§5 PSPACE and Polynomial Hierarchy

- $\mathcal{PSPACE}$-complete problems

  QBF, 3QBF, GRAPH

- Savitch's Theorem:

  $\mathcal{NSPACE}(f) \subseteq \mathcal{SPACE}(f^2)$

- SUBlinear Memory Computation,

  graph reachability problems

- Immerman-Szelepcsényi:

  $\mathcal{NSPACE}(f) = co\mathcal{NSPACE}(f)$

- Oracle Complexity and Polynomial Hierarchy:

  syntactically / semantically

- Limitations of Relativizing Proofs:

  Baker, Gill & Solovay; Bennett & Gill

QBF and PSPACE

QBF: Given Boolean term $\Phi(Y_1,\dots Y_m)$,
does it hold $\exists y_1\ \forall y_2\ \exists y_3\ \forall\dots: \Phi(y_1,\dots y_m)=1$?

$\in$co$\mathcal{NP}$?
$\in\mathcal{NP}$?
$\in\mathcal{PSPACE}$

Recursively evaluate quantifiers:

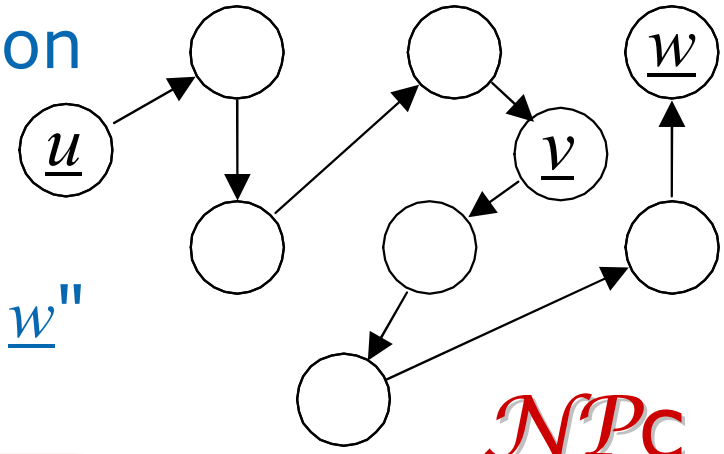
$$s(m) = s(m\text{-}1) + \text{poly}(n)$$

Theorem: QBF is $\mathcal{PSPACE}$-complete.

Proof: Let $\mathcal{A}$ decide $L\in$**PSPACE** in space $s:=\text{poly}(n)$.

Encode configurations of $\mathcal{A}$ in s bits $\underline{u}=(u_1,\dots u_s)$. Draw edge from $\underline{u}$ to $\underline{v}$ if $\underline{v}$ encodes $\mathcal{A}$'s unique config after $\underline{u}$.

$\mathcal{G}=\mathcal{G}_{\mathcal{A},s}$ digraph with $\underline{u}$=start config on input x, $\underline{w}$ *unique* accepting config.



$\mathcal{NP}$c

$\mathcal{A}$ accepts $x \Leftrightarrow P_{\mathcal{G}}(\underline{u},\underline{w},s)$,

:$\Leftrightarrow$ "$\exists$path of length $\le 2^s$ from $\underline{u}$ to $\underline{w}$"

$\Leftrightarrow \exists\underline{v}: P_{\mathcal{G}}(\underline{u},\underline{v},s\text{-}1) \wedge P_{\mathcal{G}}(\underline{v},\underline{w},s\text{-}1)$

$\Leftrightarrow \exists\underline{v}\ \forall\underline{s},\underline{t}:\ (\underline{s}=\underline{u} \wedge \underline{t}=\underline{v}) \vee (\underline{s}=\underline{v} \wedge \underline{t}=\underline{w}) \rightarrow P_{\mathcal{G}}(\underline{s},\underline{t},s\text{-}1)$

