§6 PSPACE and Polynomial Hierarchy

KAIST CS422 M. Ziegler

- $\mathcal{PSPACE}$-complete problems
  QBF, 3QBF, GRAPH
- (Savitch's Theorem:
  $\mathcal{PSPACE} = \mathcal{NPSPACE}$)
- Polynomial Hierarchy:
  syntactically / semantically
- (Baker, Gill & Solovay)

QBF and PSPACE

KAIST CS422 M. Ziegler

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

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

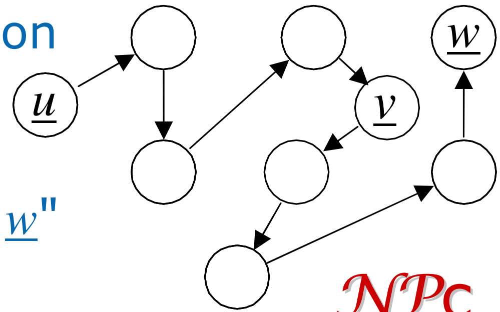
Recursively evaluate quantifiers: $s(m) = s(m\text{-}1) + \text{poly}(n)$

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

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



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

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

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

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

$\mathcal{NP}$c

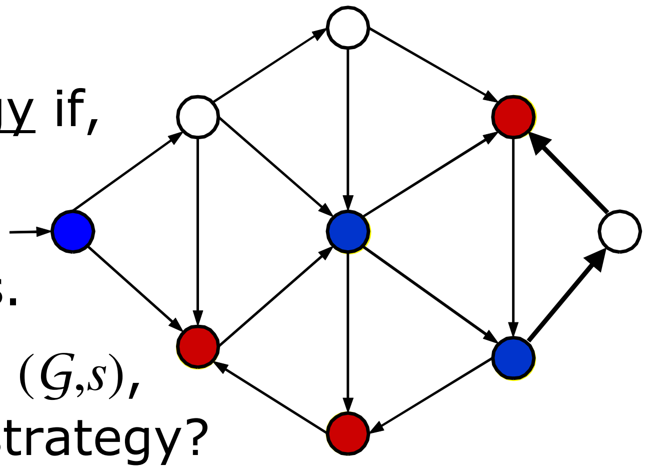
Two-Player Game on Graphs

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 $\mathcal{G}$ 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 $(\mathcal{G},s)$,
does **red** have a winning strategy?

Two-Player Game on Graphs

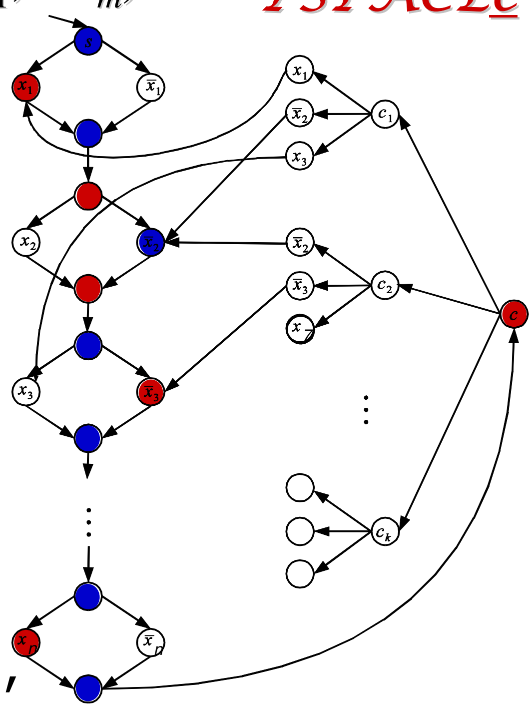
3QBF: Given Boolean term $\Phi(X_1,\ldots X_m)$ in 3CNF,
does it hold $\exists x_1\ \forall x_2\ \exists x_3\ \forall\ldots: \Phi(x_1,\ldots x_m)=1$? $\mathcal{PSPACE}c$

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 $(\mathcal{G},s)$,
does **red** have a winning strategy?

Oracle Complexity Theory

Fix $\mathcal{O}\subseteq\mathbb{N}$. An **OWHILE+** program $\mathcal{A}^{\mathcal{O}}$
has test instructions "$x_j\in\mathcal{O}$**?**"

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

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

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

Examples:

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

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: $\Delta_0\mathbf{P} = \Sigma_0\mathbf{P} = \Pi_0\mathbf{P} := \mathbf{P}$

