Lecture 04

Foundations of Probabilistic Proofs
Fall 2020
Alessandro Chiesa

Public Coins vs Private Coins

Randomness is essential for interactive proofs, and it comes in different forms.

Ex 1: in 2-message IP for GNI, the verifier's random bit b must be secret

Ex 2: in poly(n)-message IP for TQBF, all verifier randomness is sent to the prover

Today we study how these settings compare.

Def: A verifier V is public-coin if its every message is a freshly sampled uniform random string of a prescribed length. Otherwise, V is private coin.

Def: AM[K]/MA[K] are languages decidable via public-coin K-round interactive proofs where the verifier/prover moves first.

lemma (trivial) $\forall K$, $AM[K]/MA[K] \subseteq IP[K]$

A surprising result:

theorem: $\forall K$, $IP[K] \subseteq AM[K+1]$ Will not prove in class, but instead...

Revisiting Graph Non-Isomorphism

We will prove a special case: **theorem:** $GNI \in AM[1]$

<u>Idea</u>: look at graph isomorphism in a quantitative way

given (G_0, G_1), define $S := \{ H \mid H \equiv G_0 \text{ or } H \equiv G_1 \}$.

Observe that:

- can prove that $H \in S$ by giving isomorphism to G_0 or G_1
- $G_0 \equiv G_1 \rightarrow |S| = n!$
- $G_0 \not\equiv G_1 \rightarrow |S| = 2 \cdot n!$

[assuming that $aut(G_0) = aut(G_1) = id$]

can remove assumption by considering $S := \{ (H, \psi) \mid (H \equiv G_0 \vee H \equiv G_1) \wedge \psi \in aut(H) \}$

Hence, it suffices for the prover to convince the verifier that $|S| = 2 \cdot (n!)$ but not $|S| = n!$.

<u>Approach</u>:

1. recall pairwise independent hashing
2. set lower bound protocol
3. interactive proof

Pairwise Independent Hashing

A family of functions $H_{m,\ell} = \{ h : \{0,1\}^m \to \{0,1\}^\ell \}$ is pairwise independent if

$$\forall \text{ distinct } x, x' \in \{0,1\}^m \quad \forall y, y' \in \{0,1\}^\ell \qquad \Pr_{h \in H_{m,\ell}} [h(x) = y \wedge h(x') = y'] = \frac{1}{2^{2\ell}} .$$

Example: random affine function

$$H_{m,m} = \{ h_{a,b}(x) = ax + b \}_{a,b \in \mathbb{F}_{2^m}}$$

Indeed: $\Pr_{a,b} \begin{bmatrix} h_{a,b}(x) = y \\ h_{a,b}(x') = y' \end{bmatrix} = \Pr_{a,b} \begin{bmatrix} ax + b = y \\ ax' + b = y' \end{bmatrix} = \Pr_{a,b} \begin{bmatrix} a = \frac{y - y'}{x - x'} \\ b = y - ax \end{bmatrix} = \frac{1}{2^{2m}} .$

Actually we are interested in a family $H_{m,\ell}$ with $\ell < m$. So consider

$$H_{m,n} = \{ h_{a,b}(x) = ax + b \bmod 2^\ell \}_{a,b \in \mathbb{F}_{2^m}}$$

The bit truncation does not affect pairwise independence: there are $2^{m-\ell}$ choices of a s.t. $a \cdot (x - x') \bmod 2^\ell = (y - y')$ and for each such a there are $2^{m-\ell}$ choices of b s.t. $ax + b \bmod 2^\ell = y$.

So we have an efficient pairwise independent family $H_{m,\ell}$ for any m, ℓ with $\ell < m$.

Set Lower Bound Protocol

Let $S \subseteq \{0,1\}^m$ be such that $S \in NP$ (we can check that $x \in S$ with the help of a prover).
We seek an interactive proof for the promise problem "YES is $|S| \geq B$, NO is $|S| \leq \frac{B}{2}$".

P_S		$V_S(B)$
		set $\ell \in \mathbb{N}$ s.t. $2^{\ell-2} \leq B \leq 2^{\ell-1}$
	$\xleftarrow{h,\,y}$	sample $h \leftarrow H_{m,\ell}$ and $y \leftarrow \{0,1\}^\ell$
find $x \in S$ s.t. $h(x) = y$		
find proof π for "$x \in S$"	$\xrightarrow{x,\,\pi}$	$h(x) \overset{?}{=} y$ & π certifies that "$x \in S$"

Soundness: if $|S| \leq \frac{B}{2}$ then $\Pr_{h,y}[\exists x \in S : h(x) = y] \leq \sum_{x \in S} \Pr_{h,y}[h(x) = y] \leq \frac{|S|}{2^\ell} \leq \frac{1}{2}\frac{B}{2^\ell}$

