Pubic Coin Interactive Proof

Xin Li

lixints@cs.jhu.edu
Topics

• _IP for GNI_

• _Public Coin vs. Private Coin_

• _Simulating Private Coin_
**IP with private coin**

- **Definition (IP):** For an integer \( k \geq 1 \) (may depend on the input length), say a language \( L \) is in \( \text{IP}[k] \) if \( \exists \) a probabilistic poly-time TM \( V \) that can have a \( k \)-round interaction with any function \( P : \{0,1\}^* \rightarrow \{0,1\}^* \) s.t.

  \[
  x \in L \Rightarrow \exists \ P, \ Pr[\text{Out}_{V < V, P}(x) = 1] \geq 2/3 \quad \text{(completeness)}
  \]

  \[
  x \notin L \Rightarrow \forall \ P, \ Pr[\text{Out}_{V < V, P}(x) = 1] \leq 1/3 \quad \text{(soundness)}
  \]

- Define \( \text{IP} = \bigcup_{c \geq 0} \text{IP}(n^c) \)

- The verifier’s random bits are private (not seen by the prover).
Graph Non-Isomorphism

• Say two graphs $G_1$ and $G_2$ are isomorphic if there is a permutation $\pi$ of the vertices of $G_1$ that $\pi(G_1)= G_2$.

• Let $\text{GNI} = \{< G_1, G_2 >, G_1$ and $G_2$ are not isomorphic$\}$. 

• $\text{GNI} \in \text{coNP}$ and not known to be in NP.

• Show $\text{GNI} \in \text{IP}$. 
Graph Non-Isomorphism

- V: pick $i \in \{1, 2\}$ uniformly randomly. Randomly permute the vertices $G_i$ of to get a new graph $H$. Send $H$ to $P$.

- $P$: identify which of $G_1$, $G_2$ was used to produce $H$. Send that information $j \in \{1, 2\}$ to $V$.

- V: accept iff $i=j$.

- If $<G_1, G_2> \in GNP$ then $\exists P$ s.t. $Pr[\text{accept}]=1$. Otherwise $\forall P, Pr[\text{accept}] \leq 1/2$ (can be decreased to 1/3 by repetition).
Graph Non-Isomorphism

• V: pick $i \in \{1, 2\}$ uniformly randomly. Randomly permeate the vertices $G_i$ of to get a new graph $H$. Send $H$ to $P$.

• P: identify which of $G_1$, $G_2$ was used to produce $H$. Send that information $j \in \{1, 2\}$ to $V$.

• V: accept iff $i=j$.

• Note that the protocol is also zero-knowledge: the verifier is only convinced that $G_1$, $G_2$ are different, but doesn’t know the difference.
Public Coins Interactive Proof

- The IP system for GNI seems to crucially rely on the verifier’s private random bits.

- The same is true for the “two pies game”.

- Can also define an interactive proof where prover has full access to verifier’s random bits.

- This leads to the definition of Arthur-Merlin proof.
AM and MA

- For every $k$ the complexity class $AM[k]$ is defined as the subset of $IP[k]$ s.t.

- The verifier’s messages are restricted to be the random bits used.

- The verifier is not allowed to use any other random bits not in the messages.

- This kind of IP is called a public coin proof, or an Arthur-Merlin proof.
**AM proof**

- Note: $P$ still cannot predict $V$’s random bits, but can see the random bits.

- Use AM to denote the class AM[2] (AMA: AM[3], AMAM: AM[4])

- AM is the class of languages with an IP where $V$ sends a random string, and $P$ responds with a message.

- MA denotes the class where $P$ sends the first message, and $V$ uses random bits to decide acceptance/rejection.
Some Properties of $AM[k]$

• Even in a public coin proof, $P$ doesn’t immediately see all of $V$’s random bits.

• Rather, $V$’s random bits are revealed to $P$ iteratively message by message.

• For constant $k \geq 2$, $AM[k]=AM[2]$.

• It is an open problem to have a nice characterization of $AM[k(n)]$ where $k(n)$ is a slowly growing function of $n$ (e.g., $\log n$).
Simulating Private Coins

• What is the relation between IP[k] and AM[k]?

• Clearly, ∀ k, AM[k] ⊆ IP[k].

• How about the other direction?

• It seems private coin protocols are more powerful, e.g., the IP for GNI crucially uses private coins.
Simulating Private Coins

• Surprisingly, that’s not exactly the case.

