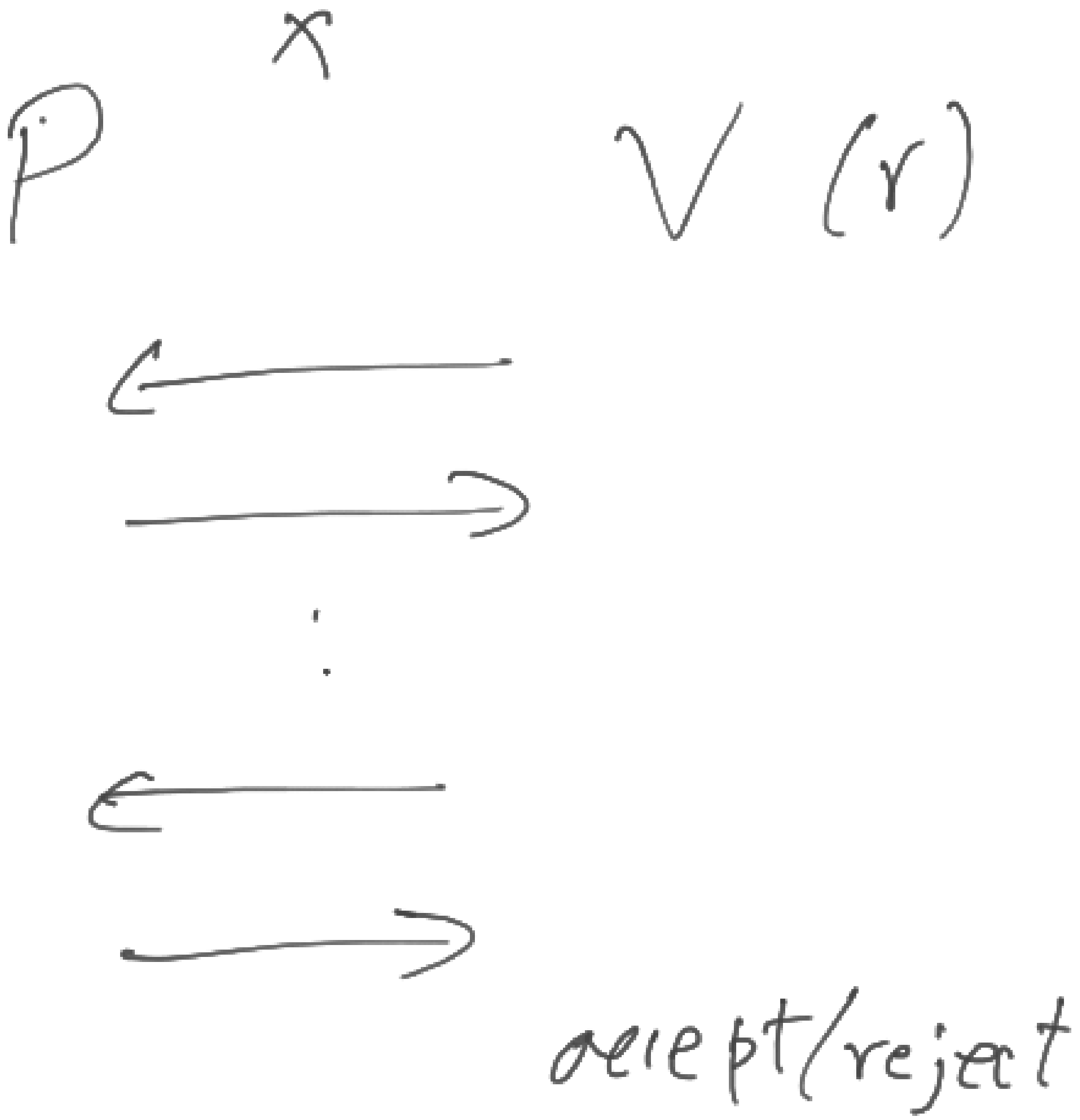
Resources in Interactive Proofs



P – comp. unbounded

V – poly time

Completeness:

If $x \in L$,

$$\Pr[\langle P, V\rangle(x) \text{ accepts}] \geq \frac{2}{3}$$

Soundness:

If $x \notin L$, $\forall P^*$

$$\Pr[\langle P^*, V\rangle(x) \text{ accepts}] \leq 1/3$$

Errors:

