – 6090
9	1	9	36	73 – 115	133 – 316	183 – 780	252 – 1713	329 – 3583	**565 – 6588**	581 – 12677
10	1	10	40 – 42	92 – 149	149 – 442	204 – 1171	292 – 2826	343 – 6090	581 – 12677	**798 – 23556**


Figure: Ramsey 1903-1930


Figure: Erdős 1913-1996

Ramsey Number — Probabilistic Method

Theorem

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

Proof.

$R(2,2) = 2, R(3,3) = 6$. Assume $k \geq 4$. Suppose $N < 2^{\frac{k}{2}}$, and consider all random red-blue colorings. Let A be a set of vertices of size k. The probability of the event A_R that the edges in A are all colored red is then $2^{-\binom{k}{2}}$. Hence the probability p_R for some k-set to be colored all red is bounded by

$$p_R = P\left(\bigcup_{|A|=k} A_R\right) \leq \sum_{|A|=k} P(A_R) = \binom{N}{k} 2^{-\binom{k}{2}} < \frac{1}{2}$$

By symmetry, $p_B < \frac{1}{2}$. So $p_R + p_B < 1$ for $N < 2^{\frac{k}{2}}$.

Complete Disorder is Impossible!

Theorem (Hales-Jewett Theorem)

For every $k, n \in \mathbb{N}^+$*, there is* $d \in \mathbb{N}^+$ *s.t. if the unit hypercubes in a* d*-dimensional hypercube* n^d *are colored in* k *colors, then there exists at least one row, column or diagonal of* n *squares, all of the same color.*

Theorem (van der Waerden Theorem)

For every $k, m \in \mathbb{N}^+$*, there is* $n \in \mathbb{N}^+$ *s.t. if the numbers from* 1 *to* n *are colored in* k *colors, then there exists at least* m *numbers in arithmetic progression, all of the same color.*

Theorem (Green-Tao Theorem)

A subset of prime numbers A *with* $\limsup_{n\to\infty} \frac{|A\cap[1,n]|}{\pi(n)} > 0$ *contains arbitrarily long arithmetic progressions, where* $\pi(n)$ *is the number of primes* $\leq n$*.*

Complete Disorder is Impossible!

Theorem (Szemerédi Theorem)

A set $A \subset \mathbb{N}$ *with* $\limsup_{n\to\infty} \frac{|A\cap[1,n]|}{n} > 0$ *contains arbitrarily long arithmetic progressions.*

Theorem (Furstenberg Multiple Recurrence Theorem)

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

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

Szemerédi Theorem $\Longleftrightarrow$ Furstenberg Multiple Recurrence Theorem

Complete Disorder is Impossible!

Theorem (Poincaré Recurrence Theorem)

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

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

Lemma (Kac's Lemma)

Let $(X, \mathcal{B}, \mu, T)$ *be a measure-preserving system and* $A \in \mathcal{B}$ *with* $\mu(A) > 0$*. Then the recurrence time* $\tau_A(x) := \min\left\{k \geq 1 : T^k x \in A\right\}$ *satisfies*

$$\int_A \tau_A(x) \mathrm{d}\mu(x) = 1$$

Equivalently, the mean recurrence time $\langle \tau_A \rangle := \frac{1}{\mu(A)} \int_A \tau_A(x) \mathrm{d}\mu(x) = \frac{1}{\mu(A)}$*.*

Correlation Supersedes Causation?

- The average recurrence time to a subset A in Poincaré recurrence theorem is the inverse of the probability of A. The probability decrease exponentially with the size (dimension) of the phase space (observables and parameters) and the recurrence time increases exponentially with that size. One can't reliably predict by "analogy" with the past, even in deterministic systems, chaotic or not.
- Given any arbitrary correlation on sets of data, there exists a large enough number such that any data set larger than that size realizes that type of correlation. Every large set of numbers, points or objects necessarily contains a highly regular pattern.
- There is no true randomness. Randomness means unpredictability with respect to some fixed theory.

Correlation Supersedes Causation?

- How to distinguish correlation from causation?
- How to distinguish content-correlations from Ramsey-type correlations?
- Ramsey-type correlations appear in all large enough databases.
- A correlation is *spurious* if it appears in a “randomly” generated database.
- How “large” is the set of spurious correlations?
- Most strings are algorithmically random.

$$P\left(\left\{x \in \mathcal{X}^n : \frac{K(x)}{n} < 1 - \delta\right\}\right) < 2^{-\delta n}$$

- Most correlations are spurious.
- It may be the case that our part of the universe is an oasis of regularity in a maximally random universe.

Complete Disorder is Impossible!

For sufficiently large n and any $x \in \mathcal{X}^n$, if $C(x) \geq n - \delta(n)$, then each block of length $\log n - \log\log n - \log(\delta(n) + \log n) - O(1)$ occurs at least once in x.

Löwenheim-Skolem Theorem

Theorem (Downward Löwenheim-Skolem Theorem)

A consistent set of sentences in a language of cardinality λ *has a model of cardinality* $\leq \lambda$*.*

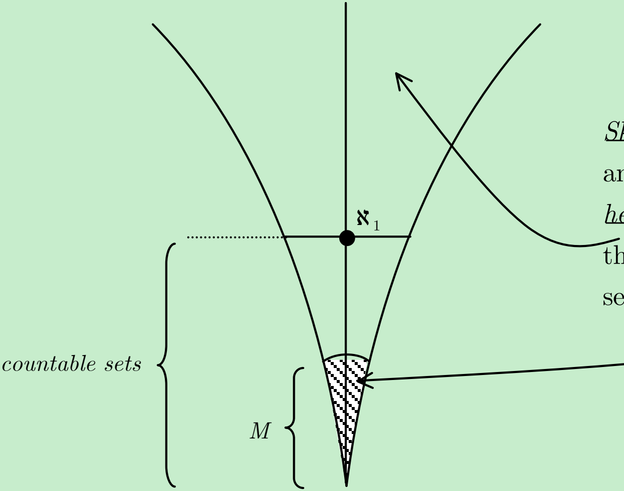
Theorem (Upward Löwenheim-Skolem Theorem)

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

Fragments of First Order Logic

1. The set of *Horn formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \wedge$.
2. The set of *regular formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \wedge, \exists$.
3. The set of *coherent formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \bot, \wedge, \vee, \exists$.
4. The set of *first order formulae* is the smallest set containing the set of atomic formulae and closed under $\top, \bot, \neg, \wedge, \vee, \rightarrow, \exists, \forall$.
5. The class of *geometric formulae* over is the smallest class containing the class of atomic formulae and closed under $\top, \bot, \wedge, \vee, \exists$ and infinitary disjunction.
6. The class of *infinitary first order formulae* is the smallest class containing the class of atomic formulae and closed under $\top, \bot, \neg, \wedge, \vee, \rightarrow, \exists, \forall$ and infinitary conjunction and infinitary disjunction.

- $\mathbb{T}$ is an algebraic theory if its signature has no relation symbols and its axioms are all of the form $\top \vdash_{\mathbf{x}} A$ where A is an atomic formula of the form $s = t$ and $\mathbf{x}$ its canonical context.
- $\mathbb{T}$ is a Horn (resp. regular, coherent, geometric) theory if all the sequents in $\mathbb{T}$ are Horn (resp. regular, coherent, geometric).
- $\mathbb{T}$ is a universal Horn theory if its axioms are all of the form $A \vdash_{\mathbf{x}} B$, where A is a finite conjunction of atomic formulae and B is an atomic formula or the formula $\bot$.
- $\mathbb{T}$ is a propositional theory if it only consists of 0-ary relation symbols.

Identity Axiom $A \vdash_{\mathbf{x}} A$

Equality $\top \vdash_{x} x = x$ and $\mathbf{x} = \mathbf{y} \wedge A \vdash_{\mathbf{z}} A[\mathbf{y}/\mathbf{x}]$ where $\mathrm{Fv}(\mathbf{x}, \mathbf{y}, A) \subset \mathbf{z}$.

