Complexity Theory

Jan Křetínský

Chair for Foundations of Software Reliability
and Theoretical Computer Science
Technical University of Munich

Summer 2016

Based on slides by Jörg Kreiker

Lecture 10

The polynomial hierarchy PH

Agenda

- ExactIndset, MinEqDNF, and bounded QBF
- Σ_i^p, Π_i^p, and PH
- properties of the polynomial hierarchy
- more examples

Exact independent set

Recall the independent set problem

$$\text{Indset} = \{\langle G, k\rangle \mid G \text{ has an independent set of size } k\}$$

which was shown to be **NP**-complete.

Exact independent set

Recall the independent set problem

$$\text{Indset} = \{\langle G, k\rangle \mid G \text{ has an independent set of size } k\}$$

which was shown to be **NP**-complete.

What about the variation

$$\text{ExactIndset} = \{\langle G, k\rangle \mid \text{the largest independent set of } G \text{ has size } k\}$$

Exact independent set

Recall the independent set problem

$$\text{Indset} = \{\langle G, k\rangle \mid G \text{ has an independent set of size } k\}$$

which was shown to be **NP**-complete.

What about the variation

$$\text{ExactIndset} = \{\langle G, k\rangle \mid \text{the largest independent set of } G \text{ has size } k\}$$

One needs to show

1. there exists an independent set of size k and
2. all other independent set have size at most k

Exact independent set

Recall the independent set problem

$$\text{Indset} = \{\langle G, k\rangle \mid G \text{ has an independent set of size } k\}$$

which was shown to be **NP**-complete.

What about the variation

$$\text{ExactIndset} = \{\langle G, k\rangle \mid \text{the largest independent set of } G \text{ has size } k\}$$

One needs to show

1. there exists an independent set of size k and
2. all other independent set have size at most k

(1) is a $\exists$ certificate (as in **NP**) while (2) is a $\forall$ certificate (as in **coNP**)!

Minimizing Boolean formulas

Let DNF be disjunctive normal form and $\equiv$ denote logic equivalence.

$$\text{MinEqDNF} = \{\langle \varphi, k \rangle \mid \text{there is a DNF formula } \psi \text{ of size at most } k \text{ s.t. } \varphi \equiv \psi\}$$

Minimizing Boolean formulas

Let DNF be disjunctive normal form and $\equiv$ denote logic equivalence.

$$\text{MinEqDNF} = \{\langle \varphi, k \rangle \mid \text{there is a DNF formula } \psi \text{ of size at most } k \text{ s.t. } \varphi \equiv \psi\}$$

What about certificates for membership?

- there exists a formula ψ such that
- for all assignments φ and ψ evaluate to the same

Minimizing Boolean formulas

Let DNF be disjunctive normal form and $\equiv$ denote logic equivalence.

$$\text{MinEqDNF} = \{\langle \varphi, k \rangle \mid \text{there is a DNF formula } \psi \text{ of size at most } k \text{ s.t. } \varphi \equiv \psi\}$$

What about certificates for membership?

- there exists a formula ψ such that
- for all assignments φ and ψ evaluate to the same

What about $\overline{\text{MinEqDNF}}$?

Σ_2^p

Recall the certificate-based definitions of **NP** and **coNP**, where $q : \mathbb{N} \to \mathbb{N}$ is a polynomial, $x \in \{0,1\}^*$ and M is a polynomial-time, det. verifier.

NP $x \in L$ iff $\exists u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

coNP $x \in L$ iff $\forall u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

Σ_2^p

Recall the certificate-based definitions of **NP** and **coNP**, where $q : \mathbb{N} \to \mathbb{N}$ is a polynomial, $x \in \{0,1\}^*$ and M is a polynomial-time, det. verifier.

NP $x \in L$ iff $\exists u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

coNP $x \in L$ iff $\forall u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

ExactIndset and MinEqDNF are in a class defined by

$$x \in L \text{ iff } \exists u \in \{0,1\}^{q(|x|)}.\forall v \in \{0,1\}^{q(|x|)}.\ M(x,u,v) = 1$$

Σ_2^p

Recall the certificate-based definitions of **NP** and **coNP**, where $q : \mathbb{N} \to \mathbb{N}$ is a polynomial, $x \in \{0,1\}^*$ and M is a polynomial-time, det. verifier.

NP $x \in L$ iff $\exists u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

coNP $x \in L$ iff $\forall u \in \{0,1\}^{q(|x|)}.\ M(x,u) = 1$

ExactIndset and MinEqDNF are in a class defined by

$$x \in L \text{ iff } \exists u \in \{0,1\}^{q(|x|)}. \forall v \in \{0,1\}^{q(|x|)}.\ M(x,u,v) = 1$$

This class is called Σ_2^p.