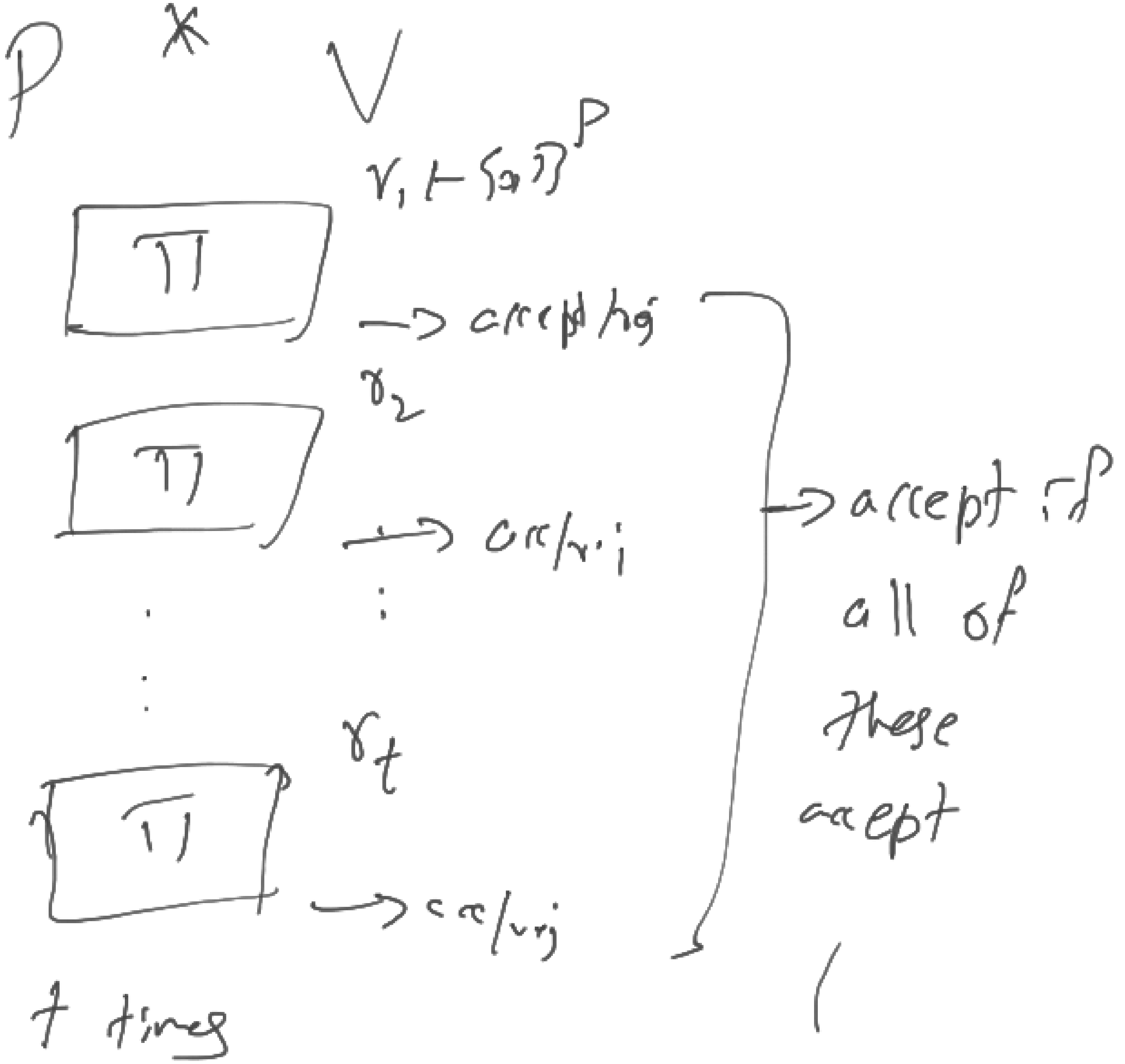
Thm: If L has an IP with completeness and soundness errors at most $1/3$, then it also has one with errors 2^{-t} for any $t \in \mathbb{N}$.

Suppose $\Pi = (P, V)$ that is a perfectly complete IP for L and has soundness error $1/3$

Π':

1. Run Π t times, independently
2. Accept ~~if~~ all the iterations accepted

Π':



Completeness:

if $x \in L$:

Since Π is perf.-complete all iters. will accept

Soundness:

if $x \notin L$:

E_i - event that i^{th} iter. accepts

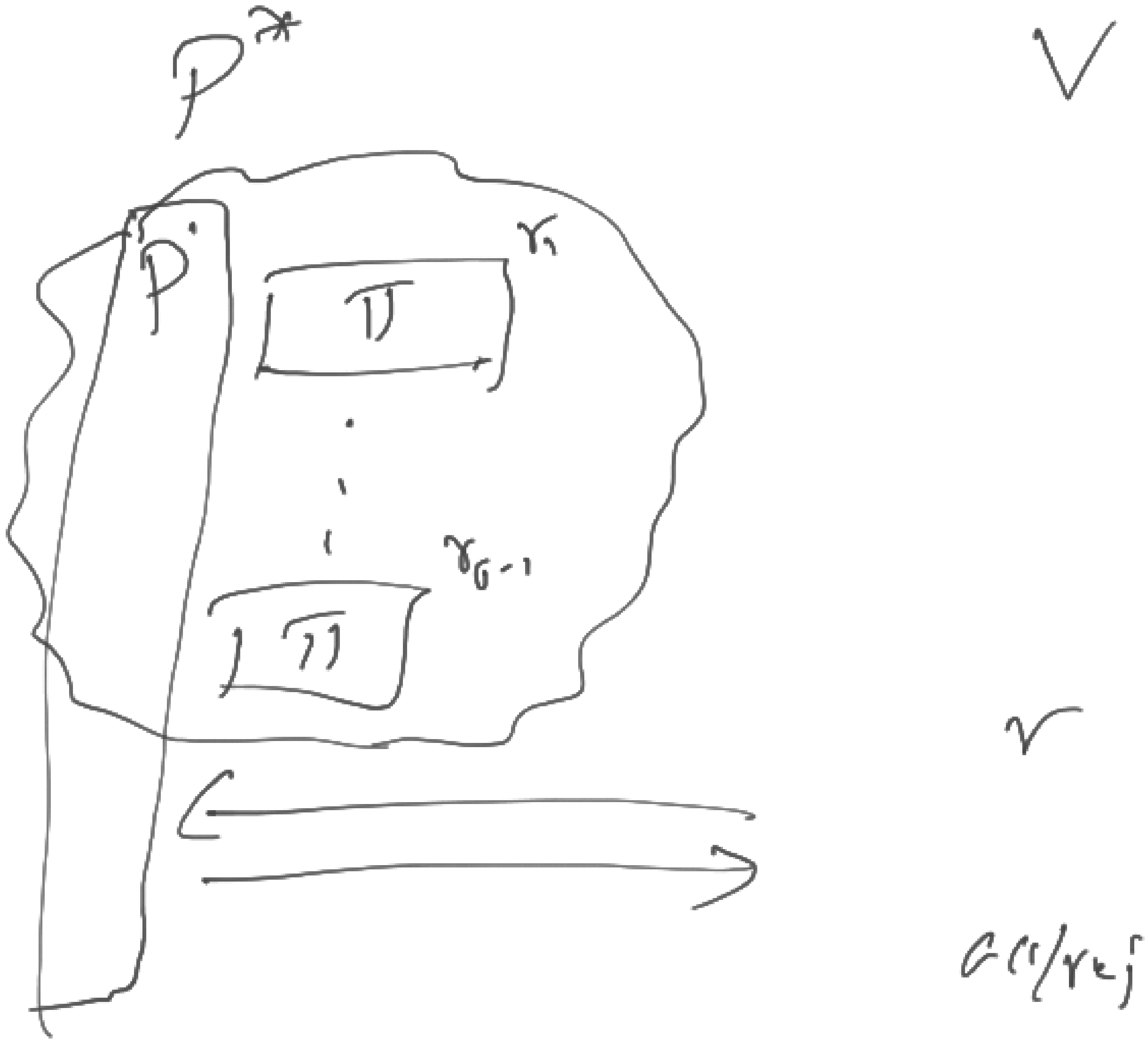
$E = E_1 \wedge \ldots \wedge E_t$

$$\Pr[E] = \Pr[E_1 \wedge \ldots \wedge E_t] = \Pr[E_1] \cdot \Pr[E_2 \mid E_1] \cdots \Pr[E_t \mid E_1 \wedge \ldots \wedge E_{t-1}]$$

$\forall i: \Pr[E_i] < 1/3$ so: $\Pr[E] < \left(\frac{1}{3}\right) \cdots \left(\frac{1}{3}\right) = \left(\frac{1}{3}\right)^t$

<u>Claim:</u> If $\Pr[E] > \frac{1}{3^t}$, then $\exists i: \Pr[E_i \mid E_1, \ldots, E_{i-1}] > \frac{1}{3}$

