Martin Ziegler
Carsten Rösnick

Distributed on 2012-02-02
Solutions to be submitted by 2012-02-09 14h25

Complexity Theory

WS 2011/2012, Exercise Sheet #12

EXERCISE 31:
Let $n \in \mathbb{N}$ and $R \subseteq \{0,1\}^n$. "$\oplus : \{0,1\}^2 \to \{0,1\}$" denotes *exclusive* or, that is binary addition modulo 2. For $\vec{x},\vec{u} \in \{0,1\}^n$ write $\vec{x} \oplus \vec{u} := (x_1 \oplus u_1, \ldots, x_n \oplus u_n)$ and $X \oplus \vec{u} := \{\vec{x} \oplus \vec{u} : \vec{x} \in X\}$. For a proposition $A(\vec{u})$ with parameter $\vec{u}$, $\Pr_{\vec{u}}[A(\vec{u})]$ denotes the probability that A becomes `true` for $\vec{u} \in \{0,1\}^n$ chosen uniformly componentwise independently at random.

a) Let $\vec{y} \in \{0,1\}^n$. Prove: $\vec{y} \in R \oplus \vec{u} \Leftrightarrow \vec{u} \oplus \vec{y} \in R \Leftrightarrow \vec{u} \in R \oplus \vec{y}$.

b) $\Pr_{\vec{u}}[\vec{y} \in R \oplus \vec{u}] = \Pr_{\vec{u}}[\vec{u} \in R]$ and $\Pr_{\vec{u},\vec{v}}[\vec{y} \in (R \oplus \vec{u}) \cap (R \oplus \vec{v})] = \Pr_{\vec{u}}[\vec{y} \in R \oplus \vec{u}] \cdot \Pr_{\vec{v}}[\vec{y} \in R \oplus \vec{v}]$.

c) Let $1 \leq n \leq p < 2^n$ and $R \subseteq \{0,1\}^p$ with $\mathrm{Card}(R) \leq 2^{-n} \cdot 2^p$.
Show that no choice of $\vec{t}_1, \ldots \vec{t}_p \in \{0,1\}^p$ satisfies $\{0,1\}^p = \bigcup_{i=1}^{p} (R \oplus \vec{t}_1)$.

EXERCISE 32:

a) Show that the following problem lies in $\mathcal{P}^{\text{CLIQUE}}$, that is, can be decided in polynomial time by a DTM permitted oracle queries to CLIQUE:

Given a graph, does the maximal clique it contains have odd size?

b) Show that the following problem MINCIRCUIT belongs to $\text{co}\mathcal{NP}^{\text{SAT}}$:

Given a circuit $C(X_1, \ldots, X_n)$, there is no strictly smaller one computing the same Boolean function $\{0,1\}^n \to \{0,1\}$.

Hint: Recall Exercise 9j). How to encode the satisfiability of a circuit into a (not too long) formula?

c) Fix $\ell \in \mathbb{N}$. Prove that the following problem lies in $\mathcal{P}^{\text{SAT}}$. Does it belong to $\mathcal{NP}$? to $\text{co}\mathcal{NP}$?

Given a Boolean function φ, can a circuit with at most ℓ gates compute φ?

d) Let $\mathcal{B}, \mathcal{C} \supseteq \mathcal{P}$ denote classes of languages closed under polynomial-time reduction and suppose C is $\mathcal{C}$–complete. Then $\mathcal{B}^{\mathcal{C}} = \mathcal{B}^{C}$.

e) Prove $\mathcal{NP} \cup \text{co}\mathcal{NP} \subseteq \mathcal{P}^{\mathcal{NP}}$.

f) If $\mathcal{NP} \cup \text{co}\mathcal{NP} = \mathcal{P}^{\mathcal{NP}}$, then $\mathcal{NP} = \text{co}\mathcal{NP}$.
Hint: Recall Exercise 15) and consider $L := (\{0\} \times A) \cup (\{1\} \times A^{\complement})$ with $\mathcal{NP}$–complete $A \notin \text{co}\mathcal{NP}$.

EXERCISE 33:
For $k \in \mathbb{N}$, class $\Sigma_k^{\mathcal{P}}$ is defined to consist of all problems of the form

$$\big\{\vec{x} \in \{0,1\}^n : n \in \mathbb{N},\ \exists \vec{y}_1 \in \{0,1\}^{\leq p(n)}\ \forall \vec{y}_2 \in \{0,1\}^{\leq p(n)}\ \exists \vec{y}_3 \in \{0,1\}^{\leq p(n)} \\ \cdots Q_k \vec{y}_k \in \{0,1\}^{\leq p(n)} : \langle \vec{x}, \vec{y}_1, \ldots, \vec{y}_k \rangle \in R\big\}$$

with $R \in \mathcal{P}$ and $p \in \mathbb{N}[N]$. Here Q_k means $'\forall'$ in case k is even, $Q_k = '\exists'$ if odd.

a) Prove: $\Sigma_1^{\mathcal{P}} = \mathcal{NP}$ and $\Sigma_k^{\mathcal{P}} \subseteq \mathcal{NP}^{\mathcal{NP}^{\cdot^{\cdot^{\cdot^{\mathcal{NP}}}}}}$ (tower of height k) and $\Sigma_k^{\mathcal{P}} \subseteq \mathsf{PSPACE}$.

b) For $A, B \in \Sigma_k^{\mathcal{P}}$, it holds $A \cap B, A \cup B \in \Sigma_k^{\mathcal{P}}$.

c) For $L \in \Sigma_k^{\mathcal{P}}$ and $q \in \mathbb{N}[N]$, it holds $\big\{\vec{x} : \exists \vec{y} \in \{0,1\}^{\leq q(|\vec{x}|)} : \langle \vec{x}, \vec{y} \rangle \in L\big\} \in \Sigma_k^{\mathcal{P}}$.

d) For $L \in \Sigma_k^{\mathcal{P}}$ and $q \in \mathbb{N}[N]$, it holds $\big\{\vec{x} : \forall y \leq q(|\vec{x}|) : \langle \vec{x}, y \rangle \in L\big\} \in \Sigma_k^{\mathcal{P}}$.

e) What about $\big\{\vec{x} : \forall \vec{y} \in \{0,1\}^{\leq q(|\vec{x}|)} : \langle \vec{x}, \vec{y} \rangle \in L\big\}$?

f) How will (would) the polynomial hierarchy look like in case $\mathcal{P} \neq \mathcal{NP} = \text{co}\mathcal{NP}$?
Draw and justify. How about the case $\Delta_2^{\mathcal{P}} \neq \Sigma_2^{\mathcal{P}} = \Pi_2^{\mathcal{P}}$?