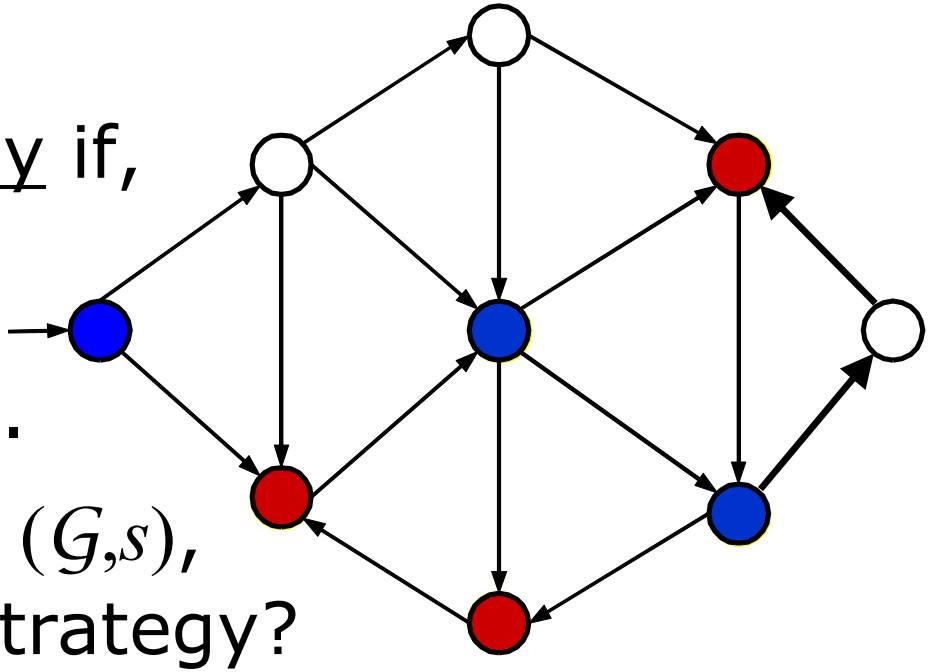
Two-Player Game on Graphs

3QBF: Given Boolean term $\Phi(X_1,\ldots X_m)$ in 3CNF,
does it hold $\exists x_1\ \forall x_2\ \exists x_3\ \forall\ldots: \Phi(x_1,\ldots x_m)=1$? $\mathcal{PSPACE}$-c

Fix digraph G with start vertex s. **Rules:**

- **Red** (start) and **blue** player alternatingly
- mark current vertex, and follow any outgoing edge
- to a yet unmarked vertex.
- Who cannot move, loses.

Red has a winning strategy if,
however **blue** reacts,
red can follow such that,
however …… **blue** looses.



Decision problem: Given (G,s),
does **red** have a winning strategy?

Two-Player Game on Graphs

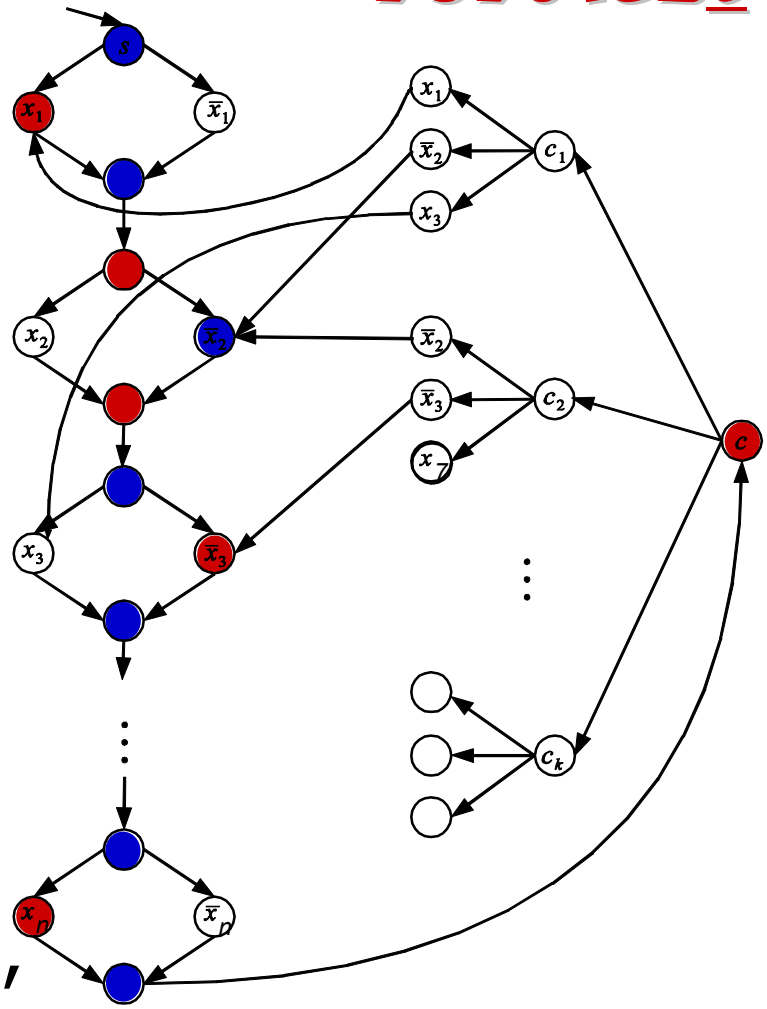
3QBF: Given Boolean term $\Phi(X_1,\ldots X_m)$ in 3CNF, does it hold $\exists x_1\ \forall x_2\ \exists x_3\ \forall\ldots\colon \Phi(x_1,\ldots x_m)=1$? $\mathcal{PSPACE}$-c

