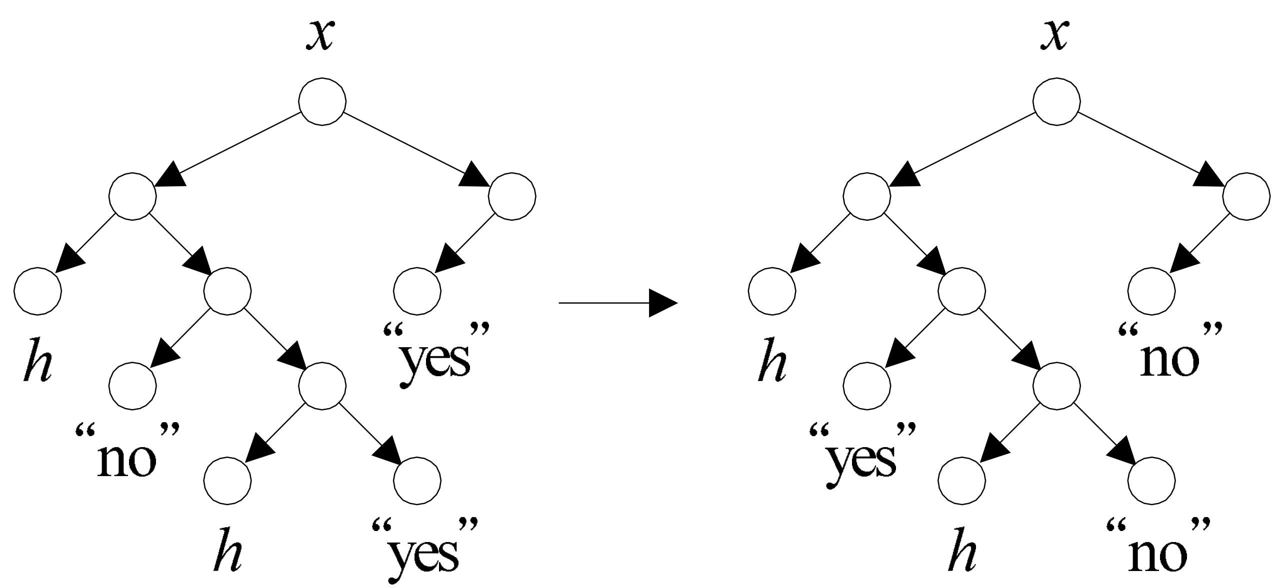
Complementing a TM's Halting States

- Let M decide L, and M' be M after "yes" $\leftrightarrow$ "no".
- If M is a deterministic TM, then M' decides $\bar{L}$.
- But if M is an NTM, then M' may not decide $\bar{L}$.
  - It is possible that both M and M' accept x (see next page).
  - When this happens, M and M' accept languages that are not complements of each other.


x
h
"no"
h
"yes"
"yes"
x
h
"yes"
h
"no"
"no"

Time Complexity under Nondeterminism

- Nondeterministic machine N decides L **in time** $f(n)$, where $f : \mathbb{N} \to \mathbb{N}$, if
  - N decides L, and
  - for any $x \in \Sigma^*$, N does not have a computation path longer than $f(|\,x\,|)$.
- We charge only the "depth" of the computation tree.

Time Complexity Classes under Nondeterminism

- NTIME($f(n)$) is the set of languages decided by NTMs within time $f(n)$.
- NTIME($f(n)$) is a complexity class.

NP

- Define
$$\text{NP} = \bigcup_{k>0} \text{NTIME}(n^k).$$
- Clearly $\text{P} \subseteq \text{NP}$.
- Think of NP as efficiently *verifiable* problems.
  - Boolean satisfiability (p. 90 and p. 153).
- The most important open problem in computer science is whether $\text{P} = \text{NP}$.

Simulating Nondeterministic TMs

Surprisingly, nondeterminism does not add power to TMs.