Given cheating prover P' for Π'
want P^* for Π

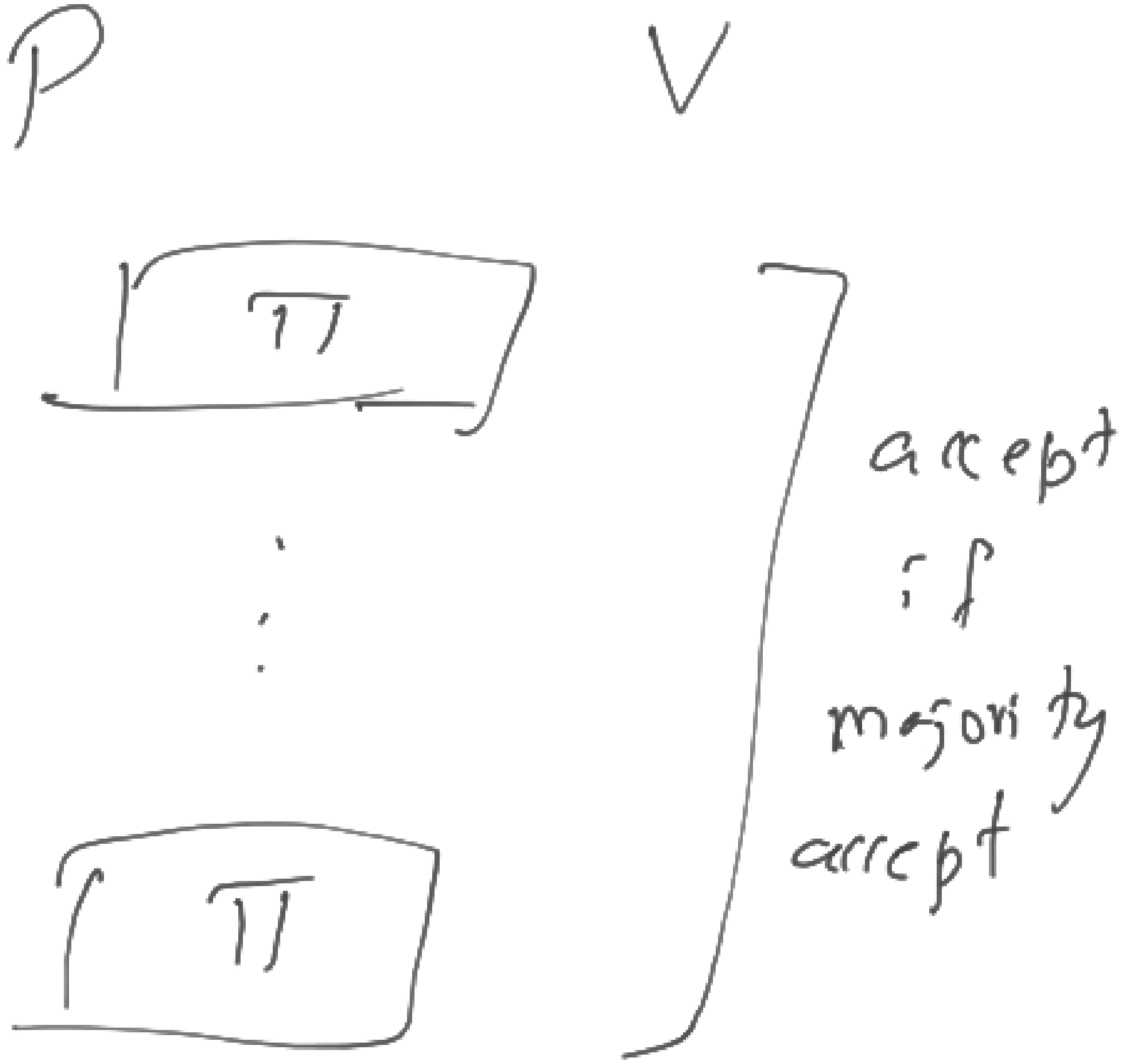


P^*:

1. Pick $r_1, \ldots, r_{i-1}$ s.t. $E_1, \ldots, E_{i-1}$ happen

2. Resume running i^{th} iteration of P' while interacting with V

$$\Pr[V \text{ acc}] = \Pr[E_i / E_1, \ldots, E_{i-1}] > 1/3$$



Completeness:

$$X_i = 1(E_i \text{ happens})$$

$$\Pr[\text{at least half of } E_i \text{ happen}]$$

$$= \Pr\left[\sum X_i > t/2\right]$$

$$E[X_i] \geq 2/3 \qquad E\left[\sum X_i\right] \geq 2t/3$$

$$\Pr\left[\sum X_i \leq t/2\right] = \Pr\left[\left(E\left[\sum X_i\right] - \sum X_i\right) \geq t/6\right] \leq e^{-\Omega(t)}$$

$$\forall \underbrace{P'}_{\text{prover for } \Pi'} \; \exists \, (\underbrace{P_1, \ldots, P_t}_{\text{provers for } \Pi}) :$$

