Nondeterministic Space Complexity Classes

- Let L be a language.
- Then
$$L \in \text{NSPACE}(f(n))$$
if there is an NTM with input and output that decides L and operates within space bound $f(n)$.
- NSPACE$(f(n))$ is a set of languages.
- As in the linear speedup theorem (Theorem 3 on p. 76), constant coefficients do not matter.

Graph Reachability

- Let $G(V, E)$ be a directed graph (**digraph**).
- REACHABILITY asks if, given nodes a and b, does G contain a path from a to b?
- Can be easily solved in polynomial time by breadth-first search.
- How about its nondeterministic space complexity?

The First Try: NSPACE$(n \log n)$

Determine the number of nodes m; {Note $m \leq n$.}
$x_1 := a$; {Assume $a \neq b$.}
for $i = 2, 3, \ldots, m$ **do**
    Guess $x_i \in \{v_1, v_2, \ldots, v_m\}$; {The ith node.}
end for
for $i = 2, 3, \ldots, m$ **do**
    if $(x_{i-1}, x_i) \notin E$ **then**
        "no";
    end if
    if $x_i = b$ **then**
        "yes";
    end if
end for
"no";

In Fact, REACHABILITY $\in$ NSPACE$(\log n)$

Determine the number of nodes m; {Note $m \leq n$.}
$x := a$;
for $i = 2, 3, \ldots, m$ **do**
    Guess $y \in \{v_1, v_2, \ldots, v_m\}$; {The next node.}
    if $(x, y) \notin E$ **then**
        "no";
    end if
    if $y = b$ **then**
        "yes";
    end if
    $x := y$;
end for
"no";

Space Analysis

- Variables m, i, x, and y each require $O(\log n)$ bits.
- Testing $(x, y) \in E$ is accomplished by consulting the input string with counters of $O(\log n)$ bits long.
- Hence
$$\text{REACHABILITY} \in \text{NSPACE}(\log n).$$
  - REACHABILITY with more than one terminal node also has the same complexity.
- REACHABILITY $\in$ P (p. 214).

Undecidability

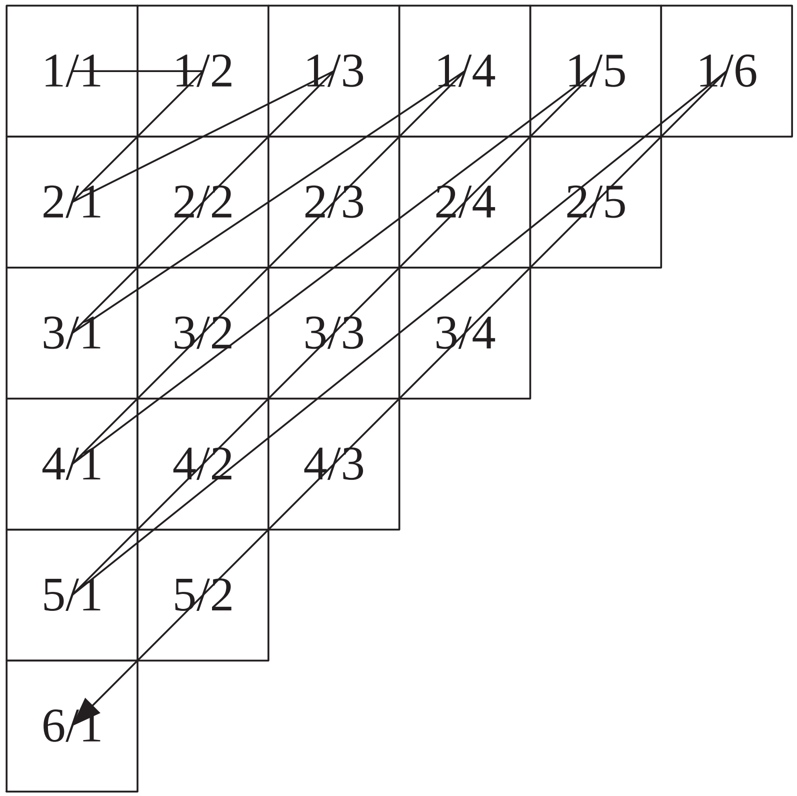
God exists since mathematics is consistent,
and the Devil exists since we cannot prove it.
— André Weil (1906–1998)