Substitution $\dfrac{A \vdash_{\mathbf{x}} B}{A[\mathbf{t}/\mathbf{x}] \vdash_{\mathbf{y}} B[\mathbf{t}/\mathbf{x}]}$ where $\mathrm{Fv}(\mathbf{t}) \subset \mathbf{y}$.

Cut $\dfrac{A \vdash_{\mathbf{x}} B \quad B \vdash_{\mathbf{x}} C}{A \vdash_{\mathbf{x}} C}$

Conjunction $A \vdash_{\mathbf{x}} \top \qquad A \wedge B \vdash_{\mathbf{x}} A \qquad A \wedge B \vdash_{\mathbf{x}} B \qquad \dfrac{A \vdash_{\mathbf{x}} B \quad A \vdash_{\mathbf{x}} C}{A \vdash_{\mathbf{x}} B \wedge C}$

Disjunction $\bot \vdash_{\mathbf{x}} A \qquad A \vdash_{\mathbf{x}} A \vee B \qquad B \vdash_{\mathbf{x}} A \vee B \qquad \dfrac{A \vdash_{\mathbf{x}} C \quad B \vdash_{\mathbf{x}} C}{A \vee B \vdash_{\mathbf{x}} C}$

Implication $\begin{array}{c} A \wedge B \vdash_{\mathbf{x}} C \\ \hline\hline A \vdash_{\mathbf{x}} B \to C \end{array}$

Existential Quantification $\begin{array}{c} A \vdash_{\mathbf{x}y} B \\ \hline\hline \exists y A \vdash_{\mathbf{x}} B \end{array}$

Universal Quantification $\begin{array}{c} A \vdash_{\mathbf{x}y} B \\ \hline\hline A \vdash_{\mathbf{x}} \forall y B \end{array}$

Distributive Axiom $A \wedge (B \vee C) \vdash_{\mathbf{x}} (A \wedge B) \vee (A \wedge C)$

Frobenius Axiom $A \wedge \exists y B \vdash_{\mathbf{x}} \exists y (A \wedge B)$ where $y \notin \mathbf{x}$.

Law of Excluded Middle $\top \vdash_{\mathbf{x}} A \vee \neg A$

Fragments of First Order Logic

In addition to the usual structural rules (Identity axiom, Equality rules, Substitution rule and Cut rule), our deduction systems consist of the following rules:

Algebraic logic	No additional rule
Horn logic	Finite conjunction
Regular logic	Finite conjunction, existential quantification and Frobenius axiom
Coherent logic	Finite conjunction, finite disjunction, existential quantification, distributive axiom and Frobenius axiom
Geometric logic	Finite conjunction, infinitary disjunction, existential quantification, ‘infinitary’ distributive axiom, Frobenius axiom
Intuitionistic FOL	All the finitary rules except for the law of excluded middle
Classical FOL	All the finitary rules

Intuitionistic Propositional Logic vs Heyting Algebra

A Heyting algebra $(H, \bot, \top, \wedge, \vee, \rightarrow, \leq)$ is a bounded lattice $(H, \bot, \top, \wedge, \vee, \leq)$ equipped with $\rightarrow$ s.t. for all $a, b, c \in H$:

1. $a \leq \top$
2. $a \wedge b \leq a$
3. $a \wedge b \leq b$
4. $a \leq b \ \ \& \ \ a \leq c \implies a \leq b \wedge c$
5. $\bot \leq a$
6. $a \leq a \vee b$
7. $b \leq a \vee b$
8. $a \leq c \ \ \& \ \ b \leq c \implies a \vee b \leq c$
9. $a \leq b \rightarrow c \iff a \wedge b \leq c$

Define $\neg a \coloneqq a \rightarrow \bot$.

Brouwer-Heyting-Kolmogorov Interpretation

- A proof of $A \wedge B$ is a pair (a, b) where a is a proof of A and b is a proof of B.
- A proof of $A \vee B$ is a pair (a, b) where a is 0 and b is a proof of A, or a is 1 and b is a proof of B.
- A proof of $A \rightarrow B$ is a function f that converts a proof a of A into a proof $f(a)$ of B.
- There is no proof of $\perp$.
- A proof of $\exists x A(x)$ is a pair (a, b) where a is an element of the domain of definition, and b is a proof of $A(a)$.
- A proof of $\forall x A(x)$ is a function f that converts an element a of the domain of definition into a proof $f(a)$ of $A(a)$.

Continuity, Metric and Topology

- A function $f : X \longrightarrow Y$ between metric spaces is *continuous* at point $a \in X$ if $\forall \varepsilon > 0 \exists \delta > 0 \forall x \in X : d_X(x, a) < \delta \rightarrow d_Y(f(x), f(a)) < \varepsilon$.
- A *metric space* (X, d) is a set X with a metric $d : X \times X \longrightarrow \mathbb{R}$ s.t. for all $x, y, z \in X$:
  1. $d(x, y) = 0 \leftrightarrow x = y$
  2. $d(x, y) = d(y, x)$
  3. $d(x, z) \leq d(x, y) + d(y, z)$

  $$e.g. \quad d(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}} \qquad d(x, y) = \max_{1 \leq i \leq n} |x_i - y_i|$$
- For the definition of continuity ("nearby" points in U go into nearby points in V), the notion of 'open set' is more **intrinsic** than that of distance.
- A function $f : X \longrightarrow Y$ between topological spaces is *continuous* if the inverse image $f^{-1}(V)$ of any open subset $V \subset Y$ is an open subset of X.
- Equivalently, f is *continuous* at point $a \in X$ if to each neighborhood V of $f(a)$ there is a neighborhood U of a for which $f(U) \subset V$.

Topological Semantics of Intuitionistic Propositional Logic

- A *topological space* $(X, \tau X)$ is a set X with a family $\tau X \subset \mathrm{P}(X)$ of subsets of X which contains $\emptyset$ and X, and is closed under finite intersections and arbitrary unions.
- The topological *interior* of a subset $S \subset X$ is

$$S^\circ := \bigcup \{U \in \tau X : U \subset S\}$$

- Define for $A, B \in \tau X$ the open set

$$A \to B := \big((X \setminus A) \cup B\big)^\circ = \bigcup \{U \in \tau X : U \cap A \subset B\}$$

  by definition, for all $U \in \tau X$,

$$U \subset A \to B \iff U \cap A \subset B$$

  Define $\neg A := A \to \bot$. Thus

$$\neg A = (X \setminus A)^\circ$$

- $A := (0,1) \cup (1,\infty), \neg A = (-\infty, 0), \neg\neg A = (0,\infty), A \cup \neg A \neq \mathbb{R}, A \subsetneq \neg\neg A.$
- A topological model of intuitionistic propositional logic is $(X, \tau X, \nu)$ where $\nu : \mathcal{P} \to \tau X$.

Contents

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

Logics about Modalities

Mary _____ married.

- is possibly (basic modal logic)
- will be (temporal logic)
- is permitted to be (deontic logic)
- is known (to A) to be (epistemic logic)
- is proved to be (provability logic)
- will be (after certain procedure) (dynamic logic)
- can be ensured (by her parents) to be (coalition logic)

Figure: Kripke

Syntax

Language

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

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

Well-Formed Formula wff

$$A ::= p \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid A \leftrightarrow A \mid \Box A \mid \Diamond A$$

- It will always be A. GA
- You ought to do A. OA
- I know A. $K_i A$
- I believe A. $B_i A$
- A is provable in T. $\Box_{\mathrm{T}} A$
- After the execution of the program α, A holds. $[\alpha]A$

Contents

Possible World Semantics

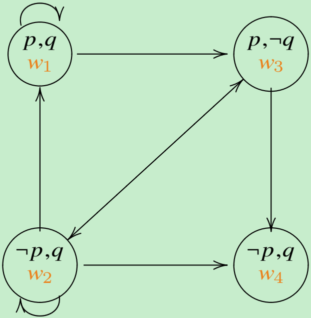
A Kripke frame is a pair $\mathcal{F} := (W, R)$, where

- $W \neq \emptyset$
- $R \subset W \times W$

A Kripke model is $\mathcal{M} := (\mathcal{F}, V) = (W, R, V)$, where $V : \mathcal{P} \to \mathrm{P}(W)$.

