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[$K$] $\leq$ IP[$K$]

A surprising result:

**Theorem:** $\forall K$, IP[$K$] $\leq$ AM[$K+1$]  

Will not prove in class, but instead...
We will prove a special case: \textbf{theorem:} GNI \in AM[1]

Idea: look at graph isomorphism in a quantitative way

given \((G_0, a_0)\), 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 \( G_1 \).
- \( G_0 \equiv G_1 \rightarrow |S| = n! \) \[\text{assuming that} \quad \text{can remove assumption by considering} \]
- \( G_0 \not\equiv G_1 \rightarrow |S| = 2 \cdot n! \) \[\text{\( \text{aut}(G_0) = \text{aut}(G_1) = \text{id} \)} \]

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

\textbf{Approach:}

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

A family of functions \( H_{m,l} = \{ h : \{0,1\}^m \rightarrow \{0,1\}^l \} \) is pairwise independent if

\[
\forall x, x' \in \{0,1\}^m, \forall y, y' \in \{0,1\}^l \quad \Pr_{h \in H_{m,l}}[h(x) = y \land h(x') = y'] = \frac{1}{2^l}.
\]

Example: random affine function

\[
H_{m,m} = \left\{ h_{a,b}(x) = ax + b \right\}_{a, b \in \mathbb{F}_2^m}
\]

Indeed:

\[
\Pr_{a, b}[h_{a,b}(x) = y] = \Pr_{a, b}[ax + b = y] = \Pr_{a, b}[a = \frac{y - y'}{x - x'}] = \frac{1}{2^m}.
\]

Actually we are interested in a family \( H_{m,l} \) with \( l < m \). So consider

\[
H_{m,l} = \left\{ h_{a,b}(x) = ax + b \mod 2^l \right\}_{a, b \in \mathbb{F}_2^m}
\]

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

So we have an efficient pairwise independent family \( H_{m,l} \) for any \( m, l \) with lcm.
Set Lower Bound Protocol

Let $S \leq \Sigma_0 \cup \Sigma_1^n$ be such that $S \in \text{NP}$ (we can check that $x \in S$ with the help of a prover). We seek an interactive proof for the promise problem "YES is $|S| > B$, NO is $|S| \leq \frac{B}{2}$.

find $x \in S$ s.t. $h(x) = y$
find proof $\pi$ for "$x \in S$"

\[ P_S \]

\[ V_S(B) \]
set $c \in \mathbb{N}$ s.t. $2^{c-2} \leq B \leq 2^{c-1}$
sample $h \leftarrow H_{m, c}$ and $y \in \{0, 1\}^c$
\[ h(x) = y \text{ & } \pi \text{ certifies that } x \in S \]

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

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

\[ \text{gap is } \frac{1}{4} \cdot \frac{B}{2^c} \geq \frac{1}{16} \]

proof: WLOG $|S| = B$ (large helps). By inclusion-exclusion principle. For every $y \in \Sigma_0 \cup \Sigma_1^n$,
\[ \Pr_{h} [\exists x \in S : h(x) = y] = \sum_{x \in S} \Pr_{h} [h(x) = y] - \frac{1}{2} \sum_{x \neq x'} \Pr_{h} [h(x) = y] = |S| \cdot \frac{1}{2^c} - \frac{1}{2} \cdot |S|^2 \cdot \frac{1}{2^{2c}} \]
\[ = \frac{|S|}{2^c} \left( 1 - \frac{|S|}{2^c} \right) = \frac{B}{2^c} \left( 1 - \frac{B}{2^{c+1}} \right) \geq \frac{B}{2^c} \left( 1 - \frac{B}{2^c} \right) = \frac{3}{4} \cdot \frac{B}{2^c} . \]
Public Coin Interactive Proof for GNI