Whatsoever we imagine is *finite*.
Therefore there is no idea, or conception
of any thing we call *infinite*.
— Thomas Hobbes (1588–1679), *Leviathan*

Infinite Sets

- A set is **countable** if it is finite or if it can be put in one-one correspondence with $\mathbb{N} = \{ 0, 1, \ldots \}$, the set of natural numbers.
  - Set of integers $\mathbb{Z}$.
    * $0 \leftrightarrow 0$.
    * $1 \leftrightarrow 1, 2 \leftrightarrow 3, 3 \leftrightarrow 5, \ldots$.
    * $-1 \leftrightarrow 2, -2 \leftrightarrow 4, -3 \leftrightarrow 6, \ldots$.
  - Set of positive integers $\mathbb{Z}^+$: $i \leftrightarrow i - 1$.
  - Set of positive odd integers: $i \leftrightarrow (i-1)/2$.
  - Set of (positive) rational numbers: See next page.
  - Set of squared integers: $i \leftrightarrow \sqrt{i}\,$.

Rational Numbers Are Countable



Cardinality

- For any set A, define $|A|$ as A's **cardinality** (size).
- Two sets are said to have the same cardinality, or

$$|A| = |B| \quad \text{or} \quad A \sim B,$$

  if there exists a one-to-one correspondence between their elements.
- 2^A denotes set A's **power set**, that is $\{B : B \subseteq A\}$.
  - E.g., $\{0, 1\}$'s power set is $2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
- If $|A| = k$, then $|2^A| = 2^k$.

Cardinality (concluded)

- Define $|A| \leq |B|$ if there is a one-to-one correspondence between A and a subset of B's.
- Obviously, if $A \subseteq B$, then $|A| \leq |B|$.
  - So $|\,\mathbb{N}\,| \leq |\,\mathbb{Z}\,|$.
  - So $|\,\mathbb{N}\,| \leq |\,\mathbb{R}\,|$.
- Define $|A| < |B|$ if $|A| \leq |B|$ but $|A| \neq |B|$.
- If $A \subsetneq B$, then $|A| < |B|$?

Cardinality and Infinite Sets

- If A and B are infinite sets, it is possible that $A \subsetneq B$ yet $|A| = |B|$.
  - The set of integers *properly* contains the set of odd integers.
  - But the set of integers has the same cardinality as the set of odd integers (p. 114).[a]
- A lot of "paradoxes."

[a] Leibniz uses it to "prove" that there are no infinite numbers (Russell, 1914).

Galileo's[a] Paradox (1638)

- The squares of the positive integers can be placed in one-to-one correspondence with all the positive integers.
- This is contrary to the axiom of Euclid[b] that the whole is greater than any of its proper parts.[c]
- Resolution of paradoxes: Pick the notion that results in "better" mathematics.
- The difference between a mathematical paradox and a contradiction is often a matter of opinions.

---

[a] Galileo (1564–1642).

[b] Euclid (325 B.C.–265 B.C.).

[c] Leibniz never challenges that axiom (Knobloch, 1999).

Hilbert's[a] Paradox of the Grand Hotel

- For a hotel with a finite number of rooms with all the rooms occupied, a new guest will be turned away.
- Now imagine a hotel with an infinite number of rooms, all of which are occupied.
- A new guest comes and asks for a room.
- "But of course!" exclaims the proprietor.
- He moves the person previously occupying Room 1 to Room 2, the person from Room 2 to Room 3, and so on.
- The new customer now occupies Room 1.

---

[a] David Hilbert (1862–1943).