- $\mathcal{M}, w \Vdash p$ if $w \in V(p)$
- $\mathcal{M}, w \Vdash \neg A$ if $\mathcal{M} \nVdash A$
- $\mathcal{M}, w \Vdash A \wedge B$ if $\mathcal{M}, w \Vdash A$ and $\mathcal{M}, w \Vdash B$
- $\mathcal{M}, w \Vdash \Box A$ if $\forall v \in W : Rwv \implies \mathcal{M}, v \Vdash A$
- $\mathcal{M}, w \Vdash \Diamond A$ if $\exists v \in W : Rwv \;\&\; \mathcal{M}, v \Vdash A$

Example



$\mathcal{M}, w_1 \Vdash p \wedge \Box p$

$\mathcal{M}, w_1 \Vdash q \wedge \Diamond q$

$\mathcal{M}, w_1 \Vdash \neg \Box q$

$\mathcal{M}, w_2 \Vdash q \wedge \Diamond \neg q$

$\mathcal{M}, w_3 \Vdash p$

$\mathcal{M}, w_3 \Vdash \Box \neg p$

$\mathcal{M}, w_4 \Vdash \Box p \wedge \neg \Diamond p$

Satisfiability & Validity

- A is satisfiable at $\mathcal{M}, w$ if $\mathcal{M}, w \Vdash A$.
- A is true in $\mathcal{M}$ ($\mathcal{M} \Vdash A$) if $\forall w \in W : \mathcal{M}, w \Vdash A$
- A is valid in a pointed frame $\mathcal{F}, w$ ($\mathcal{F}, w \Vdash A$) if $\mathcal{M}, w \Vdash A$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- A is valid in $\mathcal{F}$ ($\mathcal{F} \Vdash A$) if $\mathcal{M} \Vdash A$ for every model $\mathcal{M}$ based on $\mathcal{F}$.
- $\Vdash A$ if $\mathcal{F} \Vdash A$ for every $\mathcal{F}$.

Truth is in the eye of the beholder.

Example

$$\Vdash \Box(A \longrightarrow B) \longrightarrow \Box A \longrightarrow \Box B$$

Semantic Consequence

- local semantic consequence

$$\Gamma \Vdash_{\mathcal{C}} A \;:=\; \forall \mathcal{M} \in \mathcal{C} \forall w \in W : \mathcal{M}, w \Vdash \Gamma \implies \mathcal{M}, w \Vdash A$$

- global semantic consequence

$$\Gamma \Vdash^{g}_{\mathcal{C}} A \;:=\; \forall \mathcal{M} \in \mathcal{C} : \mathcal{M} \Vdash \Gamma \implies \mathcal{M} \Vdash A$$

Example

- $p \nVdash_{\mathcal{C}} \Box p$
- $p \Vdash^{g}_{\mathcal{C}} \Box p$

Material Implication vs Strict Implication

$$p \strictif q \coloneqq \Box(p \rightarrow q)$$

- $p \strictif q \strictif p$?
- $(p \strictif q) \vee (q \strictif r)$?
- $\neg(p \strictif q) \rightarrow (p \wedge \neg q)$?
- $(p \wedge \neg p) \strictif q$
- $p \strictif (q \vee \neg q)$
- $\Box p \strictif q \strictif p$

Accessibility

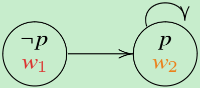
serial	$\forall x \exists y : Rxy$
reflexive	$\forall x : Rxx$
symmetric	$\forall xy : Rxy \rightarrow Ryx$
transitive	$\forall xyz : Rxy \wedge Ryz \rightarrow Rxz$
euclidean	$\forall xyz : Rxy \wedge Rxz \rightarrow Ryz$
total	$\forall xy : Rxy \vee Ryx$
isolation	$\exists x \forall y : \neg Rxy \wedge \neg Ryx$
successor reflexive	$\forall x \exists y : Rxy \wedge Ryy$
asymmetric	$\forall xy : Rxy \rightarrow \neg Ryx$
antisymmetric	$\forall xy : Rxy \wedge Ryx \rightarrow x = y$

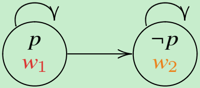
Accessibility

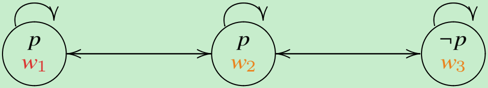
Theorem

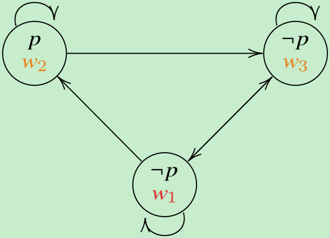
$$\begin{array}{lllcl}
D & W, R \Vdash \Box p \rightarrow \Diamond p & \iff & R \textit{ is serial} \\
T & W, R \Vdash \Box p \rightarrow p & \iff & R \textit{ is reflexive} \\
B & W, R \Vdash p \rightarrow \Box \Diamond p & \iff & R \textit{ is symmetric} \\
4 & W, R \Vdash \Box p \rightarrow \Box \Box p & \iff & R \textit{ is transitive} \\
5 & W, R \Vdash \Diamond p \rightarrow \Box \Diamond p & \iff & R \textit{ is euclidean}
\end{array}$$

Counter-model for D,T,B,4,5









Standard Translation

Definition (Standard Translation)

$$
\begin{aligned}
T_x(p) &= P(x) & T_y(p) &= P(y) \\
T_x(\neg A) &= \neg T_x(A) & T_y(\neg A) &= \neg T_y(A) \\
T_x(A \wedge B) &= T_x(A) \wedge T_x(B) & T_y(A \wedge B) &= T_y(A) \wedge T_y(B) \\
T_x(\Box A) &= \forall y(Rxy \to T_y(A)) & T_y(\Box A) &= \forall x(Ryx \to T_x(A))
\end{aligned}
$$

Theorem (Correspondence on Models)

$$\mathcal{M}, w \Vdash A \iff \mathcal{M} \vDash T_x(A)[w]$$

$$\mathcal{M} \Vdash A \iff \mathcal{M} \vDash \forall x T_x(A)$$

$$\mathcal{F}, w \Vdash A \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n T_x(A)[w]$$

$$\mathcal{F} \Vdash A \iff \mathcal{F} \vDash \forall P_1, \ldots, P_n \forall x T_x(A)$$

Tree Method for Modal Logic

$$\begin{array}{c} w \Vdash \Box A \\ | \\ w' \Vdash A \end{array}$$

if Rww' is already in the branch.

$$\begin{array}{c} w \nVdash \Box A \\ | \\ Rww' \\ w' \nVdash A \end{array}$$

where w' is new in the branch.

$$\begin{array}{c} w \Vdash \Diamond A \\ | \\ Rww' \\ w' \Vdash A \end{array}$$

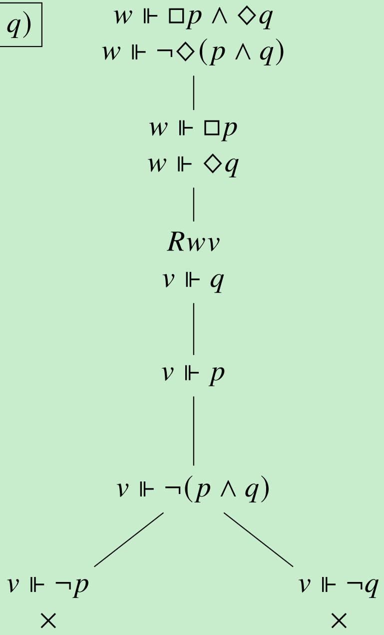
where w' is new in the branch.

$$\begin{array}{c} w \nVdash \Diamond A \\ | \\ w' \nVdash A \end{array}$$

if Rww' is already in the branch.

