Solutions to Homework 4

Interactive Proofs and the Class IP

Recall from class that the function $f : \{0,1\}^* \to \{0,1\}$ is in $\mathsf{IP}[k]$ if there exists a polynomial time PTM V (the *verifier*), a (possibly randomized) function $\mathsf{P} : \{0,1\}^* \to \{0,1\}^*$ (the *prover*) and a $k-$round interactive protocol between P and V, denoted $\langle \mathsf{P}, \mathsf{V} \rangle$ such that for all $\mathbf{x} \in \{0,1\}^*$:

- **Completeness:** if $f(\mathbf{x}) = 1$ then $\Pr\big[\langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x}) = 1\big] \geq 2/3$;
- **Soundness:** if $f(\mathbf{x}) = 0$ then for all $\mathsf{P}^* : \{0,1\}^* \to \{0,1\}^*$, $\Pr\big[\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x}) = 0\big] \geq 2/3$ (P^* denotes an adversarial prover function which might deviate from the protocol specifications).

Here, $\langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x})$ denotes the output bit of V after the protocol is run on input $\mathbf{x}$. Recall that the complexity class IP is $\bigcup_{c \geq 1} \mathsf{IP}[n^c]$, the set of functions which can be computed by an interactive proof system with a polynomial number of rounds. Recall from class that we showed that any $f : \{0,1\}^* \to \{0,1\}$ which can be computed by an interactive proof system with a deterministic verifier must be in NP. Thus, it is critical for the definition of IP that V be probabilistic. In this first exercise, we will understand a bit about what can be said about the prover.

$\mathsf{IP} \subset \mathsf{PSPACE}$

In this section, suppose $f : \{0,1\}^* \to \{0,1\}$ can be computed by a $3-$round interactive proof system $\langle \mathsf{P}, \mathsf{V} \rangle$, where P the first and third message, V sends the second. Let $\mathsf{P}_1, \mathsf{P}_3 : \{0,1\}^* \to \{0,1\}^*$ denote the prover's function for determining its first and third round messages, respectively. So syntactically, the bit $\langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x})$ is computed as follows:

- P sends $\mathbf{a}_1$ to V where $\mathbf{a}_1 \sim \mathsf{P}_1(\mathbf{x})$;
- V sends $\mathbf{a}_2$ to P where $\mathbf{a}_2 \sim \mathsf{V}_2(\mathbf{x}, \mathbf{a}_1)$;
- P sends $\mathbf{a}_3$ to V where $\mathbf{a}_3 \sim \mathsf{P}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$;
- V outputs $b \in \{0,1\}$ where $b = \mathsf{V}_{\mathsf{out}}(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$.

Now, define the functions $\mathsf{val}_0, \mathsf{val}_1, \mathsf{val}_2, \mathsf{val}_3 : \{0,1\}^* \to \mathbb{R}$ to be the expected values of the output bit b, given the protocol so far. So specifically,

- $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = \mathsf{V}_{\mathsf{out}}(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) \in \{0,1\}$;
- $\mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2) = \mathbb{E}_{\mathbf{a}_3 \sim \mathsf{P}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)}\big[\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)\big]$;

- $\mathsf{val}_1(\mathbf{x}, \mathbf{a}_1) = \mathbb{E}_{\mathbf{a}_2 \sim \mathsf{V}_2(\mathbf{x}, \mathbf{a}_1)}\big[\mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)\big]$;
- $\mathsf{val}_0(\mathbf{x}) = \mathbb{E}_{\mathbf{a}_1 \sim \mathsf{P}_1(\mathbf{x})}\big[\mathsf{val}_1(\mathbf{x}, \mathbf{a}_1)\big]$;

Note that $\mathsf{val}_0(\mathbf{x}) = \Pr\big[\langle \mathsf{P}, \mathsf{V}\rangle(\mathbf{x}) = 1\big]$.

Problem 1. Define another, deterministic prover P' where $\mathsf{P}'_1, \mathsf{P}'_3 : \{0,1\}^* \to \{0,1\}^*$ work as follows:

- $\mathsf{P}'_1(\mathbf{x})$ outputs $\mathbf{a}_1$ such that $\mathsf{val}_1(\mathbf{x}, \mathbf{a}_1)$ is optimal (breaking ties arbitrarily);
- $\mathsf{P}'_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$ outputs $\mathbf{a}_3$ such that $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ is optimal (breaking ties arbitrarily). For $i = 0, 1, 2, 3$, define val'_i analogously to val_i except with the new prover P' replacing the old prover P.

