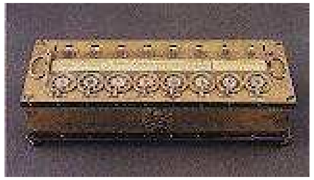
Early History of Computing.

1623.

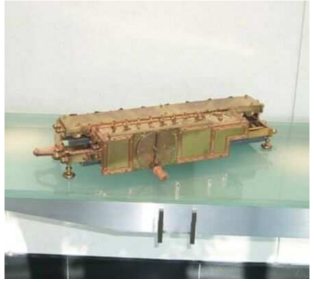
Wilhelm Schickard (1592-1635)

Blaise Pascal (1623-1662)

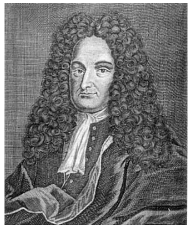
1642.



1671.



Gottfried Wilhelm von Leibniz (1646-1716)



Turing.

Alan Turing (1912-1954)

- **1936**. *On computable numbers.* The Turing Machine.
- **1938**. PhD in Princeton.
- **1939-1942**. Government Code and Cypher School at Bletchley Park.
- *Enigma*.
- **1946**. Automatic Computing Engine (ACE).
- **1948**. Reader in Manchester.
- **1950**. *Computing machinery and intelligence.* The Turing Test.
- **1952**. Arrested for violation of British homosexuality statutes.

Turing Machines (1).

Entscheidungsproblem.

Is there an algorithm that decides whether a given formula of predicate logic is a tautology or not?

Positive answer simple; negative answer hard. Define "algorithm".

Turing Machine. An idealized model of computation: an infinite tape, a finite alphabet Σ of symbols that can be on the tape, a read/write head, a finite set of actions A, a finite set S of states and a function ("programme") $F : \Sigma \times S \to A$. One of the states is designated the HALT state. Write $T := \langle \Sigma, S, A, F \rangle$. There are only countably many Turing machines.

Turing Machines (2).

Turing Machine. An idealized model of computation: an infinite tape, a finite alphabet Σ of symbols that can be on the tape, a read/write head, a finite set of actions A, a finite set S of states and a function (“programme”) $F : \Sigma \times S \to A$. One of the states is designated the HALT state. Write $T := \langle \Sigma, S, A, F \rangle$. There are only countably many Turing machines.

- Given some finite string $s \in \Sigma^*$ as input, the machine starts its computation according to F.
- There is a unique defined sequence of states that the computation runs through.
- If one of them is HALT, we say that the machine halts and write $T(s) \downarrow$.
- Otherwise, we say that the machine loops (diverges) and write $T(s) \uparrow$.
- If $T(s) \downarrow$, then the machine outputs the content of the tape. We write $T(s)$ for the output.
- We say that T accepts s if $T(s) \downarrow$ and $T(s) = 1$.
- We say that T rejects s if $T(s) \downarrow$ and $T(s) = 0$.
- A set $X \subseteq \Sigma^*$ is decidable if there is a Turing machine T such that $s \in X$ if and only if T accepts s and $s \notin X$ if and only if T rejects s.

The Universal Turing Machine (1).

Fixing a finite alphabet $\Sigma := \{\sigma_0, ..., \sigma_s\}$ and a finite set of actions $A := \{\alpha_0, ..., \alpha_a\}$, we can list all Turing machines:

If $F : \Sigma \times S \to A$ is a Turing machine programme, we can view it as a partial function
$\Phi_F : \{0, ..., s\} \times \{0, ..., n\} \to \{0, ..., a\}$ for some natural number n.

If now $\Phi : \{0, ..., s\} \times \{0, ..., n\} \to \{0, ..., a\}$ is a partial function, we assign a natural number (the "Gödel number of Φ"):

$$\mathrm{G}(\Phi) := \prod_{i \le s, j \le n} \mathrm{prime}_{ij}^{\Phi(i,j)+1}.$$

The Universal Turing Machine (2).

$$\mathrm{G}(\Phi) := \prod_{i \leq s, j \leq n} \mathrm{prime}_{ij}^{\Phi(i,j)+1}.$$

Let

$$T \subseteq \mathbb{N} := \{n\,;\, \exists F\,(\mathrm{G}(\Phi_F) = n\,)\,\}$$

be the set of numbers that are Gödel numbers of some Turing machine. Let t_n be the nth number in T and let T_n be the Turing machine such that $\mathrm{G}(\Phi_{T_n}) = t_n$.

