1 IP and perfect soundness

Let $\text{IP}'$ be the class of languages that have interactive proofs with perfect soundness and perfect completeness (i.e., in the definition of $\text{IP}$, we replace $2/3$ by $1$ and $1/3$ by $0$).

Show that $\text{IP}' \subseteq \text{NP}$.

You get bonus points if you only use the perfect soundness (not the perfect completeness).

Note: In the practice we will show that $\text{dIP} = \text{NP}$ where $\text{dIP}$ is the class of languages that has interactive proofs with deterministic verifiers. You may use that fact.

Hint: What happens if we replace the proof system by one where the verifier always uses $0$ bits as its randomness? (More precisely, whenever $V$ would use a random bit $b$, the modified verifier $V_0$ choses $b = 0$ instead.) Does the resulting proof system still have perfect soundness? Does it still have perfect completeness?

Solution. Let $L \in \text{IP}'$. We want to show that $L \in \text{NP}$. Since $\text{dIP} = \text{NP}$, it is sufficient to show that $L \in \text{dIP}$. I.e., we need to show that there is an interactive proof for $L$ with a deterministic verifier.

Since $L \in \text{IP}'$, there is an interactive proof $(P, V)$ for $L$ with perfect soundness and completeness. Let $V_0$ be the verifier that behaves like $V$, but whenever $V$ uses a random bit, $V_0$ uses $0$. Note that $V_0$ is deterministic.

We show that $(P, V_0)$ still has perfect soundness and completeness. Let $x \in L$. Then $\Pr[\langle \text{out}_V \langle V, P \rangle(x) = 1 \rangle] = 1$. That means, for any randomness $r$ that the verifier uses, its output is $1$. In particular, for $r = 0$. Thus $\Pr[\text{out}_V \langle V_0, P \rangle(x) = 1] = 1$. Thus $(P, V_0)$ has perfect completeness.

Let $x \notin L$. Then $\Pr[\langle \text{out}_V \langle V, P \rangle(x) = 0 \rangle] = 1$. That means, for any randomness $r$ that the verifier uses, its output is $0$. In particular, for $r = 0$. Thus $\Pr[\text{out}_V \langle V_0, P \rangle(x) = 0] = 1$. Thus $(P, V_0)$ has perfect soundness.

Thus $(P, V_0)$ is an interactive proof for $L$ with deterministic $V_0$. Hence $L \in \text{dIP} = \text{NP}$. Hence $L \in \text{NP}$.

If we want to show the same result without requiring perfect completeness, we proceed as follows: Let $(P, V)$ be an interactive proof for $L$ as before. Since $(P, V)$ has completeness, for any $x \in L$, we have $\Pr[\langle \text{out}_V \langle V, P \rangle(x) = 1 \rangle] > 0$. That implies that there exists a sequence of messages $m_1^x, \ldots, m_k^x$ and a sequence of random bits $r^x$ such that $V$, when running with random bits $r^x$, and receiving messages $m_1^x, \ldots, m_k^x$, returns $1$. 
Let \( P' \) be the prover that sends \( r^x, m^x_1, \ldots, m^x_k \). Let \( V' \) be the verifier that in the first round receives \( r \) and then behaves like \( V \) with randomness \( r \) for the remaining \( k \) rounds. Note that \( V' \) is deterministic.

\((P', V')\) has perfect completeness: By construction, the messages \( r^x, m^x_1, \ldots, m^x_k \) sent by \( P' \) make \( V' \) accept.

\((P', V')\) has perfect soundness: If \( x \not\in L \), then \( \Pr[\text{out}_V(V', P^*)(x) = 0] = 1 \). That means, for any randomness \( r \) that the verifier \( V' \) uses, its output is 0. When \( V \) is run with the randomness \( r \) that \( V' \) receives (no matter which randomness the malicious prover \( P^* \) sends). Thus \( \Pr[\text{out}_V(V', P^*)(x) = 0] = 1 \). Thus \((P, V')\) has perfect soundness.

Hence we have an interactive proof \((P', V')\) for \( L \) with deterministic \( V' \). Thus \( L \in \text{dIP} = \text{NP} \).

2 Interactive proof for invertible matrices

Let

\[ L := \{(M, p) : M \text{ is an invertible } n \times n \text{ matrix over } \text{GF}(p)\} \]

That is \((M, p) \in L \) if \( M \) is a square matrix and there exists a matrix \( M^{-1} \) such that \( MM^{-1} = I \mod p \). (\( I \) denotes the identity matrix.)

