Computability (1).

Turing Machine. A finitary programme T; given an input p, T either halts outputting q or loops.

A function $f : \mathbb{N} \to \mathbb{N}$ is Turing-computable if there is a Turing machine T such that for all x, we have

$$f(x) = y \leftrightarrow T(x) \downarrow y.$$

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.

Computability (2).

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)"

Computability (3).

computable	recursive
computably enumerable	recursively enumerable
Computability Theory	Recursion Theory

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

Oracle Machines.

- An oracle machine is a regular Turing machine with an extra tape on which it cannot write but only read.
- If $f : \mathbb{N} \to \mathbb{N}$ and T is an oracle machine, we say that T halts at input x with oracle f if the computation with f written on the extra tape halts. We write $T^f(x) \downarrow$.
- A function f is Turing-computable in g if for all x, we have

$$f(x) = y \leftrightarrow T^g(x) \downarrow y.$$

- **Theorem.** A function is Turing-computable in g if and only if it is in the smallest class containing projections, the successor function, and g closed under primitive recursion, substitution and μ-recursion.
- Let us write $\mathbf{C}_g$ for that class.

Relative Computability.

- We write $f \leq_{\mathrm{T}} g$ if and only if $\mathbf{C}_f \subseteq \mathbf{C}_g$.
- $\leq_{\mathrm{T}}$ is a partial preorder, *i.e.*, a transitive and reflexive relation.
- It is not antisymmetric: If f and g are computable, then $\mathbf{C}_f = \mathbf{C}_g$ is the class of computable sets.
- If f is computable, then $f \leq_{\mathrm{T}} K$ and $K \not\leq_{\mathrm{T}} f$.
- Define $f \equiv_{\mathrm{T}} g$ if and only if $f \leq_{\mathrm{T}} g$ and $g \leq_{\mathrm{T}} f$.
- $\mathcal{D} := \mathbb{N}^{\mathbb{N}}/\equiv_{\mathrm{T}}$ is a partial order called the Turing degrees.

Two questions.

- **Is $\mathcal{D}$ a linear order?**
  Are there f and g such that $f \not\leq_{\mathrm{T}} g$ and $g \not\leq_{\mathrm{T}} f$?

No!

- A set A is called computably enumerable (c.e.) if there is a Turing machine T such that

$$x \in A \leftrightarrow T(x) \downarrow .$$

- **Post's Problem**: Is there a non-computable c.e. A such that $\chi_A \not\equiv_{\mathrm{T}} K$.

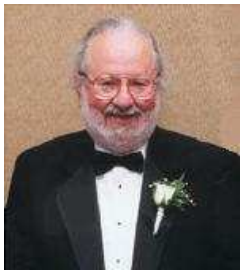
Yes! (Friedberg-Muchnik 1956/1957).

Church and his students.

Stephen Kleene

1909-1994

PhD 1934



Martin Davis

b. 1928

PhD 1950

Michael Rabin

b. 1931

PhD 1956

Dana Scott

b. 1932

PhD 1958

Raymond Smullyan

b. 1919

PhD 1959

Hilbert's Tenth Problem (1).

A diophantine equation is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = 0.$$

Hilbert's Tenth Problem. Is there an algorithm that determines given $\langle a_n, ..., a_0 \rangle$ as an input whether the Diophantine equation $a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = 0$ has an integer solution?

Answer (Davis-Putnam-Robinson-Matiyasevich; 1950-1970). **No!**

Hilbert's Tenth Problem (2).

Davis Robinson Matiyasevich Putnam

Effective Computation (1).

- Lance **Fortnow**, Steve **Homer**, A short history of computational complexity, **Bulletin of the European Association for Theoretical Computer Science** 80 (2003), p.95-133
- Juris **Hartmanis**, Observations About the Development of Theoretical Computer Science, **Annals of the History of Computing** 3 (1981), p. 42-51

Let $f : \mathbb{N} \to \mathbb{N}$ be any function and T a Turing machine. We say that T is time-bounded by f if for every input x, T halts in less than $f(x)$ steps.

Note. This is a **worst-case analysis**.

Effective Computation (2).

Let $f : \mathbb{N} \to \mathbb{N}$ be any function and T a Turing machine. We say that T is time-bounded by f if for every input x, T halts in less than $f(x)$ steps.