$$\Pr\left[\langle (P_1, \ldots, P_t), V \rangle (x) \text{ accept}\right]$$

$$\geq \Pr\left[\langle P', V \rangle (x) \text{ accept}\right]$$

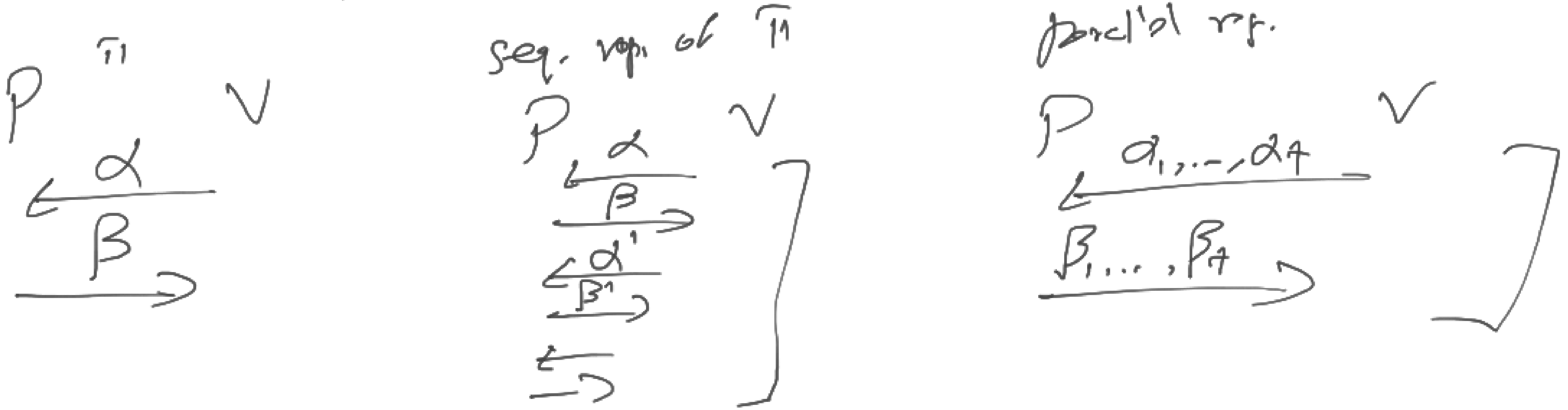
$(P_1, \ldots, P_t)$ ✓

$P_1 \quad \boxed{\Pi}$

$\vdots$

$P_t \quad \boxed{\Pi}$

- If L has an IP, it has a perfectly complete IP
- Only languages in NP have IPs with perfect soundness
- Parallel repetition also amplifies



Randomness

x

$P \qquad\qquad V\ (r)$

$$P \xleftarrow{\ \alpha_1(x;r)\ } V$$

$$P \xrightarrow{\ \beta_1\ } V$$

$$P \xleftarrow{\ \alpha_2(x,\alpha_1,\beta_1;r)\ } V$$

$$P \xrightarrow{\ \beta_2\ } V$$

$\vdots$

$(\alpha_1, \beta_1, \dots, \alpha_k, \beta_k, r)$

$\downarrow$ randomised

accept/rej

public-coin

x

$P \qquad\qquad V$

r_1

$$P \xleftarrow{\ r_1\ } V$$

$$P \xrightarrow{\ \beta_1\ } V$$

r_2

$$P \xleftarrow{\ r_2\ } V$$

$$P \xrightarrow{\ \beta_2\ } V$$

$\vdots$

$(r_1, \beta_1, r_2, \beta_2, \dots, r_k, \beta_k)$

$\downarrow$ deterministic

accept/reject

<u>Thm:</u> If L has an private-coin IP with k rounds of comm., then it has a public-coin IP with $k+2$ rounds of comm.