Bounded QBF

Another natural problem within Σ_2^p is QBF with one alternation!

$$\Sigma_2\text{SAT} = \{\exists \vec{u_1} \forall \vec{u_2}.\varphi(\vec{u_1}, \vec{u_2}) \mid \text{formula is true}\}$$

where $\vec{u_i}$ denotes a finite sequence of Boolean variables.

Bounded QBF

Another natural problem within $\mathbf{\Sigma_2^p}$ is QBF with one alternation!

$$\Sigma_2\mathrm{SAT} = \{\exists \vec{u_1} \forall \vec{u_2}.\varphi(\vec{u_1}, \vec{u_2}) \mid \text{formula is true } \}$$

where $\vec{u_i}$ denotes a finite sequence of Boolean variables.

Remarks

- in fact, Σ_2SAT is complete for $\mathbf{\Sigma_2^p}$
- more alternations lead to a whole hierarchy
- all of it is contained in **PSPACE**

Agenda

- ExactIndset, MinEqDNF, and bounded QBF ✓
- Σ_i^p, Π_i^p, and PH
- properties of the polynomial hierarchy
- more examples

Definition

Definition (Polynomial Hierarchy)

For $i \geq 1$, a language $L \subseteq \{0,1\}^*$ is in $\mathbf{\Sigma_i^p}$ if there exists a polynomial-time TM M and a polynomial q such that

$$
\begin{aligned}
& x \in L \\
& \quad \textbf{if and only if} \\
& \exists u_2 \in \{0,1\}^{q(|x|)}. \\
& \forall u_1 \in \{0,1\}^{q(|x|)}. \\
& \ldots \\
& Q_i u_i \in \{0,1\}^{q(|x|)}. \\
& \quad M(x, u_1, u_2, \ldots, u_i) = 1
\end{aligned}
$$

where Q_i is $\exists$ if i is odd and $\forall$ otherwise.

Definition

Definition (Polynomial Hierarchy)

For $i \geq 1$, a language $L \subseteq \{0,1\}^*$ is in $\mathbf{\Sigma_i^p}$ if there exists a polynomial-time TM M and a polynomial q such that

$$x \in L$$

if and only if

$$\exists u_2 \in \{0,1\}^{q(|x|)}.$$
$$\forall u_1 \in \{0,1\}^{q(|x|)}.$$
$$\dots$$
$$Q_i u_i \in \{0,1\}^{q(|x|)}.$$
$$M(x, u_1, u_2, \dots, u_i) = 1$$

where Q_i is $\exists$ if i is odd and $\forall$ otherwise.

- the polynomial hierarchy is the set $\mathbf{PH} = \bigcup_{i \geq 1} \mathbf{\Sigma_i^p}$
- $\mathbf{\Pi_i^p} = \mathbf{co\Sigma_i^p} = \{\overline{L} \mid L \in \mathbf{\Sigma_i^p}\}$

Generalization of NP and coNP

- **NP** $= \Sigma_1^p$ and **coNP** $= \Pi_1^p$

Generalization of NP and coNP

- NP $= \Sigma_1^p$ and coNP $= \Pi_1^p$
- $\Sigma_i^p \subseteq \Pi_{i+1}^p \subseteq \Sigma_{i+2}^p$

Generalization of NP and coNP

- $\mathbf{NP} = \mathbf{\Sigma_1^p}$ and $\mathbf{coNP} = \mathbf{\Pi_1^p}$
- $\mathbf{\Sigma_i^p} \subseteq \mathbf{\Pi_{i+1}^p} \subseteq \mathbf{\Sigma_{i+2}^p}$
- hence $\mathbf{PH} = \bigcup_{i \geq 1} \mathbf{\Pi_i^p}$
- $\mathbf{PH} \subseteq \mathbf{PSPACE}$

Collapse

It is an open problem whether there is an *i* such that $\Sigma_i^p = \Sigma_{i+1}^p$.

Collapse

It is an open problem whether there is an *i* such that $\mathbf{\Sigma_i^p} = \mathbf{\Sigma_{i+1}^p}$.

This would imply that $\mathbf{\Sigma_i^p} = \mathbf{PH}$: the hierarchy collapses to the *i*-th level.

Collapse

It is an open problem whether there is an *i* such that $\Sigma_i^p = \Sigma_{i+1}^p$.

This would imply that $\Sigma_i^p = \mathbf{PH}$: the hierarchy collapses to the *i*-th level.

