TU Dresden, Fakultät Informatik
Daniel Borchmann

Summer Term 2016

Advanced Topics in Complexity Theory

Exercise 7: Interactive Proofs

2016-06-07

Exercise 7.1 Show that the problem GNI of checking whether two labeled graphs on n vertices are *not* isomorphic is in IP.

Exercise 7.2 Let $n \in \mathbb{N}$. Call an integer $s \in \mathbb{Z}_n$ a *quadratic residue* modulo n if there exists some $r \in \mathbb{Z}_n$ such that $s \equiv r^2 \pmod{n}$. The problem of checking whether an element of $\mathbb{Z}_n$ is a quadratic residue modulo n is clearly in NP. It is unknown whether this problem is also a member of coNP.

The task is to show that the problem QNR of deciding whether an element of $\mathbb{Z}_n$ is *not* a quadratic residue modulo n is in IP. Consider the following protocol:

- Input: an integer $n \in \mathbb{N}$ and some $s \in \mathbb{Z}_n$.
- The verifier picks a random $b \in \{ 0, 1 \}$ and some random $x \in \mathbb{Z}_n^*$ (the set of all numbers in $\mathbb{Z}_n$ coprime to n).
  - If $b = 0$, send $y = x^2 \pmod{n}$ to the prover.
  - If $b = 1$, send $y = s \cdot x^2 \pmod{n}$ to the prover.
- Accept if the prover returns some $\ell \in \{ 0, 1 \}$ such that $\ell = b$.

Show that this is an interactive protocol for QNR.

Exercise 7.3 Show the following claims from the lecture: let V be a probabilistic verifier and let M_j be a message history of length j.

1. If j is even, i.e., the verifier sends the next message, then

$$\max_P \Pr\big(\mathrm{out}_V\langle V, P\rangle(w, M_j) = 1\big) = \sum_{m_{j+1}} \Pr_r\big(V(w, r, M_j) = m_{j+1}\big) \cdot \max_P \Pr\big(\mathrm{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1\big).$$

2. If j is odd, i.e., the prover sends the next message, then

$$\max_{m_{j+1}} \max_P \Pr\big(\mathrm{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1\big) = \max_P \Pr\big(\mathrm{out}_V\langle V, P\rangle(w, M_j) = 1\big).$$

Solution For the first claim, it is readily verified that

$$\begin{aligned}
&\max_P \Pr(\text{out}_V\langle V, P\rangle(w, M_j) = 1) \\
&= \max_P \Pr_r(\text{out}_V\langle V, P\rangle(w, r, M_j) = 1) \\
&= \max_P \sum_{m_{j+1}} \Pr_r(V(w, r, M_j) = m_{j+1}) \cdot \Pr(\text{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1) \\
&\leq \sum_{m_{j+1}} \Pr_r(V(w, r, M_j) = m_{j+1}) \cdot \max_P \Pr(\text{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1).
\end{aligned}$$

Furthermore, if $P_{m_1}, \ldots, P_{m_\ell}$ are provers maximizing all the summands, then the prover P that on receiving message history (M_j, m_{j+1}) just calls the corresponding prover $P_{m_{j+1}}$ shows that equality holds true.

For the second equation, the main idea to show this to notice that since the prover sends the message m_{j+1} we have

$$\Pr(\text{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1) \leq \Pr(\text{out}_V\langle V, P\rangle(w, M_j) = 1).$$

Indeed, if $P(w, M_j) = m_{j+1}$ we have equality, and otherwise the left hand side is just 0.

Now choose a prover Q such that

$$\max_P \Pr\big(\text{out}_V\langle V, P\rangle(w, M_j) = 1\big) = \Pr(\text{out}_V\langle V, Q\rangle(w, M_j) = 1) \tag{1}$$

and suppose $Q(w, M_j)$ and Q do not maximize the left hand side of the claim. Then there exists some prover Q' and some message m' such that

$$\Pr(\text{out}_V\langle V, Q\rangle(w, (M_j, Q(w, M_j))) = 1) < \Pr(\text{out}_V\langle V, Q'\rangle(w, (M_j, m')) = 1).$$

