Relativizing Proof Techniques

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

Most proof techniques in Complexity Theory carry over to relativized complexity classes:

$$O \text{ oracle}, \quad \mathbf{X} \subseteq \mathbf{Y} \quad \rightarrow \quad \mathbf{X}^O \subseteq \mathbf{Y}^O$$

- Halting Problem $\rightarrow$ Arithmet. Hierarchy
- Time Hierarchy $\mathbf{DTIME}(t(n)\log t(n)) \subset \mathbf{DTIME}(t(n))$
- Savitch $\mathbf{NL} \subseteq \mathbf{L}^2$, $\mathbf{NPSPACE}=\mathbf{PSPACE}$
- Immerman-Szelepcsényi $\mathbf{NL}=\mathbf{coNL}$
- *Time vs Space* $\mathbf{DTIME}(t(n)) \subseteq \mathbf{DSPACE}(t(n)/\log t(n))$

Relativizations of „P versus NP“

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

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

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

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

Define disjoint increasing sequences of finite sets

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

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

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

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

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

Define disjoint increasing sequences of finite sets

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

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

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 $C_i := C_{i-1} \cup Z$, $\underline{w} \in \Sigma^n \setminus Z$

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

HEINZ NIXDORF INSTITUTE
University of Paderborn
Algorithms and Complexity

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

Define disjoint increasing sequences of finite sets

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

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?)

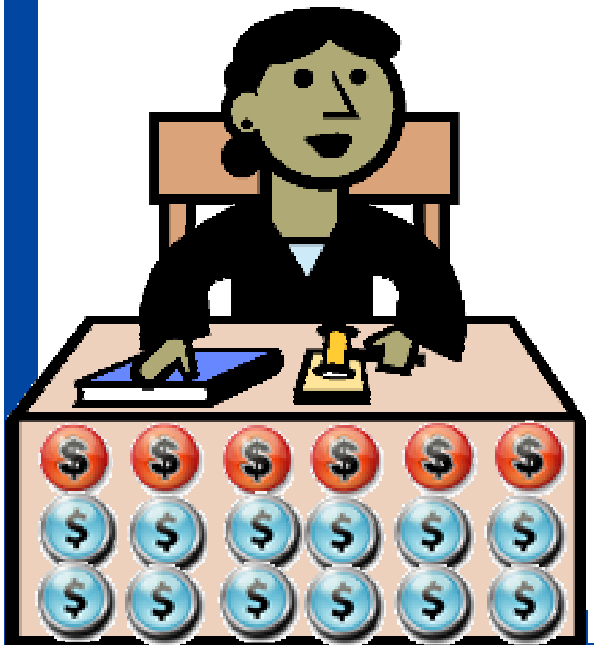
Case $1^{n_i} \in L_B \Rightarrow M_i^B$ rejects : contradiction

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

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

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