Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 22

Public vs Private Coins & Perfect Completeness

Public Coins vs Private Coins

Randomness in interactive proofs 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: How do 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 k-round public-coin IPs where the verifier/prover moves first. ("A" stands for Arthur = verifier & "M" stands for Merlin = prover)

Trivial: $\forall k$, AM[k], MA[k] $\subseteq$ IP[k]

Surprising: theorem: $\forall k$, IP[k] $\subseteq$ AM[k+1]

We study a special case of the theorem today.

Revisiting Graph Non-Isomorphism

theorem: $GNI \in AM[k=1]$ (Previously we proved that $GNI \in IP[k=1]$.)

Idea: look at graph isomorphism in a quantitative way

def: The automorphism group of a graph $G=(V,E)$ is

$$aut(G) = \{\pi : V \to V \mid \pi \text{ is a permutation and } \pi(G) = G\}$$

claim: G has $n!/|aut(G)|$ isomorphic graphs.

In particular, $|\{(H,\pi) \mid H \equiv G \wedge \pi \in aut(H)\}| = n!$

Given (G_0, G_1), define $S := \{(H,\pi) \mid (H \equiv G_0 \vee H \equiv G_1) \wedge \pi \in aut(H)\}$.

Observe that: $\begin{cases} G_0 \equiv G_1 \to |S| = n! \\ G_0 \not\equiv G_1 \to |S| = 2 \cdot n! \end{cases}$

Moreover, can prove that $(H,\pi) \in S$ by providing isomorphism to G_0 or G_1.

→ it suffices for the prover to convince the verifier that $|S| = 2 \cdot n!$

Tool: Pairwise Independent Hashing

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

$$\forall\ x, x' \in \{0,1\}^m \text{ with } x \neq x',\ \forall\ y, y' \in \{0,1\}^\ell \quad \Pr_{h \leftarrow H_{m,\ell}} \begin{bmatrix} h(x) = y \\ h(x') = y' \end{bmatrix} = \frac{1}{2^{2\ell}} .$$

EXAMPLE: $H_{m,m} = \{ h_{a,b}(x) = ax + b \}_{a,b \in \mathbb{F}_{2^m}}$ (a random affine function over $\mathbb{F}_{2^m}$)

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

The truncation to ℓ bits does NOT affect pairwise independence:
there are $2^{m-\ell}$ choices of $a \in \mathbb{F}_{2^m}$ 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. $ax + b \bmod 2^\ell = y$.

We have an efficient pairwise-independent function family $H_{m,\ell}$ for every m, ℓ with $\ell \leq m$.

Set Lower Bound Protocol

Let $S \subseteq \{0,1\}^m$ be such that $S \in NP$ (can check that $x \in S$ with the help of a proof).

GOAL: an IP for the promise problem $\left\{\begin{array}{ll} \text{YES} & \text{if } |S| \geq B \\ \text{NO} & \text{if } |S| \leq B/2 \end{array}\right\}$.

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

<u>lemma</u>: if $|S| \geq B$ then $\Pr\left[\begin{array}{c}\text{honest prover} \\ \text{convinces verifier}\end{array}\right] \geq \frac{3}{4} B \cdot \frac{1}{2^\ell}$

if $|S| \leq \frac{B}{2}$ then $\Pr\left[\begin{array}{c}\text{malicious prover} \\ \text{convinces verifier}\end{array}\right] \leq \frac{1}{2} B \cdot \frac{1}{2^\ell}$

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

<u>Soundness</u>: if $|S| \leq \frac{B}{2}$ then $\forall$ malicious prover

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

Set Lower Bound Protocol

Let $S \subseteq \{0,1\}^m$ be such that $S \in NP$ (can check that $x \in S$ with the help of a proof).

GOAL: an IP for the promise problem $\left\{ \begin{array}{ll} \text{YES} & \text{if } |S| \geq B \\ \text{NO} & \text{if } |S| \leq B/2 \end{array} \right\}$.

