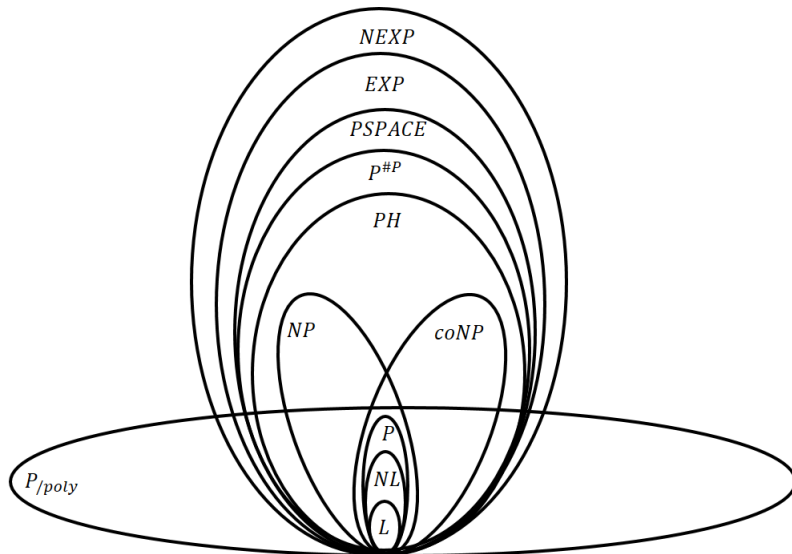


CSL853: Complexity Theory

Ragesh Jaiswal, CSE, IIT Delhi

Complexity Diagram

Our current view of complexity



Interactive Proofs

Interactive Proofs

Interactive proofs with deterministic verifier and prover

Definition (Interaction of deterministic functions)

Let $f, g : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be functions and $k \geq 0$ be an integer (allowed to depend upon the input size). A k -round interaction of f and g on input $x \in \{0, 1\}^*$, denoted by $\langle f, g \rangle(x)$ is the sequence of strings $a_1, \dots, a_k \in \{0, 1\}^*$ defined as follows:

$$\begin{aligned}a_1 &= f(x) \\a_2 &= g(x, a_1) \\&\vdots \\a_{2i+1} &= f(x, a_1, \dots, a_{2i}) \quad \text{for } 2i < k \\a_{2i+2} &= g(x, a_1, \dots, a_{2i+1}) \quad \text{for } 2i + 1 < k \\&\vdots\end{aligned}$$

The output of f at the end of the interaction denoted $out_f \langle f, g \rangle(x)$ is defined to be $f(x, a_1, \dots, a_k)$; we assume this output is in $\{0, 1\}$.

Interactive Proofs

Interactive proofs with deterministic verifier and prover

Definition (Deterministic proof systems)

We say that a language has a k -round deterministic interactive proof system if there is a deterministic TM V that on input $x, a_1, \dots, a_i$ runs in time polynomial in $|x|$, and can have a k -round interaction with any function P such that:

(Completeness) $x \in L \Rightarrow \exists P : \{0, 1\}^* \rightarrow \{0, 1\}^* \text{out}_V \langle V, P \rangle(x) = 1$

(Soundness) $x \notin L \Rightarrow \forall P : \{0, 1\}^* \rightarrow \{0, 1\}^* \text{out}_V \langle V, P \rangle(x) = 0$

Definition (The class dIP)

The class dIP contains all languages with a $k(n)$ -round deterministic interactive proof systems with $k(n)$ polynomial in n .

Theorem

dIP = NP.