(a) Prove that $\mathsf{val}'_0(\mathbf{x}) \geq \mathsf{val}_0(\mathbf{x})$ for all $\mathbf{x} \in \{0,1\}^*$. Deduce that the new protocol satisfies the completeness property; namely, deduce that when $f(\mathbf{x}) = 1$, $\Pr\big[\langle \mathsf{P}', \mathsf{V}\rangle(\mathbf{x}) = 1\big] \geq 2/3$.

Solution. Note $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = \mathsf{val}'_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$, by definition. Next, note $\mathsf{val}'_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2) \geq \mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$ holds for all $(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$ since P' outputs $\mathbf{a}_3$ which maximizes $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$. Next, for all $(\mathbf{x}, \mathbf{a}_1)$,

$$\mathsf{val}'_1(\mathbf{x}, \mathbf{a}_1) = \mathbb{E}_{\mathbf{a}_2}\big[\mathsf{val}'_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)\big] \geq \mathbb{E}_{\mathbf{a}_2}\big[\mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)\big] = \mathsf{val}_1(\mathbf{x}, \mathbf{a}_1).$$

Finally, $\mathsf{val}'_0(\mathbf{x}) \geq \mathsf{val}_0(\mathbf{x})$ since, again P' outputs $\mathbf{a}_1$ which maximizes $\mathsf{val}'_1(\mathbf{x}, \mathbf{a}_1)$. Thus, when $f(\mathbf{x}) = 1$, $\mathsf{val}'_0(\mathbf{x}) \geq \mathsf{val}_0(\mathbf{x}) \geq 2/3$, so completeness holds for $\langle \mathsf{P}', \mathsf{V}\rangle$.

(b) Prove that if $f(\mathbf{x}) = 0$, then $\Pr\big[\langle \mathsf{P}^*, \mathsf{V}\rangle(\mathbf{x}) = 0\big] \geq 2/3$ for all P^*.

Solution. Consider some cheating prover P^* playing instead of P'. Note, P^* could just as easily be thought of as a cheating prover playing in place of P. Thus, by soundness of $\langle \mathsf{P}, \mathsf{V}\rangle$, if $f(\mathbf{x}) = 0$, then $\Pr\big[\langle \mathsf{P}^*, \mathsf{V}\rangle(\mathbf{x}) = 1\big] \leq 1/3$, and so soundness holds for $\langle \mathsf{P}', \mathsf{V}\rangle$ as well.

(c) Now prove that the functions P'_3 and P'_1 can be computed by a polynomial space TM.

Solution. Note P'_3 takes input $(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$ and outputs $\mathbf{a}_3$ such that $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ is maximized. Since $\mathsf{val}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ just outputs the bit $\mathsf{V}(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$, P' can find an optimal $\mathbf{a}_3$ by searching over all possible $\mathbf{a}_3$ and, for each one, checking whether $\mathsf{V}(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = 1$ or not. This can be done in polynomial space since the space used to compute $\mathsf{V}(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ can be reused. Thus P'_3 can be computed in polynomial space.

Next, recall that $\mathsf{P}'_1(\mathbf{x})$ outputs $\mathbf{a}_1$ such that $\mathbb{E}_{\mathbf{a}_2 \sim \mathsf{V}_2(\mathbf{x}, \mathbf{a}_1)}\big[\mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)\big]$ is maximized. This again can be done in polynomial space by iterating over all $\mathbf{a}_1$ and, for each, iterating over $\mathbf{a}_2$ to compute the quantity $\mathbb{E}_{\mathbf{a}_2 \sim \mathsf{V}_2(\mathbf{x}, \mathbf{a}_1)}\big[\mathsf{val}_2(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)\big]$. Then P'_1 just picks $\mathbf{a}_1$ such that this value is optimal. The space for these computations can be reused. Thus, both messages of P' can be computed in polynomial space.

