Problem 1: $\Sigma^p_i$-completeness

Let

$$\Sigma_i^{\text{formulaSAT}} := \{ \varphi : \exists u_1 \forall u_2 \exists u_3 \ldots \varphi(u_1, \ldots, u_i) = 1 \}$$

where $\varphi$ is a Boolean circuit with $i$ multi-bit inputs. (In particular, $|u_i| \leq |\varphi|$ for all $i$.)

Show: $\Sigma_i^{\text{formulaSAT}}$ is $\Sigma^p_i$-complete.

Note: You can take the following facts for granted (i.e., you do not need to reprove them): Given a Turing machine $M(x, u_1, \ldots, u_i)$ and given integers $\ell_x, \ell_1, \ldots, \ell_i$ indicating the lengths of the different inputs, one can construct a circuit $\varphi$ in polynomial-time (in $\ell_x + \sum \ell_i$) such that $M(x, u_1, \ldots, u_i) = \varphi(x, u_1, \ldots, u_i)$ for all $x, u_1, \ldots, u_i$ of the specified lengths. Furthermore, given $\varphi$ and inputs for $\varphi$, one can compute the output of $\varphi$ with a polynomial-time TM.

Hint: The problem is easier when you use the alternative definition of $\Sigma^p_i$ (Definition 5.3 in Arora-Barak).

We restate the definition here:

**Definition 1** $L \in \Sigma^p_i$ iff there exists a polynomial-time TM $M$ and a polynomial $q$ such that for all $x$:

$$x \in L \iff \exists u_1 \in \{0, 1\}^{q(|x|)} \forall u_2 \in \{0, 1\}^{q(|x|)} \exists u_3 \in \{0, 1\}^{q(|x|)} \ldots M(x, u_1, \ldots, u_i) = 1$$

**Solution.** Given the “alternative definition”, it is easy to see that $\Sigma_i^{\text{formulaSAT}} \in \Sigma^p_i$ with $q(|x|) := |x|$ (in particular $q(|x|)$ is at least as big as the number of variables in $x$), and $M(x, u_1, \ldots, u_i)$ computing $\varphi(u_1, \ldots, u_i)$ with $\varphi := x$. (The $u_i$ are $q(|x|)$ bits long which is longer than the arguments of $\varphi$. We assume that $M$ just cuts off the superfluous bits when computing $\varphi(u_1, \ldots, u_i)$.) Hence $\Sigma_i^{\text{formulaSAT}} \in \Sigma^p_i$.

It remains to show that $\Sigma_i^{\text{formulaSAT}}$ is $\Sigma^p_i$-hard. Let $L \in \Sigma^p_i$. We to show that $L \leq_p \Sigma_i^{\text{formulaSAT}}$. I.e., we need to construct a polynomial Karp reduction to $\Sigma_i^{\text{formulaSAT}}$. Fix $M$ and $q$ as in [Definition 1]. For any $x$, there is a circuit that emulates $M(x, u_1, \ldots, u_i)$ on inputs $u_1, \ldots, u_i$ of lengths $\ell_1 := q(|x|), \ldots, \ell_i := q(|x|)$. More precisely, there is a polynomial-time computable function $f$ such that $f(x)$ returns a circuit $\varphi$ such that:

$$\forall x \in \{0, 1\}^* \forall u_1 \in \{0, 1\}^{q(|x|)} \ldots \forall u_i \in \{0, 1\}^{q(|x|)} \cdot \phi(u_1, \ldots, u_n) = M(x, u_1, \ldots, u_i)$$
We claim that \( f \) is a Karp reduction from \( L \) to \( \Sigma_i \text{formulaSAT} \). It is polynomial-time computable. And for any \( x \), we have:

\[
x \in L \iff \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \exists u_3 \in \{0,1\}^{q(|x|)} \ldots M(x, u_1, \ldots, u_i) = 1
\]

\[
\iff \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \exists u_3 \in \{0,1\}^{q(|x|)} \ldots \varphi(u_1, \ldots, u_i) = 1
\]

with \( \varphi := f(x) \)

\[
\iff f(x) \in \Sigma_i \text{formulaSAT}.
\]

So \( f \) is a Karp reduction to \( \Sigma_i \text{formulaSAT} \). Hence \( L \leq^p \Sigma_i \text{formulaSAT} \). Since \( L \) was an arbitrary language in \( \Sigma_i^p \), it follows that \( \Sigma_i \text{formulaSAT} \) is \( \Sigma_i^p \)-hard. Since it is in \( \Sigma_i^p \), it is \( \Sigma_i^p \)-complete.