Interactive Proofs

Randomized interaction

Definition (Randomized interaction)

Let $f, g : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be functions and $k \geq 0$ be an integer (allowed to depend upon the input size). A k -round randomized interaction of f and g on input $x \in \{0, 1\}^*$, denoted by $\langle f, g \rangle(x)$ is the sequence of strings $a_1, \dots, a_k \in \{0, 1\}^*$ defined as follows:

$$\begin{aligned} a_1 &= f(x, r) \\ a_2 &= g(x, a_1) \\ &\vdots \\ a_{2i+1} &= f(x, r, a_1, \dots, a_{2i}) \quad \text{for } 2i < k \\ a_{2i+2} &= g(x, a_1, \dots, a_{2i+1}) \quad \text{for } 2i + 1 < k \\ &\vdots \end{aligned}$$

Here r denotes the (private) random coins used by f . The output of f at the end of the interaction denoted $out_f \langle f, g \rangle(x)$ is defined to be $f(x, a_1, \dots, a_k)$; we assume this output is in $\{0, 1\}$. Note that here both $\langle f, g \rangle(x)$ and $out_f \langle f, g \rangle(x)$ are random variables.

Interactive Proofs

The class IP

Definition (The class $IP(k)$)

For an integer $k \geq 1$ (that may depend on the input length), we say that a language L is in $IP(k)$ if there is a probabilistic polynomial-time Turing machine V that can have k -round randomised interaction with a function $P : \{0, 1\}^* \rightarrow \{0, 1\}^*$ such that:

$$(\text{Completeness}) \quad x \in L \Rightarrow \exists P \Pr[out_V\langle V, P \rangle(x) = 1] \geq 2/3$$

$$(\text{Soundness}) \quad x \notin L \Rightarrow \forall P \Pr[out_V\langle V, P \rangle(x) = 1] \leq 1/3$$

where all probabilities are over the choice of r .

Definition (The class IP)

$$IP = \bigcup_{c \geq 1} IP(n^c).$$

Interactive Proofs

The class IP

Definition (The class $IP(k)$)

For an integer $k \geq 1$ (that may depend on the input length), we say that a language L is in $IP(k)$ if there is a probabilistic polynomial-time Turing machine V that can have k -round randomised interaction with a function $P : \{0,1\}^* \rightarrow \{0,1\}^*$ such that:

$$(\text{Completeness}) \quad x \in L \Rightarrow \exists P \Pr[out_V\langle V, P \rangle(x) = 1] \geq 2/3$$

$$(\text{Soundness}) \quad x \notin L \Rightarrow \forall P \Pr[out_V\langle V, P \rangle(x) = 1] \leq 1/3$$

where all probabilities are over the choice of r .

Definition (The class IP)

$$IP = \bigcup_{c \geq 1} IP(n^c).$$

Lemma

The class IP is unchanged if we replace the completeness parameter $2/3$ by $1 - 2^{-n^s}$ and the soundness parameter $1/3$ by 2^{-n^s} for any fixed constant $s > 0$.

Interactive Proofs

The class IP

- Show the following:
 - Let IP' denote the class obtained by allowing the prover to be probabilistic. That is, the prover's strategy can be chosen at random from some distribution on functions. Prove that $IP' = IP$.

Interactive Proofs

The class IP

- Show the following:
 - Let IP' denote the class obtained by allowing the prover to be probabilistic. That is, the prover's strategy can be chosen at random from some distribution on functions. Prove that $IP' = IP$.
 - Show that $IP \subseteq PSPACE$.

Interactive Proofs

The class IP

- Show the following:
 - Let IP' denote the class obtained by allowing the prover to be probabilistic. That is, the prover's strategy can be chosen at random from some distribution on functions. Prove that $IP' = IP$.
 - Show that $IP \subseteq PSPACE$.
 - Let IP'' denote the class obtained by changing the completeness parameter $2/3$ to 1. Prove that $IP'' = IP$.

Interactive Proofs

The class IP

- Show the following:
 - Let IP' denote the class obtained by allowing the prover to be probabilistic. That is, the prover's strategy can be chosen at random from some distribution on functions. Prove that $IP' = IP$.
 - Show that $IP \subseteq PSPACE$.
 - Let IP'' denote the class obtained by changing the completeness parameter $2/3$ to 1 . Prove that $IP'' = IP$. **We will show this later.**
 - Let IP''' denote the class obtained by changing the soundness parameter $1/3$ to 0 . Prove that $IP''' = NP$.