> "It can be shown that a single special machine of that type can be made to do the work of all. It could in fact be made to work as a model of any other machine. The special machine may be called the universal machine. (Turing 1947)."

The Universal Turing Machine (3).

Let T be the set of numbers that are Gödel numbers of some Turing machine. Let t_n be the nth number in T and let T_n be the (a) Turing machine such that $\mathrm{G}(\Phi_{T_n}) = t_n$.

A universal Turing machine is a Turing machine U with alphabet $\{0, 1\}$ such that at input $\langle n, m\rangle$ such that $n \in T$ the following happens:

- If $T_n(m)\uparrow$, then $U(n, m)\uparrow$.
- If $T_n(m)\downarrow = k$, then $U(n, m)\downarrow = k$.

The Halting Problem K is the set

$$K := \{n\,;\, U(n, n)\downarrow\}.$$

The Halting Problem.

Theorem (Turing). The Halting Problem is not decidable.

Proof. Suppose it is decidable. Then there is a Turing machine T such that

$$\begin{array}{ccccc} T(n)\downarrow = 0 & \leftrightarrow & n \in K & \leftrightarrow & U(n,n)\downarrow \\ T(n)\downarrow = 1 & \leftrightarrow & n \notin K & \leftrightarrow & U(n,n)\uparrow \end{array}$$

By universality, there is some $e \in T$ such that $T = T_e$, *i.e.*,

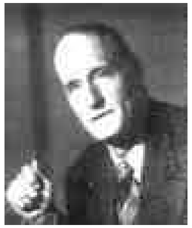
$$\begin{array}{ccccc} T(n)\downarrow = 0 & \leftrightarrow & T_e(n)\downarrow = 0 & \leftrightarrow & U(e,n)\downarrow = 0 \\ T(n)\downarrow = 1 & \leftrightarrow & T_e(n)\downarrow = 1 & \leftrightarrow & U(e,n)\downarrow = 1 \end{array}$$

Substitute $n = e$ in the above equivalences and get:

$$U(e,e)\downarrow = 1 \ \leftrightarrow \ U(e,e)\uparrow .$$

Contradiction! q.e.d.

Computability (1).



Alonzo Church 1903-1995

Stephen Kleene 1909-1994

> "Both Turing and Gödel preferred the terminology 'computable' for this class of functions. When Turing's 1939 paper appeared, he had already been recruited as a cryptanalyst three days after Britain was plunged into World War II. Gödel moved to set theory. Neither Turing nor Gödel had much influence on the terminology of the subject after 1939.
> The present terminology came from Church and Kleene. They had both committed themselves to the new 'recursive' terminology before they had ever heard of Turing or his results. (Soare 1996)"

Robert I. **Soare**, Computability and recursion, **Bulletin of Symbolic Logic** 2 (1996), p.284-321

Computability (2).

computable	recursive
computably enumerable	recursively enumerable
Computability Theory	Recursion Theory

The class of Church-recursive functions is the smallest class containing projections and the successor function closed under primitive recursion, substitution and μ-recursion.

Theorem. A function is Turing-computable if and only if it is Church-recursive.

Church-Turing Thesis. Every algorithm is represented by a Turing machine.

The *Entscheidungsproblem.*

Theorem (Church). The set of all (codes for) tautologies in predicate logic is undecidable, *i.e.*, there is no Turing machine T such that

$$\begin{array}{lcl} T(n)\downarrow = 0 & \leftrightarrow & \varphi_n \text{ is a tautology} \\ T(n)\downarrow = 1 & \leftrightarrow & \varphi_n \text{ is not a tautology.} \end{array}$$

Alonzo **Church**, An Unsolvable Problem of Elementary Number Theory, **American Journal of Mathematics** 58 (1936), p. 345-363

Gödel's Constructible Universe (1).