If $\mathcal{F}$ is a class of functions, we let $\mathbf{TIME}(\mathcal{F})$ be the class of sets decided by a machine time-bounded by some $f \in \mathcal{F}$.

Complexity Classes.

- "Linear Time Computation." $\mathbf{TIME}(\mathcal{L})$, where $\mathcal{L} := \{ax + b\,;\; a, b \in \mathbb{N}\}$.
- "Quadratic Time Computation." $\mathbf{TIME}(\mathcal{Q})$, where $\mathcal{Q} := \{ax^2 + bx + c\,;\; a, b, c \in \mathbb{N}\}$.
- "Polynomial Time Computation." $\mathbf{P} := \mathbf{TIME}(\mathcal{P})$, where $\mathcal{P}$ is the class of polynomials.

The search for the model of computation.

- Shannon's Information Theory (1938, 1948).
- Finite Automata. Kleene (1956), Shannon-McCarthy (1956).
- Martin Davis, "Computability & Unsolvability" (1958)
- Rabin-Scott, Nondeterministic computation (1959).

Nondeterministic Computation (1).

A nondeterministic Turing machine has finitely many options for actions in each given state. We say a nondeterministic machine T is time-bounded by f if for all possible computations, T halts in less than $f(x)$ steps at input x. We say a nondeterministic machine T accepts x if there is a computation that accepts x.

"branching nondeterminism"

Take a regular Turing machine T and say T is nondeterministically time-bounded by f if for all x and y, $T(x, y)$ halts in less than $f(y)$ steps. We say that T nondeterministically accepts y if there is some x such that T accepts $\langle x, y \rangle$.

"guess nondeterminism"

Nondeterministic computation (2).

Theorem. If A is a set of natural numbers, then the following are equivalent:

1. there is a Turing machine T (nondeterministically time-bounded by f) such that $x \in A$ if and only if T nondeterministically accepts x.
2. there is a nondeterministic Turing machine T (time-bounded by f) such that $x \in A$ if and only if T accepts x.

- **Context of Discovery.**
- **Context of Justification.**

Nondeterministic computation (3).

Compositeness. Given n, determine whether there is some $1 < k < n$ such that $k|n$.

The deterministic Turing machine that checks this for all k would need roughly $\frac{n}{2}!$ steps.

If k and n are given, then checking whether $k|n$ is very simple (linear in n). The nondeterministic Turing machine can check this simultaneously for all $k < n$.

Feasible Computation.

- **1963.** Juris Hartmanis, “On the computational complexity of algorithms”.
- **Blum Speed-up theorem.** There is a set A such that for each Turing machine T deciding A in time f, there is T^* deciding A in f^* wher $f^*(x) := \frac{f(x)}{n}$.
- Linear time is highly dependent of the model of computation.
- **Theorem** (Cobham; 1964). $\mathbf{P}$ is independent of the model of computation.
- *Consensus* (“effective Church-Turing thesis”): $\mathbf{P}$ is a formalization of “feasible computation”.
- **1965** (Edmonds). $\mathbf{NP}$ as a formalization for feasible checkability. $\mathbf{NP}$ is the class of sets that are decided by a nondeterministic polynomial-time Turing machine.

Satisfiability (1).

- **Church's Theorem.** There is no decision algorithm for predicate logic.
- Decision algorithm for propositional logic: Write truth-table.
- For a formula of length n with k propositional variables, this requires $2^k \cdot n$ steps.
- *Question.* Is there a polynomial algorithm for propositional logic (Gödel 1956)?

Conjunctive normal form. A literal is either a propositional variable or a negated propositional variable, an n-clause is a disjunction of n literals. A formula is in conjunctive normal form if it is a conjunction of clauses.

Satisfiability (2).

Conjunctive normal form. A literal is either a propositional variable or a negated propositional variable, an n-clause is a disjunction of n literals. A formula is in conjunctive normal form if it is a conjunction of clauses.

Theorem. Every propositional formula is equivalent to a formula in conjunctive normal form.

The set $\mathbf{SAT}$ is the set of all formulas in conjunctive normal form that are satisfiable, *i.e.*, there is an assignment of truth values to the propositional variables such that the formula is true.

n-$\mathbf{SAT}$ is $\mathbf{SAT}$ restricted to formulae containing only n-clauses. 2-$\mathbf{SAT}$ is solvable in polynomial time.

