Relativizations of „P versus NP“

Theorem: There exist oracles *A* and *B* such that

$$\mathbf{P}^A = \mathbf{NP}^A \qquad \text{and} \qquad \mathbf{P}^B \neq \mathbf{NP}^B \quad !$$

Proof (Baker&Gill&Solovay‘75)**:** *A*, see Exercise.

For every $B \subseteq \{0,1\}^* =: \Sigma^*$, $L_B := \{ 1^{|\underline{w}|} : \underline{w} \in B \} \in \mathbf{NP}^B$.

Now use diagonalization to construct *B*: $L_B \notin \mathbf{P}^B$:

Let $M_1^?, M_2^?, \ldots$ be computable enumeration of all DTMs $M_i^?$ with running time watchdog n^i+i.

Define disjoint increasing sequences of finite sets

$$\emptyset =: B_0 \subseteq B_1 \subseteq B_2 \subseteq B_3 \subseteq \ \ldots \ \bigcup B_i =: B$$

$$\emptyset =: C_0 \subseteq C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots \ \bigcup C_i =: C, \quad B \cap C = \emptyset$$

$L_B = \{\, 1^{|\underline{w}|} : \underline{w} \in B \,\} \notin \mathbf{P}^B$

$M_1^?, M_2^?, \ldots$: all DTMs $M_i^?$ with running time $\leq n^i+i$.

Define disjoint increasing sequences of finite sets

$\emptyset \subseteq B_1 \subseteq B_2 \subseteq B_3 \subseteq \ldots B \qquad \emptyset \subseteq C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots C$

i-1$\rightarrow i$: Take $n_i > n_{i-1}$ s.t. $B_{i-1}, C_{i-1} \subseteq \Sigma^{<n_i} \wedge \quad 2^{n_i} > n_i^i + i$

Now 'simulate' $M_i^?$ on input $\underline{x} := 1^{n_i}$:

Start with $Z := \emptyset$; oracle queries "$\underline{y} \in ?$"

- in case $\underline{y} \in B_{i-1}$, answer **yes**
- in case $\underline{y} \in C_{i-1}$, answer **no**
- otherwise answer **no** and let $Z := Z \cup \{\underline{y}\}$

If accepts, let $B_i := B_{i-1} \subseteq \Sigma^{<n_i}$ and $C_i := C_{i-1} \cup Z$;

if rejects, $B_i := B_{i-1} \cup \{\underline{w}\}$ and $C_i := C_{i-1} \cup Z$, $\underline{w} \in \Sigma^{n_i} \setminus Z$

$L_B = \{ 1^{|\underline{w}|} : \underline{w} \in B \} \notin \mathbf{P}^B$

$M_1^?, M_2^?, \ldots$: all DTMs $M_i^?$ with running time $\leq n^i + i$.

Define disjoint increasing sequences of finite sets

$\emptyset \subseteq B_1 \subseteq B_2 \subseteq B_3 \subseteq \ldots \qquad \emptyset \subseteq C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots$

Suppose $L_B \in \mathbf{P}^B$, decided in polytime by prog M^B

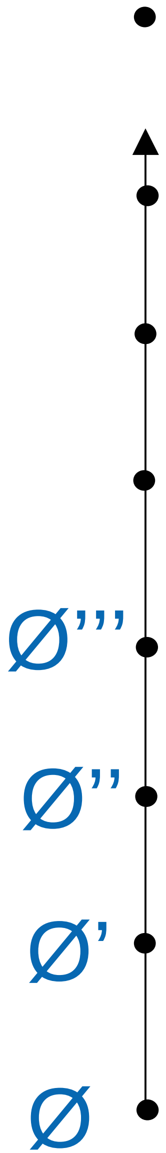
W.l.o.g. time$\leq n^i + i$ and $M^? = M_i^?$ for some i (why?)

Case $1^{n_i} \in L_B \Rightarrow M_i^B$ rejects : contradiction

Case $1^{n_i} \notin L_B \Rightarrow M_i^B$ accepts : contradiction ■

Take $n_i > n_{i-1}$; Consider $M_i^{B_{i-1}}$ on input $\underline{x} := 1^{n_i}$:
If accepts, let $B_i := B_{i-1} \subseteq \Sigma^{<n_i}$;
if rejects, $B_i := B_{i-1} \cup \{\underline{w}\}$, $\underline{w} \in \Sigma^{n_i} \setminus Z$

