HVSZK - Completeness

$SZK \subseteq HVSZK$

For constants $\alpha, \beta \in [0,1]$ s.t. $\alpha^2 > \beta$

- $SC^{\beta,\alpha} \in HVSZK$
- Any $L \in HVSZK$ reduces to $SC^{\beta,\alpha}$

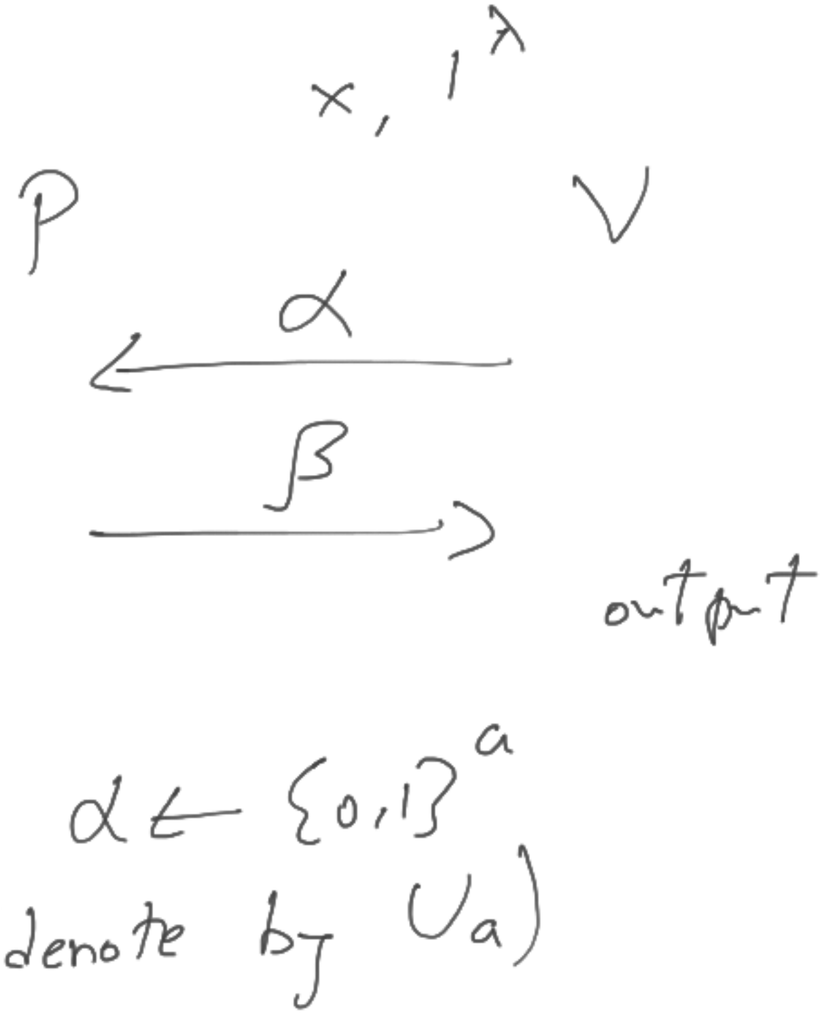
$R: x \longrightarrow (C_0, C_1)$

$x \in L \Rightarrow \Delta(D_{C_0}, D_{C_1}) < \beta$

$x \notin L \Rightarrow \Delta(D_{C_0}, D_{C_1}) > \alpha$

L has an HVSZK proof s.t.:

- it has two message
- it is public-coin
- completeness, soundness and ZK errors are negligible in λ



$\text{View}_V^P(x, r) = (\alpha, \beta, \cancel{\text{output}})$

(A, B) rand. vars.

$S(x, 1^\lambda) = (\alpha_S, \beta_S, \cancel{\text{outputs}})$

(A_S, B_S) rand. vars.

zero-knowledge

zk + completeness

$x \in L : \Delta(A_S, V_a) < \text{negl}(\lambda)$ AND $\Pr_{(\alpha_S, \beta_S) \leftarrow (A_S, B_S)}\left[V(x, \alpha_S, \beta_S) = \text{reject}\right] < \text{negl}(\lambda)$

$x \notin L : \Delta(A_S, V_a) > 0.1$ OR $\Pr_{(\alpha_S, \beta_S) \leftarrow (A_S, B_S)}\left[V(x, \alpha_S, \beta_S) = \text{reject}\right] > 0.1$

S-plays $A_S \approx V_a$, then $\Pr_{\alpha_S \leftarrow A_S}\left[\exists \beta_S : V(x, \alpha_S, \beta_S) = \text{accept}\right] < \text{negl}(\lambda)$

(soundness)