Hilbert's Paradox of the Grand Hotel (concluded)

- Now imagine a hotel with an infinite number of rooms, all taken up.
- An infinite number of new guests come in and ask for rooms.
- "Certainly," says the proprietor.
- He moves the occupant of Room 1 to Room 2, the occupant of Room 2 to Room 4, and so on.
- Now all odd-numbered rooms become free and the infinity of new guests can be accommodated in them.
- "There are many rooms in my Father's house, and I am going to prepare a place for you." (*John* 14:3)

David Hilbert (1862–1943)

The point of philosophy is
to start with something so simple
as not to seem worth stating,
and to end with something
so paradoxical that no one will believe it.
— Bertrand Russell (1872–1970)

Cantor's Theorem

Theorem 6 *The set of all subsets of* $\mathbb{N}$ $(2^{\mathbb{N}})$ *is infinite and not countable.*

- Suppose $(2^{\mathbb{N}})$ is countable with $f : \mathbb{N} \to 2^{\mathbb{N}}$ being a bijection.[a]
- Consider the set $B = \{k \in \mathbb{N} : k \notin f(k)\} \subseteq \mathbb{N}$.
- Suppose $B = f(n)$ for some $n \in \mathbb{N}$.

---

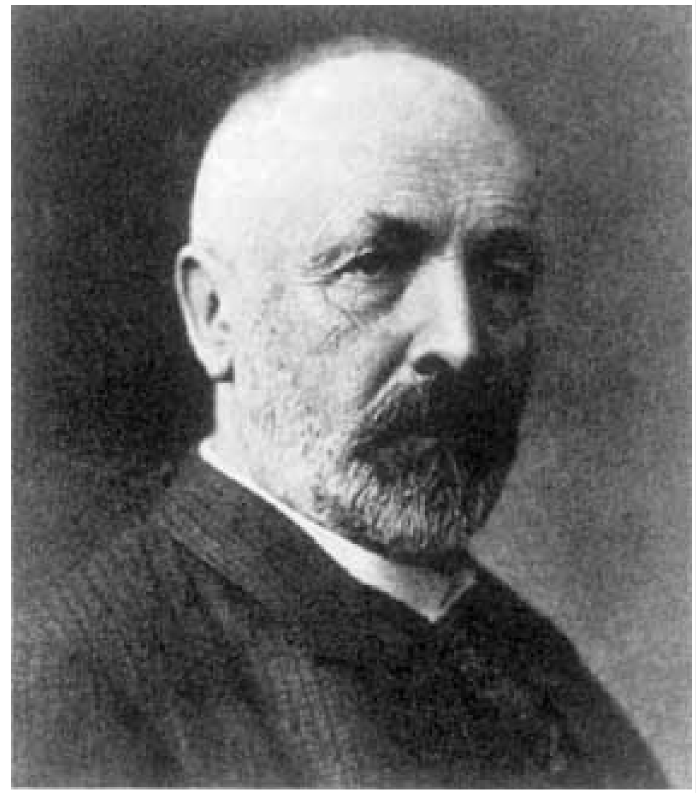
[a] Note that $f(k)$ is a subset of $\mathbb{N}$.

The Proof (concluded)

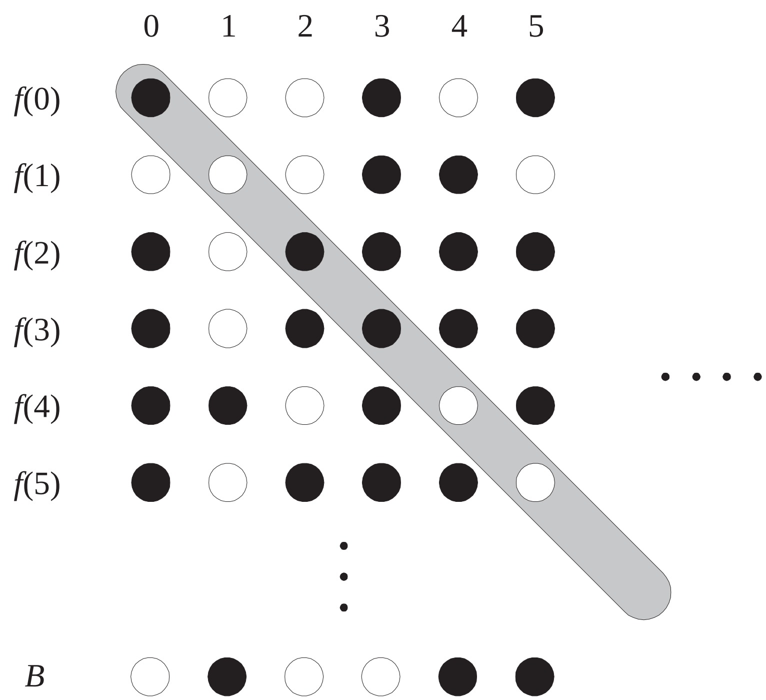
- If $n \in f(n) = B$, then $n \in B$, but then $n \notin B$ by B's definition.
- If $n \notin f(n) = B$, then $n \notin B$, but then $n \in B$ by B's definition.
- Hence $B \neq f(n)$ for any n.
- f is not a bijection, a contradiction.