Some useful facts:

- The best known algorithm for matrix multiplication uses \( \Omega(n^{2.3728639\ldots}) \) arithmetic operations over \( \text{GF}(p) \) for \( n \times n \) matrices.
- To the best of my knowledge, the fastest algorithm for deciding whether a matrix is invertible runs in deterministic polynomial-time but also runs uses \( \Omega(n^{2.3728639\ldots}) \) arithmetic operations over \( \text{GF}(p) \).
- Multiplying an \( n \times n \) matrix with an \( n \)-dimensional vector takes \( O(n^2) \) operations over \( \text{GF}(p) \). (To compute \( y = Mx \), simply compute \( y_i = \sum_j M_{ij}x_j \) for all \( i \).)

(a) Design a 0-round interactive proof for \( L \) with perfect completeness and perfect soundness.

Note: “0-round” is not a typo.

Solution. Our 0-round protocol has no interaction. On input \((M, p)\), the verifier \( V \) decides whether there is an inverse of \( M \) over \( \text{GF}(p) \) (there is a deterministic polynomial-time algorithm for that). If so, \( V \) outputs \( \text{out}_V := 1 \) else \( \text{out}_V := 0 \). (If \( M \) is not a square matrix over \( \text{GF}(p) \), \( V \) also outputs 0.)

If \((M, p) \in L \), then \( M \) is invertible. So \( V \) will output 1 with probability 1, hence we have perfect completeness.

If \((M, p) \notin L \), then \( M \) is not invertible. So \( V \) will output 1 with probability 0, hence we have perfect soundness. (This holds for any prover \( P^* \), because the verifier does not even interact with \( P^* \).)

(In fact, reasoning along the same lines shows that \( \text{IP}[0] = \text{BPP} \).)
(b) Design a 2-round interactive proof for $L$ with perfect completeness and with soundness $1/p$ where the verifier $V$ makes only $O(n^2)$ arithmetic operations and where each message consists only of $n$ elements of $GF(p)$. (I.e., the communication complexity is $O(n \log p)$.) Prove the completeness of the interactive proof.

**Note:** The solution from (a) does not work here because the verifier takes more than $O(n^2)$ operations. Also, a natural proof would be for the prover to just send $M^{-1}$, and the verifier checks whether $M^{-1}M = I$. But that takes $\Omega(n^2)$ operations.

**Hint:** If $M$ is not invertible, for any $x$, how many $x'$ with $Mx = Mx'$ are there? And be inspired (but not too closely) by the graph non-isomorphism proof.

**Solution.** The interactive proof $(P,V)$ is the following:

- The verifier $V$ picks a uniformly random $x \in GF(p)^n$ and sends $y := Mx$. (Computing $y$ takes $O(n^2)$ operations.)
- The (honest) prover $P$ returns $x' := M^{-1}y$.
- $V$ checks whether $M$ is indeed a square matrix over $GF(p)$ and whether $x = x'$.

If so $V$ accepts (outputs 1).

This interactive proof has perfect completeness: If $M$ is invertible, $M^{-1}M = I$, hence $x' = M^{-1}y = M^{-1}Mx = Ix = x$. Thus the verifier accepts with probability 1.

(c) Show that the protocol from (b) has soundness $1/p$.

**Hint:** What is the size of the kernel of $M$? Show that this implies that there are at least $p$ different values $x'$ with $Mx = Mx'$?

**Solution.** To show soundness $1/p$, we need to show that if $\langle M, p \rangle \notin L$, then the verifier accepts with probability at most $1/p$, for any prover $P^*$. Thus, assume that $\langle M, p \rangle \notin L$. That is, $M$ is not invertible over $p$. Let $\ker M$ denote the kernel of $M$. Since $M$ is not invertible, $\ker M \neq \{0\}$. Since $\ker M$ is a vector space over $GF(p)$, its size is a power of $p$. Hence $t := |\ker M| \geq p$.

Hence, for any $y \in GF(p)^n$, there are exactly $t$ vectors $x$ with $y = Mx$. Since $x$ is chosen uniformly random by $V$, each of those $x$ with $y = Mx$ has probability $1/t$ of being the one chosen by $V$, given that $V$ sends $y$. Thus, the prover guesses $x$ with probability at most $1/t$. Hence the verifier accepts with probability at most $1/t \leq 1/p$. 