Rephrased question. $\mathbf{SAT} \in \mathbf{P}$?

Reduction functions.

We say that A is polynomially reducible to B if there is a total function $f : \mathbb{N} \to \mathbb{N}$ that is in $\mathbf{P}$ such that

$$x \in A \leftrightarrow f(x) \in B.$$

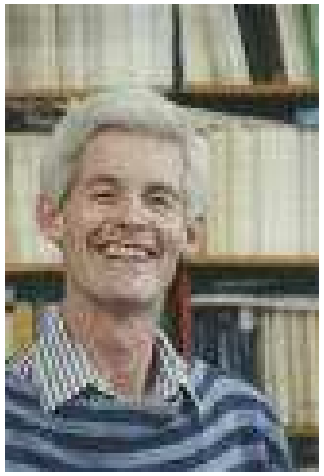
We write $A \leq_{\text{poly}} B$.

Note: If $A \leq_{\text{poly}} B$ and $B \in \mathbf{P}$, then $A \in \mathbf{P}$.

A set H is called $\mathbf{NP}$-hard if for all $A \in \mathbf{NP}$, we have $A \leq_{\text{poly}} B$. A set is called $\mathbf{NP}$-complete if it is $\mathbf{NP}$-hard and in $\mathbf{NP}$.

If there is an $\mathbf{NP}$-complete set that is in $\mathbf{P}$, then $\mathbf{P} = \mathbf{NP}$.

Cook's Theorem.



Stephen Cook (b. 1940)

Leonid Levin (b. 1948)

Theorem (Cook 1971, Levin 1973). $\mathbf{SAT}$ is $\mathbf{NP}$-complete.

Therefore: If there is a polynomial-time algorithm to solve the satisfiability problem, then $\mathbf{P} = \mathbf{NP}$.

Question (Cook, 1971). $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$.

Hilbert's Problems Once Again.

- **Hilbert's First Problem.** *The Continuum Hypothesis.* "What is the cardinality of the real numbers?"
- **Hilbert's Second Problem.** *Consistency of Arithmetic.* "Is there a finitistic proof of the consistency of the arithmetical axioms?"
- **Hilbert's Tenth Problem.** *Solvability of Diophantine Equations.* "Is there an algorithm that determines whether a given Diophantine equation has a solution or not?"

Back to Set Theory.

Standard axiomatization: ZF "Zermelo-Fraenkel Set Theory".

- **Question 1.** Does $\mathsf{ZF} \vdash \mathsf{AC}$?
- **Question 2.** What is the cardinality of the real numbers?

Cardinals & Ordinals (1).

- **Question 1.** Does ZF $\vdash$ AC?
- **Question 2.** What is the cardinality of the real numbers?

Cardinality. Two sets A and B are called equinumerous if there is a bijection $\pi : A \to B$. Equinumerosity is an equivalence relation. The cardinality of A is its equinumerosity equivalence class.

Ordinals. If $\mathbf{L}$ and $\mathbf{L}^*$ are wellorders (linear orders without descending chains), then either $\mathbf{L}$ is orderisomorphic to an initial segment of $\mathbf{L}^*$ or vice versa. The class of wellorders is wellordered by

$\mathbf{L} \preccurlyeq \mathbf{L}^* \leftrightarrow$ $\mathbf{L}$ is orderisomorphic to an initial segment of $\mathbf{L}^*$.

Ordinals are the equivalence classes of orderisomorphism.

Cardinals & Ordinals (2).

Cardinality. The cardinality of A is its equinumerosity equivalence class.

Ordinals. Ordinals are the equivalence classes of orderisomorphism.

$$\mathrm{Ord} = \{0, 1, 2, 3, ..., \infty = \omega, \omega + 1, \omega + 2, ..., \omega \cdot 2, ...\}.$$

Zermelo's Wellordering Theorem says: AC implies that every cardinality contains a wellorderable set.