Proof (reduction from **3QBF**):

Let $\Phi = C_1 \wedge C_2 \wedge \ldots \wedge C_k$

See illustration for

$\Phi = (x_1 \vee \neg x_2 \vee x_3)$
$\wedge (\neg x_2 \vee \neg x_3 \vee x_7)$
$\wedge \ldots \wedge C_k$



Theorem: The following is $\mathcal{PSPACE}$-complete:

Decision problem: Given (G,s), does **red** have a winning strategy?

Walter Savitch's Theorem

Def: For nondecreasing $f:\mathbb{N}\to\mathbb{N}$, let $\mathbf{TIME}(f) :=$
$\{ L\subseteq\mathbb{N}$ decidable by a **WHILE+** program in time $O(f(n))\ \}$

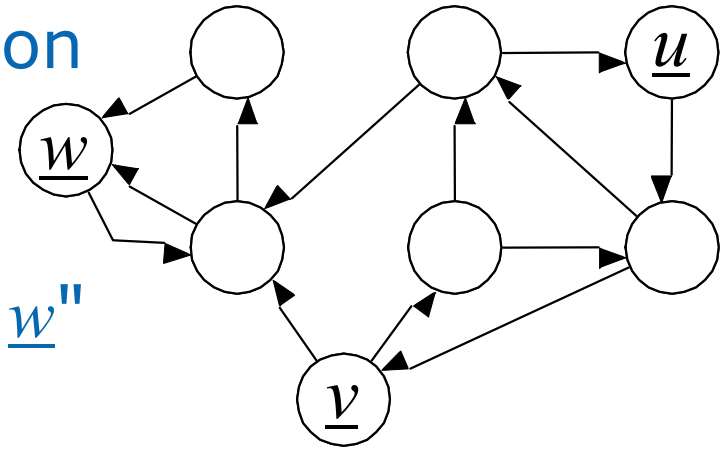
Same $\mathbf{NTIME}(f)$, $\mathbf{SPACE}(f)$, $\mathbf{NSPACE}(f)$: nondet. **WHILE+**

Theorem: For „every" $s:\mathbb{N}\to\mathbb{N}$, $\mathbf{NSPACE}(s)\subseteq\mathbf{SPACE}(s^2)$.

Proof: Let nondet. $\mathcal{A}$ accept L in space $s:=s(n)$

Encode *configurations* of $\mathcal{A}$ in s bits $\underline{u}=(u_1,\ldots u_s)$. Draw edge from $\underline{u}$ to $\underline{v}$ if $\underline{v}$ encodes $\mathcal{A}$'s possible config after $\underline{u}$.

$\mathcal{G}=\mathcal{G}_{\mathcal{A},s}$ digraph with $\underline{u}$=start config on input x, $\underline{w}$ unique accepting config.



$\mathcal{A}$ accepts $x \Leftrightarrow P_{\mathcal{G}}(\underline{u},\underline{w},s)$,
$:\Leftrightarrow$ "$\exists$path of length $\leq 2^s$ from $\underline{u}$ to $\underline{w}$"
$\Leftrightarrow \exists\underline{v}: P_{\mathcal{G}}(\underline{u},\underline{v},s\text{-}1) \wedge P_{\mathcal{G}}(\underline{v},\underline{w},s\text{-}1)$