**Theorem:** \( \text{GNI} \in \text{AM}[1] \)

We use the set lower bound protocol on \( S := \{H \in \{0,1\}^n \mid H \equiv \text{Go} \land H \equiv \text{G}_i \} \). \( S := \{(H,y) \mid \ldots\} \)

\[ P(G_0, G_i) \]

\[ \begin{array}{c}
\text{find } H \in S \text{ s.t. } h(H) = y \\
\text{and find iso } \phi: H \rightarrow G_b
\end{array} \]

\[ \begin{array}{c}
V(G_0, G_i) \\
B := 2 \cdot n!, \quad m := n^2
\end{array} \]

set \( \ell \) s.t. \( 2^\ell - 2 \leq B \leq 2^\ell - 1 \) \( \ell = \Theta(n \log n) \)

sample \( h \in H_{m,B} \) and \( y \in \{0,1\}^\ell \)

\[ h(H) \equiv y \text{ and } (\phi(H) = G_0 \text{ or } \phi(H) = G_i) \]

**Completeness:** if \((G_0, G_i) \in \text{GNI}\) then \( |S| = 2 \cdot n! \) so

\[ Pr[\text{honest prover convinces verifier}] = Pr[\exists H \in S : h(H) = y] \geq \frac{3}{4} \cdot \frac{B}{2^\ell}. \]

**Soundness:** if \((G_0, G_i) \notin \text{GNI}\) then \( |S| = n! \) so

\[ Pr[\text{malicious prover convinces verifier}] = Pr[\exists H \in S : h(H) = y] \leq \frac{1}{2} \cdot \frac{B}{2^\ell}. \]
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 \( 	ext{QWI} \) with perfect completeness.

The ideas behind the theorem are related to Laustenmann's proof that \( \text{BPP} \subseteq \Sigma^p_2 \).

Suppose \( L \) is decidable by a probabilistic polynomial-time algorithm \( M \) with error bound \( \varepsilon \). By repetition (\& majority) we can assume that \( \varepsilon < \frac{1}{m} \). [\( m \) is \# random bits] Given \( x \), define \( A(x) = \{ \text{re} \in \{0,1\}^m : M(x; r) = 1 \} \).

If \( x \in L \) then \( |A(x)| \geq (1-\varepsilon)2^m \), and can show by probabilistic method that

\[ \exists s^{(i)}_1, \ldots, s^{(i)}_m \in \{0,1\}^m \ \forall \text{re} \in \{0,1\}^m \ \exists i \in [m] \ s^{(i)}_i \oplus \text{re} \in A(x) \equiv \exists y \forall z \ \phi(x, y, z) = 1 \]

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

\[ \forall s^{(i)}_1, \ldots, s^{(i)}_m \in \{0,1\}^m \ \exists i \in [m] \ s^{(i)}_i \oplus \text{re} \in A(x) \equiv \forall y \exists z \ \bar{\phi}(x, y, z) \]
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 $\frac{1}{3} \cdot \frac{1}{m}$. [This is WLOG because we can parallel repeat & rule by majority.]

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

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

If $x \in L$ then $|A(P(x), x)| \geq (1-\varepsilon)2^m$.
If $x \not\in L$ then $|A(\tilde{P}, x)| \leq \varepsilon 2^m$.

Similarities with Laurmann's proof: $\exists / \exists \notin$ characterization of $x \in L / x \not\in L$.

Differences: the randomness shift must account for multiple rounds.
The new interactive proof for \( L \) is as follows:

\[
P^*(x)
\]

find \( s^{(0)},...,s^{(m)} \in \{0,1\}^m \) such that \( \forall i \in \{0,1\}^m \ \exists i \in [m] \ s^{(i)} \in A(P,x) \)

\[
[\text{for } i=1,...,m:\ a_j^{(i)} := P(x, s_j^{(i)} \oplus r_j, ..., s_{j-1}^{(i)} \oplus r_{j-1})]
\]

\[
\begin{array}{c}
\overset{s^{(0)},...,s^{(m)} \in \{0,1\}^m}{\downarrow} \\
\overset{\text{for } j=1,...,k:}{\downarrow} \\
\overset{a_j^{(i)} \rightarrow a_j^{(m)}}{\downarrow} \\
\overset{r_j}{\downarrow} \\
\overset{\text{for } i=1,...,m:}{\uparrow} \\
\overset{V(x, a_1^{(i)} a_2^{(i)} \ldots a_k^{(i)} ; s^{(i)} \oplus r) = 1}{\uparrow}
\end{array}
\]