(d) Deduce that any $f \in \mathsf{IP}[3]$ can be computed by an interactive proof system where P is implemented by a deterministic, polynomial space TM. Since V is a polynomial time PTM, and the computation of any polynomial time PTM can be also computed by a deterministic polynomial space TM, this implies that $\mathsf{IP}[3] \subset \mathsf{PSPACE}$. This holds more generally for protocols with more rounds; we focused on 3−round protocols for simplicity only. Thus, we have shown that $\mathsf{IP} \subset \mathsf{PSPACE}$!

Solution. So f can be compute by an interacitve proof system $\langle \mathsf{P}', \mathsf{V} \rangle$ where both P' and V are polynomial space macines. Thus, $f \in \mathsf{PSPACE}$.

The Soda-Pop Protocol for Graph Non-Isomorphism

Recall the function $f_{\mathsf{GNI}} : \{0,1\}^* \to \{0,1\}$ takes two graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ with the same vertices as input, and outputs 1 if there is no permutation $\pi : V \to V$ such that $E_2 = \pi(E_1)$, and outputs 0 otherwise. We mentioned in class that f_{GNI} is the complement of the graph isomorphism function $f_{\mathsf{GI}} : \{0,1\}^* \to \{0,1\}$ which takes graphs G_1 and G_2 and outputs 1 if $E_2 = \pi(E_1)$ for some permutation $\pi : V \to V$, and outputs 0 otherwise. Recall that f_{GNI} being the complement of f_{GI} means that $f_{\mathsf{GNI}} = 1 - f_{\mathsf{GI}}$. It is clear that $f_{\mathsf{GI}} \in \mathsf{NP}$ (since the permutation is the witness), and so $f_{\mathsf{GNI}} \in \mathsf{coNP}$. It is difficult to even imagine how to efficiently compute functions in coNP, since rather than having to find a single permutation such that $E_2 = \pi(E_1)$, you have to establish that $E_2 \neq \pi(E_1)$ holds for all permutations π. There doesn't seem to be clear way to certify this type of thing so that an efficient machine can validate it. Nevertheless, in class we saw that f_{GNI} can be computed by a simple 2−round interactive proof system. Recall this was the proof system $\langle \mathsf{P}, \mathsf{V} \rangle$:

Input: Both P and V get $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ as input.

1. V draws $c \sim \{1, 2\}$ and a random permutation $\pi \sim \mathsf{Perm}(V)$ (the set of permutations $V \to V$), and sends H to P where $H = \big(V, \pi(E_c)\big)$.

2. P returns $c' \in \{1, 2\}$ to V.

Output: V outputs 1 if $c' = c$, and outputs 0 otherwise.

In the protocol description above, we are being intentionally vague about how P computes its second message. This is because we are getting ready to prove soundness, and when proving soundness P^* is adversarial and so will deviate from the protocol specs anyway. However, to be formal, the honest P will output $c' \in \{1, 2\}$ such that H is isomorphic to $G_{c'}$. Note that when $f_{\mathsf{GNI}}(G_1, G_2) = 1$, H can be isomorphic to at most one of the G_i (since if H were isomorphic to both, then G_1 would be isomorphic to G_2 and so $f_{\mathsf{GNI}}(G_1, G_2)$ would equal 0). The following exercise will walk you through the proof of soundness of this protocol.

Problem 2. Let $\mathsf{P}^* : \{0,1\}^* \to \{0,1\}^*$ be an arbitrary adversarial prover, so specifically P^* takes a graph H as input and outputs $c' \in \{1, 2\}$. Define the sets S_1 and S_2 to be the set of H's that make P^* output 1 and 2, respectively. Assume that $f_{\mathsf{GNI}}(G_1, G_2) = 0$. Prove that for both $c' \in \{1, 2\}$,

$$\Pr_{\pi \sim \mathsf{Perm}(V)}\big[H \in S_{c'} \big| c = 1\big] = \Pr_{\pi \sim \mathsf{Perm}(V)}\big[H \in S_{c'} \big| c = 2\big].$$

You may assume that for all distinct $\pi, \pi' \in \mathsf{Perm}(V)$, the permuted graphs $\big(V, \pi(E_1)\big)$ and $\big(V, \pi'(E_1)\big)$ are different (thus $\big(V, \pi(E_2)\big)$ and $\big(V, \pi'(E_2)\big)$ are also different, since G_1 and G_2 are isomorphic). Deduce that when $f_{\mathsf{GNI}}(G_1, G_2) = 0$, $\Pr\big[\langle \mathsf{P}^*, \mathsf{V} \rangle(G_1, G_2) = 1\big] \leq 1/2$. This proves soundness since this probability can be amplified by repetition to be less than $1/3$.