Completeness: if $|S| \geq B$ then $\Pr_{h,y}[\exists x \in S : h(x) = y] \geq \frac{3}{4}\frac{B}{2^\ell}$

gap is $\frac{1}{4}\frac{B}{2^\ell} \geq \frac{1}{16}$

in completeness we do not use randomness of y

proof: WLOG $|S| = B$ (larger helps). By inclusion-exclusion principle. For every $y \in \{0,1\}^n$,

$$\Pr_h[\exists x \in S : h(x) = y] \geq \sum_{x \in S} \Pr_h[h(x) = y] - \frac{1}{2}\sum_{\substack{x,x' \in S \\ x \neq x'}} \Pr_h\left[\begin{matrix} h(x) = y \\ h(x') = y \end{matrix}\right] = |S| \cdot \frac{1}{2^\ell} - \frac{1}{2} \cdot |S|^2 \cdot \frac{1}{2^{2\ell}}$$

$$= \frac{|S|}{2^\ell}\left(1 - \frac{|S|}{2^{\ell+1}}\right) = \frac{B}{2^\ell}\left(1 - \frac{B}{2^{\ell+1}}\right) \geq \frac{B}{2^\ell}\left(1 - \frac{1}{4}\right) = \frac{3}{4}\frac{B}{2^\ell}.$$

Public Coin Interactive Proof for GNI

theorem: $GNI \in AM[1]$

We use the set lower bound protocol on $S := \{H \in \{0,1\}^{n^2} \mid H \equiv G_0 \text{ or } H \equiv G_1\}$. $[S := \{(H,\psi) \mid \dots\}]$

$P(G_0, G_1)$		$V(G_0, G_1)$
		$B := 2 \cdot n!$, $m := n^2$
		set ℓ s.t. $2^{\ell-2} \leq B \leq 2^{\ell-1}$ $[\ell = O(n \log n)]$
find $H \in S$ s.t. $h(H) = y$	$\xleftarrow{h,y}$	sample $h \in H_{m,\ell}$ and $y \leftarrow \{0,1\}^\ell$
and find iso $\phi : H \to G_b$	$\xrightarrow{H,\phi}$	$h(H) \stackrel{?}{=} y$ and $(\phi(H) = G_0$ or $\phi(H) = G_1)$

Completeness: if $(G_0, G_1) \in GNI$ then $|S| = 2 \cdot n!$ so

$$\Pr\left[\begin{array}{c}\text{honest prover}\\ \text{convinces verifier}\end{array}\right] = \Pr_{h,y}\left[\exists H \in S : h(H) = y\right] \geq \frac{3}{4} \cdot \frac{B}{2^\ell}.$$

Soundness: if $(G_0, G_1) \notin GNI$ then $|S| = n!$ so

$$\Pr\left[\begin{array}{c}\text{malicious prover}\\ \text{convinces verifier}\end{array}\right] = \Pr_{h,y}\left[\exists H \in S : h(H) = y\right] \leq \frac{1}{2} \cdot \frac{B}{2^\ell}.$$

Perfect Completeness for Public Coins

The set lower bound protocol introduced a completeness error.
This is not essential:

theorem: If L has a k-round public-coin interactive proof then L has a $(k+1)$-round public-coin interactive proof with perfect completeness.

For example, we get a 2-round public-coin IP for GNI with perfect completeness.

The ideas behind the theorem are related to Lautemann's proof that $BPP \subseteq \Sigma_2^P$.

Suppose L is decidable by a probabilistic polynomial-time algorithm M with error bound ε. By repetition (& majority) we can assume that $\varepsilon < \frac{1}{m}$. [$m$ is # random bits]
Given x, define $A(x) = \{r \in \{0,1\}^m \mid M(x;r) = 1\}$.
If $x \in L$ then $|A(x)| \geq (1-\varepsilon)2^m$, and can show by probabilistic method that

$$\exists s^{(1)}, \dots, s^{(m)} \in \{0,1\}^m \; \forall r \in \{0,1\}^m \; \exists i \in [m] \; s^{(i)} \oplus r \in A(x) \equiv \exists y \forall z \; \phi(x,y,z) = 1$$

$\Rightarrow L \in \Sigma_2^P$

If $x \notin L$ then $|A(x)| \leq \varepsilon \cdot 2^m$, and can show by union bound that

$$\forall s^{(1)}, \dots, s^{(m)} \in \{0,1\}^m \; \exists r \in \{0,1\}^m \; \forall i \in [m] \; s^{(i)} \oplus r \notin A(x) \equiv \forall y \exists z \; \overline{\phi(x,y,z)}$$

theorem: If L has a k-round public-coin interactive proof then L has a $(k+1)$-round public-coin interactive proof with perfect completeness.

Proof:

Let (P,V) be a k-round public-coin IP for L.

Let m be the number of random bits used by the verifier.

We assume that the completeness and soundness errors are bounded by $\varepsilon \le \frac{1}{3}\cdot\frac{1}{m}$.

[This is WLOG because we can parallel repeat & rule by majority.]

Given a malicious prover $\tilde{P}$ and instance x, define

$$A(\tilde{P},x) := \{ r \in \{0,1\}^m \mid \langle \tilde{P}, V(x;r) \rangle = 1 \}.$$

If $x \in L$ then $|A(P(x),x)| \geq (1-\varepsilon)2^m$.