<u>Set lower bounds</u>

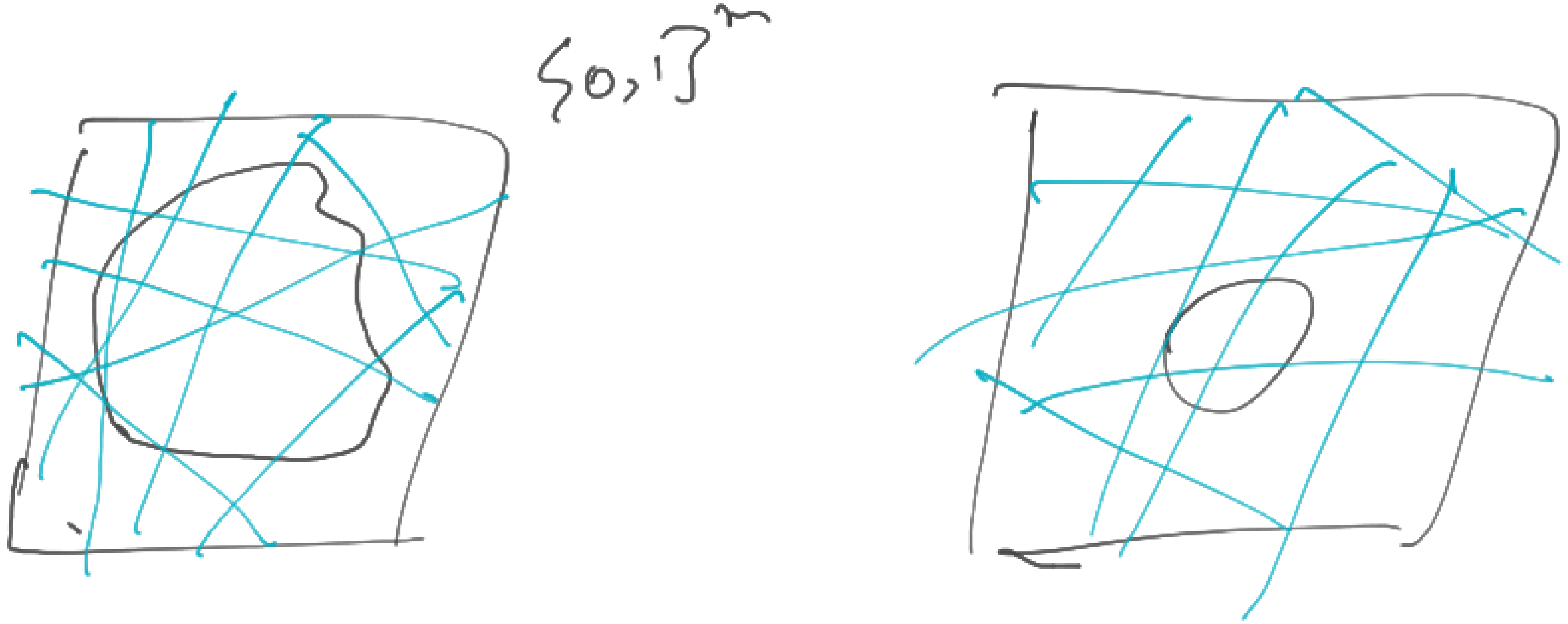
Given a set $S \subseteq \{0,1\}^m$ as a membership oracle:

$$M_S : \{0,1\}^m \to \{0,1\} \quad : \quad M_S(x) = 1 \text{ iff. } x \in S$$

and $t \leq m$.

Protocol that: if $|S| \geq 2^t$ accept w.h.p.

$|S| < 2^t/10$ reject w.h.p.



S

$|S| \geq 2^t$

$|S| \leq 2^t/10$

Protocol 1:

$A \leftarrow \{0,1\}^{t\times m},\ b \leftarrow \{0,1\}^t$

- V samples a random fn. $h: \{0,1\}^m \to \{0,1\}^t$, send to P
- P find $x \in S$ s.t. $h_{A,b}(x) = 0^t$
- V accepts iff $h_{A,b}(x) = 0$ and $M_S(x) = 1$

E_x = event that $h(x)=0$

$(\exists x\in S : h(x)=0) \equiv \bigvee_{x\in S} E_x$

Completeness: if $|S|\geq 2^t$

$$\Pr_h[\exists x\in S : h(x)=0] \geq \sum_{x\in S} \Pr[h(x)=0] - \sum_{\substack{\{x,x'\}\\ x\neq x'\\ x,x'\in S}} \Pr[h(x)=0 \wedge h(x')=0]$$

inclusion exclusion

$$= |S|\cdot\frac{1}{2^t} - {}^{|S|}C_2 \cdot \Pr[h(x)=0]\cdot \Pr[h(x')=0]$$

$$= \frac{|S|}{2^t} - \frac{|S|(|S|-1)}{2}\cdot\left(\frac{1}{2^t}\right)^2 \geq 1/2$$

Soundness: if $|S| < 2^t/10$

$$\Pr_h[\exists x\in S : h(x)=0] \leq \sum_{x\in S} \Pr_h[h(x)=0] = |S|\cdot\frac{1}{2^t} < \frac{1}{10}$$

Pairwise-Independent Hash family:

A family $H = \{h : X \to Y\}$ s.t. $\forall x_1 \neq x_2 \in X$ and $\forall y_1, y_2 \in Y$,

$$\Pr_{h \leftarrow H}\left[h(x_1) = y_1 \wedge h(x_2) = y_2\right] = \frac{1}{|Y|^2}$$

Example:

$H = \{h_{A,b} : \{0,1\}^m \to \{0,1\}^t\}$

$A \in \{0,1\}^{t \times m}$, $b \in \{0,1\}^t$

$h_{A,b}(x) = A \cdot x + b$ over $GF(2)$

Claim: H is pairwise-indep.