Since $\preccurlyeq$ is a wellorder, there is a least ordinal α that is not equinumerous to the natural numbers. We call it ω_1. AC gives us a wellorder $\sqsubseteq$ of the real numbers. We know by Cantor that

$$\omega_1 \preccurlyeq \langle \mathbb{R}, \sqsubseteq \rangle$$

There is a least ordinal $\mathfrak{c} = 2^{\aleph_0}$ such that $\mathbb{R}$ and $\mathfrak{c}$ are equinumerous. Again, $\omega_1 \leq \mathfrak{c}$.

The Continuum Hypothesis (1).

CH. $\omega_1 = \mathfrak{c}$. The least ordinal that is not equinumerous to the natural numbers is the least ordinal that is equinumerous to the real numbers.

Equivalently, if $A \subseteq \mathbb{R}$ is a set of real numbers, then A is either finite or countable, or there is a bijection between A and $\mathbb{R}$.

Sketch. Suppose $\omega_1 < \mathfrak{c}$. Let $\sqsubseteq$ be a wellorder of $\mathbb{R}$ such that $\langle \mathbb{R}, \sqsubset \rangle$ and $\mathfrak{c}$ are orderisomorphic. Let $\pi : \mathbb{R} \to \mathfrak{c}$ be the orderisomorphism.
Since $\omega_1 < \mathfrak{c}$, there is a proper initial segment I of $\mathfrak{c}$ that is orderisomorphic to ω_1. Look at $\pi^{-1}[I] \subseteq \mathbb{R}$. This is a set of reals equinumerous to ω_1, so it cannot be fi nite or countable. But since $\omega_1 < \mathfrak{c}$, it cannot be equinumerous to $\mathbb{R}$. q.e.d.

The Continuum Hypothesis (2).

Hilbert (1900). *"Es erhebt sich nun die Frage, ob das Continuum auch als wohlgeordnete Menge aufgefaßt werden kann, was Cantor bejahen zu müssen glaubt."*

In other words: CH implies "there is a wellordering of the real numbers".

- **Question 1.** Does $\mathsf{ZF} \vdash \mathsf{AC}$?
- **Question 2.** Does $\mathsf{ZF} \vdash \mathsf{CH}$?
- **Question 2*.** Does $\mathsf{ZFC} \vdash \mathsf{CH}$?

All of these questions were wide open in 1930.

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 defi ned by formulae: Let X be given, then $A \subseteq X$ is defi ned over X if there is a formula φ and fi nitely many parameters $p_0, ..., p_n \in X$ such that

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

Let $\mathrm{Def}(X) := \{A \subseteq X\,;\ A$ is defi ned 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 $\mathsf{ZFC} + \mathsf{CH}$ is consistent.

Consequences.

- **Question 1**, **Question 2** and **Question 2*** cannot have a negative answer.
- The system $\mathsf{ZFC} + \mathsf{CH}$ cannot be logically stronger than ZF, *i.e.*, $\mathsf{ZFC} + \mathsf{CH} \nvdash \mathrm{Cons}(\mathsf{ZF})$.
- $\mathbf{L}$ is tremendously important for the investigation of logical strength. It turns out that if there is a measurable cardinal, then $\mathbf{L} \models$ "there are inaccessible but no measurable cardinals" (Scott; next time).
- $\mathbf{L}$ is a minimal model of set theory.

Gödel's Constructible Universe (3).

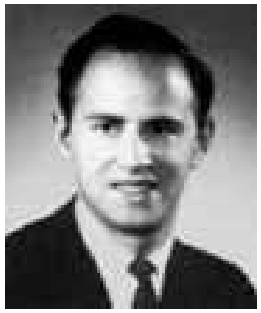
A new axiom? $\mathbf{V}=\mathbf{L}$. "The set-theoretic universe is minimal".

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.

Solovay.

Robert Solovay

- **1962**. Correspondence with Mycielski about the Axiom of Determinacy.
- **1963**. Development of Forcing as a method.
- **1963**. Solves the measure problem: it is consistent with ZF that all sets are Lebesgue measurable.
- **1964**. PhD University of Chicago (advisor: Saunders Mac Lane).
- **1975**. Baker-Gill-Solovay: There are oracles p and q such that $\mathbf{P}^p = \mathbf{NP}^p$ and $\mathbf{P}^q \neq \mathbf{NP}^q$.
- **1976**. Solovay-Woodin: Solution of the Kaplansky problem in the theory of Banach algebras.
- **1977**. Solovay-Strassen algorithm for primality testing.