Example — Tree Method for Modal Logic

$$\boxed{\Vdash \Box p \land \Diamond q \to \Diamond(p \land q)}$$



$w \Vdash \Box p \land \Diamond q$

$w \Vdash \neg\Diamond(p \land q)$

$w \Vdash \Box p$

$w \Vdash \Diamond q$

Rwv

$v \Vdash q$

$v \Vdash p$

$v \Vdash \neg(p \land q)$

$v \Vdash \neg p$

×

$v \Vdash \neg q$

×

Contents

Formal System = Axiom + Inference Rule

Axiom Schema

	tautologies
Dual	$\Diamond A \leftrightarrow \neg\Box\neg A$
K	$\Box(A \to B) \to \Box A \to \Box B$
D	$\Box A \to \Diamond A$
T	$\Box A \to A$
B	$A \to \Box\Diamond A$
4	$\Box A \to \Box\Box A$
5	$\Diamond A \to \Box\Diamond A$
L	$\Box(\Box A \to A) \to \Box A$

Inference Rule

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

Intuitionistic Logic vs Modal Logic

$$\mathrm{S4} := K + T + 4$$

$$\mathrm{Grz} := \mathrm{S4}{+}\Box(\Box(A \to \Box A) \to A) \to A$$

$$\begin{aligned} p^* &:= \Box p \\ (\neg A)^* &:= \Box\neg A^* \\ (A \wedge B)^* &:= A^* \wedge B^* \\ (A \vee B)^* &:= A^* \vee B^* \\ (A \to B)^* &:= \Box(A^* \to B^*) \end{aligned}$$

$$\vdash_{\mathrm{I}} A \iff \vdash_{\mathrm{S4}} A^* \iff \vdash_{\mathrm{Grz}} A^*$$

$$\mathrm{GL} := K + L$$

$$\begin{aligned} p' &:= p \\ (\neg A)' &:= \neg A' \\ (A \wedge B)' &:= A' \wedge B' \\ (A \vee B)' &:= A' \vee B' \\ (A \to B)' &:= A' \to B' \\ (\Box A)' &:= A' \wedge \Box A' \end{aligned}$$

$$\begin{aligned} \vdash_{\mathrm{Grz}} A &\iff \vdash_{\mathrm{GL}} A' \\ \vdash_{\mathrm{I}} A &\iff \vdash_{\mathrm{GL}} (A^*)' \end{aligned}$$

$$\boxed{\Box(\Box A \to A) \to \Box A \vdash_{\mathrm{GL}} \Box A \to \Box\Box A}$$

- $A \land \Box A \land \Box\Box A \to A \land \Box A$
- $A \to \Box(A \land \Box A) \to A \land \Box A$ $\quad\Box(p \land q) \leftrightarrow \Box p \land \Box q$
- $\Box(\Box(A \land \Box A) \to A \land \Box A) \to \Box(A \land \Box A)$ $\quad$ L
- $\Box A \to \Box(A \land \Box A)$
- $\Box A \to \Box\Box A$

Theorem

$W, R \Vdash \Box(\Box A \rightarrow A) \rightarrow \Box A \iff$ *R is transitive & R is reverse well-founded: there are no chains $w_0 R w_1 R w_2 \ldots$.*

Proof.

Assume $R w_0 w_1$ and $R w_1 w_2$, but not $R w_0 w_2$. Setting $V(p) := W \setminus \{w_1, w_2\}$ makes L false at w_0.
Assume R is transitive, and there is an ascending sequence $w_0 R w_1 R w_2 \ldots$. Then $V(p) := W \setminus \{w_0, w_1, w_2, \ldots\}$ refutes L at w_0.
Conversely, if L fails at w_0, there must be an infinite upward sequence of $\neg p$-worlds. This arises by taking any successor of w_0 where p fails, and repeatedly applying the truth of $\Box(\Box p \rightarrow p)$ — using the transitivity of the frame.

Remark: transitivity is definable in first order logic, but well-foundedness can't be defined in first order logic. Frame truth is a second order notion.

Provability Logic

Theorem (Craig Interpolation)

If $\mathrm{GL} \vdash A \to B$, *then there is a* C *with* $\mathrm{Var}(C) \subset \mathrm{Var}(A) \cap \mathrm{Var}(B)$ *s.t.*

$$\mathrm{GL} \vdash A \to C \quad \textit{and} \quad \mathrm{GL} \vdash C \to B$$

Corollary (Beth Definability)

Assume $\mathrm{GL} \vdash A(p) \wedge A(q) \to (p \leftrightarrow q)$ *where* $q \notin \mathrm{Var}(A)$ *and* $A(q)$ *is obtained from* $A(p)$ *by replacing all occurrences of* p *by* q. *Then there exists a formula* B *with* $\mathrm{Var}(B) \subset \mathrm{Var}(A) \setminus \{p\}$ *s.t.*

$$\mathrm{GL} \vdash A(p) \to (p \leftrightarrow B)$$

Proof.

Let B be an interpolant for $\mathrm{GL} \vdash A(p) \wedge p \to (A(q) \to q)$.

Provability Logic

Theorem (Uniqueness of Fixpoint)

If p *occurs only boxed in* $A(p)$ *and* $q \notin \mathrm{Var}(A)$, *then*

$$\mathrm{GL} \vdash \boxdot\Big(\big(p \leftrightarrow A(p)\big) \wedge \big(q \leftrightarrow A(q)\big)\Big) \to (p \leftrightarrow q)$$

where $\boxdot A := A \wedge \Box A$.

Corollary

If p *occurs only boxed in* $A(p)$, *then*

$$\mathrm{GL} \vdash B \leftrightarrow A(B) \;\&\; \mathrm{GL} \vdash C \leftrightarrow A(C) \implies \mathrm{GL} \vdash B \leftrightarrow C$$

Theorem (Existence of Fixpoint)

If p *occurs only boxed in* $A(p)$, *then there exists a formula* B *with* $\mathrm{Var}(B) \subset \mathrm{Var}(A) \setminus \{p\}$ *s.t.*

$$\mathrm{GL} \vdash B \leftrightarrow A(B)$$

$$\boxed{\text{Uniqueness of Fixpoint + Beth Definability} \implies \text{Existence of Fixpoint}}$$

$$\mathrm{GL} \vdash \neg\Box\bot \leftrightarrow \neg\Box(\neg\Box\bot) \qquad\qquad \mathrm{GL} \vdash \top \leftrightarrow \Box\top$$

Soundness & Completeness

Definition (Theorem & Local Syntactic Consequence)

- $\vdash_S A$
- $\Gamma \vdash_S A$ if $\vdash_S \bigwedge_{i=1}^{n} B_i \rightarrow A$ for some finite subset $\{B_1, \ldots, B_n\} \subset \Gamma$.

Theorem (Soundness & Completeness)

Let S be the normal system $KX_1 \ldots X_n$ and $C = \bigcap_{i=1}^{n} C_i$ where each C_i is the corresponding class of frames for axiom schema X_i.

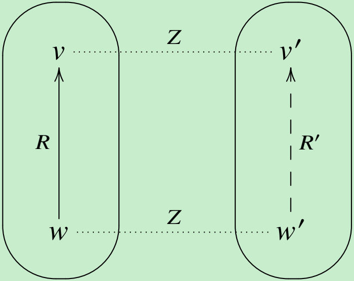
$$\Gamma \vdash_S A \iff \Gamma \Vdash_C A$$

Bisimulation

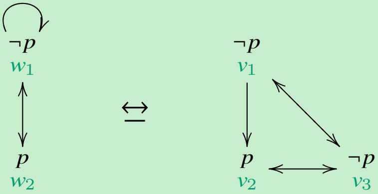
Definition (Bisimulation)

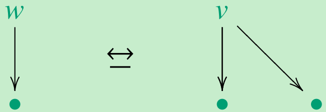
A bisimulation $Z : \mathcal{M} \leftrightarroweq \mathcal{M}'$ between Kripke models $\mathcal{M} = (W, R, V)$ and $\mathcal{M}' = (W', R', V')$ is a binary relation $Z \subset W \times W'$ s.t.