Theorem 4 *Suppose language L is decided by an NTM N in time $f(n)$. Then it is decided by a 3-string deterministic TM M in time $O(c^{f(n)})$, where $c > 1$ is some constant depending on N.*

- On input x, M goes down every computation path of N using depth-first search.[a]
  - M does *not* need to know $f(n)$.
  - As N is time-bounded, the depth-first search will not run indefinitely.

[a] You may have to switch to breadth-first search if $f(n)$ can be infinite.

The Proof (concluded)

- If some path leads to "yes," then M enters the "yes" state.
- If none of the paths leads to "yes," then M enters the "no" state.
- Note that every path has a finite length by definition.

Corollary 5 $\text{NTIME}(f(n))) \subseteq \bigcup_{c>1} \text{TIME}(c^{f(n)})$.

NTIME vs. TIME

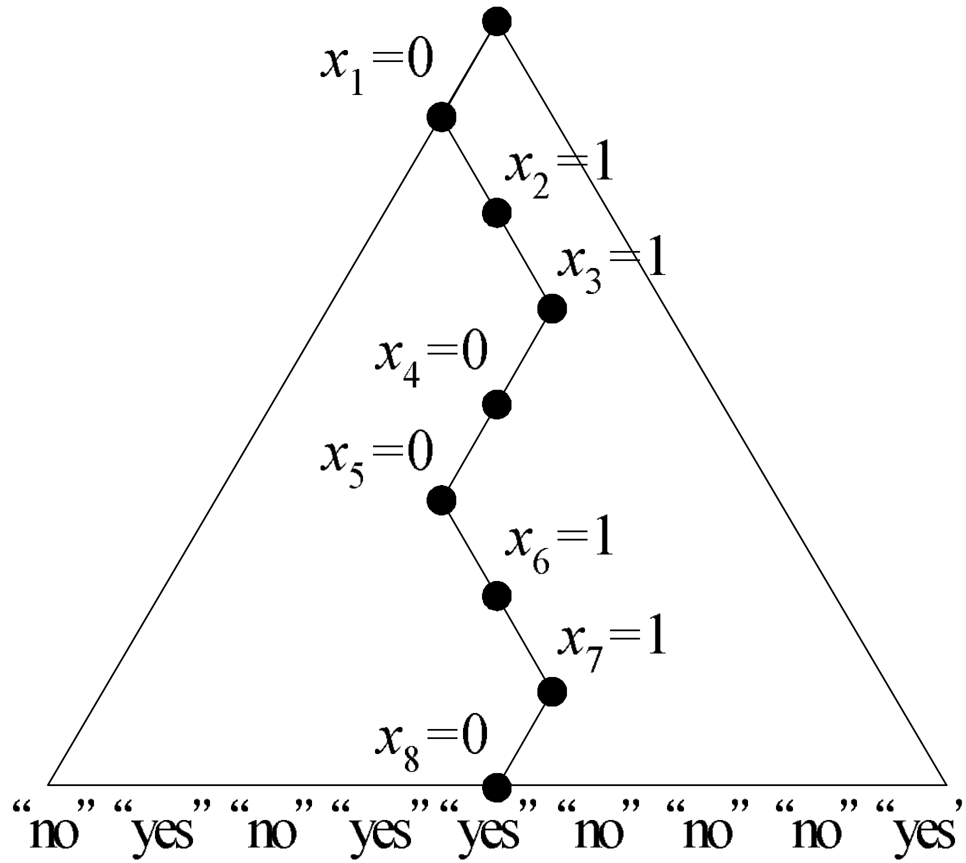
- Does converting an NTM into a TM require exploring all of the computation paths of the NTM as done in Theorem 4 (p. 87)?
- This is the most important question in theory with practical implications.