Interactive Proofs

Graph non-isomorphism and Quadratic nonresiduosity

- Let $GNI = \{\langle G_0, G_1 \rangle : \text{Graphs } G_0 \text{ and } G_1 \text{ are non-isomorphic}\}$

Theorem

$GNI \in IP$.

- Given a prime number p , a number a is said to be quadratic residue mod p if there is another number b such that $a \equiv b^2 \pmod{p}$.
- Let $QNR = \{(a, p) :$
 p is prime and a is not a quadratic residue mod $p\}$.
- Claim: $QNR \in coNP$.

Theorem

$QNR \in IP$.

Interactive Proofs

$$P^{\#P} \subseteq IP$$

- Does IP contain NP? **Yes**
- Does IP contain coNP?

Theorem

$$P^{\#P} \subseteq IP$$

Interactive Proofs

$$P^{\#P} \subseteq IP$$

Theorem

$$P^{\#P} \subseteq IP$$

Proof.

- Let $\#SAT_{\geq} = \{\langle \psi, k \rangle : \psi \text{ is a 3CNF formula that has } \geq k \text{ satisfying assignments}\}$.
- Claim 1: It is sufficient to show that $\#SAT_{\geq} \in IP$.

Interactive Proofs

$$P^{\#P} \subseteq IP$$

Theorem

$$P^{\#P} \subseteq IP$$

Proof.

- Let $\#SAT_{\geq} = \{\langle \psi, k \rangle : \psi \text{ is a 3CNF formula that has } \geq k \text{ satisfying assignments}\}$.
- Claim 1: It is sufficient to show that $\#SAT_{\geq} \in IP$.

Lemma

Let $SUMP = \{\langle g, k, p \rangle : p \text{ is prime, } g \text{ is a degree } d \text{ polynomial in } n \text{ variables such that } k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n) \pmod{p}\}$. Then $SUMP \in IP$.

Interactive Proofs

$$\mathsf{P}^{\#P} \subseteq \mathsf{IP}$$

Lemma

Let $\text{SUMP} = \{ \langle g, k, p \rangle : p \text{ is prime, } g \text{ is a degree } d \text{ polynomial in } n \text{ variables such that } k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n) \pmod{p} \}$. Then $\text{SUMP} \in \mathsf{IP}$.

Proof.

- All calculations are modulo p .
- Given that $n > 1$, define $h(X_1) = \sum_{b_2 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} g(X_1, b_2, \dots, b_n)$
- Protocol
 - Verifier: If $n = 1$ check if $g(0) + g(1) \geq k$. If so accept, else reject. If $n \geq 2$, ask P to send $h(X_1)$.
 - Prover: Send some polynomial $s(X_1)$.
 - Verifier: Reject if $s(0) + s(1) < k$, else pick a random number $a \in \{1, \dots, p-1\}$. Recursively use the same protocol to check that $s(a) = \sum_{b_2, \dots, b_n \in \{0,1\}} g(a, b_2, \dots, b_n)$.

Interactive Proofs

$$P^{\#P} \subseteq IP$$

Lemma

Let $SUMP = \{ \langle g, k, p \rangle : p \text{ is prime, } g \text{ is a degree } d \text{ polynomial in } n \text{ variables such that } k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n) \pmod{p} \}$. Then $SUMP \in IP$.

Proof.