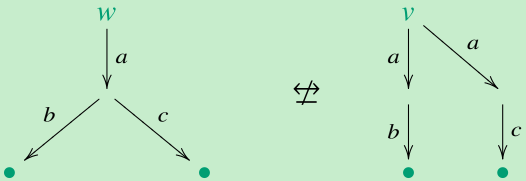
1. If Zww' then w and w' satisfy the same proposition letters.
2. If Zww' and Rwv, then there exists $v' \in W'$ s.t. Zvv' and $R'w'v'$.
3. If Zww' and $R'w'v'$, then there exists $v \in W$ s.t. Zvv' and Rwv.



Bisimulation — Example







$$\Box_a(\Diamond_b\top \wedge \Diamond_c\top)$$

Bisimulation

Theorem (van Benthem Characterization Theorem)

Let $A(x)$ be a first order formula. Then $A(x)$ is bisimulation invariant iff it is (equivalent to) the standard translation of a modal formula.

Theorem (van Benthem2007)

An abstract modal logic extending basic modal logic and satisfying compactness and bisimulation invariance is equally expressive as the basic modal logic K.

Contents

Logic of Knowledge

- 什么是密码? 你知我知。
- 微信群是干嘛的? 制造公共知识。
- 邮件密送是干嘛的? 你知他知，他不知你知，且这是你我的公共知识。
- “代我问他好”是干嘛的? 让你知道我尊重他。
- 送什么礼物给太太? 我知道她也知道对她有用的。
- 广告语的意义? 制造带意义的动作传递知识。
- 《三体》中的黑暗森林法则：爱好和平的公共知识难以达成。
- 如何建设健康学术环境：让他知道你知道学术规范。
- 狼人杀? 理性利用别人的不理性。
- 付费知识分享平台：让你相信你知道很多。
- Would you like to come up to my apartment to see my etchings?
  阿 Q：我想和你困觉!
  Nash: Could we just go straight to the sex? $\not\checkmark$

Reasoning about Knowledge

- Knowledge is power: act properly to achieve goals;
- Knowledge is time: to make decisions more efficiently;
- Knowledge is money: can be traded;
- Knowledge is responsibility: to prove someone is guilty;
- Knowledge is you: to identify oneself;
- Knowledge is an immune system: to protect you;
- Knowledge satisfies our curiosity.

"The only good is knowledge and the only evil is ignorance." — *Socrates*

$$\boxed{\text{know the unknown from the known}}$$

- There are things we know we know. There are things we know we don't know. There are things we don't know we don't know.

$$\exists x K K x \wedge \exists x K \neg K x \wedge \exists x \neg K \neg K x$$

- 知之为知之，不知为不知，是知也。

$$Kp \to KKp \quad \& \quad \neg Kp \to K\neg Kp$$

"Real knowledge is to know the extent of one's ignorance." — *Confucius*

- Mutual Knowledge:

  everybody in G knows p.

- Distributed Knowledge:

  everybody in G would know p
  if agents in G shared all their information.

- Common Knowledge:

  everybody in G knows p,
  everybody knows that everybody knows,
  and so on.

Mutual Knowledge

Suppose a group $G \subset \{1 \dots n\}$ of agents, everyone in G knows A:

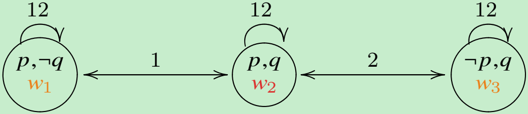
$$\begin{aligned} E_G A &:= \bigwedge_{i \in G} K_i A \\ R_E &:= \bigcup_{i \in G} R_i \end{aligned}$$

$$\mathcal{M}, w \Vdash E_G A \quad \text{iff} \quad \forall v \in W : R_E w v \implies \mathcal{M}, v \Vdash A$$

Distributed Knowledge

$$R_D \;:=\; \bigcap_{i \in G} R_i$$

$$\mathcal{M}, w \Vdash D_G A \quad \text{iff} \;\; \forall v \in W : R_D w v \implies \mathcal{M}, v \Vdash A$$



$$w_2 \vDash K_1 p \wedge \neg K_1 q \wedge K_2 q \wedge \neg K_2 p \wedge D_{\{1,2\}}(p \wedge q)$$

Common Knowledge

$$E_G^1 A := E_G A$$
$$E_G^{k+1} A := E_G E_G^k A$$
$$C_G A := \bigwedge_{k=1}^{\infty} E_G^k A$$

$$R^1 := R$$
$$R^{k+1} := R \circ R^k$$
$$R \circ S := \{(x, y) : \exists z (Rxz \wedge Szy)\}$$
$$R^* := \bigcup_{k=1}^{\infty} R^k$$

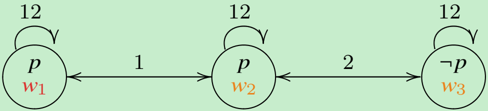
$$R_C := \left(\bigcup_{i \in G} R_i \right)^*$$

$$\mathcal{M}, w \Vdash C_G A \text{ iff } \forall v \in W : R_C wv \implies \mathcal{M}, v \Vdash A$$

A Hierarchy of States of Knowledge

$$C_G A \implies \cdots E_G^k A \implies \cdots E_G A \implies \bigvee_{i \in G} K_i A \implies D_G A \implies A$$

Can we easily have full common knowledge?



$$w_1 \vDash E_{\{1,2\}}p \wedge \neg C_{\{1,2\}}p$$

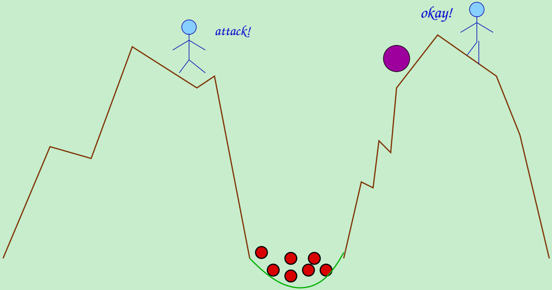
假设 C 秘密的分别给了 A 和 B 两个数字 2 和 3，他只告诉他们俩这两个数字是相邻的自然数。令 p 为“两数字之和小于一千万”，请问 p 是 A 和 B 的公共知识么？

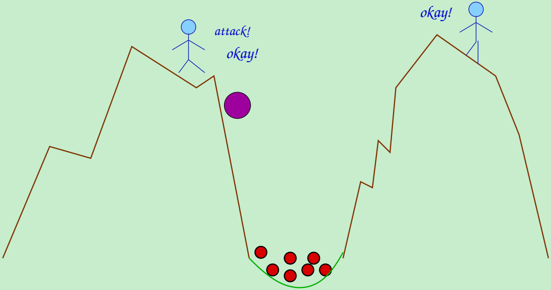
$$(0,1) \xleftrightarrow{B} (2,1) \xleftrightarrow{A} \underline{(2,3)} \xleftrightarrow{B} (4,3) \xleftrightarrow{A} (4,5) \xleftrightarrow{B} (6,5) \cdots$$

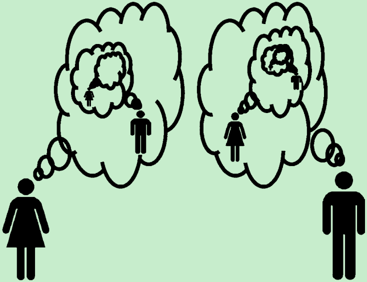
$$(2,3) \Vdash \neg K_B K_A K_B (x + y \leq 10)$$

A and B commonly know that B's number is odd.