Georg Cantor (1845–1918)

Kac and Ulam (1968), "[If] one had to name a single person whose work has had the most decisive influence on the present spirit of mathematics, it would almost surely be Georg Cantor."



Cantor's Diagonalization Argument Illustrated



A Corollary of Cantor's Theorem

Corollary 7 *For any set T, finite or infinite,*

$$|\,T\,| < |\,2^T\,|.$$

- The inequality holds in the finite T case as $k < 2^k$.
- Assume T is infinite now.
- To prove $|\,T\,| \leq |2^T|$, simply consider $f(x) = \{x\} \in 2^T$.
  - f maps a member of $T = \{\,a, b, c, \ldots\,\}$ to the corresponding member of $\{\,\{\,a\,\}, \{\,b\,\}, \{\,c\,\}, \ldots\,\} \subseteq 2^T$.
- To prove the strict inequality $|\,T\,| \lneq |2^T|$, we use the same argument as Cantor's theorem.

A Second Corollary of Cantor's Theorem

Corollary 8 *The set of all functions on* $\mathbb{N}$ *is not countable.*

- It suffices to prove it for functions from $\mathbb{N}$ to $\{0, 1\}$.
- Every function $f : \mathbb{N} \to \{0, 1\}$ determines a subset of $\mathbb{N}$:

$$\{n : f(n) = 1\} \subseteq \mathbb{N},$$

  and vice versa.
- So the set of functions from $\mathbb{N}$ to $\{0, 1\}$ has cardinality $|\, 2^{\mathbb{N}} \,|$.
- Cantor's theorem (p. 124) then implies the claim.

Existence of Uncomputable Problems

- Every program is a finite sequence of 0s and 1s, thus a nonnegative integer.[a]
- Hence every program corresponds to some integer.
- The set of programs is countable.

[a]Different binary strings may be mapped to the same integer (e.g., "001" and "01"). To prevent it, use the lexicographic order as the mapping or simply insert "1" as the most significant bit of the binary string before the mapping (so "001" becomes "1001"). Contributed by Mr. Yu-Chih Tung (R98922167) on October 5, 2010.

Existence of Uncomputable Problems (concluded)

- A function is a mapping from integers to integers.
- The set of functions is not countable by Corollary 8 (p. 129).
- So there are functions for which no programs exist.[a]

---

[a]As a nondeterministic program may not compute a function, we consider only deterministic programs for this sentence. Contributed by Mr. Patrick Will (`A99725101`) on October 5, 2010.

Universal Turing Machine[a]

- A **universal Turing machine** U interprets the input as the *description* of a TM M concatenated with the *description* of an input to that machine, x.
  - Both M and x are over the alphabet of U.
- U simulates M on x so that

$$U(M; x) = M(x).$$

- U is like a modern computer, which executes any valid machine code, or a Java Virtual machine, which executes any valid bytecode.

[a] Turing (1936).

The Halting Problem

- **Undecidable problems** are problems that have no algorithms.
- Equivalently, they are languages that are not recursive.
- We knew undecidable problems exist (p. 130).
- We now define a concrete undecidable problem, the **halting problem**:

$$H = \{M; x : M(x) \neq \nearrow\}.$$

  – Does M halt on input x?