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

lemma: if $|S| \geq B$ then $\Pr\left[\begin{array}{l}\text{honest prover}\\ \text{convinces verifier}\end{array}\right] \geq \frac{3}{4} B \cdot \frac{1}{2^\ell}$

if $|S| \leq \frac{B}{2}$ then $\Pr\left[\begin{array}{l}\text{malicious prover}\\ \text{convinces verifier}\end{array}\right] \leq \frac{1}{2} B \cdot \frac{1}{2^\ell}$

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

Completeness: WLOG $|S| = B$ (larger $|S|$ increases acceptance probability). For every $y \in \{0,1\}^\ell$,

randomness of y is not used for completeness

$$\Pr\left[\begin{array}{l}\text{honest prover}\\ \text{convinces verifier}\end{array}\right] = \Pr_h\left[\exists x \in S : h(x) = y\right] \geq \sum_{x \in S} \Pr[h(x) = y] - \sum_{\substack{x, x' \in S \\ x \neq x'}} \Pr\left[\begin{array}{l} h(x) = y \\ h(x') = y \end{array}\right] = |S| \cdot \frac{1}{2^\ell} - \binom{|S|}{2} \cdot \frac{1}{2^{2\ell}}$$

Inclusion-Exclusion Bound
$\Pr[\cup_i E_i] \geq \sum_i \Pr[E_i] - \sum_{i \neq j} \Pr[E_i \cap E_j]$

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

Public Coin Interactive Proof for GNI

theorem: GNI $\in$ AM[K=1]

Apply the set lower bound protocol on $S := \left\{ (H,\pi) \in \{0,1\}^{n^2+n\log n} \;\middle|\; \begin{array}{l}(H \equiv G_0 \vee H \equiv G_1) \\ \wedge\ \pi \in \mathrm{aut}(H)\end{array} \right\}$.

$P(G_0,G_1)$		$V(G_0,G_1)$
		$B := 2 \cdot n!$, $m := n^2 + n \cdot \log n$
		Set ℓ s.t. $2^{\ell-2} \leq B \leq 2^{\ell-1}$ [and so $\ell = O(n \cdot \log n)$]
Find $(H,\pi) \in S$ s.t. $h(H,\pi) = y$.	$\xleftarrow{h,\,y}$	Sample $h \leftarrow H_{m,\ell}$ and $y \leftarrow \{0,1\}^\ell$.
Find isomorphism ϕ from H to G_b.	$\xrightarrow{(H,\pi),\,\phi}$	Check that $h(H,\pi) = y$ and $(H,\pi) \in S$.
		[$(\phi(H) = G_0 \vee \phi(H) = G_1) \wedge \pi \in \mathrm{aut}(H)$]

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

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

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

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

Perfect Completeness for Public Coins

The set lower bound protocol introduces a completeness error.

This is NOT essential:

<u>theorem</u>: If L has a k-round public-coin IP
then L has a $(k+1)$-round public-coin IP with perfect completeness.

Example: We showed that $GNI \in AM[k=1]$, so we deduce that $GNI \in AM[\varepsilon_c = 0, k=2]$.
(GNI has a 2-round public-coin IP with perfect completeness.)

We proceed in several steps.

- Warmup: simple protocol to reduce (but not eliminate) completeness error.
- Review: Lautemann's proof that $BPP \subseteq \Sigma_2^P$.
- Proof: we build on warmup and review.

Warmup: Reduce Completeness Error

Repeat the protocol multiple times and accept if AT LEAST one execution accepts.

$P_*(x)$:

$V_*(x)$:

For $j = 1, \ldots, k$:

$\forall i \in [t],\ a_j^{(i)} := P(x, \rho_1^{(i)}, \ldots, \rho_{j-1}^{(i)})$ $\xrightarrow{a_j^{(1)}, \ldots, a_j^{(t)}}$

$\xleftarrow{\rho_j^{(1)}, \ldots, \rho_j^{(t)}}$ Sample $\rho_j^{(1)}, \ldots, \rho_j^{(t)} \in \{0,1\}^{r_j}$.

$\exists i \in [t]\ V(x, a_1^{(i)}, \ldots, a_k^{(i)}; \rho_j) = 1$

For every repetition parameter $t \in \mathbb{N}$:

- $\varepsilon_c \mapsto \varepsilon_c' = \varepsilon_c^t$ $\quad \Pr[\langle P_*(x), V_*(x) \rangle = 0] = \left(\Pr[\langle P(x), V(x) \rangle = 0]\right)^t \leq \varepsilon_c^t$
- $\varepsilon_s \mapsto \varepsilon_s' = t \cdot \varepsilon_s$ $\quad \Pr[\langle P_*(x), V_*(x) \rangle = 1] \leq t \cdot \Pr[\langle P(x), V(x) \rangle = 1] \leq t \cdot \varepsilon_s$
- $k \mapsto k' = k$ $\quad$ The t executions are in parallel.
- $c \mapsto c' = t \cdot c$ $\quad$ Each execution contributes c bits of communication.