Johan von Neumann

(1903-1957)

Kurt Gödel

(1906-1978)

- Usual ("von Neumann") construction of the set-theoretic universe is built on the ordinals and the power set operation: $\mathbf{V}_{\alpha+1} := \wp(\mathbf{V}_\alpha)$.
- Constructible approach (Gödel). Only add those subsets that are defined by formulae: Let X be given, then $A \subseteq X$ is defined over X if there is a formula φ and finitely many parameters $p_0, ..., p_n \in X$ such that

$$x \in A \leftrightarrow X \models \varphi[x, p_0, ..., p_n].$$

Let $\mathrm{Def}(X) := \{A \subseteq X\ ;\ A \text{ is defined over } X\} \subseteq \wp(X)$.

$\mathbf{L}_{\alpha+1} := \mathrm{Def}(\mathbf{L}_\alpha)$.

Gödel's Constructible Universe (2).

$\mathbf{V}_{\alpha+1} := \wp(\mathbf{V}_\alpha)$.
$\mathbf{L}_{\alpha+1} := \mathrm{Def}(\mathbf{L}_\alpha)$.

Let $\mathbf{L}$ be the universe defined by Gödel's $\mathbf{L}$-operation. Then:

Theorem (Gödel; 1938). $\mathbf{L} \models \mathsf{ZFC} + \mathsf{CH}$.

Corollary. If ZF is consistent, then ZFC + CH is consistent.

Consequences.

- **Question 1**, **Question 2** and **Question 2*** cannot have a negative answer.
- The system ZFC + CH cannot be logically stronger than ZF, *i.e.*, $\mathsf{ZFC} + \mathsf{CH} \not\vdash \mathrm{Cons}(\mathsf{ZF})$.
- $\mathbf{L}$ is a minimal model of set theory.

Gödel's Constructible Universe (3).

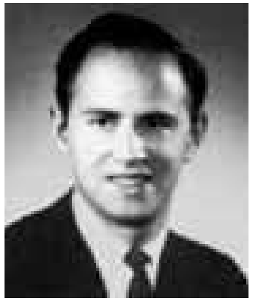
A new axiom? $\mathbf{V}{=}\mathbf{L}$. "The set-theoretic universe is minimal".

Gödel Rephrased. $\mathsf{ZF} + \mathbf{V}{=}\mathbf{L} \vdash \mathsf{AC} + \mathsf{CH}$.

Possible solutions.

- Prove $\mathbf{V}{=}\mathbf{L}$ from ZF.
- Assume $\mathbf{V}{=}\mathbf{L}$ as an axiom. ($\mathbf{V}{=}\mathbf{L}$ is generally not accepted as an axiom of set theory.)
- Find a different proof of AC and CH from ZF.
- Prove AC and CH to be independent by creating models of $\mathsf{ZF} + \neg\mathsf{AC}$, $\mathsf{ZF} + \neg\mathsf{CH}$, and $\mathsf{ZFC} + \neg\mathsf{CH}$.

Cohen.

 Paul Cohen (b. 1934)

Technique of Forcing (1963). Take a model M of ZFC and a partial order $\mathbb{P} \in M$. Then there is a model construction of a new model $M^{\mathbb{P}}$, the forcing extension. By choosing $\mathbb{P}$ carefully, we can control properties of $M^{\mathbb{P}}$.

Let $\kappa > \omega_1$. If $\mathbb{P}$ is the set of finite partial functions from $\kappa \times \omega$ into 2, then $M^{\mathbb{P}} \models \neg$CH.

Theorem (Cohen). ZFC $\nvdash$ CH.

Theorem (Cohen). ZF $\nvdash$ AC.

Modal logic (1).

Modalities.

- *“the standard modalities”*. “necessarily”, “possibly”.
- *temporal*. “henceforth”, “eventually”, “hitherto”.
- *deontic*. “it is obligatory”, “it is allowed”.
- *epistemic*. “p knows that”.
- *doxastic*. “p believes that”.

Modal logic (2).