H Is Recursively Enumerable

- Use the universal TM U to simulate M on x.
- When M is about to halt, U enters a "yes" state.
- If $M(x)$ diverges, so does U.
- This TM accepts H.

H Is Not Recursive[a]

- Suppose H is recursive.
- Then there is a TM M_H that *decides* H.
- Consider the program $D(M)$ that calls M_H:

```
if M_H(M; M) = "yes" then
    ↗; {Writing an infinite loop is easy.}
else
    "yes";
end if
```

[a] Turing (1936).

H Is Not Recursive (concluded)

- Consider $D(D)$:
  - $D(D) = \nearrow \Rightarrow M_H(D; D) =$ "yes" $\Rightarrow D; D \in H \Rightarrow D(D) \neq \nearrow$, a contradiction.
  - $D(D) =$ "yes" $\Rightarrow M_H(D; D) =$ "no" $\Rightarrow D; D \notin H \Rightarrow D(D) = \nearrow$, a contradiction.

Comments

- Two levels of interpretations of M:
  - A sequence of 0s and 1s (data).
  - An encoding of instructions (programs).
- There are no paradoxes with $D(D)$.
  - Concepts should be familiar to computer scientists.
  - Feed a C compiler to a C compiler, a Lisp interpreter to a Lisp interpreter, a sorting program to a sorting program, etc.

Cantor's Paradox (1899[a])

- Let T be the set of all sets.[b]
- Then $2^T \subseteq T$ because 2^T is a set.
- But we know[c] $|\,2^T\,| > |\,T\,|$ (p. 128)!
- We got a "contradiction."
- Are we willing to give up Cantor's theorem?
- If not, what is a set?

---

[a] In a letter to Richard Dedekind. First published in Russell (1903).

[b] Recall this ontological argument for the existence of God by St Anselm (1033–1109) in the 11th century: If something is possible but is not part of God, then God is not the greatest possible object of thought, a contradiction.

[c] Really?

Self-Loop Paradoxes[a]

Russell's Paradox (1901): Consider $R = \{A : A \notin A\}$.

- If $R \in R$, then $R \notin R$ by definition.
- If $R \notin R$, then $R \in R$ also by definition.
- In either case, we have a "contradiction."[b]

Eubulides: The Cretan says, "All Cretans are liars."

Liar's Paradox: "This sentence is false."

Hypochondriac: a patient (like Gödel) with imaginary symptoms and ailments.

---

[a] E.g., Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid* (1979) or Quine, *The Ways of Paradox and Other Essays* (1966).

[b] Gottlob Frege (1848–1925) to Bertrand Russell in 1902, "Your discovery of the contradiction $[\cdots]$ has shaken the basis on which I intended to build arithmetic."

Self-Loop Paradoxes (continued)

Sharon Stone in *The Specialist* (1994): "I'm not a woman you can trust."

***Spin City* (1996–2002):** "I am not gay, but my boyfriend is."

***Numbers* 12:3, Old Testament:** "Moses was the most humble person in all the world [$\cdots$]" (attributed to Moses).

Self-Loop Paradoxes (concluded)

***The Egyptian Book of the Dead*:** "ye live in me and I would live in you."

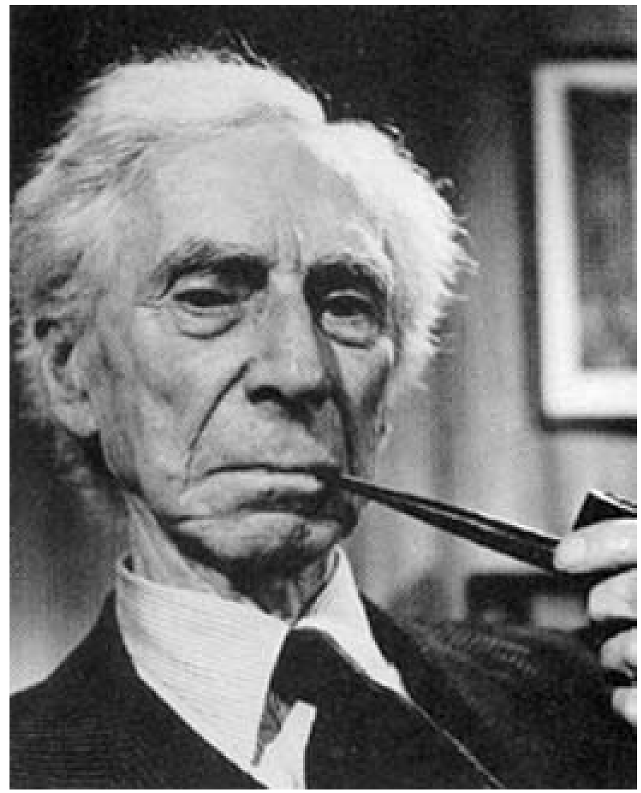
***John* 17:21, New Testament:** "just as you are in me and I am in you."