• Theorem (Goldwasser-Sipser’87): \( \forall k: \mathbb{N} \rightarrow \mathbb{N} \text{ with } k(n) \text{ computable in } \text{poly}(n) \text{ time,} \)
  \[
  \text{IP}[k] \subseteq \text{AM}[k+2]
  \]

• We’ll prove a special case and sketch the proof for the general case.

• Theorem: GNI \( \in \text{AM}[2] \)
Simulating Private Coins

• Theorem: $\text{GNI} \in \text{AM}[2]$

• Key idea: look at GNI in a more quantitative way.

• $\text{GNI} = \{< G_1, G_2 >, \ G_1 \text{ and } G_2 \text{ are not isomorphic} \}$. 

• Consider the following set of labeled graphs $\mathcal{S} = \{H: H \cong G_1 \text{ or } H \cong G_2 \}$. 
Simulating Private Coins

• $S = \{ H : H \cong G_1 \text{ or } H \cong G_2 \}$.

• Important property: it is easy to certify that a graph $H$ is in $S$ (by providing the permutation mapping $H$ to either $G_1$ or $G_2$).

• An $n$ vertex graph $G$ has at most $n!$ equivalent graphs.

• For simplicity, assume both $G_1$ and $G_2$ have exactly $n!$ equivalent graphs.
Simulating Private Coins

• \( S = \{ H : H \cong G_1 \text{ or } H \cong G_2 \} \).

• For simplicity, assume both \( G_1 \) and \( G_2 \) have exactly \( n! \) equivalent graphs.

• The size of \( S \) differ by a factor of 2 depending on whether \( G_1 \cong G_2 \).

• If \( G_1 \cong G_2 \), then \( |S| = n! \); otherwise \( |S| = 2n! \).
Simulating Private Coins

• In general, however, $G_1$ or $G_2$ may have less than $n!$ equivalent graphs.

• This happens iff $\exists$ a non-trivial automorphism $\pi$, i.e., a non-identity permutation $\pi$ s.t. $\pi(G) = G$.

• These $\pi$ form the automorphism group of $G$, $\text{aut}(G)$.

• $S = \{(H, \pi), H \cong G_1 \text{ or } H \cong G_2 \text{ and } \pi \in \text{aut}(H)\}$. 
Simulating Private Coins

• $S = \{(H, \pi), H \cong G_1 \text{ or } H \cong G_2 \text{ and } \pi \in \text{aut}(H)\}$.

• (1) membership in $S$ can be certified using a short certificate.

• (2) If $G_1 \cong G_2$, then $|S| = n!$ (case a); otherwise $|S| = 2n!$ (case b).

• For GNI, prover only needs to convince verifier that case b holds, using a set lower bound protocol.
Set Lower Bound Protocol

• Assumption: $\exists$ a set $S$ whose definition is know to both $P$ and $V$.

• Membership in $S$ can be certified using a short (poly length) certificate.

• The set lower bound protocol is a public coin interactive proof that allows $P$ to certify the approximate size of $S$. 
Set Lower Bound Protocol

• A public coin interactive proof that allows $P$ to certify the approximate size of $S$.

• Suppose the prover’s claimed size of $S$ is $k$.

  • If $|S| \geq k$, then $\exists P$, $\Pr [\text{Out}_V <V, P> = 1] \geq 2/3$.

  • If $|S| \leq k/2$, then $\forall P$, $\Pr [\text{Out}_V <V, P> = 1] \leq 1/3$. 
**Tools: Pairwise Independent Hash Functions**

- Let $H_{n,k}$ be a collection of functions from $\{0,1\}^n$ to $\{0,1\}^k$.

- Say $H_{n,k}$ is pairwise independent if $\forall \ x, x' \in \{0,1\}^n$ with $x \neq x'$ and $\forall \ y, y' \in \{0,1\}^k$, $
  \Pr[h(x)=y \land h(x')=y'] = 2^{-2k} = \Pr[h(x)=y] \Pr[h(x')=y']$, where $h$ is chosen uniformly from $H_{n,k}$.

- Equivalently, $\forall \ x, x' \in \{0,1\}^n$ with $x \neq x'$, if $h$ is chosen uniformly from $H_{n,k}$ then $(h(x), h(x'))$ is distributed uniformly over $\{0,1\}^k \times \{0,1\}^k$. 
Tools: Pairwise Independent Hash Functions

• Construction: ∀ n, define $H_{n,n}$ to be $\{h_{a,b}\}$ where $\forall a, b \in \{0,1\}^n (GF(2^n))$, $h_{a,b}(x)=ax+b$.

• Theorem: $H_{n,n}$ is a collection of pairwise independent hash functions (if $k < n$, can output $k$ bits instead of $n$ bits).