Solution. Suppose $G_1 \simeq G_2$, so that $f_{\mathsf{GNI}}(G_1, G_2) = 0$. The key point is that the verifier's message H is independent of the choice bit c. This is because H is a random graph which is isomorphic to G_c, but since $G_1 \simeq G_2$, being isomorphic to G_1 and being isomorphic to G_2 are equivalent conditions. So specifically, let us define the random variable $\mathcal{H}_c$ to be the random process which draws a random graph H isomorphic to G_c and outputs H. Then $\mathcal{H}_1 \equiv \mathcal{H}_2$, and so for any set S, $\Pr_{H\sim\mathcal{H}_1}\big[H \in S\big] = \Pr_{H\sim\mathcal{H}_2}\big[H \in S\big]$. So if S_1 and S_2 are the sets on which P^* returns $c' = 1$ and $c' = 2$, respectively, then $\Pr_{H\sim\mathcal{H}_1}\big[H \in S_{c'}\big] = \Pr_{H\sim\mathcal{H}_2}\big[H \in S_{c'}\big]$. Thus,

$$\begin{aligned}
\Pr\big[\langle \mathsf{P}^*, \mathsf{V}\rangle(G_1, G_2) = 1\big] &= \Pr\big[c = 1 \;\&\; c' = 1\big] + \Pr\big[c = 2 \;\&\; c' = 2\big] \\
&= \frac{1}{2} \cdot \Pr_{H\sim\mathcal{H}_1}\big[H \in S_1\big] + \frac{1}{2} \cdot \Pr_{H\sim\mathcal{H}_2}\big[H \in S_2\big] \\
&= \frac{1}{2} \cdot \Big[\Pr_{H\sim\mathcal{H}_1}\big[H \in S_1\big] + \Pr_{H\sim\mathcal{H}_1}\big[H \in S_2\big]\Big] \leq \frac{1}{2}.
\end{aligned}$$

We have used that $\mathcal{H}_1 \equiv \mathcal{H}_2$ for the first equality on the third line, and that $S_1 \cap S_2 = \emptyset$ for the second equality on the third line.

Public Coin Proofs

Recall from class that a public coin interactive proof system is one where every time V needs to send a message it simply draws and sends a random string. Since V must be randomized in any non-trivial interactive proof system, requiring that V do nothing more than sample and send random strings is, in some sense, requiring that the proof system is as simple as possible while still maintaining the possibility to compute functions outside of NP. As we will see in the exercises in this section, the simplicity of public coin proof systems turns out to allow them to be analyzed quite thoroughly using techniques from mathematics.

Note that soda-pop protocols are *not* public coin. Indeed, in the soda-pop protocol for graph non-isomorphism, V chooses a random $c \sim \{1, 2\}$ and needs to keep this value hidden from P. Certainly if P knew whether V chose $c = 1$ or $c = 2$ (*i.e.*, if V chose Coke or Pepsi) then P could answer correctly (*i.e.*, such that $c' = c$) with probability 1. It is critical to the soundness of soda-pop protocol that V has access to randomness which is *private* from the prover.

Now, recall that $f : \{0,1\}^* \to \{0,1\}$ is in the class $\mathsf{AM}[k]$ if it can be computed by a $k-$round public coin interactive proof system $\langle \mathsf{P}, \mathsf{V}\rangle$. We define $\mathsf{AM} = \bigcup_{c\geq 1} \mathsf{AM}[c]$ (note: AM only of the functions with *constant round* public coin interactive proofs, as supposed to IP which consists of functions with *polynomial round* interactive proofs). In this section you will prove several theorems regarding the class AM.

Some Properties of AM

Problem 3. Let $\mathsf{AM}_{\mathsf{pc}}[k]$ be the set of functions which can be computed by a $k-$round public coin interactive proof with perfect completeness, and let $\mathsf{AM}_{\mathsf{pc}} = \bigcup_{c\geq 1} \mathsf{AM}_{\mathsf{pc}}[c]$. Prove that $\mathsf{AM}[2] \subset \mathsf{AM}_{\mathsf{pc}}[3]$.