Partially Ordered Sets

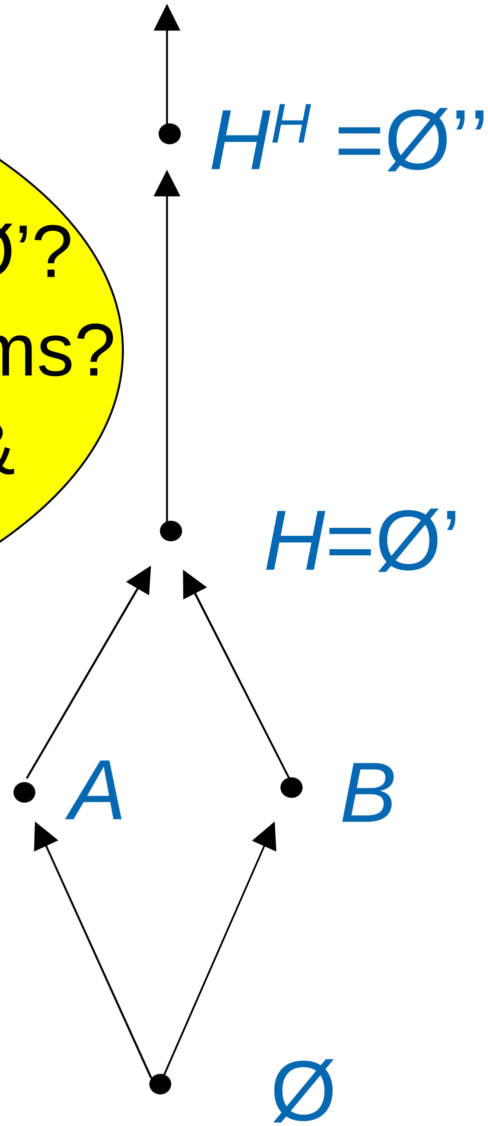


Emil Post 1944:

a) Is anything in between Ø and Ø'?

b) Are there incomparable problems?

Answered 1956/57 by Friedberg & Muchnik: such *A*,*B* exist!



Two Incomparable Problems

Proof idea: Show there exist semidec $A,B \subseteq \mathbb{N}$ such that

To each DTM $P^?$ exists $\underline{x}[P]$ s.t.: $\underline{x} \in A \iff P^B$ accepts $\underline{x}$

To each DTM $Q^?$ exists $\underline{y}[Q]$ s.t.: $\underline{y} \in B \iff Q^A$ accepts $\underline{y}$

Start with $\underline{x},\underline{y}:=0$, $A,B:=\emptyset$. Enumerate all DTMs $P^?,Q^?$.

- If P^B accepts $\underline{x}$, set $A:=A\cup\{\underline{x}\}$; else keep A.
  Let $\underline{x} := \underline{x} + 1$
- If Q^A accepts $\underline{y}$, set $B:=B\cup\{\underline{y}\}$; else keep B.
  Let $\underline{y} := \underline{y} + 1$

But oracles A, B change, may later violate witness condition "$\underline{x} \in A \Rightarrow P^B$ accepts $\underline{x}$"…

Two Incomparable Problems

Proof idea: Show there exist semidec $A,B\subseteq\mathbb{N}$ such that

To each DTM $P^?$ exists $\underline{x}[P]$ s.t.: $\underline{x}\in A \Leftrightarrow P^B$ accepts $\underline{x}$

To each DTM $Q^?$ exists $\underline{y}[Q]$ s.t.: $\underline{y}\in B \Leftrightarrow Q^A$ accepts $\underline{y}$

Start with $\underline{x},\underline{y}:=0$, $A,B:=\emptyset$. Enumerate all DTMs $P^?,Q^?$.

- If P^B accepts $\underline{x}$, set $A:=A\cup\{\underline{x}\}$
  and $\underline{y}$:= max{ $\underline{y}$, largest oracle query by P^B on $\underline{x}$ } +1
- If Q^A accepts $\underline{y}$, set $B:=B\cup\{\underline{y}\}$
  and $\underline{x}$:= max{ $\underline{x}$, largest oracle query by Q^A on $\underline{y}$ } +1

But oracles A, B change, may later violate witness condition "$\underline{x}\in A \Leftarrow P^B$ accepts $\underline{x}$"…

Finite Injury Priority Method

To each DTM $P^?$ exists $\underline{x}[P]$ s.t.: $\underline{x} \in A \Leftrightarrow P^B$ accepts $\underline{x}$
To each DTM $Q^?$ exists $\underline{y}[Q]$ s.t.: $\underline{y} \in B \Leftrightarrow Q^A$ accepts $\underline{y}$

Maintain lists $(P,\underline{x})$ and $(Q,\underline{y})$ with 'candidate' witnesses
$(P,\underline{x})$ **active** if simulation P^B on $\underline{x}$ still running; else *inactive*
E.g. $L_A = (P_1,\underline{x}_1)$, $(P_2,\underline{x}_2)$, $(P_3,\underline{x}_3)$; $L_B = (Q_1,\underline{y}_1)$, $(Q_2,\underline{y}_2)$.