• Pf: $\forall x, x'$ with $x \neq x'$ and $\forall y, y'$, $h(x)=y$ and $h(x')=y'$ iff $ax+b=y$ and $ax'+b=y'$.

• This gives $a=(y-y')/(x-x')$ and $b=y-ax$. So $(a, b)$ is completely determined and thus $Pr=2^{-2n}$. 
Set Lower Bound Protocol

• Assumption: ∃ a set $S \subseteq \{0,1\}^m$ whose definition is know to both $P$ and $V$.

• Membership in $S$ can be certified using a short (poly length) certificate.

• Both parties know a number $k$.

• If $|S| \geq k$, then $\exists P$, $Pr[Out_V <V, P>=1] \geq 2/3$; If $|S| \leq k/2$, then $\forall P$, $Pr[Out_V <V, P>=1] \leq 1/3$. 
Set Lower Bound Protocol

• Let \( t \) be an integer s.t. \( 2^{t-2} < k \leq 2^{t-1} \). Let \( H_{m,t} \) be a collection of pair-wise independent hash functions from \( \{0,1\}^m \) to \( \{0,1\}^t \).

• \( V \): Randomly pick a function \( h \) from \( H_{m,t} \), and a random \( y \) from \( \{0,1\}^t \). Send \( h, y \) to \( P \).

• \( P \): Try to find an \( x \in S \) s.t. \( h(x) = y \). Send \( x \) to \( V \) with a certificate that \( x \in S \).

• \( V \): If \( h(x) = y \) and the certificate checks out, accept; otherwise reject.
Set Lower Bound Protocol

• Analysis: when can P make V accept?

• \textit{It happens iff} \( h, y \) happen to be \( s.t. \exists x \in S \text{ satisfying } h(x)=y \).

• Now analyze the probability that this happens.

• Show a gap of the probabilities in the two cases.
Set Lower Bound Protocol

- **Claim:** Let $S \subseteq \{0,1\}^m$ be s.t. $|S| \leq 2^{t-1}$. Let $p^* = |S|/2^t$.

  - Then $3p^*/4 \leq \Pr[\exists \ x \in S, h(x) = y] \leq P^*$.

- Assume claim holds. If $|S| \leq k/2 \leq 2^{t-2}$ then $\Pr[\exists \ x \in S, h(x) = y] \leq P^* = 1/2 * k/2^t$.

- If $|S| \geq k$ then $\Pr[\exists \ x \in S, h(x) = y] > 3/4 * k/2^t$. So there is a gap between the two cases (note $k/2^t$ is a constant).
Set Lower Bound Protocol

• Claim: Let $S \subseteq \{0,1\}^m$ be s.t. $|S| \leq 2^{t-1}$. Let $p^* = |S|/2^t$.

• Then $3p^*/4 \leq \Pr[\exists x \in S, h(x)=y] \leq P^*$. Probability over random choice of $h$ and $y$.

• Upper bound: follows trivially from the fact that for any fixed $h$, $h(x)$ has size at most $|S|$.

• Show that $\forall y \in \{0,1\}^t$, $\Pr[\exists x \in S, h(x)=y] \geq 3p^*/4$. 
Set Lower Bound Protocol

• Show that $\forall y \in \{0,1\}^t$, $\Pr[\exists x \in S, h(x) = y] \geq 3p^*/4$.

• $\forall x \in \{0,1\}^m$ define the $E_x$ as the event that $h(x) = y$.

• $\Pr[\exists x \in S, h(x) = y] = \Pr[U_x \in S \ E_x] \geq \sum_{x \in S} \Pr[E_x] - 1/2 \sum_{x \neq x' \in S} \Pr[E_x \cap E_{x'}]$ (inclusion-exclusion).

• By pair-wise independence, $\Pr[E_x] = 2^{-t}$ and $\Pr[E_x \cap E_{x'}] = 2^{-2t}$ and the claim follows.
AM Protocol for GNI

• Using the set lower bound protocol, the protocol for GNI is as follows.

• $V$ and $P$ run several iterations of the set lower bound protocols in parallel.

• Set $p^* = \frac{k}{2^t}$ and $V$ accept iff at least $\frac{5p^*}{8}$ fraction of iterations accept.

• The completeness and soundness now become $\geq \frac{2}{3}$ and $\leq \frac{1}{3}$ respectively. The # of rounds stay at 2. Can even get perfect completeness ($\Pr[\text{accept}] = 1$).
Sketch of the proof $IP[k] \subseteq AM[k+2]$

- Idea: $P$ demonstrates to $V$ an approximate lower bound of the size of the set of random strings which would make the private $V$ accept.

