TU Dresden, Fakultät Informatik
Daniel Borchmann

Summer Term 2016

Advanced Topics in Complexity Theory

Exercise 10: The Polynomial Hierarchy and the Complexity of Graph Isomorphism[1]

2016-07-05

The problem of *graph isomorphism* (GI), i.e., deciding whether two graphs are isomorphic, has occurred frequently in our considerations so far. However, the exact complexity of GI is unknown to date. In particular, it is not known whether GI is a problem in P, although recent results suggest that if GI is not in P, then it is not "very far away": GI can be solved in quasi-polynomial time.

On the other hand, it is not believed that GI is NP-complete. The reason for this is that in this case the *polynomial hierarchy* would *collapse* to the second level. Showing this is the purpose of this exercise, for which we shall make use of the existence of a perfect public-coin protocol for GNI.

Let us first recall the definition of the polynomial hierarchy (PH).

Definition 10.1 Inductively define the following complexity classes:

$$\begin{aligned} \Sigma_0^p &:= \Pi_0^p := \mathsf{P}, \\ \Sigma_{i+1}^p &:= \mathsf{NP}^{\Sigma_i^p}, \\ \Pi_{i+1}^p &:= \mathsf{coNP}^{\Sigma_i^p}. \end{aligned}$$

Define the *polynomial hierarchy* by

$$\mathsf{PH} = \bigcup_{i \in \mathbb{N}} \Sigma_i^p. \qquad \diamondsuit$$

Exercise 10.2 Show the following claims

1. $\Sigma_i^p = \mathsf{co}\Pi_i^p$;
2. $\Sigma_i^p \subseteq \Sigma_{i+1}^p$ and $\Pi_i^p \subseteq \Sigma_{i+1}^p$;

for all $i \in \mathbb{N}$.

Various natural problems are known to be complete for some level of the polynomial hierarchy. On of those problems is the following: a propositional formula φ is called *minimal* if every propositional formula that is equivalent to φ is at least as long as φ.

Exercise 10.3 Show that the problem of deciding whether a propositional formula φ is minimal is in Π_2^p.

[1] This exercise is based on Sanjeev Arora and Boaz Barak: *Computational Complexity A Modern Approach*, Cambridge University Press, 2009, Section 8.2.4

The classes Σ_k^p and Π_k^p have natural complete example which arise as "restrictions" of TQBF to some particular form.

Let $k \in \mathbb{N}$. Then a Σ_kQBF-formula is a QBF-formula of the form

$$\exists x_1 \forall x_2 \ldots Q x_k . \varphi(x_1, x_2, \ldots, x_k),$$

where $Q \in \{ \exists, \forall \}$ depending on whether k is odd or even. A Π_kQBF-formula is a QBF-formula of the form

$$\forall x_1 \exists x_2 \ldots Q x_k . \varphi(x_1, x_2, \ldots, x_k),$$

where again $Q \in \{ \exists, \forall \}$ depending on whether k is even or odd.

Theorem 10.4 Let $k \in \mathbb{N}$. Then the problem $\Sigma_k\mathsf{TQBF}$ of deciding the validity of Σ_kQBF-formulas is complete for Σ_k^p. Dually, the problem $\Pi_k\mathsf{TQBF}$ of deciding validity of Π_kQBF-formulas is complete for Π_k^p.

Indeed, this shows that $\mathsf{PH} \subseteq \mathsf{PSpace}$. Additionally, while it is not known whether this inclusion is strict, it is widely believed that it is.

We say that the polynomial hierarchy *collapses* if there exists some $k \in \mathbb{N}$ such that $\mathsf{PH} = \Sigma_k^p$. Since this is not believed to happen, every assumption that results in the collapse of PH is taken as a strong indication against this assumption.

Exercise 10.5 Show that if $\Sigma_k^p = \Pi_k^p$ for some $k \in \mathbb{N}$, then $\mathsf{PH} = \Sigma_k^p$.

Exercise 10.6 Show that if $\mathsf{PH} = \mathsf{PSpace}$, then PH collapses.

We now want to show the main result of this exercise.

Theorem 10.7 If GI is NP-complete, then $\Sigma_2^p = \Pi_2^p$.

To show this, it is clearly sufficient to show $\Sigma_2^p \subseteq \Pi_2^p$, because then $\mathsf{co}\Sigma_2^p \subseteq \mathsf{co}\Pi_2^p$.

Let $\psi = \exists x \in \{ 0, 1 \}^n \forall y \in \{ 0, 1 \}^n . \varphi(x, y)$ be some $\Sigma_2\mathsf{TQBF}$ formula. We want to show that under the assumption of GI being NP-complete, the formula ψ is equivalent to some $\Pi_2\mathsf{TQBF}$ formula. This shows $\Sigma_2^p \subseteq \Pi_2^p$.

Exercise 10.8 Use the NP-completeness of GI to show that there exists a polynomial-time computable function f such that ψ is equivalent to

$$\exists x \in \{ 0, 1 \}^n . (g(x) \in \mathsf{GNI}),$$

where $g(x) = f(\varphi_x)$ and φ_x is the formula φ with the variables x fixed.

By what has been discussed in the lecture, we know $\mathsf{GNI} \in \mathsf{AM}[2]$ with perfect completeness. Using amplification, we can furthermore assume that the soundness of this protocol is *strictly* less than 2^{-n} for inputs of length n. Let V be the verifier of this protocol, and denote with m the length of the random message of the verifier and with m' the length of the response of the prover.

Exercise 10.9 Show that ψ is equivalent to

$$\forall r \in \{0,1\}^m \exists x \in \{0,1\}^n \exists a \in \{0,1\}^{m'}.\big(V(g(x), r, a) = 1\big). \tag{1}$$

Hint: In the case that ψ is false, use the fact that

$$\forall y \in \{0,1\}^n.(g(x) \notin \mathsf{GNI})$$

to derive the existence of some $r \in \{0,1\}^m$ such that for each $x \in \{0,1\}^n$ the prover has no response to cause the verifier to accept $g(x)$ when the random message is r (you may find the proof of $\mathsf{BPP} \subseteq \mathsf{P/poly}$ inspirational here). Conclude that in this case

$$\exists r \in \{0,1\}^m \forall x \in \{0,1\}^n \forall a \in \{0,1\}^{m'}.\big(V(g(x), r, a) = 0\big).$$

Since (1) is a Π_2QBF formula, we have shown that the validity of ψ can be decided in Π_2^p, and thus $\Sigma_2^p \subseteq \Pi_2^p$ as required.