The completeness error can be made arbitrarily small, but NOT zero.

BUT: a clever twist on this protocol achieves perfect completeness.

Review: Lautemann Theorem

theorem: $BPP \subseteq \Sigma_2^P$

Recall that $L \in \Sigma_2^P \leftrightarrow \exists$ polynomial-time algorithm D s.t. $\begin{cases} x \in L \to \exists y \forall z \;\; D(x,y,z)=1 \\ x \notin L \to \forall y \exists z \;\; D(x,y,z)=0 \end{cases}$

Let L be decidable by a polynomial-time probabilistic algorithm M with $\begin{cases} \text{YES-error } \alpha \\ \text{NO-error } \beta \end{cases}$.

We use the probabilistic method to show the two conditions:

- If $x \in L$ then (provided $t > -\frac{r}{\log \alpha}$) $\exists \sigma^{(1)},\dots,\sigma^{(t)} \in \{0,1\}^r \; \forall \rho \in \{0,1\}^r \; (\exists i \in [t] \; M(x;\sigma^{(i)} \oplus \rho) = 1)$:

$$\Pr_{\sigma^{(1)},\dots,\sigma^{(t)}}[\exists \rho \in \{0,1\}^r \, (\forall i \in [t] \; M(x;\sigma^{(i)} \oplus \rho) = 0)] \leq \sum_{\rho \in \{0,1\}^r} \Pr_{\sigma^{(1)},\dots,\sigma^{(t)}}[\forall i \in [t] \; M(x;\sigma^{(i)} \oplus \rho) = 0]$$

For t large enough MOST $\sigma^{(1)},\dots,\sigma^{(t)}$ are good.

$$= 2^r \cdot \Pr_{\rho^{(1)},\dots,\rho^{(t)}}[\forall i \in [t] \; M(x;\rho^{(i)}) = 0] \leq 2^r \cdot \alpha^t < 1.$$

- If $x \notin L$ then (provided $t < \frac{1}{\beta}$) $\forall \sigma^{(1)},\dots,\sigma^{(t)} \in \{0,1\}^r \; \exists \rho \in \{0,1\}^r \; (\forall i \in [t] \; M(x;\sigma^{(i)} \oplus \rho) = 0)$:

Fix $\sigma^{(1)},\dots,\sigma^{(t)} \in \{0,1\}^r$. For every $i \in [t]$, $\Pr_{\rho \in \{0,1\}^r}[M(x;\sigma^{(i)} \oplus \rho) = 1] = \Pr_{\rho \in \{0,1\}^r}[M(x;\rho) = 1] \leq \beta$.

Hence,

$$\Pr_{\rho \in \{0,1\}^r}[\exists i \in [t] \; M(x;\sigma^{(i)} \oplus \rho) = 1] \leq \sum_{i \in [t]} \Pr_{\rho \in \{0,1\}^r}[M(x;\sigma^{(i)} \oplus \rho) = 1] \leq t \cdot \beta < 1.$$

The condition $\exists t \in \mathbb{N} \;\; -\frac{r}{\log \alpha} < t < \frac{1}{\beta}$ can be achieved by repetition (and taking majority).

Eg, for $\alpha_0, \beta_0 = 1/3$, ℓ-wise error reduction gives $\alpha, \beta = \exp(-\ell)$, yielding $O(\ell \cdot r) < t < \exp(\ell)$.

Proof of Perfect Completeness for IPs [1/3]

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

Let r be the randomness complexity of V, divided by rounds as $r_1,\dots,r_k$ with $\sum_{j\in[k]} r_j = r$.

For every repetition parameter $t\in\mathbb{N}$ the new public-coin IP (P_*,V_*) is as follows:

$P_*(x)$:

Find $\sigma^{(1)},\dots,\sigma^{(t)}\in\{0,1\}^r$ s.t.

$\forall \rho\in\{0,1\}^r\ \exists i\in[t]\ \langle P(x),V(x,\sigma^{(i)}\oplus\rho)\rangle=1$

$$\xrightarrow{\sigma^{(1)},\dots,\sigma^{(t)}}$$

For $j=1,\dots,k$:

$\forall i\in[t],\ a_j^{(i)} := P(x,\sigma_1^{(i)}\oplus\rho_1,\dots,\sigma_{j-1}^{(i)}\oplus\rho_{j-1})$

$$\xrightarrow{a_j^{(1)},\dots,a_j^{(t)}}$$

$$\xleftarrow{\rho_j}$$

$V_*(x)$:

Sample $\rho_j\in\{0,1\}^{r_j}$.