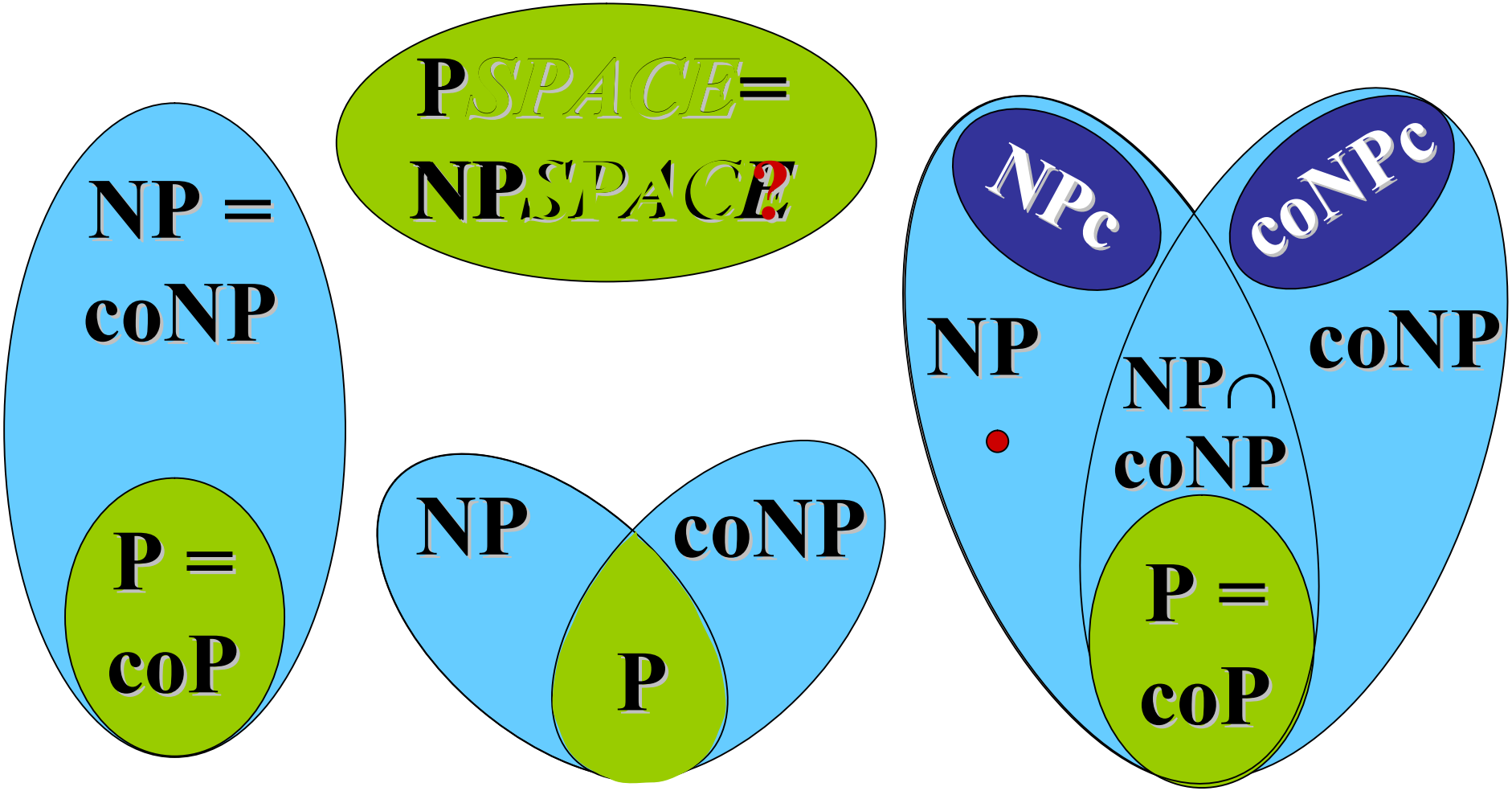
Recursive algorithm of depth s stores $\underline{v}$ in s bits: $O(s^2)$

Recall: Cases for $\mathcal{P}$ vs. $\mathcal{NP}$

Recall: For nondecreasing $f:\mathbb{N}\to\mathbb{N}$, let $\mathbf{TIME}(f) :=$

$\{ L\subseteq\mathbb{N}$ decidable by a **WHILE+** program in time $O(f(n))\ \}$

Same **NTIME**(f), **SPACE**(f), **NSPACE**(f): nondet. **WHILE+**



SUBlinear Memory Computation

KAIST

$\mathcal{P} := (x_j := 0 \mid x_j := 1 \mid x_j := x_i \pm x_k \mid \mathcal{P} ; \mathcal{P} \mid x_j := x_i \div 2 \mid$
$x_j :=$ guess $\mid x_j{:=}\mathrm{TEST}(x_k) \mid$ WHILE x_i DO $\mathcal{P}$ END $)$

Input *not* charged for memory, accessed *bit*-wise:

"$\mathrm{TEST}(x_k)$" returns x_k-th bit of input.