- For each n:=0,1,…
  - –Add entry $(n,\underline{x})$ to list. For **active** $(P,\underline{a})$ increasing in P
  - –If P^B accepts $\underline{a}$ within $\leq n$ steps, set $A:=A\cup\{\underline{a}\}$ and $\underline{y}$:=1+max{ $\underline{y}$, largest oracle query by P^B on $\underline{a}$ } and make $(P$,a) **inactive**. For all $(Q,\underline{b})$ with $Q>P$ do
    - replace $(Q,\underline{b})$ with (Q,$\underline{y}$++) made **active**.
  - –Add entry $(n,\underline{y})$ to list. For **active** $(Q,\underline{b})$ increasing in Q

Finite Injury Priority Method

To each DTM $P^?$ exists $\underline{x}[P]$ s.t.: $\underline{x} \in A \Leftrightarrow P^B$ accepts $\underline{x}$

To each DTM $Q^?$ exists $\underline{y}[Q]$ s.t.: $\underline{y} \in B \Leftrightarrow Q^A$ accepts $\underline{y}$

Maintain lists $(P,\underline{x})$ and $(Q,\underline{y})$ with 'candidate' witnesses

- For each n:=0,1,…
  - –Add entry $(n,\underline{x})$ to list. For **active** $(P,\underline{a})$ increasing in P
  - –If P^B accepts $\underline{a}$ within $\leq n$ steps, set $A:=A\cup\{\underline{a}\}$ and $\underline{y}$:=1+max{ $\underline{y}$, largest oracle query by P^B on $\underline{a}$ } and make $(P,\underline{a})$ **inactive**. For all $(Q,\underline{b})$ with $Q>P$ do
    - replace $(Q,\underline{b})$ with $(Q,\underline{y}{+}{+})$ made **active**.
  - –Add entry $(n,\underline{y})$ to list. For **active** $(Q,\underline{b})$ increasing in Q
  - –If Q^A accepts $\underline{b}$ within $\leq n$ steps, set $B:=B\cup\{\underline{b}\}$ and $\underline{x}$:=1+max{ $\underline{x}$, largest oracle query by Q^A on $\underline{b}$ } and make $(Q,\underline{b})$ **inactive**. For all $(P,\underline{a})$ with $P>Q$ do
    - replace $(P,\underline{a})$ with $(P,\underline{x}{+}{+})$ made **active**.

Finite Injury Priority Method

Candidates for "$\underline{y} \in B \Leftrightarrow Q^A$ accepts $\underline{y}$" change („**injury**")
but only a **finite** number of times:

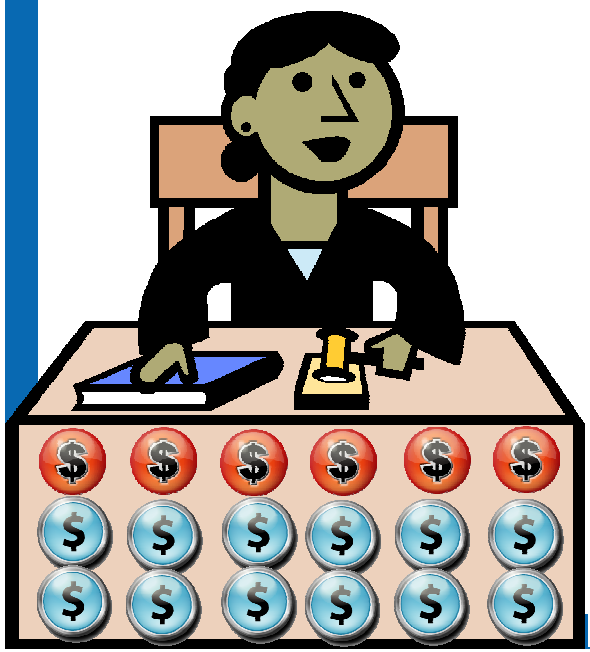
- namely when some $P<Q$ terminates („**priority**")

and, once settled, does satisfy the witness condition!
Both *A*,*B* are enumerated, hence semi-decidable.

- For each n:=0,1,…
  - –Add entry $(n,\underline{x})$ to list. For **active** $(P,\underline{a})$ increasing in P
  - –If P^B accepts $\underline{a}$ within $\leq n$ steps, set $A:=A\cup\{\underline{a}\}$
    and $\underline{y}:=1+\max\{\ \underline{y}$, largest oracle query by P^B on $\underline{a}$ }
    and make $(P,$a) **inactive**. For all $(Q,\underline{b})$ with $Q>P$ do
    - replace $(Q,\underline{b})$ with $(Q,\underline{y}{+}{+})$ made **active**.
  - –Add entry $(n,\underline{y})$ to list. For all **active** $(Q,\underline{b})$ in list:

Priority Diagonalization: Trading with the Devil

- You have countably many coins
  - Devil takes one of them
  - and gives you two new ones,
  - Then repeat.
- How many coins do you ultimately own ?



......
......
......

NONE!

Courtesy of Joel D. Hamkins