A Nondeterministic Algorithm for Satisfiability

ϕ is a boolean formula with n variables.

```
for i = 1, 2, ..., n do
    Guess x_i ∈ {0, 1}; {Nondeterministic choice.}
end for
{Verification:}
if φ(x_1, x_2, ..., x_n) = 1 then
    "yes";
else
    "no";
end if
```

The Schematic Computation Tree for Satisfiability



Analysis

- The algorithm decides language $\{\phi : \phi \text{ is satisfiable}\}$.
  - The computation tree is a complete binary tree of depth n.
  - Every computation path corresponds to a particular truth assignment out of 2^n.
  - ϕ is satisfiable iff there is a truth assignment that satisfies ϕ.
  - But there is a truth assignment that satisfies ϕ iff there is a computation path that results in "yes."
- General paradigm: Guess a "proof" and then verify it.

The Traveling Salesman Problem

- We are given n cities $1, 2, \ldots, n$ and integer distances d_{ij} between any two cities i and j.
- Assume $d_{ij} = d_{ji}$ for convenience.
- The **traveling salesman problem** (TSP) asks for the total distance of the shortest tour of the cities.
- The decision version TSP (D) asks if there is a tour with a total distance at most B, where B is an input.
- Both problems are extremely important but equally hard (p. 348 and p. 442).

A Nondeterministic Algorithm for TSP (D)

for $i = 1, 2, \ldots, n$ **do**

  Guess $x_i \in \{1, 2, \ldots, n\}$; {The ith city.}[a]

end for

$x_{n+1} := x_1$;

{Verification stage:}

if $x_1, x_2, \ldots, x_n$ are distinct and $\sum_{i=1}^{n} d_{x_i, x_{i+1}} \leq B$ **then**

  "yes";

else

  "no";

end if

---

[a] Can be made into a series of $\log_2 n$ *binary* choices for each x_i so that the next-state count (2) is a constant, independent of input size. Contributed by Mr. Chih-Duo Hong (R95922079) on September 27, 2006.

Analysis

- Suppose the input graph contains at least one tour of the cities with a total distance at most B.
- Then there is a computation path that leads to "yes."[a]
- Suppose the input graph contains no tour of the cities with a total distance at most B.
- Then every computation path leads to "no."

[a] It does not mean the algorithm will follow that path. It just means such a computation path exists.

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. 67), 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 the nondeterministic space complexity?

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

$x_1 := a$; {Assume $a \neq b$.}
for $i = 2, 3, \ldots, n$ **do**
  Guess $x_i \in \{v_1, v_2, \ldots, v_n\}$; {The ith node.}
end for
for $i = 2, 3, \ldots, n$ **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$(\log n)$

```
x := a;
for i = 2, 3, ..., n do
    Guess y ∈ {v_1, v_2, ..., v_n}; {The next node.}
    if (x, y) ∉ E then
        "no";
    end if
    if y = b then
        "yes";
    end if
    x := y;
end for
"no";
```

Space Analysis

- Variables 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
$$\textsc{reachability} \in \text{NSPACE}(\log n).$$
  - REACHABILITY with more than one terminal node also has the same complexity.
- REACHABILITY $\in$ P (p. 193).