Public-coin protocol for 2-message IPs

$$P \qquad x \qquad V(r)$$

$$\xleftarrow{\ \alpha\ }$$

$$\xrightarrow{\ \beta\ }$$

$V(x, \alpha, \beta; r) \to$ accept / reject

$r \in \{0,1\}^{\ell}$

$\alpha \in \{0,1\}^{a}$

$$\forall \alpha, \ \Pr[V(x; r) = \alpha] = \frac{1}{2^{\ell - a}}$$

Simplifying assumptions:

- Perfectly complete
- Soundness error $< 1/100$
- Every message α is equally likely

$$S = \left\{ \alpha \;\middle|\; \begin{array}{l} \text{If first message} = \alpha\text{, then} \\ P \text{ can make } V \text{ accept} \\ \text{w.p. } 1 \end{array} \right\}$$

If $x \in L$: $|S| = 2^a$

$x \notin L$: $|S| \leq 2^a/100$

$$S = \{\alpha \mid \exists \beta : |\overbrace{\{r \mid V(x;r)=\alpha \wedge V(x,\alpha,\beta;r)=acc\}}^{S_{\alpha,\beta}}|$$

$$|S_{\alpha,\beta}| \geq 2^{l-a}\}$$

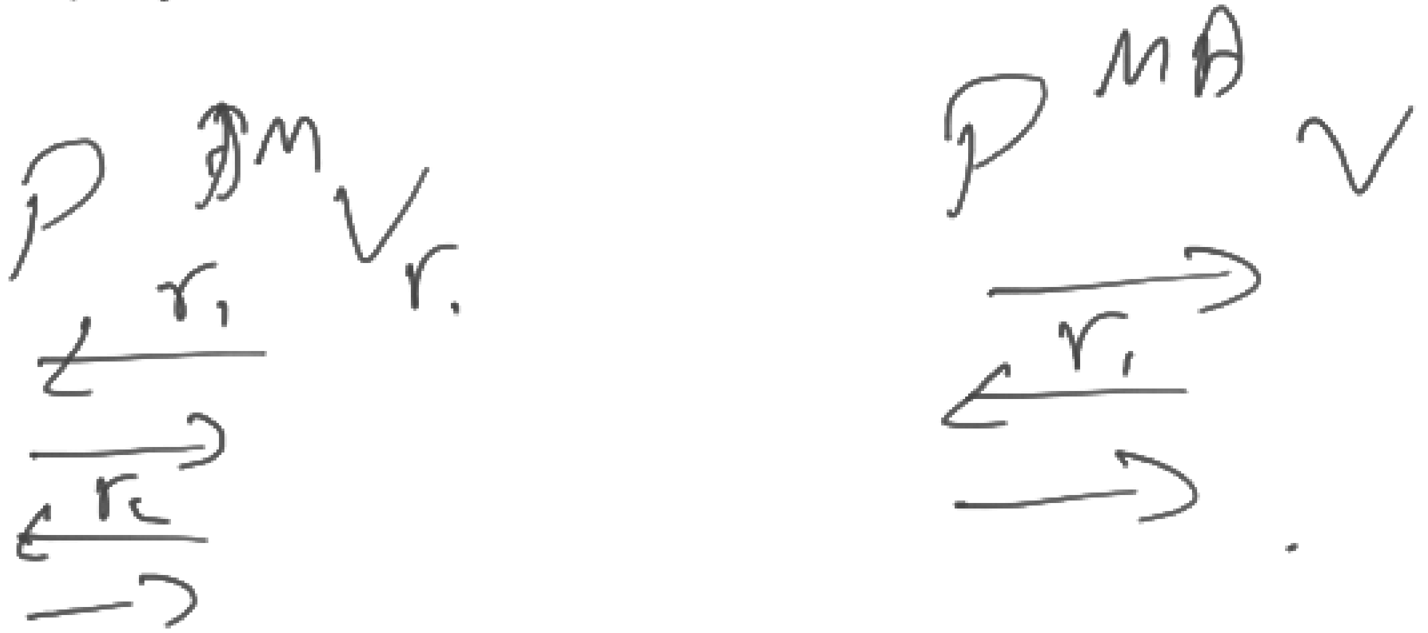
$$\begin{array}{ccl}
P & x & V \\
 & \xleftarrow{\quad h \quad} & \text{l.b. for } S \\
 & \xrightarrow{\quad \alpha,\beta \quad} & h(\alpha)=0 \\
 & & \alpha \in S \equiv \text{l.b. for } S_{\alpha,\beta} \\
 & \xleftarrow{\quad h' \quad} & \\
 & \xrightarrow{\quad r \quad} & V(x;r)=\alpha \\
 & & V(x,\alpha,\beta;r)=acc
\end{array}$$

Rounds:

Def 1 AM Proofs: Public-coin constant-round IPs

AM[k] – Public-coin IP with k messages starting with the verifier

MA[k] – " " " starts with the Prover



Thm: $AM[k+2] \subseteq AM[k]$

$AM = AM[2]$

$MA = MA[2]$

Thm: $MA \subseteq AM$

x

$P \quad\quad\quad V$

$P \xrightarrow{\beta} V$

$r \leftarrow \{0,1\}^p$

$V(x, \beta; r)$

$= acc/rej$

$|\beta| = b$

x

$P \quad\quad\quad V$

r

$P \xleftarrow{r} V$

$P \xrightarrow{\beta} V$

$V(x, \beta; r)$

$= acc/rej$

AM Protocol:

1. V sample $r_1, \dots, r_{100d} \leftarrow \{0,1\}^p$, send to P

2. P sends β

3. V checks whether majority of $V(x, \beta; r_i)$ accept

Completeness: If $x \in L$: $\exists \beta$: $\Pr[V(x, \beta; r) \text{ accept}] \geq 2/3$

$\Rightarrow E[|\{r_i \mid V(x, \beta; r_i) \text{ accepts}\}|] \geq \frac{2}{3} \cdot 100d$

Soundness: If $x \notin L$: for any β, $\Pr_r[V(x,\beta;r) \text{ acc}] < 1/3$

for any β, $E\left[\left|\{i \mid V(x,\beta;r_i) \text{ accepts}\}\right|\right] \le \frac{1}{3} \cdot 100b$

AM[4]

P $\qquad$ V

$P \xleftarrow{\alpha_1} V$

$P \xrightarrow{\beta_1} V$

$P \xleftarrow{\alpha_2} V$

$P \xrightarrow{\beta_2} V$

P $\qquad$ V

$P \xleftarrow{\alpha_1} V$

$P \xleftarrow{\alpha_2^1, \dots, \alpha_2^{100b}} V$

$P \xrightarrow{\beta_1} V$

$P \xrightarrow{\beta_2} V$

AM[2]

P $\qquad$ V

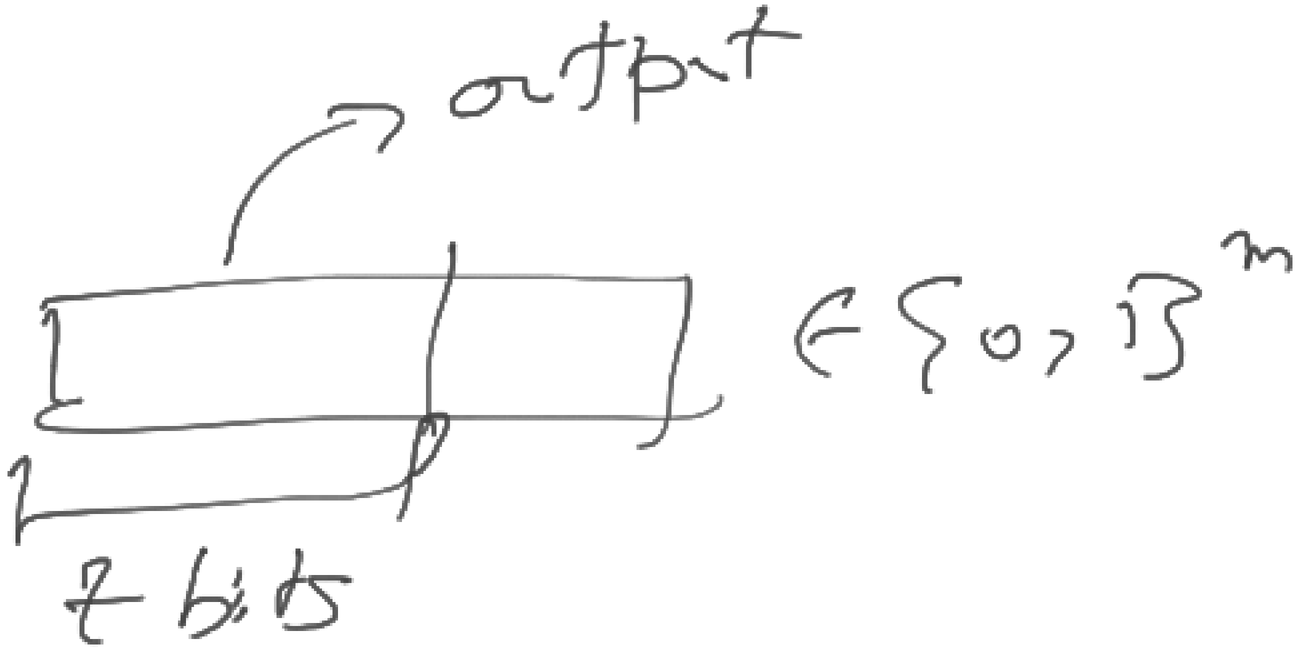
$P \xleftarrow{\alpha_1, \alpha_2^i} V$

$P \xrightarrow{\beta_1, \beta_2} V$

$GF[2^m]$

$H = \{h : \{0,1\}^m \to \{0,1\}^t\}$

$h_{a,b}(x) = ax + b \longrightarrow$



$a, b \in GF[2^m]$