# Homework 4

due Friday Feb 18, 2022

**Directions:** Do all problems.

## 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 $\mathsf{V}$ (the *verifier*), a (possibly randomized) function $\mathsf{P} : \{0,1\}^* \to \{0,1\}^*$ (the *prover*) and a $k-$round interactive protocol between $\mathsf{P}$ and $\mathsf{V}$, 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 $\mathsf{P}^* : \{0,1\}^* \to \{0,1\}^*$, $\Pr\big[\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x}) = 0\big] \geq 2/3$ ($\mathsf{P}^*$ 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 $\mathsf{V}$ after the protocol is run on input $\mathbf{x}$. Recall that the complexity class $\mathsf{IP}$ 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 $\mathsf{NP}$. Thus, it is critical for the definition of $\mathsf{IP}$ that $\mathsf{V}$ 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 $\mathsf{P}$ the first and third message, $\mathsf{V}$ 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:

- $\mathsf{P}$ sends $\mathbf{a}_1$ to $\mathsf{V}$ where $\mathbf{a}_1 \sim \mathsf{P}_1(\mathbf{x})$;
- $\mathsf{V}$ sends $\mathbf{a}_2$ to $\mathsf{P}$ where $\mathbf{a}_2 \sim \mathsf{V}_2(\mathbf{x}, \mathbf{a}_1)$;
- $\mathsf{P}$ sends $\mathbf{a}_3$ to $\mathsf{V}$ where $\mathbf{a}_3 \sim \mathsf{P}_3(\mathbf{x}, \mathbf{a}_1, \mathbf{a}_2)$;
- $\mathsf{V}$ 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 $\mathsf{P}'$ 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 $\mathsf{val}'_i$ analogously to $\mathsf{val}_i$ except with the new prover $\mathsf{P}'$ replacing the old prover $\mathsf{P}$.

**(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 $f(\mathbf{x}) = 1$, $\Pr\big[\langle \mathsf{P}', \mathsf{V}\rangle(\mathbf{x}) = 1\big] \geq 2/3$.

**(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 $\mathsf{P}^*$.

**(c)** Now prove that the functions $\mathsf{P}'_3$ and $\mathsf{P}'_1$ can be computed by a polynomial space TM.

**(d)** Deduce that any $f \in \mathsf{IP}[3]$ can be computed by an interactive proof system where $\mathsf{P}$ is implemented by a deterministic, polynomial space TM. Since $\mathsf{V}$ 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 $\mathsf{IP} \subset \mathsf{PSPACE}$!

# 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 $f_{\mathsf{GNI}}$ 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 $f_{\mathsf{GNI}}$ being the complement of $f_{\mathsf{GI}}$ 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 $\mathsf{coNP}$, 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 $\pi$. 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 $f_{\mathsf{GNI}}$ 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 $\mathsf{P}$ and $\mathsf{V}$ get $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ as input.

**1.** $\mathsf{V}$ 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 $\mathsf{P}$ where $H = \big(V, \pi(E_c)\big)$.

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

**Output:** $\mathsf{V}$ outputs 1 if $c' = c$, and outputs 0 otherwise.

In the protocol description above, we are being intentionally vague about how $\mathsf{P}$ computes its second message. This is because we are getting ready to prove soundness, and when proving soundness $\mathsf{P}^*$ is adversarial and so will deviate from the protocol specs anyway. However, to be formal, the honest $\mathsf{P}$ 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 $\mathsf{P}^*$ 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 $\mathsf{P}^*$ 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 $1/3$.

# Public Coin Proofs

Recall from class that a public coin interactive proof system is one where every time $\mathsf{V}$ needs to send a message it simply draws and sends a random string. Since $\mathsf{V}$ must be randomized in any non-trivial interactive proof system, requiring that $\mathsf{V}$ 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 $\mathsf{NP}$. 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, $\mathsf{V}$ chooses a random $c \sim \{1,2\}$ and needs to keep this value hidden from $\mathsf{P}$. Certainly if $\mathsf{P}$ knew whether $\mathsf{V}$ chose $c = 1$ or $c = 2$ (*i.e.*, if $\mathsf{V}$ chose Coke or Pepsi) then $\mathsf{P}$ could answer correctly (*i.e.*, such that $c' = c$) with probability 1. It is critical to the soundness of soda-pop protocol that $\mathsf{V}$ 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: $\mathsf{AM}$ only of the functions with *constant round* public coin interactive proofs, as supposed to $\mathsf{IP}$ which consists of functions with *polynomial round* interactive proofs). In this section you will prove several theorems regarding the class $\mathsf{AM}$.

## 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

$\mathsf{AM}[2] \subset \mathsf{AM}_{\mathsf{pc}}[3]$.

**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, $\mathsf{AM}$ 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.

# 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 $\mathsf{P}^*$, $\Pr\big[\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x}) = 0\big] \geq 2/3$.

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 $\mathsf{V}$ 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 $\mathsf{P}^*$, $\Pr\big[g\big(\langle \mathsf{P}^*, \mathsf{V} \rangle(\mathbf{x})\big) = 0\big] \geq 1 - \delta$.

We call $\delta$ 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 $f \leq_{\delta+\delta'} h$.

**(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 $\delta'$. Describe another proof system $\langle \mathsf{P}', \mathsf{V}' \rangle$ which computes $f$ with completeness parameter 1 and soundness parameter $\delta + \delta'$.