Solution. Suppose $f \in \mathsf{AM}[2]$. Then f is computed by a two-round public coin interactive proof system $\langle \mathsf{P}, \mathsf{V}\rangle$ with completeness $1 - 2^{-n}$ and soundness 2^{-n} (completeness $1 - 2^{-n}$ and soundness 2^{-n} can be obtained from completeness $2/3$ and soundness $1/3$ by amplification).

Let $r \in \{0,1\}^m$ denote the first message of $\langle \mathsf{P}, \mathsf{V} \rangle$ (sent by V), and let $a \in \{0,1\}^m$ denote P's response. So after the protocol is complete, V outputs $\mathsf{V}(\mathbf{x}, r, a)$. We describe another public coin interactive proof $\langle \mathsf{P}', \mathsf{V}' \rangle$ with three rounds and perfect completeness which computes f. Let $k \in \mathbb{N}$ be a parameter which will be set later; $\langle \mathsf{P}', \mathsf{V}' \rangle$ works as follows.

Input: P' and V' both take $\mathbf{x} \in \{0,1\}$ as input;

1. P' sends $s_1, \ldots, s_k \in \{0,1\}^m$ to V';

2. V' draws $r \sim \{0,1\}^m$ and sends r to P';

3. P' sends a to V';

Output: V' outputs 1 if $\exists\ i \in \{1, \ldots, k\}$ such that $\mathsf{V}(\mathbf{x}, r \oplus s_i, a) = 1$, and outputs 0 otherwise.

The symbol $\oplus$ is the coordinate-wise XOR of bit-strings. We now prove (perfect) completeness and soundness of $\langle \mathsf{P}', \mathsf{V}' \rangle$. The key idea is the same as in the proof of the Sipser-Gács Theorem. For this purpose, prior to the proofs of completeness and soundness, let us set some notation. Consider the two round protocol $\langle \mathsf{P}, \mathsf{V} \rangle$. Given an input $\mathbf{x}$, define the set

$$\mathsf{G}_{\mathbf{x}} = \big\{ r \in \{0,1\}^m : \exists a \text{ s.t. } \mathsf{V}(\mathbf{x}, r, a) = 1 \big\}.$$

Note that when $f(\mathbf{x}) = 1$, $|\mathsf{G}_{\mathbf{x}}| \geq (1 - 2^{-n}) \cdot 2^m$, and when $f(\mathbf{x}) = 0$, $|\mathsf{G}_{\mathbf{x}}| \leq 2^{-n} \cdot 2^m$. Just as in the Sipser-Gács theorem, the key idea is that when $f(\mathbf{x}) = 1$ there exist k shifts of $\mathsf{G}_{\mathbf{x}}$ which, together, cover all of $\{0,1\}^m$, while when $f(\mathbf{x}) = 0$, this cannot be the case. We now proceed formally, starting with soundness (it's easier).

Soundness: Suppose $f(\mathbf{x}) = 0$ and so $\Pr_{r \sim \{0,1\}^m}\big[r \in \mathsf{G}_{\mathbf{x}}\big] \leq 2^{-n}$. Thus, $\forall\ s_1, \ldots, s_k \in \{0,1\}^m$,

$$\Pr_{r \sim \{0,1\}^m}\Big[\exists i \in \{1, \ldots, k\} \text{ s.t. } r \oplus s_i \in \mathsf{G}_{\mathbf{x}}\Big] \leq k \cdot 2^{-n} \ll \frac{1}{2},$$

by the union bound. In words, this means that no matter what first message $(s_1, \ldots, s_k)$ P^* sends, with probability at most $1/2$ over the random second message sent by V', there will exist some third message a which will make V' accept. Thus, soundness holds for $\langle \mathsf{P}', \mathsf{V}' \rangle$.