Example: input $(b_0\, b_1 \ldots b_{n-1})_2$, output $\#_1 \leq n$

Counter for $\#_1$ uses $O(\log n)$ bits:

$\mathrm{COUNT}_1 \in$ FL
=FLOGSPACE

FL: output $y{=}f(x)$ bit-wise,
closed under composition!

dirREACH $\in$ NL

Example: input $\langle\, G{=}(V,E),\, s,t{\in}V \,\rangle$,
output **1** if ∃directed path from s to t in G, **0** else.

Un/directed Un/reachability

dirUNREACH ∈ NL

Gödel Prize'95 (with Róbert Szelepcsényi)

dirREACH ∈ L² (Savitch)

undirREACH ∈ L

Grace Hopper Award'05, *Gödel Prize*'09 (w/Avi Wigderson and Salil Vadhan

dirREACH ∈ NL

Example: input $\langle G=(V,E), s,t\in V \rangle$, output **1** if ∃directed path from s to t in G, **0** else.

Immerman-Szelepcsényi

dirUNREACH ∈ NL

Theorem: For „every" $s \geq \log$,

NSPACE(s)=coNSPACE(s)

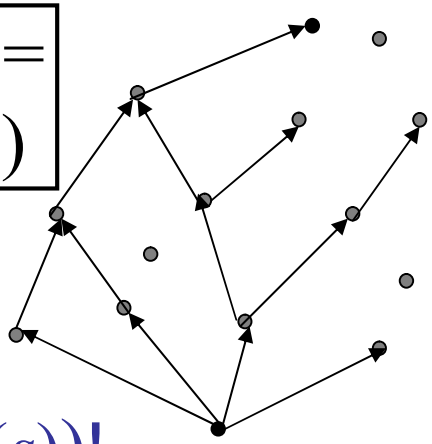
$m=2^{O(s)}$: *un*reachability $u \nrightarrow v$

"guess and verify $f(x)$"

Proof: Recall digraph $\mathcal{G}=\mathcal{G}_{\mathcal{A},s}$ u=initial, v=accepting config.

$\mathcal{G}(m)$:= { config w has dist $\leq m$ from u },

$N(m) := \#\mathcal{G}(m)$



a) For each m, $\mathcal{G}(m) \in$ **NSPACE**($O(s)$).

b) If $m \to N(m)$ is computable in **NSPACE**($O(s)$),
then $\mathcal{G} \setminus \mathcal{G}(m) \in$ **NSPACE**($O(s)$)

c) $m \to N(m) \leq 2^{O(s)}$ is computable in **NSPACE**($O(s)$)!

Immerman-Szelepcsényi (II)

b) On input $w \in \mathcal{G}$ and $m \in \mathbb{N}$,
compute $M := N(m) = \#$config.s reachable in m steps.
Initialize counter $C := 0$. For each possible config $w' \neq w$:

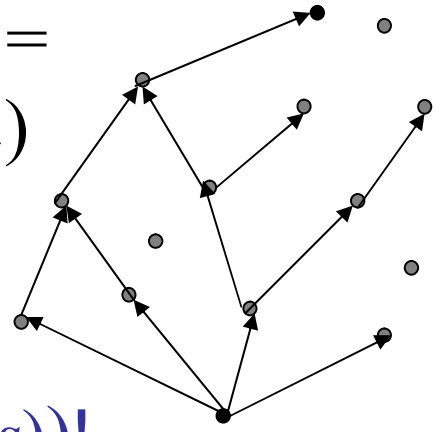
- **Guess** whether w' is reachable within m steps or not:
  If **yes**, increment C & guess path u to w' of length$\leq m$
  - If no such path gets guessed, abort

If $C < M$, abort; else stop and accept!

Why correct?

Proof: Recall digraph $\mathcal{G} = \mathcal{G}_{\mathcal{A},s}$ u=initial, v=accepting config.

$\mathcal{G}(m) := \{$ config w has dist $\leq m$ from $u \}$, $N(m) := \#\mathcal{G}(m)$



a) For each m, $\mathcal{G}(m) \in \mathbf{NSPACE}(O(s))$.

b) If $m \to N(m)$ is computable in $\mathbf{NSPACE}(O(s))$,
then $\mathcal{G} \setminus \mathcal{G}(m) \in \mathbf{NSPACE}(O(s))$

c) $m \to N(m) \leq 2^{O(s)}$ is computable in $\mathbf{NSPACE}(O(s))$!