Most researchers believe that the hierarchy does not collapse.

Collapse

It is an open problem whether there is an i such that $\Sigma_i^p = \Sigma_{i+1}^p$.

This would imply that $\Sigma_i^p = \mathbf{PH}$: the hierarchy collapses to the i-th level.

Most researchers believe that the hierarchy does not collapse.

Theorem (Collapse)

- *For every $i \geq 1$, if $\Sigma_i^p = \Pi_i^p$ then $\mathbf{PH} = \Sigma_i^p$*
- *If $\mathbf{P} = \mathbf{NP}$ then $\mathbf{PH} = \mathbf{P}$, i.e. the hierarchy collapses to $\mathbf{P}$.*

Completeness

For each level of the hierarchy completeness is defined in terms of polynomial Karp reductions.

Completeness

For each level of the hierarchy completeness is defined in terms of polynomial Karp reductions.

- if there exists a **PH**-complete language, then the hierarchy collapses
- **PH** $\neq$ **PSPACE** unless the hierarchy collapses

Completeness

For each level of the hierarchy completeness is defined in terms of polynomial Karp reductions.

- if there exists a **PH**-complete language, then the hierarchy collapses
- **PH** $\neq$ **PSPACE** unless the hierarchy collapses

Theorem (bounded QBF)

For each $i \geq 1$, Σ_iSAT is $\mathbf{\Sigma_i^p}$-complete, where Σ_iSAT is the language of true quantified Boolean formulas of the form

$$\exists \vec{u_1} \forall \vec{u_2} \dots Q_i \vec{u_i} . \varphi(\vec{u_1}, \vec{u_1}, \dots, \vec{u_i})$$

Agenda

- ExactIndset, MinEqDNF, and bounded QBF ✓
- Σ_i^p, Π_i^p, and PH ✓
- properties of the polynomial hierarchy ✓
- more examples

Integer Expressions

An integer expression I is defined by the following BNF for binary numbers $\vec{b}$:

$$I ::= \vec{b} \mid I + I \mid I \cup I$$

The language $\mathcal{L}(I) \subseteq \mathbb{N}$ is defined by

- $\mathcal{L}(\vec{b}) = \{n\}$ where n is the natural number represented by $\vec{b}$
- $\mathcal{L}(I_1 + I_2) = \{n_1 + n_2 \mid n_i \in \mathcal{L}(I_i)\}$
- $\mathcal{L}(I_1 \cup I_2) = \mathcal{L}(I_1) \cup \mathcal{L}(I_2)$

Example: $\mathcal{L}(1 + (2 \cup 3 + 4)) = \{3, 8\}$

A set $M \subseteq \mathbb{N}$ is connected if for all $x, z \in M$ and every $x < y < z$ also $y \in M$.

A component of M is a maximal connected subset of M.

Integer Expressions

- membership of a number in the language of an integer expression: **NP**-complete
- integer expression inequivalence: Σ_2^p-complete
- *Does* $\mathcal{L}(I)$ *have a component of size at least* k?: Σ_3^p-complete

Regular Expressions

Consider regular expressions with union and concatentation only. In addition, we define an interleaving operator on words

$$x_1 x_2 \dots x_k \mid y_1 y_2 \dots y_k$$
$$=$$
$$x_1 y_1 x_2 y_2 \dots x_k y_k$$

where y_i can be strings of arbitrary length.

Regular expression equivalence for star-free expressions with interleaving is Π_2^p-complete.

Context-free languages

Consider context-free grammars defining unary languages.

- $\{\langle G_1, G_2\rangle \mid \mathcal{L}(G_1) \neq \mathcal{L}(G_2)\}$ is $\mathbf{\Sigma_2^p}$-complete
- note that for non-unary languages this problem is undecidable

What have we learnt?

- the polynomial hierarchy is a natural generalization of **NP** and **coNP**
- bounded alternation QBFs are complete problems for each level of the hierarchy
- in the limit – unbounded alternations – the hierarchy approaches **PSPACE**
- the hierarchy is widely believed not to collapse to any level

Up next: time/space tradeoffs, **TISP**(f, g)

Further Reading

- survey on complete problems for various levels of the hierarchy:
  - *Schaefer and Umans* Completeness in the Polynomial-Time Hierarchy — A Compendium
- PH can be equivalently characterized using alternating TMs (see exercise)
  - for a survey on alternation see *Chandra, Kozen, Stockmeyer* Alternation in Journal of the ACM 28(1), 1981.
  - `http://portal.acm.org/citation.cfm?id=322243`