**Completeness:** Suppose that \( x \in L \).
If \( P^* \) succeeds in finding "good" \( s^{(0)},...,s^{(m)} \) then \( P^* \) convinces \( V^* \) w.p. 1.

So we argue that there exist good \( s^{(0)},...,s^{(m)} \) via the probabilistic method:

\[
\Pr_{s^{(0)},...,s^{(m)}} \left[ \exists r \in [0,1]^m \forall i \in [m] \ s^{(i)} \oplus r \in A(P,x) \right] = \sum_{r \in [0,1]^m} \Pr_{s^{(0)},...,s^{(m)}} \left[ \forall i \in [m] \ s^{(i)} \oplus r \in A(P,x) \right]
\]

\[
= 2^m \cdot \Pr_{s^{(0)},...,s^{(m)}} \left[ \forall i \in [m] \ s^{(i)} \in A(P,x) \right] \leq 2^m \cdot \frac{1}{2^m} = 2^m \cdot \left( \frac{1}{2^m} \right)^m < 1.
\]

The computation actually tells us that most choices of \( s^{(0)},...,s^{(m)} \) 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 \( \varepsilon \leq \frac{1}{3} \frac{1}{m} \).

Fix a malicious prover \( \tilde{P} \), get \((s^{i_1}, \ldots, s^{i_m}) = \tilde{P}(1)\), and define:

\[
A(\tilde{P}, x, i) := \{ r \in \{0,1\}^m | V(x, \tilde{P}(r)_i, \tilde{P}(r, i)_{i_2, \ldots, i_m}; s^{i} \oplus r) = 1 \}.
\]

claim: \( |A(\tilde{P}, x, i)| \leq 3 \cdot 2^m \)

proof: Suppose \( |A(\tilde{P}, x, i)| > 3 \cdot 2^m \). We construct \( \tilde{P}_i \) that convinces \( V \) w.p. \( \geq \varepsilon \) (a contradiction).

First \( \tilde{P}_i \) runs \( \tilde{P} \) to get \( s^{i_2}, \ldots, s^{i_m} \in \{0,1\}^m \) and saves \( s^{(i)} \).

Then \( \forall j \in [K] \), having received verifier messages \( r_1, \ldots, r_{j-1} \), \( \tilde{P}_i \) computes its next message \( q_j \) as:

\[
\tilde{P}_i (r_1, \ldots, r_{j-1}) := \tilde{P}(r_1 \oplus s^{i_1}, \ldots, r_{j-1} \oplus s^{(i)}_{j-1}); i.
\]

We argue that \( r \in A(\tilde{P}, x, i) \leftrightarrow s^{(i)} \oplus r \in A(\tilde{P}_i, x) \), so \( |A(\tilde{P}_i, x)| = |A(\tilde{P}, x, i)| > 3 \cdot 2^m \) (contradiction).

\( r \in A(\tilde{P}, x, i) \leftrightarrow V(x, \tilde{P}(r)_i, \tilde{P}(r, i)_{i_2, \ldots, i_m}; s^{(i)} \oplus r) = 1 \)

\( \leftrightarrow V(x, \tilde{P}_i (s^{(i)} \oplus r_i), \tilde{P}_i (s^{(i)} \oplus r_i, s^{(i)} \oplus r_{i_2}); \ldots; s^{(i)} \oplus r) = 1 \leftrightarrow s^{(i)} \oplus r \in A(\tilde{P}_i, x) \).