1 IP and perfect soundness

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

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

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

Note: In the practice we will show that $\mathbf{dIP} = \mathbf{NP}$ where $\mathbf{dIP}$ 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 $V_0$ chooses $b = 0$ instead.) Does the resulting proof system still have perfect soundness? Does it still have perfect completeness?

2 Interactive proof for invertible matrices

Let

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

That is $(M, p) \in L$ iff $M$ 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 $GF(p)$ 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 $GF(p)$.
- Multiplying an $n \times n$ matrix with an $n$-dimensional vector takes $O(n^2)$ operations over $GF(p)$. (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.
(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 $\Omega(n^{2.3728639\ldots})$ 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.

(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 $Mx = Mx'$?