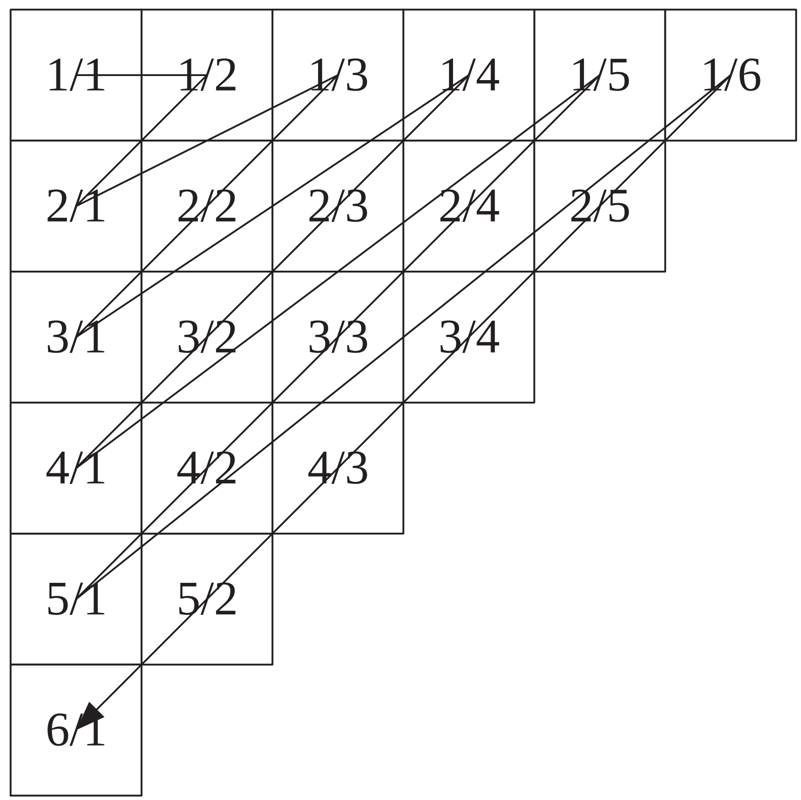
Undecidability

It seemed unworthy of a grown man
to spend his time on such trivialities,
but what was I to do?
— Bertrand Russell (1872–1970),
Autobiography, Vol. I

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 $\mathbb{Z}^+$: $i - 1 \leftrightarrow i$.
  - Set of odd integers: $(i-1)/2 \leftrightarrow i$.
  - Set of rational numbers: See next page.

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.
- Define $|A| < |B|$ if $|A| \leq |B|$ but $|A| \neq |B|$.
- Obviously, if $A \subseteq B$, then $|A| \leq |B|$.
- But 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. 103).
- A lot of "paradoxes" arise.

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.
- 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 opinion.

---

[a] Galileo (1564–1642).
[b] Euclid (325 B.C.–265 B.C.).

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)

Cantor's[a] 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.[b]
- 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] Georg Cantor (1845–1918). According to Kac and Ulam, "[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."

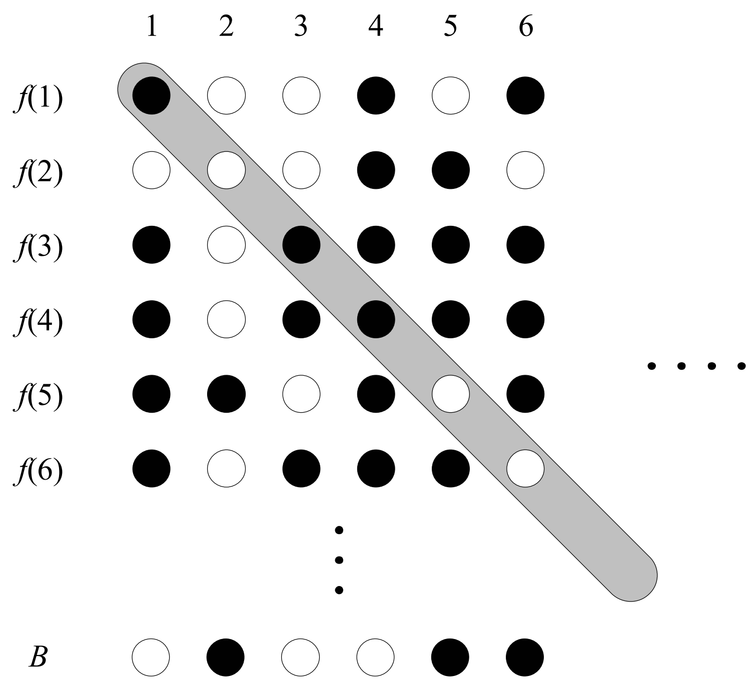
[b] Note that $f(k)$ is a subset of $\mathbb{N}$.

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)

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 a 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.