***Pagan & Christian Creeds* (1920):** "I was moved to Odin, myself to myself."

Soren Kierkegaard in *Fear and Trembling* (1843): "to strive against the whole world is a comfort, to strive with oneself is dreadful."

Bertrand Russell (1872–1970)

Karl Popper (1974), "perhaps the greatest philosopher since Kant."



Reductions in Proving Undecidability

- Suppose we are asked to prove that L is undecidable.
- Suppose L' (such as H) is known to be undecidable.
- Find a computable transformation R (called **reduction**) from L' to L such that[a]

$$\forall x \, \{x \in L' \text{ if and only if } R(x) \in L\}.$$

- Now we can answer "$x \in L'$?" for *any* x by asking "$R(x) \in L$?" because they have the same answer.
  - L' is said to be **reduced** to L.

[a] Contributed by Mr. Tai-Dai Chou (`J93922005`) on May 19, 2005.

Reductions in Proving Undecidability (concluded)

- If L were decidable, "$R(x) \in L$?" becomes computable and we have an algorithm to decide L', a contradiction!
- So L must be undecidable.

Theorem 9 *Suppose language L_1 can be reduced to language L_2. If L_1 is not recursive, then L_2 is not recursive.*

More Undecidability

- $H^* = \{M : M \text{ halts on all inputs}\}$.
  - We will reduce H to H^*.
  - Given the question "$M; x \in H$?", construct the following machine (this is the reduction):[a]

$$M_x(y)\ \{M(x);\}$$

  - M halts on x if and only if M_x halts on all inputs.
  - In other words, $M; x \in H$ if and only if $M_x \in H^*$.
  - So if H^* were recursive, H would be recursive, a contradiction.

---

[a] Simplified by Mr. Chih-Hung Hsieh (D95922003) on October 5, 2006. M_x ignores its input y; x is part of M_x's code but not M_x's input.

More Undecidability (concluded)

- $\{M; x : \text{there is a } y \text{ such that } M(x) = y\}$.
- $\{M; x : \text{the computation } M \text{ on input } x \text{ uses all states of } M\}$.
- $\{M; x; y : M(x) = y\}$.

Complements of Recursive Languages

The **complement** of L, denoted by $\bar{L}$, is the language $\Sigma^* - L$.

Lemma 10 *If L is recursive, then so is $\bar{L}$.*

- Let L be decided by M, which is deterministic.
- Swap the "yes" state and the "no" state of M.
- The new machine decides $\bar{L}$.

Recursive and Recursively Enumerable Languages

Lemma 11 (Kleene's theorem) *L is recursive if and only if both L and $\bar{L}$ are recursively enumerable.*

- Suppose both L and $\bar{L}$ are recursively enumerable, accepted by M and $\bar{M}$, respectively.
- Simulate M and $\bar{M}$ in an *interleaved* fashion.
- If M accepts, then halt on state "yes" because $x \in L$.
- If $\bar{M}$ accepts, then halt on state "no" because $x \notin L$.
- Note that either M or $\bar{M}$ (but not both) must accept the input.

A Very Useful Corollary and Its Consequences

Corollary 12 *L is recursively enumerable but not recursive, then $\bar{L}$ is not recursively enumerable.*

- Suppose $\bar{L}$ is recursively enumerable.
- Then both L and $\bar{L}$ are recursively enumerable.
- By Lemma 11 (p. 148), L is recursive, a contradiction.