- All calculations are modulo p .
- Given that $n > 1$, define $h(X_1) = \sum_{b_2 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} g(X_1, b_2, \dots, b_n)$
- Protocol
 - Verifier: If $n = 1$ check if $g(0) + g(1) \geq k$. If so accept, else reject. If $n \geq 2$, ask P to send $h(X_1)$.
 - Prover: Send some polynomial $s(X_1)$.
 - Verifier: Reject if $s(0) + s(1) < k$, else pick a random number $a \in \{1, \dots, p-1\}$. Recursively use the same protocol to check that $s(a) = \sum_{b_2, \dots, b_n \in \{0,1\}} g(a, b_2, \dots, b_n)$.
- Claim 1: If $k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n)$, then there is a prover that makes the verifier accept.
- Claim 2: If $k > \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n)$, then the probability that the verifier rejects is at least $(1 - d/p)^n$. □

Interactive Proofs

$$P^{\#P} \subseteq IP$$

Theorem

$$P^{\#P} \subseteq IP$$

Proof.

- Let $\#SAT_{\geq} = \{\langle \psi, k \rangle : \psi \text{ is a 3CNF formula that has } \geq k \text{ satisfying assignments}\}$.
- Claim 1: It is sufficient to show that $\#SAT_{\geq} \in IP$.

Lemma

Let $SUMP = \{\langle g, k, p \rangle : p \text{ is prime, } g \text{ is a degree } d \text{ polynomial in } n \text{ variables such that } k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n) \pmod{p}\}$. Then $SUMP \in IP$.

- Claim 2: Given a 3CNF formula $\psi(x_1, \dots, x_n)$ in n variables having m clauses, there exists a polynomial $g_{\psi}(X_1, \dots, X_n)$ of degree $3m$ and in n variables such that for any $b_1, \dots, b_n \in \{0, 1\}$, $\psi(b_1, \dots, b_n) = g_{\psi}(b_1, \dots, b_n)$.

Interactive Proofs

$$P^{\#P} \subseteq IP$$

Theorem

$$P^{\#P} \subseteq IP$$

Proof.

- Let $\#SAT_{\geq} = \{\langle \psi, k \rangle : \psi \text{ is a 3CNF formula that has } \geq k \text{ satisfying assignments}\}$.
- Claim 1: It is sufficient to show that $\#SAT_{\geq} \in IP$.

Lemma

Let $SUMP = \{\langle g, k, p \rangle : p \text{ is prime, } g \text{ is a degree } d \text{ polynomial in } n \text{ variables such that } k \leq \sum_{b_1, \dots, b_n \in \{0,1\}} g(X_1, \dots, X_n) \pmod{p}\}$. Then $SUMP \in IP$.

- Claim 2: Given a 3CNF formula $\psi(x_1, \dots, x_n)$ in n variables having m clauses, there exists a polynomial $g_{\psi}(X_1, \dots, X_n)$ of degree $3m$ and in n variables such that for any $b_1, \dots, b_n \in \{0, 1\}$, $\psi(b_1, \dots, b_n) = g_{\psi}(b_1, \dots, b_n)$.
- Pick a large prime between 2^n and 2^{2^n} and use the protocol in the lemma. $\square$

Interactive Proofs

IP = PSPACE

Theorem

IP = PSPACE

Proof.

- Claim 1: It is sufficient to show that TQBF $\in$ IP.
- Claim 2: Given a TQBF formula $\psi = \forall x_1 \exists x_2 \forall x_3 \dots \exists x_n \phi(x_1, \dots, x_n)$, we can construct a polynomial P_ϕ such that $\psi \in$ TQBF if and only if

$$\prod_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \prod_{b_3 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} P_\phi(b_1, \dots, b_n) \neq 0.$$

- Question: What is the issue if we try to argue the same way as when showing $P^{\#P} \subseteq$ IP?

Interactive Proofs

IP = PSPACE

Theorem

IP = PSPACE

Proof.