$\exists i\in[t]\ V(x,a_1^{(i)},\dots,a_k^{(i)};\sigma^{(i)}\oplus\rho)=1$

- $\varepsilon_c \mapsto \varepsilon_c'=0$ Provided that $t>-\frac{r}{\log\varepsilon_c}$, as we prove soon.
- $\varepsilon_s \mapsto \varepsilon_s'=t\cdot\varepsilon_s$ As we prove soon. It is <1 provided that $t<\frac{1}{\varepsilon_s}$.
- $k \mapsto k'=k+1$ The are t (correlated) executions in parallel, plus an extra message.
- $c \mapsto c'=t\cdot(c+r)$ Each execution contributes c bits, plus $t\cdot r$ bits in the extra message.

The condition $\exists t\in\mathbb{N}\ -\frac{r}{\log\varepsilon_c}<t<\frac{1}{\varepsilon_s}$ can be achieved by repetition (and taking majority).

Proof of Perfect Completeness for IPs

$P_*(x)$:

Find $\sigma^{(1)},\dots,\sigma^{(t)} \in \{0,1\}^r$ s.t.

$\forall \rho \in \{0,1\}^r \; \exists i \in [t] \; \langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 1$

$\xrightarrow{\sigma^{(1)},\dots,\sigma^{(t)}}$

$V_*(x)$:

For $j = 1,\dots,k$:

$\forall i \in [t]$, $a_j^{(i)} := P(x, \sigma_1^{(i)} \oplus \rho_1, \dots, \sigma_{j-1}^{(i)} \oplus \rho_{j-1})$

$\xrightarrow{a_j^{(1)},\dots,a_j^{(t)}}$

$\xleftarrow{\rho_j}$

Sample $\rho_j \in \{0,1\}^{r_j}$.

$\exists i \in [t] \; V(x, a_1^{(i)},\dots,a_k^{(i)}; \sigma^{(i)} \oplus \rho) = 1$

Completeness:

$\forall \rho \in \{0,1\}^r \; (\exists i \in [t] \; \langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 1)$

Suppose that $x \in L$.

If $P_*(x)$ finds "good" $\sigma^{(1)},\dots,\sigma^{(t)}$ then $P_*(x)$ convinces $V_*(x)$ with probability 1.

They exist:

$$\Pr_{\sigma^{(1)},\dots,\sigma^{(t)}}\left[\exists \rho \in \{0,1\}^r \; \forall i \in [t] \; \langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 0\right] \leq \sum_{\rho \in \{0,1\}^r} \Pr_{\sigma^{(1)},\dots,\sigma^{(t)}}\left[\forall i \in [t] \; \langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 0\right]$$

$$= 2^r \cdot \Pr_{\rho^{(1)},\dots,\rho^{(t)}}\left[\forall i \in [t] \; \langle P(x), V(x, \rho^{(i)})\rangle = 0\right] \leq 2^r \cdot \varepsilon_c^t < 1.$$

$t > -\frac{r}{\log \varepsilon_c}$

Proof of Perfect Completeness for IPs

Soundness: Suppose that $x \notin L$ and fix a malicious prover $\tilde{P}_*$.

For every $i \in [t]$, define $\tilde{P}_i$ against V as follows:

- Run $\tilde{P}_*$ to obtain $(\sigma^{(1)}, \dots, \sigma^{(t)})$.
- In round $j \in [k]$ (having received $\rho_1, \dots, \rho_{j-1}$ from V):
  - compute the next message as $a_j := \tilde{P}_*(\rho_1 \oplus \sigma_1^{(i)}, \dots, \rho_{j-1} \oplus \sigma_{j-1}^{(i)})[i]$.

Define $(\sigma^{(1)}, \dots, \sigma^{(t)}) := \tilde{P}_*$ (the prover's first message).