Perfect Completeness: Now suppose $f(\mathbf{x}) = 1$ and so $\Pr_{r \sim \{0,1\}^m}\big[r \in \mathsf{G}_{\mathbf{x}}\big] \geq 1 - 2^{-n}$. Consider the random process which, for a fixed $r \in \{0,1\}^m$, draws $s \sim \{0,1\}^m$ and declares success if $r \oplus s \in \mathsf{G}_{\mathbf{x}}$. Note, for all $r \in \{0,1\}^m$, $\Pr_s\big[\text{success}\big] \geq 1 - 2^{-n}$. Now modify the experiment so that it draws $s_1, \ldots, s_k \sim \{0,1\}^m$ and declares success if $r \oplus s_i \in \mathsf{G}_{\mathbf{x}}$ for some $i \in \{1, \ldots, k\}$. Note for all $r \in \{0,1\}^m$,

$$\Pr_{s_1, \ldots, s_k}\big[\neg\text{success}\big] = \Pr_s\big[\neg\text{success in first experiment}\big]^k \leq 2^{-nk} < 2^{-m},$$

since we set $k = m/n + 1$. Finally, define one more experiment which draws $s_1, \ldots, s_k \sim \{0,1\}^m$ and outputs success if success holds in the second experiment for all $r \in \{0,1\}^m$. We have

$$\Pr_{s_1, \ldots, s_k}\big[\neg\text{success}\big] \leq \sum_{r \in \{0,1\}^m} \Pr_{s_1, \ldots, s_k}\big[\neg\text{success in second experiment with } r\big] < 2^m \cdot 2^{-m} = 1.$$

Thus, the probability of failure in the third experiment is *strictly* less than 1 and so there exists some $s_1, \ldots, s_k$ which leads to success in the third experiment. In other words, this means that there exist $s_1, \ldots, s_k$ such that for all $r \in \{0,1\}^m$, $r \oplus s_i \in \mathsf{G}_{\mathbf{x}}$ for some i. Thus, $\langle \mathsf{P}', \mathsf{V}' \rangle$ has perfect completeness since no matter what message V' sends, there will be a third message which P' can send to make V' accept.

Problem 4. Prove that $\mathsf{AM}[3] \subset \mathsf{AM}[2]$. Similar arguments show $\mathsf{AM}[c+1] \subset \mathsf{AM}[c]$ and $\mathsf{AM}_{\mathsf{pc}}[c+1] \subset \mathsf{AM}_{\mathsf{pc}}[c]$ for all constants c, and (you do not have to show this). As a result, AM and $\mathsf{AM}_{\mathsf{pc}}$ collapse: $\mathsf{AM}_{\mathsf{pc}} = \mathsf{AM} = \mathsf{AM}[2]$. Thus, if a function can be computed by a constant round public coin protocol, then it can be computed by a 2−round public coin protocol with perfect completeness.

Solution. Suppose $f \in \mathsf{AM}[3]$. Let $\langle \mathsf{P}, \mathsf{V} \rangle$ be a three round public coin interactive proof system which computes f and has perfect completeness and soundness $1/2$. Let (a, r, b) be the three messages of $\langle \mathsf{P}, \mathsf{V} \rangle$, let the first prover message $a \in \{0,1\}^\ell$ and the second message is from V and so is a random string $r \sim \{0,1\}^m$. We describe a two-round public coin interactive proof system $\langle \mathsf{P}', \mathsf{V}' \rangle$ which also computes f. Let $k \in \mathbb{N}$ be a parameter to be set later. $\langle \mathsf{P}', \mathsf{V}' \rangle$ works as follows.

Input: P' and V' both take $\mathbf{x} \in \{0,1\}$ as input;

2. V' draws $r_1, \ldots, r_k \sim \{0,1\}^m$ and sends $r_1, \ldots, r_k$ to P';

3. P' sends $a, b_1, \ldots, b_k$ to V';

Output: V' outputs 1 if $\mathsf{V}(\mathbf{x}, a, r_i, b_i) = 1$ for all $i = 1, \ldots, k$, and outputs 0 otherwise.

We prove perfect completeness and soundness.

Perfect Completeness: Suppose $f(\mathbf{x}) = 1$. Then there exists an a such that for all r there exists a b such that $\mathsf{V}(\mathbf{x}, a, r, b) = 1$. So in $\langle \mathsf{P}', \mathsf{V}' \rangle$, upon receiving $r_1, \ldots, r_k$ from V', P' just returns a and $b_1, \ldots, b_k$ such that $\mathsf{V}(\mathbf{x}, a, r_i, b_i) = 1$ for all i; V' therefore outputs 1 with probability 1.