Thus

$$\begin{aligned}
\Pr(\text{out}_V\langle V, Q\rangle(w, (M_j, Q(w, M_j))) = 1) &< \Pr(\text{out}_V\langle V, Q'\rangle(w, (M_j, m')) = 1) \\
&\leq \Pr(\text{out}_V\langle V, Q'\rangle(w, M_j) = 1) \\
&\leq \max_P \Pr(\langle V, P\rangle(w, M_j) = 1),
\end{aligned}$$

contradicting our assumption (1). Thus

$$\begin{aligned}
\max_P \Pr(\text{out}_V\langle V, P\rangle(w, M_j) = 1) &= \Pr(\text{out}_V\langle V, Q\rangle(w, M_j) = 1) \\
&= \Pr(\text{out}_V\langle V, Q\rangle(w, (M_j, Q(w, M_j))) = 1) \\
&= \max_{m_{j+1}} \max_P \Pr(\text{out}_V\langle V, P\rangle(w, (M_j, m_{j+1})) = 1).
\end{aligned}$$

□

Exercise 7.4 Let $s \in \mathbb{N}$. Show that if we replace in the definition of IP the completeness parameter by $1 - 2^{-n^s}$ and the soundness parameter by 2^{-n^s}, then the resulting class will again be IP.

The main idea is to repeat the original protocol a suitable number of times and to take the majority of the outcomes as the outcome of the repetitions. To show that the resulting completeness and soundness parameters are indeed as required, use the following weaker version of the so called *Chernoff Bounds*: let $X_1, X_2, \ldots, X_n$ be independent variables over $\{ 0, 1 \}$ and let $\mu = \mathrm{E}(\sum_{i=1}^{n} X_i)$. Then for each δ we have

$$\Pr\Big(\sum_{i=1}^{n} X_i \geq (1+\delta)\mu\Big) \leq e^{-\delta^2\mu},$$
$$\Pr\Big(\sum_{i=1}^{n} X_i \leq (1-\delta)\mu\Big) \leq e^{-\delta^2\mu}.$$

Solution Let $L \in \mathsf{IP}$, let V be some probabilistic verifier for L, let P be some optimal prover for V, and let $w \in \Sigma^*$. Let n be the number of iterations. Define for $i \in \{ i, \ldots, n \}$ the random variable X_i by

$$X_i(r) \coloneqq \begin{cases} 1 & \mathrm{out}_V\langle V, P\rangle(w, r) = 1, \\ 0 & \mathrm{out}_V\langle V, P\rangle(w, r) = 0. \end{cases}$$

for randomly chosen r. If $w \in L$, then $\Pr(X_i = 1) \geq 2/3$, and if $w \notin L$, then $\Pr(X_i = 1) \leq 1/3$.

Consider first the case $x \in L$. Then $\mathrm{E}(X_i) \geq 2/3$ for all i, and in particular $\mu \coloneqq \mathrm{E}(\sum_{i=1}^{n} X_i) \geq 2/3$. The probability that our majority approach returns the *wrong* answer is then

$$\Pr\Big(\sum_{i=1}^{n} X_i \leq \frac{n}{2} - 1\Big).$$

From Chernoff's bound we obtain

$$\Pr(\sum_{i=1}^{n} X_i \leq (1-\delta)\mu) \leq e^{-\delta^2\mu},$$

where $(1-\delta)\mu = \frac{n}{2} - 1$, i.e., $\delta = \frac{1}{\mu}(1 - \frac{n}{2}) + 1$. Because $\mu \geq \frac{2}{3}n$, we obtain $\delta \geq \frac{1}{4} + \frac{3}{2n}$, and thus

$$e^{-\delta^2\mu} \leq e^{-\frac{2}{3}n(\frac{1}{4}+\frac{3}{2n})} = e^{-\frac{1}{6}n-1} \leq e^{-\frac{1}{6}n}.$$

If $x \notin L$, then $0 \leq \mu \leq 1/3$. Applying Chernoff's bound

$$\Pr\Big(\sum_{i=1}^{n} X_i \geq (1+\delta)\mu\Big) \leq e^{-\delta^2\mu},$$

we obtain that the error probability in this case is bounded by $e^{-\delta^2\mu}$ for $(1+\delta)\mu = n/2$, i.e., $\delta = n/(2\mu) - 1$. Because of $\mu \leq 1/3n$, we have $\delta \geq 1/2$, and thus

$$e^{-\delta^2\mu} = e^{-\frac{2}{3}n\cdot\frac{1}{2}} = e^{-\frac{n}{3}}.$$

In summary, in both cases we can decrease the error probability exponentially with a polynomial number of iterations. This shows the claim. □