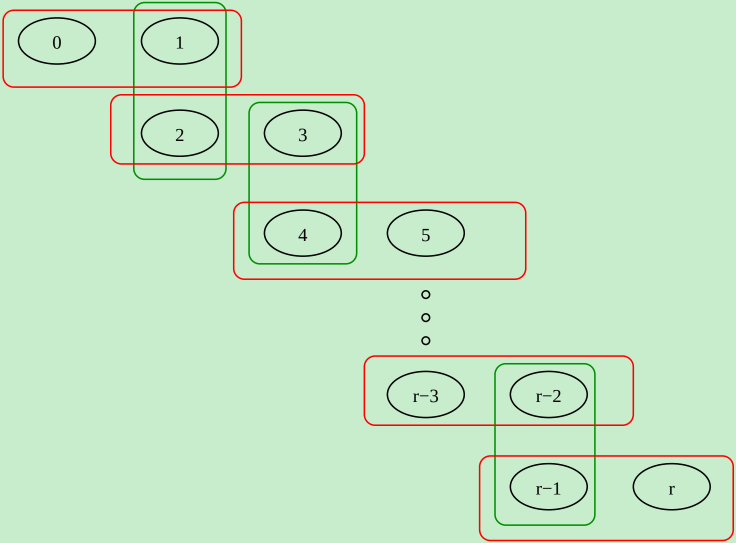
Coordinated Attack







Coordinated Attack



《三体》— 黑暗森林

黑暗森林-猜疑链

如果你认为我是善意的，这并不是你感到安全的理由，因为按照第一条公理，善意文明并不能预先把别的文明也想成善意的，所以，你现在还不知道我是怎么认为你的，你不知道我认为你是善意还是恶意；进一步，即使你知道我把你也想象成善意的，我也知道你把我想象成善意的，但是我不知道你是怎么想我怎么想你怎么想我的……

“Every driver must drive on the right.”

What kind of knowledge is enough to let people feel safe in driving on the right?

Aumann’s Agreement Theorem

Theorem (Aumann’s Agreement Theorem)

If two people are genuine Bayesian rationalists with common priors, and their posteriors are common knowledge, then these posteriors are equal.

如果两个人有相同的先验知识，则他们不可能对有分歧的后验知识（经过各自的实验获取私人信息）形成公共知识。简而言之，如果出发点信息是公共知识，则不管怎么根据进一步的私人证据进行充分的更新和交流，大家都不可能最后 agree to disagree!

Epistemic Logic

- Knowledge $\mathrm{S5} := K + T + 4 + 5$

知之为知之(4)，不知为不知(5)，是知也

- Belief $K + D + 4 + 5$
- Common Knowledge

$$\mathrm{S5}$$

$$+$$

$$C_G A \leftrightarrow A \wedge E_G C_G A$$

$$+$$

$$A \wedge C_G(A \to E_G A) \to C_G A$$

- Distributed Knowledge

$$\mathrm{S5}$$

$$+$$

$$D_{\{i\}} A \leftrightarrow K_i A$$

$$+$$

$$D_G A \to D_{G'} A \quad \text{if} \quad G \subset G'$$

Knowledge vs Belief

1. $K(p \to q) \to Kp \to Kq$
2. $Kp \to p$
3. $Kp \to KKp$
4. $\neg Kp \to K\neg Kp$

1. $B(p \to q) \to Bp \to Bq$
2. $Bp \to \neg B\neg p$
3. $Bp \to Bp$
4. $\neg Bp \to B\neg Bp$

1. $Kp \to Bp$
2. $Bp \to BKp$
3. $Bp \to KBp$
4. $\neg Kp \to K\neg Bp$

$$\boxed{Bp \leftrightarrow \neg K\neg Kp}$$

Fitch's Paradox

All knowable truths are known.

$\forall p(p \to \Diamond Kp) \vdash \forall p(p \to Kp)$

1.	$K(p \land \neg Kp)$	Assumption
2.	$Kp \land K\neg Kp$	$K(p \land q) \to Kp \land Kq$
3.	Kp	
4.	$K\neg Kp$	
5.	$\neg Kp$	$Kp \to p$
6.	$\neg K(p \land \neg Kp)$	
7.	$\neg\Diamond K(p \land \neg Kp)$	$\vdash \neg p \implies \vdash \neg\Diamond p$
8.	$p \land \neg Kp$	Assumption
9.	$\Diamond K(p \land \neg Kp)$	$p \to \Diamond Kp$
10.	$\neg(p \land \neg Kp)$	
11.	$p \to Kp$	

Fitch's Paradox

1.	$B(p \wedge \neg Bp)$	Assumption
2.	$Bp \wedge B\neg Bp$	$B(p \wedge q) \rightarrow Bp \wedge Bq$
3.	Bp	
4.	BBp	$Bp \rightarrow BBp$
5.	$B\neg Bp$	
6.	$BBp \wedge B\neg Bp$	
7.	$\neg(BBp \wedge B\neg Bp)$	$\neg(Bp \wedge B\neg p)$
8.	$\neg B(p \wedge \neg Bp)$	

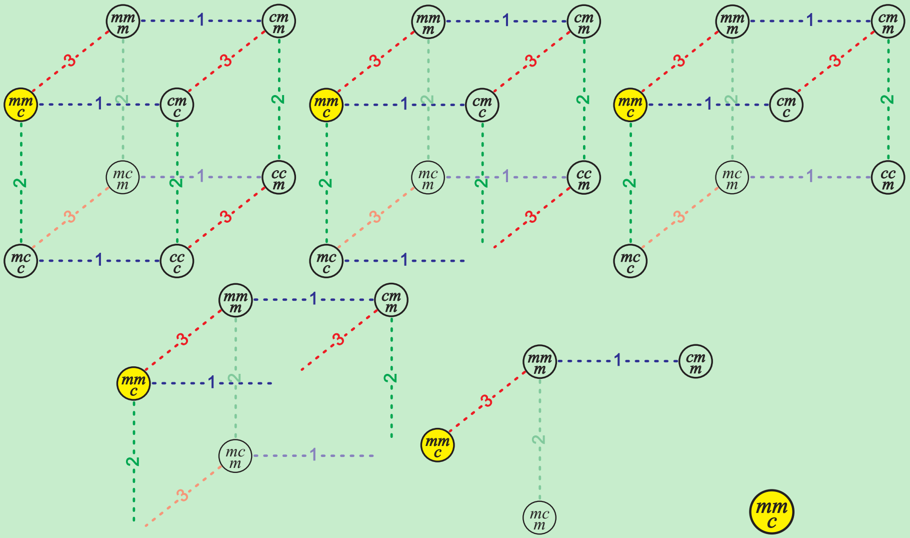
Negative Introspection

1. $\neg p \wedge BKp$ suppose you falsely believes that you know p
2. $\neg Kp$ knowledge implies truth
3. $K\neg Kp$ negative introspection
4. $B\neg Kp$ knowledge implies belief
5. $B\bot$

Information Update — Muddy Children Problem

Problem (Muddy Children Problem)

Consider k of n children get mud on their heads. Each child can see the mud on others but can't see his or her own head. Their father says "at least one is muddy." He then asks the following question repeatedly: "does anyone know whether you have mud on your own head?" Assuming that the children are intelligent, honest, and answer simultaneously, what will happen?



1. “At least one is muddy. Does anyone. . . ?” $\neg K_1 m_1 \land \neg K_2 m_2 \land \neg K_3 m_3$
2. “Does anyone. . . ?” $K_1 m_1 \land K_2 m_2 \land \neg K_3 m_3$
3. $K_3 \neg m_3$

Public Announcement Logic

$$A ::= p \mid \neg A \mid A \wedge A \mid K_i A \mid [A]A$$

$$\mathcal{M}, w \Vdash [B]A \text{ iff } \mathcal{M}, w \Vdash B \implies \mathcal{M}{\restriction_B}, w \Vdash A$$

$$\mathcal{M}, w \Vdash \langle B \rangle A \text{ iff } \mathcal{M}, w \Vdash B \ \& \ \mathcal{M}{\restriction_B}, w \Vdash A$$

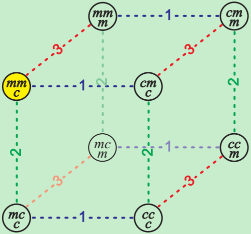
where

$$\mathcal{M}{\restriction_B} \coloneqq \left(W', \{R'_i\}_{i \in G}, V'\right)$$

and

$$W' \coloneqq \{w \in W : \mathcal{M}, w \Vdash B\} \quad R'_i \coloneqq R_i{\restriction_{W' \times W'}} \quad V'(p) \coloneqq V(p) \cap W'$$