Soundness: Suppose $f(\mathbf{x}) = 0$ and so for all a, $\Pr_{r \sim \{0,1\}^m}\left[\exists b \text{ s.t. } \mathsf{V}(\mathbf{x}, a, r, b) = 1\right] \leq 1/2$. As in the previous problem, let

$$\mathsf{G}_{(\mathbf{x},a)} = \left\{ r \in \{0,1\}^m : \exists b \text{ s.t. } \mathsf{V}(\mathbf{x}, a, r, b) = 1 \right\}.$$

So when $f(\mathbf{x}) = 0$, for all $a \in \{0,1\}^\ell$ it holds that $\Pr_{r \sim \{0,1\}^m}\left[r \in \mathsf{G}_{(\mathbf{x},a)}\right] \leq 1/2$. Thus, for all $a \in \{0,1\}^\ell$,

$$\Pr_{r_1, \ldots, r_k \sim \{0,1\}^m}\left[r_i \in \mathsf{G}_{(\mathbf{x},a)} \ \forall\ i\right] \leq 2^{-k} = \frac{1}{2} \cdot 2^{-\ell},$$

since we set $k = \ell + 1$. This means

$$\Pr_{r_1, \ldots, r_k}\left[\exists a \text{ s.t. } r_i \in \mathsf{G}_{(\mathbf{x},a)} \ \forall\ i\right] \leq \frac{1}{2},$$

by the union bound. In other words, with probability at most $1/2$ over the random message of V', there exists a response by P' which will make V' accept. Thus, $\langle \mathsf{P}', \mathsf{V}' \rangle$ has soundness $1/2$.

Interactive Reductions

In the unit on $\mathsf{NP}-$completeness, we saw the power of polynomial time reductions as a method to demonstrate that the difficulty of solving two (possibly very different-looking) problems using TMs, might be related. Now that we have moved on to computations being done by two TMs interacting through a protocol, we will need a notion of reduction which reflects this structure. To define this notion properly we will need to slightly generalize our notion of a function $f : \{0,1\}^* \to \{0,1\}$ to a *semi-function* $f : \{0,1\}^* \to \{0,1\} \cup \{\perp\}$ where we think of $f(\mathbf{x}) = \perp$ as some sort of "failure symbol" meaning that f is unable to compute an output on input $\mathbf{x}$. Just like for normal functions, we say that an interactive proof system $\langle \mathsf{P}, \mathsf{V} \rangle$ *computes* a semi-function $f : \{0,1\}^* \to \{0,1\} \cup \{\perp\}$ if the following completeness and soundness properties hold.

- **Completeness:** If $f(\mathbf{x}) = 1$ then $\Pr\big[\langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x}) = 1\big] \geq 2/3$.
- **Soundness:** If $f(\mathbf{x}) = 0$ then for all P^*, $\Pr\big[\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x}) = 0\big] \geq 2/3$.

So, in words, the proof system computes the semi-function if the proof system is likely to output $f(\mathbf{x})$ whenever $f(\mathbf{x}) \neq \perp$ *and we don't care what the system outputs when* $f(\mathbf{x}) = \perp$.

Definition (Interactive Reductions). A $\delta-$*interactive reduction* between two semi-functions $f, g : \{0,1\}^* \to \{0,1\} \cup \{\perp\}$ is an interactive protocol $\langle \mathsf{P}, \mathsf{V} \rangle$ in which the polytime PTM V outputs a string at the end (rather than a bit like in interactive proofs), in which the following completeness and soundness properties hold.

- **Completeness:** If $f(\mathbf{x}) = 1$ then $g\big(\langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x})\big) = 1$.
- **Soundness:** If $f(\mathbf{x}) = 0$ then for all P^*, $\Pr\big[g\big(\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x})\big) = 0\big] \geq 1 - \delta$.

We call δ the *soundness parameter* of the reduction. If there is a $\delta-$interactive reduction from f to g, we write $f \leq_\delta g$.

Problem 5. Do both of the following.