Immerman-Szelepcsényi (III)

c) Inductively "guess and verify" $N(m+1)$ from $N(m)$:

Initialize counter $C':=0$. For each possible config w':

- **Guess** whether w' is reachable in $m+1$ steps or not.

If **yes**, increment C' & guess path to w' of length$\leq m+1$

☐ If no such path gets guessed, abort.

If **no**, init. counter $C:=0$. For each possible config w:

- **Guess** whether w is reachable in m steps or not.

If **yes**, but if $\exists$edge from w to w': abort

If **yes**, increment C & guess path to w of length$\leq m$

☐ If no such path gets guessed, abort.

If $C<N(m)$, abort.

Output $C'=N(m+1)$.

c) $m \to N(m) \leq 2^{O(s)}$ is computable in $\mathbf{NSPACE}(O(s))$!

Oracle Complexity Theory

Fix $O \subseteq \mathbb{N}$. An **OWHILE+** program $\mathcal{A}^O$
may make **queries** "$x_j \in O$**?**"

Definition: Fix some class $\mathbf{C}$ of subsets $L \subseteq \mathbb{N}$.

$\mathbf{P}^{\mathbf{C}} := \{ L \subseteq \mathbb{N}$ decided by polytime **OWHILE+** $\mathcal{A}^O$, $O \in \mathbf{C} \}$

$\mathbf{NP}^{\mathbf{C}} := \{ L \subseteq \mathbb{N}$ accep. nondet.poly. **OWHILE+** $\mathcal{A}^O$, $O \in \mathbf{C} \}$

$\mathbf{PSPACE}^{\mathbf{C}} = \{ L \subseteq \mathbb{N}$ decide in poly.mem w/oracle $O \in \mathbf{C} \}$

Examples:

"Given a Boolean expression φ, is it *shortest* among all semantically equivalent ones ψ?"

a) **MinBF** $\in \mathbf{coNP}^{\mathrm{SAT}} = \mathbf{coNP}^{\mathbf{NP}} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$

b) $\mathbf{P}^{\mathbf{P}} = \mathbf{P}$, $\mathbf{NP}^{\mathbf{P}} = \mathbf{NP}$, $\mathbf{PSPACE}^{\mathbf{PSPACE}} = \mathbf{PSPACE}$

c) $\mathbf{NP} \cup \mathbf{coNP} \subseteq \mathbf{P}^{\mathbf{NP}}$; „≠“ unless $\mathbf{NP} = \mathbf{coNP}$