Muddy Children Problem



$$\mathcal{M}, mmc \Vdash m_1 \wedge m_2 \wedge \neg m_3$$

$$\mathcal{M}, mmc \Vdash E_{\{1,2,3\}}P$$

$$\mathcal{M}, mmc \Vdash \neg C_{\{1,2,3\}}P$$

$$\mathcal{M}, mmc \Vdash \neg K_1 m_1 \wedge K_1 m_2$$

$$\mathcal{M}, mmc \Vdash K_1 K_3 m_2 \wedge K_1 \neg K_2 m_2$$

$$\mathcal{M}\restriction_P, mcc \Vdash K_1 m_1$$

$$\mathcal{M}\restriction_P, mmc \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$$

$$\mathcal{M}\restriction_P, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$$

$$\mathcal{M}\restriction_P\restriction_{\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3}, mmm \Vdash \langle \neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \rangle Q_1 \vee Q_2 \vee Q_3$$

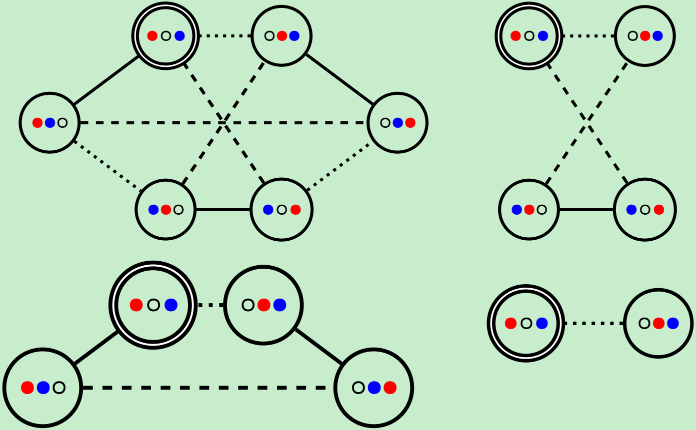
1. "At least one is muddy." $P := m_1 \vee m_2 \vee m_3$
2. "Does anyone. . . ?" $\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3$ where $Q_i := K_i m_i \vee K_i \neg m_i$
3. "Does anyone. . . ?" $Q_1 \wedge Q_2 \wedge \neg Q_3$

$$\mathcal{M}, mmc \Vdash [P][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3][Q_1 \wedge Q_2 \wedge \neg Q_3]\big(K_1 m_1 \wedge K_2 m_2 \wedge K_3 \neg m_3\big)$$

$$\mathcal{M}, mmm \Vdash [P][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3][\neg Q_1 \wedge \neg Q_2 \wedge \neg Q_3]\big(K_1 m_1 \wedge K_2 m_2 \wedge K_3 m_3\big)$$

Three Cards Puzzle

- 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”.



Birthday Puzzle

A and **B** want to know when **C**'s birthday is.
C provides a list of 10 possible dates:

$$\begin{array}{lll} 5.15 & 5.16 & 5.19 \\ 6.17 & 6.18 & \\ 7.14 & 7.16 & \\ 8.14 & 8.15 & 8.17 \end{array}$$

C then tells **A** and **B** separately the month and the day of her birthday.

- **A:** I don't know when **C**'s birthday is, but I know that **B** also does not know.
- **B:** At first I didn't know, but now I know.
- **A:** Then I also know it.

Russian Cards

Russian Cards

- From a pack of seven known cards "0123456" A and B each draw three cards and C gets the remaining card.
- How can A and B openly inform each other about their cards, without C learning of any of their cards who holds it?

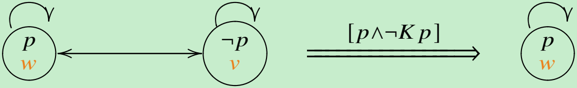
- Assume A' hand is ijk and the remaining cards is $lmno$. Choose one from ijk, say i, and choose two from $lmno$, say lm. Three of the hands are ijk, ilm, ino. From lm choose one, say l, and from no choose one, say n. Two hands are jln, kmo. A announces these five hands.
- B announces C's card.

Unsuccessful Update

$$\Vdash [p]C_G p$$

$$\Vdash [C_G A]C_G A$$

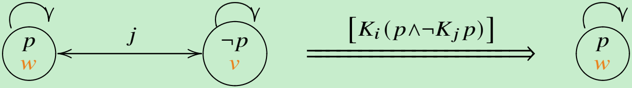
$$\overset{?}{\Vdash} [A]C_G A \qquad \overset{?}{\Vdash} [A]KA \qquad \overset{?}{\Vdash} [A]A$$



$$\mathcal{M}, w \Vdash (p \wedge \neg Kp) \wedge [p \wedge \neg Kp]\, Kp$$

Remark: If the goal of the announcing person was to “spread the truth of this formula,” then this attempt was clearly unsuccessful.

Unsuccessful Update



$$\mathcal{M}, w \Vdash (p \wedge \neg K_j p) \wedge K_i(p \wedge \neg K_j p) \wedge \left[K_i(p \wedge \neg K_j p)\right] K_i K_j p$$

- $\langle B \rangle A \leftrightarrow B \land [B]A$
- $[B](A \to C) \leftrightarrow ([B]A \to [B]C)$
- $[B]p \leftrightarrow (B \to p)$
- $[B]\neg A \leftrightarrow (B \to \neg A)$?
- $[B]\neg A \leftrightarrow \neg [B]A$?
- $[B]\neg A \leftrightarrow (B \to \neg [B]A)$
- $[B]K_i A \leftrightarrow (B \to K_i(B \to [B]A))$
- $[B]K_i A \leftrightarrow (B \to K_i [B]A)$
- $[B][C]A \leftrightarrow [B \land C]A$?
- $[B][C]A \leftrightarrow [B \land [B]C]A$
- $\dfrac{A}{[B]A} \qquad \dfrac{A(p)}{A(B)}$? $\qquad \dfrac{A \leftrightarrow B}{[A]C \leftrightarrow [B]C} \qquad \dfrac{A \leftrightarrow B}{[C]A \leftrightarrow [C]B}$

Public Announcement Logic (PAL)

Axiom Schema

1. tautologies
2. $K_i(A \to B) \to K_iA \to K_iB$
3. $[B]p \leftrightarrow (B \to p)$
4. $[B]\neg A \leftrightarrow (B \to \neg[B]A)$
5. $[B](A \land C) \leftrightarrow [B]A \land [B]C$
6. $[B]K_iA \leftrightarrow (B \to K_i[B]A)$
7. $[B][C]A \leftrightarrow [B \land [B]C]A$

Inference Rule

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

Expressive Power

Theorem

PAL *is equally expressive as basic modal logic.*

Proof.

$$
\begin{aligned}
t(\top) &= \top \\
t(p) &= p \\
t(\neg A) &= \neg t(A) \\
t(A \wedge B) &= t(A) \wedge t(B) \\
t(K_i A) &= K_i t(A)
\end{aligned}
\qquad
\begin{aligned}
t([B]\top) &= t(B \rightarrow \top) \\
t([B]p) &= t(B \rightarrow p) \\
t([B]\neg A) &= t(B \rightarrow \neg [B]A) \\
t([B](A \wedge C)) &= t([B]A \wedge [B]C) \\
t([B]K_i A) &= t(B \rightarrow K_i [B]A) \\
t([B][C]A) &= t([B \wedge [B]C]A)
\end{aligned}
$$

$$\Vdash A \leftrightarrow t(A)$$

Succinctness

Theorem

PAL *is complete w.r.t. the standard semantics of Public Announcement Logic.*

Proof.

$$\Vdash A \implies \Vdash t(A) \implies \vdash_{\mathrm{K}} t(A) \implies \vdash_{\mathrm{PAL}} t(A) \implies \vdash_{\mathrm{PAL}} A$$

Theorem

PAL *is exponentially more succinct than modal logic on arbitrary models.*

$$A_0 \coloneqq \top$$

$$A_{n+1} \coloneqq \langle\langle A_n\rangle\Diamond_1\top\rangle\Diamond_2\top$$

where $\Diamond_i A \coloneqq \neg K_i \neg A$ and $\langle B\rangle A \coloneqq \neg[B]\neg A$.