For some $x \in L$: $\Delta(A_S, V_a) < 0.1$

AND $\Pr[V(x, \alpha_S, \beta_S) = \text{reject}] < 0.1$

$$\Pr_{\alpha \leftarrow A}[\exists \beta : V(x, \alpha, \beta) = \text{accept}] \geq \Pr_{\alpha \leftarrow A_S}[\exists \beta : V(x, \alpha, \beta) = \text{accept}] - \Delta(A, A_S)$$

$$\geq 0.9 - 0.1 = 0.8 > \text{negl}(\lambda)$$

$D_0(x)$: 1. Sample $\alpha \leftarrow \{0,1\}^a$

2. Output (α, accept)

$C_0: \{0,1\}^a \to \{0,1\}^a \times \{0,1\}$

$C_0(r) \to (r, 1)$

$D_1(x)$: 1. $(\alpha_s, \beta_s) \leftarrow S(x;r)$

2. $(\alpha_s', \beta_s') \leftarrow S(x;r')$ set output$' = V(x, \alpha_s', \beta_s')$

3. Output $(\alpha_s, \text{output}')$

$C_1: \{0,1\}^{2s} \to \{0,1\}^a \times \{0,1\}$

$C_1(r, r')$

$x \in L$: $\Delta((A, \text{accept}), (A_s, V(x, A_s', B_s'))) \le \Delta(A, A_s) + \Delta(\text{accept}, V(x, A_s', B_s'))$

$\le \text{negl}(\lambda) + \text{negl}(\lambda)$

$x \notin L$: $\ge \max[\Delta(A, A_s), \Delta(\text{accept}, V(x, A_s', B_s'))] \ge 0.1$

$L \in SZK$: poly-time V

$x \longrightarrow (C_0, C_1) : \{0,1\}^n \longrightarrow \{0,1\}^m$

$size(C_0), size(C_1) \leq poly(m)$

$depth(C_0), depth(C_1) \leq poly(m)$ anything better??

$L \in SZK_L$: poly-time, log space V

$size(C_0), size(C_1) \leq poly(m)$

$depth(C_0), depth(C_1) \leq \log^2(m)$

$\leq O(1)$ randomised encodings

Properties of SZK

$$HVSZK = \text{public-coin } HVSZK = SZK$$

(ZK set lower bounds) (coin-tossing protocols)

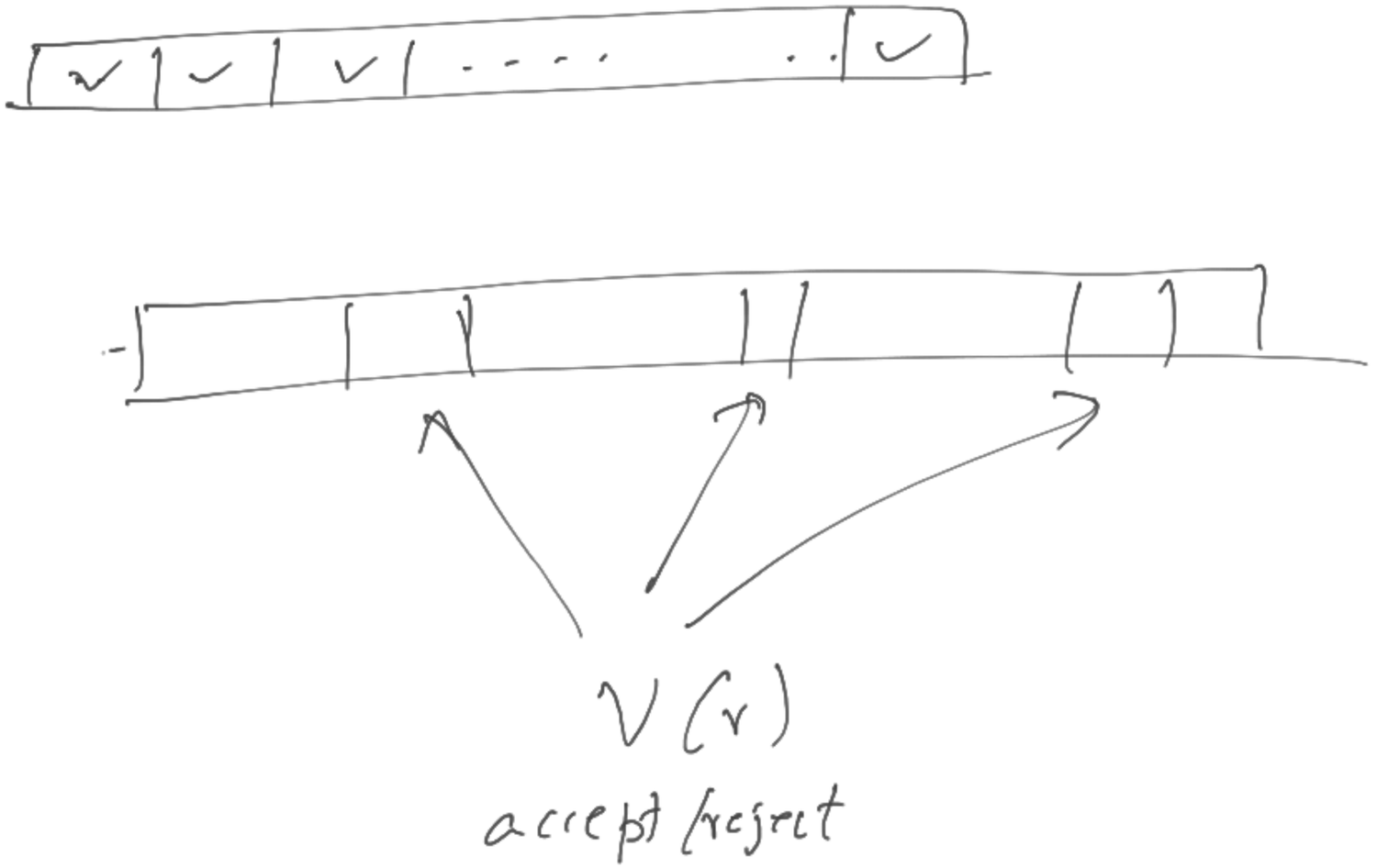
$$SZK = co\text{-}SZK \subseteq AM \cap coAM$$