Semantic Polynomial Hierarchy

Def: $\Delta_0 P = \Sigma_0 P = \Pi_0 P := P$

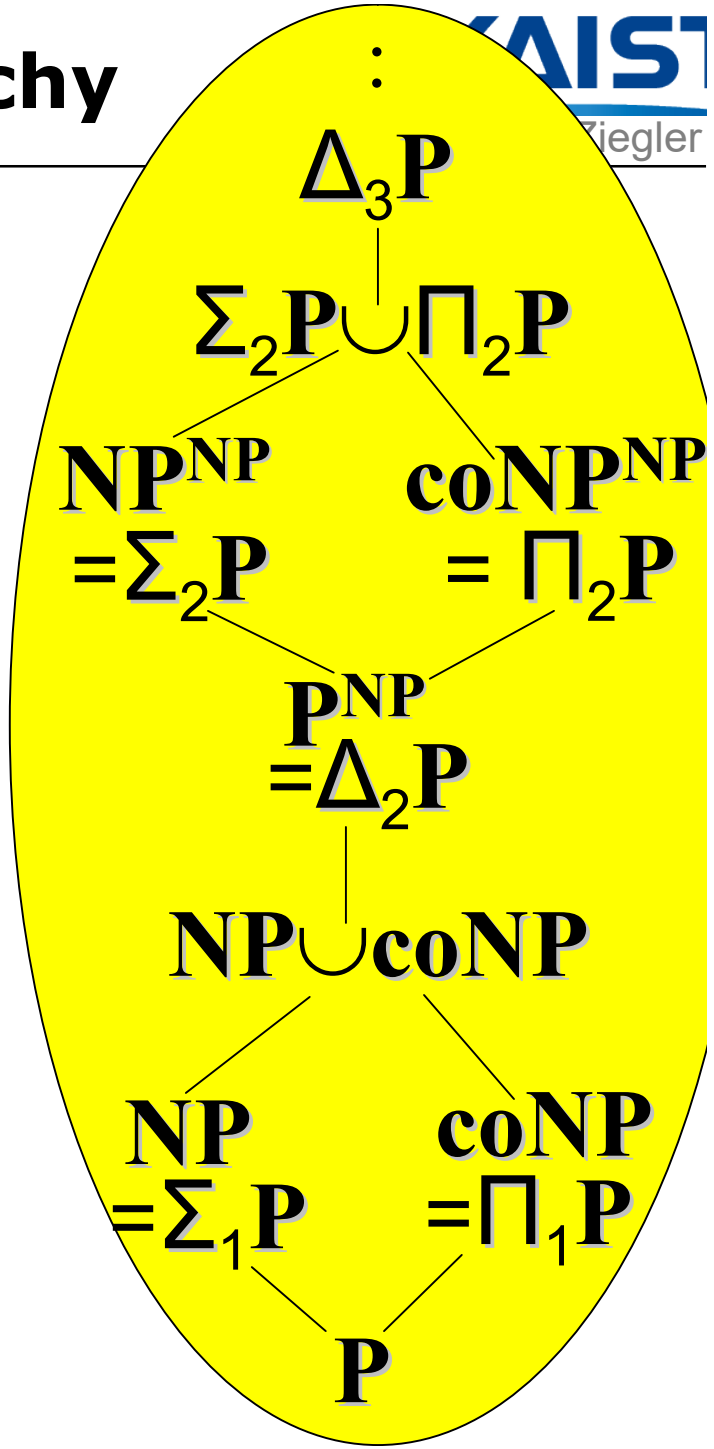
- $\Delta_{k+1} P := P^{\Sigma_k P} = P^{\Pi_k P}$
- $\Sigma_{k+1} P := NP^{\Sigma_k P} = NP^{\Pi_k P}$
- $\Pi_{k+1} P := coNP^{\Sigma_k P} = coNP^{\Pi_k P}$
- $PH := \bigcup \Sigma_k P$

Lemma: a) $\Delta_k P = \text{co-}\Delta_k P$

b) $\Delta_k P \subseteq \Sigma_k P \cap \Pi_k P$

c) $\Sigma_k P \cup \Pi_k P \subseteq \Delta_{k+1} P$

d) $PH \subseteq PSPACE$



Syntactic Polynomial Hierarchy

Abbreviate $\mathbb{N}_n := \{ y \in \mathbb{N} : \ell(y) \le n \}$

Theorem: a) $L \subseteq \mathbb{N}$ belongs to **coNP** iff

$L = \{ x \mid \forall y \in \mathbb{N}_{\mathrm{poly}(n)} : \langle x,y \rangle \in V \}$ for some $V \in \mathbf{P}$

$\ell(y) \ge \mathrm{poly}(n)$, $n := \ell(x)$

b) L belongs to Σ_{k+1} iff

$L = \{ x \mid \exists y \in \mathbb{N}_{\mathrm{poly}(n)} : \langle x,y \rangle \in W \}$ for some $W \in \Pi_k$ or Σ_k

c) L belongs to Π_{k+1} iff

$L = \{ x \mid \forall y \in \mathbb{N}_{\mathrm{poly}(n)} : \langle x,y \rangle \in Z \}$ for some $Z \in \Sigma_k$ or Π_k

d) L belongs to Σ_k iff

"$\exists$" if k odd, "$\forall$" else

$L = \{ x \mid \exists y_1 \in \mathbb{N}_{\mathrm{poly}(n)} \; \forall y_2 \in \mathbb{N}_{\mathrm{poly}(n)} \; \exists y_3 \cdots$

$Q_k y_k \in \mathbb{N}_{\mathrm{poly}(n)} : \langle x, y_1, y_2, \ldots y_k \rangle \in A \}$ for some $A \in \mathbf{P}$

$$\Sigma_{k+1}\mathbf{P} = \mathbf{NP}^{\Sigma_k \mathbf{P}} = \mathbf{NP}^{\Pi_k \mathbf{P}} \quad \Pi_{k+1}\mathbf{P} = \mathbf{coNP}^{\Sigma_k \mathbf{P}} = \mathbf{coNP}^{\Pi_k \mathbf{P}}$$

Limitations of Relativizing Proofs

Proof "methods" for solving **P/NP/PSPACE** ?