Modalities as operators.
McColl (late XIXth century); Lewis-Langford (1932). $\Diamond$ as an operator on propositional expressions:

$$\Diamond\varphi \rightsquigarrow \text{“Possibly } \varphi\text{”.}$$

$\Box$ for the dual operator:

$$\Box\varphi \rightsquigarrow \text{“Necessarily } \varphi\text{”.}$$

Iterated modalities:

$$\Box\Diamond\varphi \rightsquigarrow \text{“It is necessary that } \varphi \text{ is possible”.}$$

Modal logic (3).

What modal formulas should be axioms? This depends on the interpretation of $\Diamond$ and $\Box$.

Example. $\Box\varphi \rightarrow \varphi$ ("axiom $\mathbf{T}$").

- *Necessity interpretation.* "If φ is necessarily true, then it is true."
- *Epistemic interpretation.* "If p knows that φ, then φ is true."
- *Doxastic interpretation.* "If p believes that φ, then φ is true."
- *Deontic interpretation.* "If φ is obligatory, then φ is true."

Early modal semantics.

Topological Semantics (McKinsey / Tarski). Let $\langle X, \tau \rangle$ be a topological space and $V : \mathbb{N} \to \wp(X)$ a valuation for the propositional variables.

$\langle X, \tau, x, V \rangle \models \Diamond\varphi$ if and only if x is in the closure of $\{z\,;\, \langle X, \tau, z, V \rangle \models \varphi\}$.

$\langle X, \tau \rangle \models \varphi$ if for all $x \in X$ and all valuations V, $\langle X, \tau, x, V \rangle \models \varphi$.

Theorem (McKinsey-Tarski; 1944). $\langle X, \tau \rangle \models \varphi$ if and only if $\mathbf{S4} \vdash \varphi$.

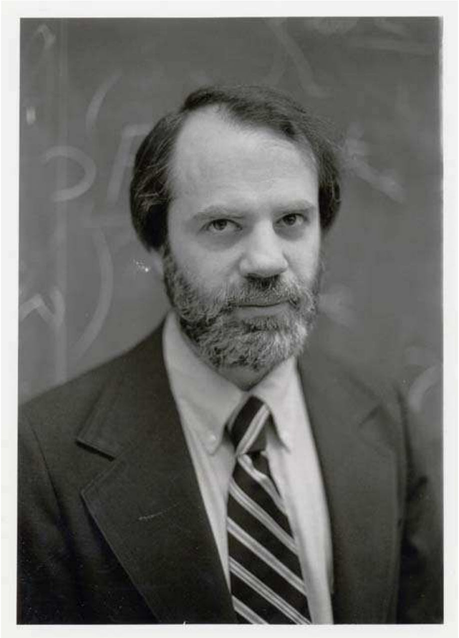
$(\mathbf{S4} = \{\mathbf{T}, \Box\Box\varphi \to \Box\varphi\})$

Possible Worlds.

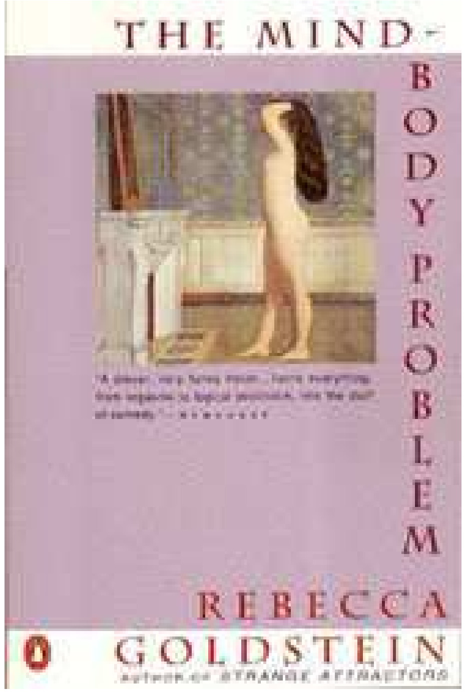
Leibniz: There are as many possible worlds as there are things that can be conceived without contradiction. φ is necessarily true if its negation implies a contradiction.

$\rightsquigarrow$ φ is necessarily true if it is true in all possible worlds.

Kripke.



Saul Kripke
(b. 1940)



- Saul **Kripke**, A completeness theorem in modal logic, **Journal of Symbolic Logic** 24 (1959), p. 1-14.
- “*Naming and Necessity*”.