- Recall that in the private coin protocol $IP[k]$,

  - $x \in L \Rightarrow \exists P, \Pr[Out_{V < V, P}(x)=1] \geq 2/3$ and $x \notin L \Rightarrow \forall P, \Pr[Out_{V < V, P}(x)=1] \leq 1/3$.

- There is a gap between the two probabilities, so can use the set lower bound protocol, but need to proceed round by round.
Graph Isomorphism

• Question: can GI be NP-complete?

• Theorem: If GI is NP-complete, then $PH=\Sigma_2^p$.

• Proof: we show that if GI is NP-complete, then $\Sigma_2^p \subseteq \Pi_2^p \Rightarrow PH=\Sigma_2^p$.

• Suppose GI is NP-complete, then GNI is coNP-complete.
Graph Isomorphism

• GNI is coNP-complete => \( \neg \text{SAT} \leq_p \text{GNI} \).

• \( \exists \) a polynomial time computable function \( f \) s.t. \( \forall \ n \ \text{variable formula } \Phi \),
  \( \forall y \ \Phi(y) \text{ is True iff } f(\Phi) \in \text{GNI} \)

• Consider any \( \Sigma_2 \text{SAT formula } \psi = \exists x \in \{0,1\}^n \ \forall y \in \{0,1\}^n \ \Phi(x, y) \).

• \( \Sigma_2 \text{SAT is } \Sigma_2^p \text{ complete. We show that } \Sigma_2 \text{SAT} \in \Pi_2^p \).
Graph Isomorphism

• Consider any $\Sigma_2$ SAT formula $\psi = \exists x \in \{0,1\}^n \forall y \in \{0,1\}^n \Phi(x, y)$.

• $\exists$ a polynomial time computable function $f$ s.t. $\forall$ $n$ variable formula $\Phi$,
  $\forall y \Phi(y)$ is True iff $f(\Phi) \in \text{GNI}$

• $\psi$ is equivalent to $\exists x \in \{0,1\}^n g(x) \in \text{GNI}$, where $g(x)=f(\Phi(x, y))$.

• Using parallel repetition, GNI has an AM proof with perfect completeness and soundness $< 2^{-n}$.
Graph Isomorphism

• Let $V$ be the verifier’s algorithm. Let $m$ be the length of $V$’s random bits, and $m'$ be the length of $P$’s message.

• $\psi$ is equivalent to $\exists x \in \{0,1\}^n \ g(x) \in \text{GNI}$, where $g(x)=f(\Phi(x, y))$.

• $\psi$ is True=> $\exists x \in \{0,1\}^n \ \forall r \in \{0,1\}^m \ \exists a \in \{0,1\}^{m'} V(g(x), r, a)=1$ (perfect completeness)

  => $\forall r \in \{0,1\}^m \ \exists x \in \{0,1\}^n \ \exists a \in \{0,1\}^{m'} V(g(x), r, a)=1$ (*)

• $\psi$ is False => $\forall x \in \{0,1\}^n \ g(x) \notin \text{GNI}$.
Graph Isomorphism

• $\psi$ is True $\Rightarrow \forall \, r \in \{0,1\}^m \exists \, x \in \{0,1\}^n \exists \, a \in \{0,1\}^{m'} \, V(g(x), r, a)=1$ (*)

• $\psi$ is False $\Rightarrow \forall \, x \in \{0,1\}^n \, g(x) \not\in \text{GNI}$.

• Since soundness $< 2^{-n}$, $\exists$ an $r \in \{0,1\}^m$ that makes $V$ reject on every input $x$.

• $\psi$ is False $\Rightarrow \exists \, r \in \{0,1\}^m \, \forall \, x \in \{0,1\}^n \, \forall \, a \in \{0,1\}^{m'} \, V(g(x), r, a)=0$.

Because the public coin protocol
Graph Isomorphism

- \( \psi \) is True => \( \forall r \in \{0,1\}^m \exists x \in \{0,1\}^n \exists a \in \{0,1\}^{m'} V(g(x), r, a)=1 \) (*)

- \( \psi \) is False => \( \exists r \in \{0,1\}^m \forall x \in \{0,1\}^n \forall a \in \{0,1\}^{m'} V(g(x), r, a)=0. \)

- Thus, deciding \( \psi \) is equivalent to deciding (*) which \( \in \Pi_2 \).

- Hence, GI is NP-complete => \( \Sigma_2 \subseteq \Pi_2 \).