"Relativized Hierarchy" $\forall A$: $\mathbf{P}^A \subseteq \mathbf{NP}^A \subseteq \mathbf{PSPACE}^A$

"Relativized Savitch" $\forall A$: $\mathbf{NPSPACE}^A = \mathbf{PSPACE}^A$

Theorem (BGS'75 ; BG'81; RST'15):

a) There exists an oracle $A \subseteq \mathbb{N}$ s.t. $\mathbf{P}^A = \mathbf{NP}^A$.

b) There exists an oracle $B \subseteq \mathbb{N}$ s.t. $\mathbf{P}^B \neq \mathbf{NP}^B$.

c) With probability 1, random $B \subseteq \mathbb{N}$ has $\mathbf{P}^B \neq \mathbf{NP}^B$.

d) With probability 1 w.r.t random oracle $B \subseteq \mathbb{N}$, the polynomial hierarchy is *in*finite.

$\forall x \in \mathbb{N}: \mathbb{P}(x \in B) = ½$ independently at random

Proof a) $A := \mathbf{QBF}$ or any other **PSPACE**-complete problem

Bennett & Gill (1981)

$$\mathbb{P}[x\in L_B \wedge \mathcal{A}^B(x)\downarrow] = \mathbb{P}[x\in L_B \mid \mathcal{A}^B(x)\downarrow] \cdot \mathbb{P}[\mathcal{A}^B(x)\downarrow]$$

$$L_B := \{\, x=4^n \mid \exists y<2^n: \forall z<n: \; 4^n+y\cdot n+z\in B \,\} \in \mathbf{NP}^B$$

q

Suppose alorithm $\mathcal{A}^B$ decides L_B in time $\mathrm{poly}(n)$:

On input $x=4^n$ can make at most $\mathrm{poly}(n) << 2^{n-1}$, $n\to\infty$ many different queries "$q_j\in B$?", $q_j = 4^n+y_j\cdot n+z_j$

With prob. $p_x = \mathbb{P}[(x\notin L_B \wedge \mathcal{A}^B(x)\uparrow) \vee (x\in L_B \wedge \mathcal{A}^B(x)\downarrow)]$ **>0.1**,

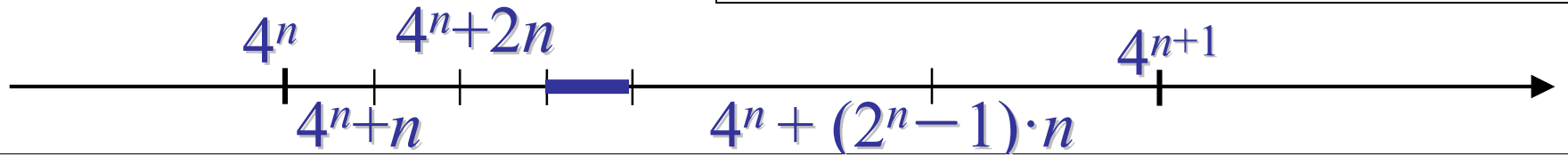
$\mathcal{A}^B$ errs on input $x=4^n$.

$\Rightarrow$ $\mathcal{A}^B$ decides L_B with prob. $\le \prod_n (1-p_{4^n}) = \mathbf{0}$.

$$\mathbb{P}_B[\forall z<n: \; 4^n+y\cdot n+z\in B] = 2^{-n},$$

$$\mathbb{P}_B[\exists y<2^n \; \forall z<n: \; 4^n+y\cdot n+z\in B]$$

$$= 1-(1-2^{-n})^{2^n} \to 1-1/e \approx 0.63$$



Recap of §5

- $\mathcal{PSPACE}$-complete problems

  QBF, 3QBF, GRAPH

- Savitch's Theorem:

  $\mathcal{NSPACE}(f) \subseteq \mathcal{SPACE}(f^2)$

- SUBlinear Memory Computation,

  graph reachability problems

- Immerman-Szelepcsényi:

  $\mathcal{NSPACE}(f) = co\mathcal{NSPACE}(f)$

- Oracle Complexity and Polynomial Hierarchy:

  syntactically / semantically

- Limitations of Relativizing Proofs:

  Baker, Gill & Solovay; Bennett & Gill

Quiz for §5

This section introduced and employed
the "*Reachability Method*"
in three important theorems
regarding space (=memory) complexity.

Please state these three theorems!