Announcement and Common Knowledge

$$\frac{P \to [Q]A \quad P \land Q \to E_G P}{P \to [Q] C_G A}$$

'Common knowledge induction' is a special case.
Take $P \coloneqq A$ and $Q \coloneqq \top$.

$$C_G(A \to E_G A) \to A \to C_G A$$

Propositional Dynamic Logic

$$A ::= \top \mid p \mid \neg A \mid A \land A \mid [\alpha]A$$
$$\alpha ::= a \mid A? \mid \alpha;\alpha \mid \alpha \cup \alpha \mid \alpha^*$$

$$\mathcal{M}, w \Vdash [\alpha]A \ \text{ iff } \ \forall v \in W : R_\alpha wv \implies \mathcal{M}, v \Vdash A$$

where

$$\begin{aligned} R_{A?} &:= \{(w,w) : \mathcal{M}, w \Vdash A\} \\ R_{\alpha;\beta} &:= \big\{(w,v) : \exists u\big(R_\alpha wu \land R_\beta uv\big)\big\} \\ R_{\alpha\cup\beta} &:= R_\alpha \cup R_\beta \\ R_{\alpha^*} &:= \bigcup_{n=0}^{\infty} R_{\alpha^n} \end{aligned}$$

Propositional Dynamic Logic (PDL)

Axiom Schema

1. tautologies
2. $[\alpha](A \to B) \to [\alpha]A \to [\alpha]B$
3. $[B?]A \leftrightarrow (B \to A)$
4. $[\alpha;\beta]A \leftrightarrow [\alpha][\beta]A$
5. $[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
6. $[\alpha^*]A \leftrightarrow A \wedge [\alpha][\alpha^*]A$
7. $A \wedge [\alpha^*](A \to [\alpha]A) \to [\alpha^*]A$

Inference Rule

$$\frac{A \quad A \to B}{B}\,[\mathsf{MP}] \qquad\qquad \frac{A}{[\alpha]A}\,[\mathsf{N}]$$

PDL is sound and weak complete.

PDL is not compact. $\{\langle a^*\rangle p, \neg p, \neg\langle a\rangle p, \neg\langle a;a\rangle p, \neg\langle a;a;a\rangle p, \dots\}$

Its satisfiability is decidable (in EXPTIME).

First Order Dynamic Logic

Axiom Schema

1. FOL
2. PDL
3. $\langle x := t\rangle A \leftrightarrow A[t/x]$

Inference Rule

$$\frac{A \quad A \to B}{B}\ [\text{MP}] \qquad \frac{A \to [\alpha^n]B, \quad n \in \omega}{A \to [\alpha^*]B}\ [\text{IC}]$$

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

Application

$$\begin{aligned}
\textbf{skip} &\coloneqq \top? \\
\textbf{fail} &\coloneqq \bot? \\
\textbf{if } B \textbf{ then } \alpha \textbf{ else } \beta &\coloneqq B?;\alpha \cup \neg B?;\beta \\
\textbf{while } B \textbf{ do } \alpha &\coloneqq (B?;\alpha)^*;\neg B? \\
\textbf{repeat } \alpha \textbf{ until } B &\coloneqq \alpha;(\neg B?;\alpha)^*;B? \\
\{A\}\ \alpha\ \{B\} &\coloneqq A \longrightarrow [\alpha]B
\end{aligned}$$

$$[(x = m \land y = n)?]\Big\langle\, (x \neq y?; (x > y?; x \leftarrow x - y) \cup (x < y?; y \leftarrow y - x))^*\, ; x = y?\Big\rangle x = \mathrm{gcd}(m, n)$$

Hoare Logic

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}}$$

$$\frac{}{\{P[t/x]\}\ x := t\ \{P\}}$$

$$\frac{\{P\}\ \alpha\ \{Q\} \quad \{Q\}\ \beta\ \{R\}}{\{P\}\ \alpha ; \beta\ \{R\}}$$

$$\frac{\{B \wedge P\}\ \alpha\ \{Q\} \quad \{\neg B \wedge P\}\ \beta\ \{Q\}}{\{P\}\ \textbf{if}\ B\ \textbf{then}\ \alpha\ \textbf{else}\ \beta\ \{Q\}}$$

$$\frac{P_1 \rightarrow P_2 \quad \{P_2\}\ \alpha\ \{Q_2\} \quad Q_2 \rightarrow Q_1}{\{P_1\}\ \alpha\ \{Q_1\}}$$

$$\frac{\{P \wedge B\}\ \alpha\ \{P\}}{\{P\}\ \textbf{while}\ B\ \textbf{do}\ \alpha\ \{\neg B \wedge P\}}$$

$$\{x = 4 \wedge y = 3\}\ \textbf{if}\ x < y\ \textbf{then}\ z := x; y := y + 1\ \textbf{else}\ z := y; z := z + 1\ \{x = 4 \wedge y = 3 \wedge z = 4\}$$

庄子《秋水》

庄子《秋水》

庄子与惠子游于濠梁之上。

1. 庄子：鲦鱼出游从容，是鱼之乐也。
2. 惠子：子非鱼，安知鱼之乐?
3. 庄子：子非我，安知我不知鱼之乐?
4. 惠子：我非子，固不知子矣；子固非鱼也，子之不知鱼之乐，全矣。
5. 庄子：请循其本。子曰‘汝安知鱼乐’云者，既已知吾知之而问我。我知之濠上也。

庄子《秋水》

- 惠子：子非鱼，安知鱼之乐？

$$\forall xy(K_x Hy \vee K_x \neg Hy \to Fy \to Fx)$$

$$\forall x(K_x Hf \vee K_x \neg Hf \to x = f)$$

- 庄子：子非我，安知我不知鱼之乐？

$$\forall xy(K_x K_y Hf \vee K_x \neg K_y Hf \to x = y)$$

- 惠子：我非子，固不知子矣；子固非鱼也，子之不知鱼之乐，全矣。

For any ‘subjective’ formula A,

$$\frac{\forall xy\big(K_x A(y) \vee K_x \neg A(y) \to x = y\big) \quad h \neq z \quad z \neq f}{\neg K_z Hf \wedge \neg K_h \neg K_z Hf}$$

Moore’s Paradox?

Gödel's Proof of God's Existence

Ax.1 Either a property or its negation is positive, but not both. $\forall X[P(\neg X) \leftrightarrow \neg P(X)]$

Ax.2 A property necessarily implied by a positive property is positive. $\forall X \forall Y\, [P(X) \wedge \Box \forall x[X(x) \rightarrow Y(x)] \rightarrow P(Y)]$

Th.1 Positive properties are possibly exemplified. $\forall X[P(X) \rightarrow \Diamond \exists x X(x)]$

Df.1 A *God-like* being possesses all positive properties. $G(x) := \forall X[P(X) \rightarrow X(x)]$

Ax.3 The property of being God-like is positive. $P(G)$

Th.2 Possibly, God exists. $\Diamond \exists x G(x)$

Ax.4 Positive properties are necessarily positive. $\forall X[P(X) \rightarrow \Box P(X)]$

Df.2 An *essence* of an individual is a property necessarily implying any of its properties. $E(X,x) := X(x) \wedge \forall Y(Y(x) \rightarrow \Box \forall y(X(y) \rightarrow Y(y)))$

Th.3 Being God-like is an essence of any God-like being. $\forall x[G(x) \rightarrow E(G,x)]$

Df.3 *Necessary existence* of an individual is the necessary exemplification of all its essences. $N(x) := \forall X[E(X,x) \rightarrow \Box \exists y X(y)]$

Ax.5 Necessary existence is a positive property. $P(N)$

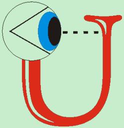
Th.4 Necessarily, God exists. $\Box \exists x G(x)$

Pride and Prejudice

$$C_{\text{Human}}\left(\forall x\Big(\,\text{Man}(x) \land \text{Single}(x) \land \text{Fortune}(x) \rightarrow \right.$$

$$\left.\text{Desire}_x\Big(\exists y\big(\,\text{Woman}(y) \land \text{Marry}(x, y)\big)\Big)\Big)\right)$$

— *Jane Austen*



Thanks