Corollary 13 *$\bar{H}$ is not recursively enumerable.*[a]

---

[a]Recall that $\bar{H} = \{M; x : M(x) = \nearrow\}$.

R, RE, and coRE

RE: The set of all recursively enumerable languages.

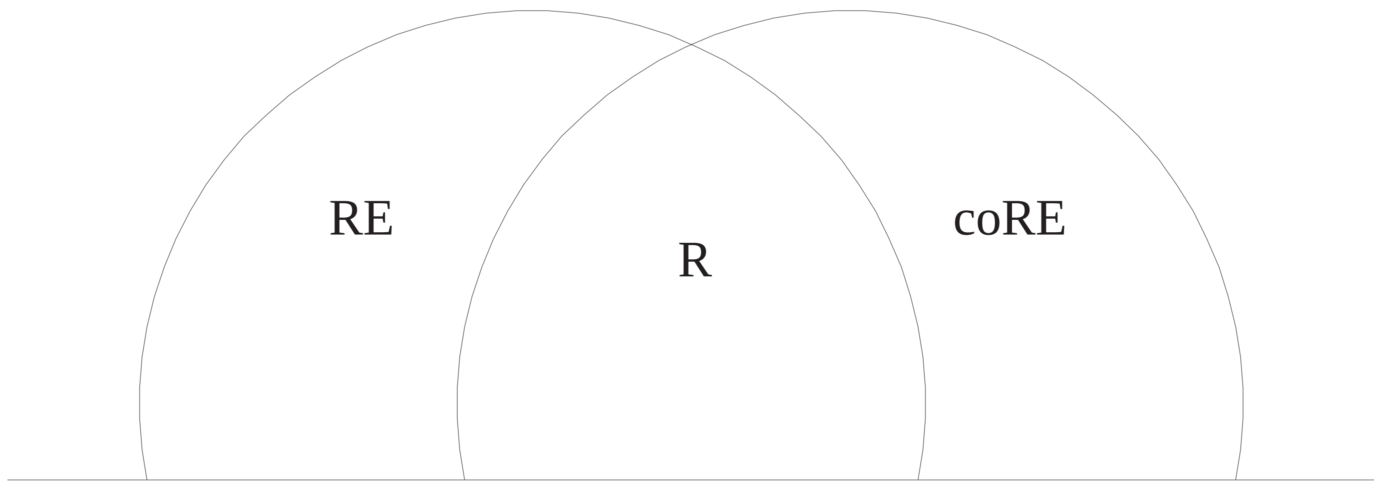
coRE: The set of all languages whose complements are recursively enumerable.

R: The set of all recursive languages.

- Note that coRE is not $\overline{\text{RE}}$.
  - $\text{coRE} = \{ L : \overline{L} \in \text{RE} \}$.
  - $\overline{\text{RE}} = \{ L : L \notin \text{RE} \}$.

R, RE, and coRE (concluded)

- R = RE $\cap$ coRE (p. 148).
- There exist languages in RE but not in R and not in coRE.
  - Such as H (p. 134, p. 135, and p. 149).
- There are languages in coRE but not in RE.
  - Such as $\bar{H}$ (p. 149).
- There are languages in neither RE nor coRE.


RE
R
coRE

Undecidability in Logic and Mathematics

- First-order logic is undecidable (answer to Hilbert's "*Entscheidungsproblem*" (1928)).[a]
- Natural numbers with addition and multiplication is undecidable.[b]
- Rational numbers with addition and multiplication is undecidable.[c]

---

[a] Church (1936).
[b] Rosser (1937).
[c] Robinson (1948).

Undecidability in Logic and Mathematics (concluded)

- Natural numbers with addition and equality is decidable and complete.[a]
- Elementary theory of groups is undecidable.[b]

---

[a] Presburger's Master's thesis (1928), his only work in logic. The direction was suggested by Tarski. Mojžesz Presburger (1904–1943) died in a concentration camp during World War II.

[b] Tarski (1949).

Julia Hall Bowman Robinson (1919–1985)

Alfred Tarski (1901–1983)