For every $i \in [t]$,

$$\Pr_{\rho \in \{0,1\}^r}\left[V(x, \tilde{P}_*(\rho_1)[i], \dots, \tilde{P}_*(\rho_1, \dots, \rho_k)[i]; \sigma^{(i)} \oplus \rho) = 1 \right]$$

$$= \Pr_{\rho \in \{0,1\}^r}\left[V(x, \tilde{P}_i(\sigma_1^{(i)} \oplus \rho_1), \dots, \tilde{P}_i(\sigma_1^{(i)} \oplus \rho_1, \dots, \sigma_k^{(i)} \oplus \rho_k); \sigma^{(i)} \oplus \rho) = 1 \right]$$

$$= \Pr_{\rho \in \{0,1\}^r}\left[V(x, \tilde{P}_i(\rho_1), \dots, \tilde{P}_i(\rho_1, \dots, \rho_k); \rho) = 1 \right] \leq \varepsilon_s .$$

We conclude that

$$\Pr_{\rho \in \{0,1\}^r}\left[\langle \tilde{P}_*, V_*(x;\rho) \rangle = 1 \right] = \Pr_{\rho \in \{0,1\}^r}\left[\exists i \in [t] \; V(x, \tilde{P}_*(\rho_1)[i], \dots, \tilde{P}_*(\rho_1, \dots, \rho_k)[i]; \sigma^{(i)} \oplus \rho) = 1 \right]$$

$$\leq \sum_{i \in [t]} \Pr_{\rho \in \{0,1\}^r}\left[V(x, \tilde{P}_*(\rho_1)[i], \dots, \tilde{P}_*(\rho_1, \dots, \rho_k)[i]; \sigma^{(i)} \oplus \rho) = 1 \right] \leq t \cdot \varepsilon_s < 1 .$$

$t < \frac{1}{\varepsilon_s}$

The Case of IOPs: Private to Public Coins

The IP transformation does not extend to IOPs:

the set lower bound protocol does NOT preserve query complexity.

Nevertheless a similar theorem holds:

<u>theorem</u>: If L has a k-round IOP with

then L has a $O(k)$-round public-coin IOP

The proof approach is as follows:

k-round IOP —[private-to-public transformation for IPs]→ $(k+1)$-round public-coin IP —[IP-to-IOP transformation]→ $O(k)$-round public-coin IOP

(An IOP can be viewed as an IP.)

(Makes the verifier read $O(1)$ bits from each message.)

A key ingredient of the IP-to-IOP transformation is Index-Decodable PCPs,

a strengthening of the notion of Holographic PCPs.

The Case of IOPs: Perfect Completeness

The IP transformation extends to IOPs with a moderate increase in query complexity: $q \mapsto q' = t \cdot q = O\left(-\frac{r}{\log \varepsilon_c}\right) \cdot q$.

Since usually $r = \Omega(\log n)$, q' is super-constant even if $q = O(1)$.

We can preserve query complexity (up to a small additive constant) with a small tweak:

$P_*(x)$:

Find $\sigma^{(1)},\dots,\sigma^{(t)} \in \{0,1\}^r$ s.t.

$\forall \rho \in \{0,1\}^r \ \exists i \in [t] \ \langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 1$

$\xrightarrow{\sigma^{(1)},\dots,\sigma^{(t)}}$

$V_*(x)$:

For $j = 1,\dots,k$:

$\forall i \in [t]$, $a_j^{(i)} := P(x, \sigma_1^{(i)} \oplus \rho_1, \dots, \sigma_{j-1}^{(i)} \oplus \rho_{j-1})$ $\xrightarrow{a_j^{(1)},\dots,a_j^{(t)}}$

$\xleftarrow{\rho_j}$ Sample $\rho_j \in \{0,1\}^{r_j}$.

Find $i \in [t]$ s.t. $\langle P(x), V(x, \sigma^{(i)} \oplus \rho)\rangle = 1$ $\xrightarrow{i}$ $V(x, a_1^{(i)}, \dots, a_k^{(i)}; \sigma^{(i)} \oplus \rho) = 1$

The IOP prover tells the IOP verifier which execution accepts.

➡ The IOP verifier reads $i \in [t]$, then reads $\sigma^{i} \in \{0,1\}^r$, and then checks the i-th execution with randomness $\sigma^{(i)} \oplus \rho$.

Note: the IOP verifier is adaptive.

New parameters:

- $\varepsilon_c \mapsto \varepsilon_c' = 0$
- $\varepsilon_s \mapsto \varepsilon_s' = t \cdot \varepsilon_s$
- $k \mapsto k' = k+1$
- $|\Sigma| \mapsto |\Sigma'| = \max\{|\Sigma|, 2^r, t\}$
- $\ell \mapsto \ell' = t \cdot \ell + t + 1$
- $q \mapsto q' = q+2$
- $r \mapsto r' = r$