Kripke semantics (1).

Let M be a set and $R \subseteq M \times M$ a binary relation. We call $\mathbf{M} = \langle M, R \rangle$ a Kripke frame. Let $V : \mathbb{N} \to \wp(M)$ be a valuation function. Then we call $\mathbf{M}^V = \langle M, R, V \rangle$ a Kripke model.

$$\begin{array}{rcl}
\mathbf{M}^V, x \models \mathrm{p}_n & \text{iff} & x \in V(n) \\
\mathbf{M}^V, x \models \Diamond\varphi & \text{iff} & \exists y(xRy \;\&\; \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V, x \models \Box\varphi & \text{iff} & \forall y(xRy \to \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V \models \varphi & \text{iff} & \forall x(\mathbf{M}^V, x \models \varphi) \\
\mathbf{M} \models \varphi & \text{iff} & \forall V(\mathbf{M}^V \models \varphi)
\end{array}$$

Kripke semantics (2).

$$\begin{array}{rcl}
\mathbf{M}^V, x \models \Diamond\varphi & \text{iff} & \exists y (xRy \ \& \ \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V, x \models \Box\varphi & \text{iff} & \forall y (xRy \rightarrow \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V \models \varphi & \text{iff} & \forall x (\mathbf{M}^V, x \models \varphi) \\
\mathbf{M} \models \varphi & \text{iff} & \forall V (\mathbf{M}^V \models \varphi)
\end{array}$$

- Let $\langle M, R \rangle$ be a reflexive frame, *i.e.*, for all $x \in M$, xRx.
  Then $\mathbf{M} \models \mathbf{T}$.
  ($\mathbf{T} = \Box\varphi \rightarrow \varphi$)
- Let $\langle M, R \rangle$ be a transitive frame, *i.e.*, for all $x, y, z \in M$, if xRy and yRz, then xRz.
  Then $\mathbf{M} \models \Box\Box\varphi \rightarrow \Box\varphi$.

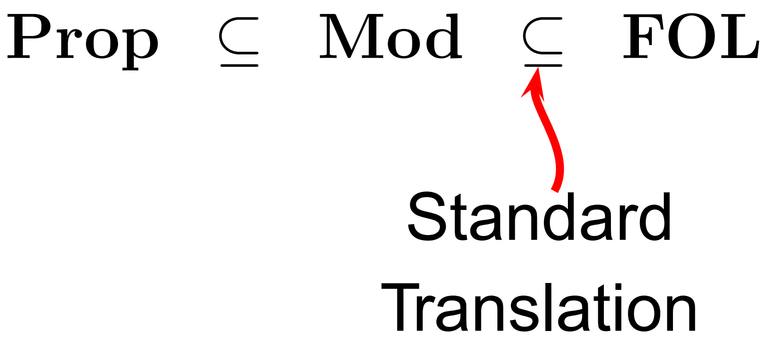
Kripke semantics (3).

Theorem (Kripke).

1. $\mathbf{T} \vdash \varphi$ if and only if for all reflexive frames $\mathbf{M}$, we have $\mathbf{M} \models \varphi$.
2. $\mathbf{S4} \vdash \varphi$ if and only if for all reflexive and transitive frames $\mathbf{M}$, we have $\mathbf{M} \models \varphi$.
3. $\mathbf{S5} \vdash \varphi$ if and only if for all frames $\mathbf{M}$ with an equivalence relation R, we have $\mathbf{M} \models \varphi$.

Modal Propositional Logic.

- **Propositional Logic:** $\mathbf{Prop}$. Propositional variables p_i, $\wedge$, $\vee$, $\neg$, $\rightarrow$.
- **Modal Logic.** $\mathbf{Prop}+\,\Box, \Diamond$.
- **First-order logic.** $\mathbf{Prop}+\,\forall, \exists$, function symbols $\dot{\mathrm{f}}$, relation symbols $\dot{\mathrm{R}}$.



$$\mathbf{Prop} \quad \subseteq \quad \mathbf{Mod} \quad \subseteq \quad \mathbf{FOL}$$

Standard Translation