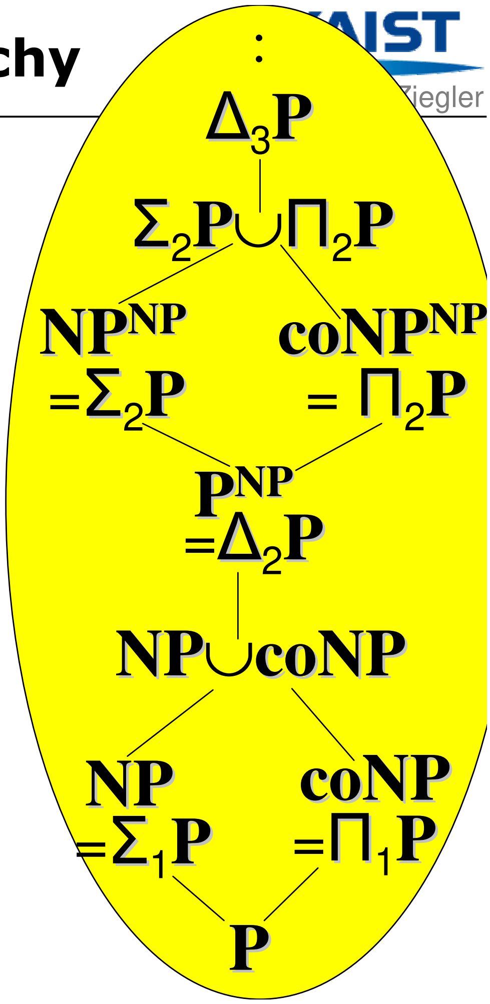
- $\Delta_{k+1}\mathbf{P} := \mathbf{P}^{\Sigma_k\mathbf{P}} = \mathbf{P}^{\Pi_k\mathbf{P}}$
- $\Sigma_{k+1}\mathbf{P} := \mathbf{NP}^{\Sigma_k\mathbf{P}} = \mathbf{NP}^{\Pi_k\mathbf{P}}$
- $\Pi_{k+1}\mathbf{P} := \mathbf{coNP}^{\Sigma_k\mathbf{P}} = \mathbf{coNP}^{\Pi_k\mathbf{P}}$
- $\mathrm{PH} :=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

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

b) $\Delta_k\mathbf{P} \subseteq \Sigma_k\mathbf{P} \cap \Pi_k\mathbf{P}$

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

d) $\mathrm{PH} \subseteq \mathbf{PSPACE}$



Syntactic Polynomial Hierarchy

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

Theorem: a) $L\subseteq\mathbb{N}$ belongs to **coNP** iff
$L = \{\, x \mid \forall y\in\mathbb{N}_{\text{poly}(n)} : \langle x,y\rangle\in V \,\}$ for some $V\in\mathbf{P}$ $\quad n:=\ell(x)$

b) L belongs to Σ_{k+1} iff
$L = \{\, x \mid \exists y\in\mathbb{N}_{\text{poly}(n)} : \langle x,y\rangle\in W \,\}$ for some $W\in\Pi_k$ or Σ_k

c) L belongs to Π_{k+1} iff
$L = \{\, x \mid \forall y\in\mathbb{N}_{\text{poly}(n)} : \langle x,y\rangle\in Z \,\}$ for some $Z\in\Sigma_k$ or Π_k

d) L belongs to Σ_k iff $\quad$ "$\exists$" if k odd, "$\forall$" else
$L = \{\, x \mid \exists y_1\in\mathbb{N}_{\text{poly}(n)}\ \forall y_2\in\mathbb{N}_{\text{poly}(n)}\ \exists y_3\ldots$
$\quad Q_k y_k\in\mathbb{N}_{\text{poly}(n)} : \langle x,y_1,y_2,\ldots y_k\rangle\in A \,\}$ for some $A\in\mathbf{P}$

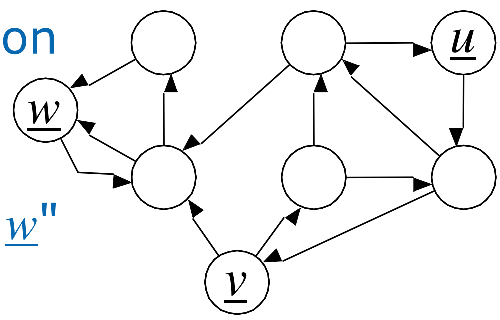
$\Sigma_{k+1}\mathbf{P} = \mathbf{NP}^{\Sigma_k\mathbf{P}} = \mathbf{NP}^{\Pi_k\mathbf{P}} \quad \Pi_{k+1}\mathbf{P} = \mathbf{coNP}^{\Sigma_k\mathbf{P}} = \mathbf{coNP}^{\Pi_k\mathbf{P}}$

Walter Savitch's Theorem

Def: For nondecreasing $f:\mathbb{N}\to\mathbb{N}$, let $\text{TIME}(f) :=$
$\{\, L\subseteq\{0,1\}^*$ decidable by WHILE+ program in time $f(n)$ $\}$
Similarly NTIME(f), SPACE(f), NSPACE(f): nondet. WHILE+

Theorem: For any polynom. p, $\text{NSPACE}(p)\subseteq\text{SPACE}(p^2)$

Proof: Let nondet. $\mathcal{A}$ accept L in space $s:=p(n)$
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: $O(s^2)$