Problem 2: The collapse of the polynomial-hierarchy

(a) Show: If any two of \( \Sigma_1^p, \Sigma_2^p, \ldots, \Pi_1^p, \Pi_2^p, \ldots \) are equal, then the polynomial-hierarchy collapses.

Note: In the practice we already showed that if \( \Sigma_i^p = \Pi_i^p \), the polynomial-hierarchy collapses. (You can use that fact.) But you need to show that the same holds for any other two classes, too. (Also \( \Sigma \)'s with \( \Sigma \)'s, different levels, etc.)

Solution. In the lecture, we proved:

\[
\Sigma_i^p = \Pi_i^p \implies \text{polynomial hierarchy collapses} \tag{2}
\]

Note also that directly from the definitions of the complexity classes, we have that \( \Sigma_i^p \subseteq \Sigma_j^p \) and \( \Pi_i^p \subseteq \Pi_j^p \) if \( i < j \), and \( \Pi_i^p \subseteq \Sigma_{i+1}^p \), and \( \Sigma_i^p \subseteq \Pi_{i+1}^p \).

If \( \Sigma_i^p \subseteq \Pi_i^p \), then \( \Pi_i^p = \text{co-} \Sigma_i^p \subseteq \text{co-} \Pi_i^p = \Sigma_i^p \) and thus \( \Sigma_i^p = \Pi_i^p \). With \( \tag{2} \) this implies:

\[
\Sigma_i^p \subseteq \Pi_i^p \implies \text{polynomial hierarchy collapses} \tag{3}
\]

Analogously (with \( \Sigma \) and \( \Pi \) exchanged), we show

\[
\Pi_i^p \subseteq \Sigma_i^p \implies \text{polynomial hierarchy collapses} \tag{4}
\]

If \( \Sigma_i^p = \Sigma_j^p \) with \( i < j \), then \( \Sigma_j = \Sigma_i \subseteq \Pi_{i+1} \subseteq \Pi_j \), hence \( \Sigma_j \subseteq \Pi_j \). With \( \tag{3} \) this implies

\[
\Sigma_i^p = \Sigma_j^p \text{ with } i < j \implies \text{polynomial hierarchy collapses} \tag{5}
\]

Analogously (with \( \Sigma \) and \( \Pi \) exchanged), we show

\[
\Pi_i^p = \Pi_j^p \text{ with } i < j \implies \text{polynomial hierarchy collapses} \tag{6}
\]

If \( \Sigma_i^p = \Pi_j^p \) with \( i < j \), then \( \Pi_i^p \subseteq \Pi_j^p = \Sigma_i^p \). With \( \tag{4} \) this implies

\[
\Sigma_i^p = \Pi_j^p \text{ with } i < j \implies \text{polynomial hierarchy collapses} \tag{7}
\]
Analogously (with $\Sigma$ and $\Pi$ exchanged), we show

\[ \Pi_i^p = \Sigma_j^p \text{ with } i < j \implies \text{polynomial hierarchy collapses} \quad (8) \]

Equations $(2), (5), (6), (7), (8)$ cover all required cases.

(b) Show: If graph isomorphism is NP-complete, then there is a $PH$-complete language.

**Note:** You may use all facts that were mentioned in the lecture, even those mentioned without proof. Also facts from other problems in this homework. No complex proofs are required for this problem, it follows easily from the right facts.

**Solution.** In the lecture, we learned that: If graph isomorphism is NP-complete, then the polynomial-hierarchy collapses (Section 8.2.4 in Arora-Barak). If the polynomial-hierarchy collapses, $PH = \Sigma_i^p$ for some $i$. From Problem 1 we know that $\Sigma_i^{\text{formulaSAT}}$ is $\Sigma_i^p$-complete. Thus $\Sigma_i^{\text{formulaSAT}}$ is $PH$-complete since $PH = \Sigma_i^p$.