- Claim 1: It is sufficient to show that $\text{TQBF} \in \text{IP}$.
- Claim 2: Given a TQBF formula $\psi = \forall x_1 \exists x_2 \forall x_3 \dots \exists x_n \phi(x_1, \dots, x_n)$, we can construct a polynomial P_ϕ such that $\psi \in \text{TQBF}$ if and only if

$$\prod_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \prod_{b_3 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} P_\phi(b_1, \dots, b_n) \neq 0.$$

- Question: What is the issue if we try to argue the same way as when showing $\text{P}^{\#P} \subseteq \text{IP}$? **The large degree**
- Lemma 1: Given any multivariate polynomial $p(X_1, \dots, X_n)$, we can construct a *multilinear polynomial* $q(X_1, \dots, X_n)$ such that $p(\cdot)$ and $q(\cdot)$ agree on all values $X_1, \dots, X_n \in \{0, 1\}$.

Interactive Proofs

IP = PSPACE

Lemma

Given any multivariate polynomial $p(X_1, \dots, X_n)$, we can construct a multilinear polynomial $q(X_1, \dots, X_n)$ such that $p(\cdot)$ and $q(\cdot)$ agree on all values $X_1, \dots, X_n \in \{0, 1\}$.

Proof.

Definition (Linearization operator)

Let $p(X_1, \dots, X_n)$ be a polynomial, the linearisation operator wrt a variable X_i on polynomial p , denoted by $L_{X_i}p$, is defined to be the following polynomial:

$$L_{X_i}(p) = X_i \cdot p(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) + (1 - X_i) \cdot p(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_n)$$

- Claim 1: Let $g(X_1, \dots, X_n) = L_{X_1}L_{X_2}\dots L_{X_n}p(X_1, \dots, X_n)$. Then g and p agree on values of variables $X_1, \dots, X_n \in \{0, 1\}$. □

Interactive Proofs

IP = PSPACE

Lemma

Given any multivariate polynomial $p(X_1, \dots, X_n)$, we can construct a multilinear polynomial $q(X_1, \dots, X_n)$ such that $p(\cdot)$ and $q(\cdot)$ agree on all values $X_1, \dots, X_n \in \{0, 1\}$.

Proof.

Definition (Linearization operator)

Let $p(X_1, \dots, X_n)$ be a polynomial, the linearisation operator wrt a variable X_i on polynomial p , denoted by $L_{X_i}p$, is defined to be the following polynomial:

$$L_{X_i}(p) = X_i \cdot p(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) + (1 - X_i) \cdot p(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_n)$$

- Claim 1: Let $g(X_1, \dots, X_n) = L_{X_1}L_{X_2}\dots L_{X_n}p(X_1, \dots, X_n)$. Then g and p agree on values of variables $X_1, \dots, X_n \in \{0, 1\}$. □

Definition ($\forall$ and $\exists$ operator on polynomial)

Let $p(X_1, \dots, X_n)$ be a polynomial, the $\forall, \exists$ operators wrt a variable X_i on polynomial p , denoted by $\forall_{X_i}p$ $\exists_{X_i}$ respectively, is defined to be the following polynomials:

$$\forall_{X_i}(p) = p(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) \cdot p(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_n)$$

$$\exists_{X_i}(p) = p(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) + p(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_n)$$

Interactive Proofs

IP = PSPACE

Theorem

IP = PSPACE

Proof.

- Claim 1: It is sufficient to show that $\text{TQBF} \in \text{IP}$.
- Claim 2: Given a TQBF formula $\psi = \forall x_1 \exists x_2 \forall x_3 \dots \exists x_n \phi(x_1, \dots, x_n)$, we can construct a polynomial P_ϕ such that $\psi \in \text{TQBF}$ if and only if

$$\prod_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \prod_{b_3 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} P_\phi(b_1, \dots, b_n) \neq 0.$$