If $x \notin L$ then $\forall \tilde{P}$ $|A(\tilde{P},x)| \leq \varepsilon 2^m$.

Similarities with Lautemann's proof: $\exists\forall / \forall\exists$ characterization of $x \in L / x \notin L$.

Differences: the randomness shift must account for multiple rounds

The new interactive proof for L is as follows:

$(r_1,\dots,r_k) \in \{0,1\}^m$ verifier randomness

$P^*(x)$		$V^*(x;r)$
find $s^{(1)},\dots,s^{(m)} \in \{0,1\}^m$ such that $\forall r \in \{0,1\}^m \; \exists i \in [m] \; s^{(i)} \oplus r \in A(P,x)$	$\xrightarrow{s^{(1)},\dots,s^{(m)} \in \{0,1\}^m}$	
	for $j = 1,\dots,k$:	
$\left[\begin{array}{l}\text{for } i=1,\dots,m: \\ \quad a_j^{(i)} := P(x, s_1^{(i)} \oplus r_1, \dots, s_{j-1}^{(i)} \oplus r_{j-1})\end{array}\right]$	$\xrightarrow{a_j^{(1)},\dots,a_j^{(m)}}$	
	$\xleftarrow{r_j}$	
		$\bigvee_{i=1}^{m} V(x, a_1^{(i)} a_2^{(i)} \dots a_k^{(i)}; s^{(i)} \oplus r) = 1$

Completeness: Suppose that $x \in L$.

If P^* succeeds in finding "good" $s^{(1)},\dots,s^{(m)}$ then P^* convinces V^* w.p. 1.

So we argue that there exist good $s^{(1)},\dots,s^{(m)}$ via the probabilistic method:

$$\Pr_{s^{(1)},\dots,s^{(m)}}\left[\exists r \in \{0,1\}^m \; \forall i \in [m] \; s^{(i)} \oplus r \notin A(P,x)\right] \leq \sum_{r \in \{0,1\}^m} \Pr_{s^{(1)},\dots,s^{(m)}}\left[\forall i \in [m] \; s^{(i)} \oplus r \notin A(P,x)\right]$$

$$= 2^m \cdot \Pr_{s^{(1)},\dots,s^{(m)}}\left[\forall i \in [m] \; s^{(i)} \notin A(P,x)\right] \leq 2^m \varepsilon^m \leq 2^m \cdot \left(\frac{1}{3m}\right)^m < 1.$$

[the computation actually tells us that most choices of $s^{(1)},\dots,s^{(m)}$ are good]

Soundness: Suppose that $x \notin L$. We argue that the soundness error is at most $\frac{1}{3}$.

For this it suffices to show that for a fixed $i \in [m]$ the probability that a malicious prover wins the i-th execution is at most $\varepsilon \leq \frac{1}{3} \cdot \frac{1}{m}$.

Fix a malicious prover $\tilde{P}$, get $(s^{(1)}, \dots, s^{(m)}) := \tilde{P}(\perp)$, and define:

$$A(\tilde{P}, x, i) := \{ r \in \{0,1\}^m \mid V(x, \tilde{P}(r_1)_i, \tilde{P}(r_1, r_2)_i, \dots; s^{(i)} \oplus r) = 1 \}.$$

claim: $|A(\tilde{P}, x, i)| \leq \varepsilon \cdot 2^m$

proof: Suppose $|A(\tilde{P}, x, i)| > \varepsilon \cdot 2^m$. We construct $\tilde{P}_i$ that convinces V w.p. $> \varepsilon$ (a contradiction).

First $\tilde{P}_i$ runs $\tilde{P}$ to get $s^{(1)}, \dots, s^{(m)} \in \{0,1\}^m$ and saves $s^{(i)}$.

Then $\forall j \in [k]$, having received verifier messages $r_1, \dots, r_{j-1}$, $\tilde{P}_i$ computes its next message a_j as:

$$\tilde{P}_i(r_1, \dots, r_{j-1}) := \tilde{P}(r_1 \oplus s_1^{(i)}, \dots, r_{j-1} \oplus s_{j-1}^{(i)})_i.$$

We argue that $r \in A(\tilde{P}, x, i) \leftrightarrow s^{(i)} \oplus r \in A(\tilde{P}_i, x)$, so $|A(\tilde{P}_i, x)| = |A(\tilde{P}, x, i)| > \varepsilon \cdot 2^m$ (contradiction).

$$r \in A(\tilde{P}, x, i) \leftrightarrow V(x, \tilde{P}(r_1)_i, \tilde{P}(r_1, r_2)_i, \dots; s^{(i)} \oplus r) = 1$$
$$\leftrightarrow V(x, \tilde{P}_i(s_1^{(i)} \oplus r_1), \tilde{P}_i(s_1^{(i)} \oplus r_1, s_2^{(i)} \oplus r_2), \dots; s^{(i)} \oplus r) = 1 \leftrightarrow s^{(i)} \oplus r \in A(\tilde{P}_i, x).$$