(a) Suppose that $f, g, h : \{0,1\}^* \to \{0,1\} \cup \{\perp\}$ are semi-functions and $\delta, \delta' > 0$ are soundness parameters such that $f \leq_\delta g$ and $g \leq_{\delta'} h$ hold. Prove that $f \leq_{\delta+\delta'} h$.

Solution. We are given that $f \leq_\delta g$ via the interactive reduction $\langle \mathsf{P}, \mathsf{V} \rangle$ and that $g \leq_{\delta'} h$ via the interactive reduction $\langle \mathsf{P}', \mathsf{V}' \rangle$. Let $\langle \mathsf{P}'', \mathsf{V}'' \rangle$ be the interactive reduction which on input $\mathbf{x}$:

- computes $\mathbf{x}' \sim \langle \mathsf{P}, \mathsf{V} \rangle(\mathbf{x})$;
- computes $\mathbf{x}'' \sim \langle \mathsf{P}', \mathsf{V}' \rangle(\mathbf{x}')$, and V'' outputs $\mathbf{x}''$.

Note that if $f(\mathbf{x}) = 1$, then $g(\mathbf{x}') = 1$ holds with probability 1 by the perfect completeness of $\langle \mathsf{P}, \mathsf{V} \rangle$, and so $h(\mathbf{x}'') = 1$ holds with probability 1 by the perfect completeness of $\langle \mathsf{P}', \mathsf{V}' \rangle$. On the other hand, if $f(\mathbf{x}) = 0$, then $g(\mathbf{x}') = 0$ holds with probability $1-\delta$ by the soundness of $\langle \mathsf{P}, \mathsf{V} \rangle$. If $g(\mathbf{x}') = 0$ then $h(\mathbf{x}'') = 0$ holds with probability $1 - \delta'$ by the soundness of $\langle \mathsf{P}', \mathsf{V}' \rangle$. Thus, putting these together, if $f(\mathbf{x}) = 0$ then $h(\mathbf{x}'') = 0$ holds with probability $1 - \delta - \delta'$. Thus $\langle \mathsf{P}'', \mathsf{V}'' \rangle$ is an interactive reduction from f to h with perfect completeness and soundness $1 - (\delta + \delta')$. This proves $f \leq_{\delta+\delta'} h$ as required.

(b) Suppose that $f, g : \{0,1\}^* \to \{0,1\} \cup \{\perp\}$ are semi-functions and $\delta, \delta' > 0$ are soundness parameters. Suppose that $f \leq_\delta g$ and that $\langle \mathsf{P}, \mathsf{V} \rangle$ is an interactive proof system which computes g with completeness parameter 1 and soundness parameter δ'. Describe another proof system $\langle \mathsf{P}', \mathsf{V}' \rangle$ which computes f with completeness parameter 1 and soundness parameter $\delta + \delta'$.

Solution. Suppose $f \leq_\delta g$ via the interactive reduction $\langle \mathsf{P}', \mathsf{V}' \rangle$ and that g is computed by the interactive proof system $\langle \mathsf{P}, \mathsf{V} \rangle$. Then the interactive proof system computing f is $\langle \mathsf{P}'', \mathsf{V}'' \rangle$ which works as follows on input $\mathbf{x}$:

- first P'' and V'' run $\langle \mathsf{P}', \mathsf{V}' \rangle$ on input $\mathbf{x}$, obtaining output $\mathbf{x}'$;
- next P'' and V'' run $\langle \mathsf{P}, \mathsf{V} \rangle$ on input $\mathbf{x}'$, V'' outputs the resulting output bit.

To prove completeness, note that if $f(\mathbf{x}) = 1$ then $g(\mathbf{x}') = 1$ holds with probability 1, in which case V'' outputs 1 with probability 1 by the perfect completeness of $\langle \mathsf{P}, \mathsf{V} \rangle$. To prove soundness, note that if $f(\mathbf{x}) = 0$, then $g(\mathbf{x}') = 0$ holds with probability $1 - \delta$. If $g(\mathbf{x}') = 0$ holds, then V'' outputs 0 with probability $1 - \delta'$ by the soundness of $\langle \mathsf{P}, \mathsf{V} \rangle$. Thus, in total, if $f(\mathbf{x}) = 0$ then V'' outputs 0 with probability at least $1 - \delta - \delta'$, proving soundness.