- Claim 3: Consider $\forall x_1 L_{x_1} \exists x_2 L_{x_1} L_{x_2} \forall x_3 L_{x_1} L_{x_2} L_{x_3} \dots \exists x_n L_{x_1} \dots L_{x_n} P_\phi(X_1, \dots, X_n)$. If we take out any number of quantifiers from the front of the expression, the resulting polynomial is degree bounded.
- Lemma 2: Let $g(X_1, \dots, X_n)$ be some polynomial. Let $U(Y_1, \dots, Y_l) = \mathcal{O}g(X_1, \dots, X_n)$ where $\mathcal{O}$ is one of the three operators $\exists_{X_1}, \forall_{X_1}, L_{X_1}$. Let d be the degree of g w.r.t. X_1 . There is a verifier such that for any $C, a_1, \dots, a_l$, if $C = U(a_1, \dots, a_l)$, then there is a prover that makes the verifier accept. Otherwise it accepts with probability at most $d/p + \epsilon$, where ϵ is the probability that a prover can make the verifier accept the assertion that $C' = g(a'_1, \dots, a'_k)$ when $C' \neq g(a'_1, \dots, a'_k)$

Interactive Proofs

IP = PSPACE

Lemma

Let $g(X_1, \dots, X_n)$ be some polynomial. Let $U(Y_1, \dots, Y_l) = \mathcal{O}g(X_1, \dots, X_n)$ where $\mathcal{O}$ is one of the three operators $\exists_{X_1}, \forall_{X_1}, L_{X_1}$. Let d be the degree of g w.r.t. X_1 . There is a verifier such that for any $C, a_1, \dots, a_l$, if $C = U(a_1, \dots, a_l)$, then there is a prover that makes the verifier accept. Otherwise it accepts with probability at most $d/p + \epsilon$, where ϵ is the probability that a prover can make the verifier accept the assertion that $C' = g(a'_1, \dots, a'_k)$ when $C' \neq g(a'_1, \dots, a'_k)$.

Proof.

- The verifier does the following:
 - Case 1 ($\mathcal{O} = \exists_{X_1}$): The prover provides a degree d polynomial $s(X_1)$ that is supposed to be $g(X_1, a_2, \dots, a_n)$. The verifier checks if $s(0) + s(1) = C$. If not, then it rejects, otherwise it picks a random $a \in \{1, \dots, p-1\}$ and asks the prover to prove $s(a) = g(a, a_2, \dots, a_n)$.
 - Case 2 ($\mathcal{O} = \forall_{X_1}$): Same as above except that verifier checks $s(0) \cdot s(1) = C$.
 - Case 3 ($\mathcal{O} = L_{X_1}$): Same as above except that the verifier checks $a_1 \cdot s(0) + (1 - a_1) \cdot s(1) = C$.

Interactive Proofs

IP = PSPACE

Theorem

IP = PSPACE

Proof.

- Claim 1: It is sufficient to show that TQBF $\in$ IP.
- Claim 2: Given a TQBF formula $\psi = \forall x_1 \exists x_2 \forall x_3 \dots \exists x_n \phi(x_1, \dots, x_n)$, we can construct a polynomial P_ϕ such that $\psi \in$ TQBF if and only if

$$\prod_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \prod_{b_3 \in \{0,1\}} \dots \sum_{b_n \in \{0,1\}} P_\phi(b_1, \dots, b_n) \neq 0.$$

- Claim 3: Consider $\forall x_1 L_{x_1} \exists x_2 L_{x_1} L_{x_2} \forall x_3 L_{x_1} L_{x_2} L_{x_3} \dots \exists x_n L_{x_1} \dots L_{x_n} P_\phi(X_1, \dots, X_n)$. If we take out any number of quantifiers from the front of the expression, the resulting polynomial is degree bounded.
- Lemma 2: Let $g(X_1, \dots, X_n)$ be some polynomial. Let $U(Y_1, \dots, Y_l) = \mathcal{O}g(X_1, \dots, X_n)$ where $\mathcal{O}$ is one of the three operators $\exists x_1, \forall x_1, L_{x_1}$. Let d be the degree of g w.r.t. X_1 . There is a verifier such that for any $C, a_1, \dots, a_l$, if $C = U(a_1, \dots, a_l)$, then there is a prover that makes the verifier accept. Otherwise it accepts with probability at most $d/p + \epsilon$, where ϵ is the probability that a prover can make the verifier accept the assertion that $C' = g(a'_1, \dots, a'_k)$ when $C' \neq g(a'_1, \dots, a'_k)$
- Claim 4: There is a verifier that is “fooled” by a cheating prover with probability at most $\frac{n^2 d}{p}$.