$\exists L \in SZK$ that is hard on average $\Rightarrow$ One-way functions
Pseudorandom generators
Commitment schemes

$\Downarrow \Rightarrow$

statistically far distributions that are computationally indistinguishable

Probabilistically Checkable Proofs (PCPs)



PCP verifier V is a PPT algorithm has input x, uses randomness r, and has oracle access to the "proof" π, denoted by $V^{\pi}(x;r)$, and outputs accept/reject.

Say $\pi \in \{0,1\}^m$

V can call the oracle with "query" $i \in [m]$, and gets response $\pi[i]$.

V is a PCP verifier for lang L if:

Completeness: if $x \in L$: $\exists \pi$: $P_r[V^{\pi}(x;r) = \text{accept}] = 1$

Soundness: if $x \notin L$: $\forall \pi'$: $P_r[V^{\pi'}(x;r) = \text{accept}] < 1/2$

Parameter of interest:

- query complexity of V - q
- randomness complexity of V - ρ

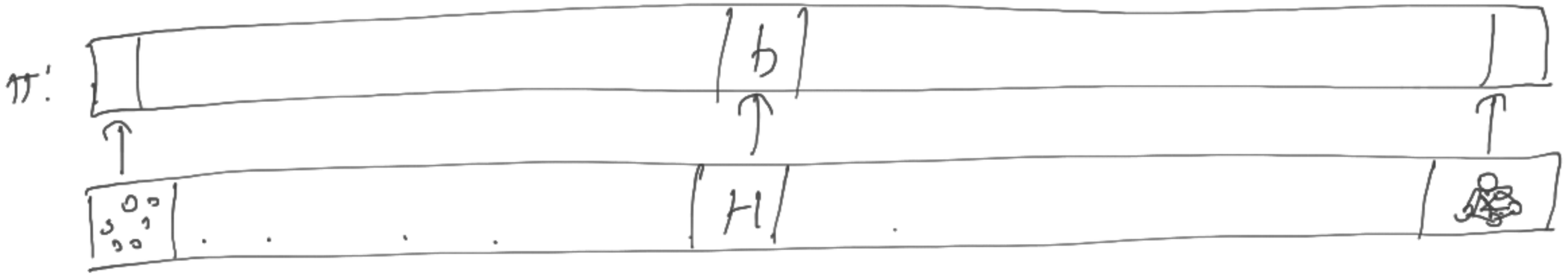
In any PCP system,

$|\pi| \leq q \cdot 2^{\rho}$

PCP$[q, \rho]$ - V makes $O(q)$ queries, uses $O(\rho)$ random bits

PCP for GNI

(G_0, G_1) s.t. G_0 and G_1 are non-isomorphic both over n vertices



$b = 0$; if $H \equiv G_0$

1 ; if $H \equiv G_1$

0 or 1 else

graphs over n vertices $= 2^{{}^nC_2} = |\Pi|$

$V^{\Pi}(G_0, G_1)$: 1. Sample random bit b and relabelling R

2. Query $b' \leftarrow \Pi[R(G_b)]$

3. Accept iff $b = b'$

Completeness: $H \in R(G_b)$ is isomorphic to G_b

so $\Pi[H] = b$

Soundness: Prob that V queries H is same indep. of b
($G_0 \equiv G_1$) $\Pi'[H]$ is fixed, so $b \neq \Pi'[H]$ w.p. $1/2$

Thm: If L has an IP with V's randomness complexity p, $2k$ messages, V's messages are of length a, P's messages of length b.

Then, L has a $PCP[bk, p]$ with proof length at most $O(bk \cdot 2^{ak})$

Corollaries: $GNI \in PCP[1, n \log n]$

$IP \subseteq PCP[\text{poly}(n), \text{poly}(n)]$