Public Vs Private Coins

Interactive Proofs

The class AM

- The definition of IP involved the verifier using *private* coin tosses.
- Suppose the verifier was constrained to make its coin tosses public.
How weak does the resulting complexity class become?

Definition ($AM(k)$)

For every k the complexity class $AM(k)$ is defined as the subset of $IP(k)$ obtained when we restrict the verifier's messages to be random bits, and not allowing it to use any other random bits that are not contained in these messages.

Definition (AM)

$AM = AM(2)$.

Definition (MA)

$L \in MA$ if there is a proof system where the prover first sends a message to the verifier and the verifier makes a decision based on the message from the prover and its random coin tosses.

- Such proofs are called Arthur-Merlin proofs/games.

Interactive Proofs

The class AM

Definition ($AM(k)$)

For every k the complexity class $AM(k)$ is defined as the subset of $IP(k)$ obtained when we restrict the verifier's messages to be random bits, and not allowing it to use any other random bits that are not contained in these messages.

Definition (AM)

$AM = AM(2)$.

Definition (MA)

$L \in MA$ if there is a proof system where the prover first sends a message to the verifier and the verifier makes a decision based on the message from the prover and its random coin tosses.

- Some known facts about AM:
 - Show that $MA \subseteq AM$

Interactive Proofs

The class AM

- Some known facts about AM:
 - Show that $MA \subseteq AM$

Theorem (Babai, Moran, 1988)

For every constant $k \geq 2$, $AM(k+1) = AM(k)$.

Interactive Proofs

The class AM

- Some known facts about AM:
 - Show that $MA \subseteq AM$

Theorem (Babai, Moran, 1988)

For every constant $k \geq 2$, $AM(k+1) = AM(k)$.

Theorem (Goldwasser, Sipser, 1987)

For every $k : \mathbb{N} \rightarrow \mathbb{N}$ with $k(n)$ computable in $\text{poly}(n)$, $IP(k) \subseteq AM(k+2)$.

- Argue that $GNI \in AM$.

Interactive Proofs

Set lower bound protocol

- The set lower bound protocol is a public coin protocol where the prover and verifier are given $S \subseteq \{0,1\}^m$ such that membership in S can be easily certified. The prover and the verifier are also given an integer K .
 - If $|S| \geq K$, then there should be a prover that makes the verifier accept with probability $\geq 2/3$.
 - If $|S| \leq K/2$, then no prover should make the verifier accept with probability greater than $1/3$.
- Such a protocol helps us to get a two round public coin protocol for GNI. This follows from the following observation:
 - Consider the set $S = \{(H, \pi) : H \cong G_1 \text{ or } H \cong G_2 \text{ and } \pi \in \text{Aut}(H)\}$. A permutation $\pi \in \text{aut}(H)$ if $\pi(H)$ is the same as H .
 - If $G_1 \not\cong G_2$, then $|S| = 2(n!)$
 - If $G_1 \cong G_2$, then $|S| = n!$.

Interactive Proofs

Set lower bound protocol

- The set lower bound protocol is a public coin protocol where the prover and verifier are given $S \subseteq \{0,1\}^m$ such that membership in S can be easily certified. The prover and the verifier are also given an integer K .
 - If $|S| \geq K$, then there should be a prover that makes the verifier accept with probability $\geq 2/3$.
 - If $|S| \leq K/2$, then no prover should make the verifier accept with probability greater than $1/3$.
- The Goldwasser-Sipser Set Lower Bound protocol indeed helps us to construct such a protocol.

End