PCPs : Hardness of Approximation, Constructions

$PCP[q, p]$ - V makes $\leq q$ queries
uses $\leq p$ random bits

$IP \subseteq PCP[poly, poly]$

$PCP[q, p] \subseteq NTIME[q \cdot 2^p]$

for any $L \in PCP[q, p]$, $\exists$ alg. V running in time $q \cdot 2^p$
s.t. $\forall x \in L \; \exists w$ s.t. $V(x, w)$ accepts
$\forall x \notin L \; \forall w^*$, $V(x, w^*)$ rejects

$L \in PCP[q, p] \subseteq NTIME[q \cdot 2^p]$

Suppose $x \in L$ has PCP proof π, verifier V

For any $r \in \{0,1\}^p$, queries made by $V(x;r)$: $\underbrace{(i_1^r, \ldots, i_q^r)}_{I_r}$

if $i_1^{\vec{0}} = i_1^{0\ldots1}$, $\pi(i_1^{\vec{0}}) = \pi(i_1^{0\ldots1})$

$$w = \underbrace{\Big(\underbrace{\pi(i_1^{\vec{0}}), \ldots, \pi(i_q^{\vec{0}})}_{q}, \underbrace{\pi(i_1^{0\ldots01}), \ldots, \pi(i_q^{0\ldots1})}_{0\ldots01}, \ldots, (\quad)\Big)}_{2^p}$$

$V_N(x, w)$:- Iterate through $r \in \{0,1\}^p$, check that $V(x, \pi(I_r); r)$ accepts

- Check w is consistent

$$PCP[poly, log] \subseteq NP = NTIME[poly]$$

$$NP \subseteq PCP[poly, 0]$$

$$NP \subseteq PCP[O(1), log] \quad - \text{ PCP Theorem}$$

3

$$PCP[2, log] \subseteq P$$

$$NP \subseteq PCP[O(1), poly] \quad - \text{ we will see}$$

Hardness of Approximation

k-CSP : Variables $(x_1, \ldots, x_m)$ — x k-constant

NP-Complete Constraints $(\phi_1, \ldots, \phi_t)$ — ϕ

$$\phi_i : \{0,1\}^k \longrightarrow \{0,1\}$$

$$\phi_i(x_{i_1}, \ldots, x_{i_k}) = \left((x_{i_1} \vee x_{i_2}) \wedge (x_{i_3} \oplus x_{i_1})\right) \vee \ldots$$

Does there exist assignment to $(x_1, \ldots, x_m)$ that satisfies all the ϕ_i's?

NP-hard

Max-k-CSP: find assignment that maximises # of satisfied ϕ_i's.

$OPT(\Phi)$ - max. # of Φ_i's that are satisfied by any assignment

Max-kCSP: find x s.t. $OPT(\Phi)$ constraints satisfied

δ-approximate Max-kCSP: find x s.t. $\delta \cdot OPT(\Phi)$ constraints satisfied

Approximation Hardness from PCPs

$NP \subseteq PCP[k, c\log(n)]$

L - NP-hard that has $PCP[k, c\log n]$ with verifier V

$V(z; r)$: 1. Queries $(i_1^r, \ldots, i_k^r)$ to get $\Pi[i_1^r], \ldots, \Pi[i_k^r]$

$r \in \{0,1\}^{c\log n}$ 2. Run $V_r^z(\Pi[i_1^r], \ldots, \Pi[i_k^r]) \longrightarrow$ accept/reject

$$|\Pi| \le q \cdot 2^p \le k \cdot 2^{c\log n} = \text{poly}(n) = m, \quad |r| = c\log(n)$$

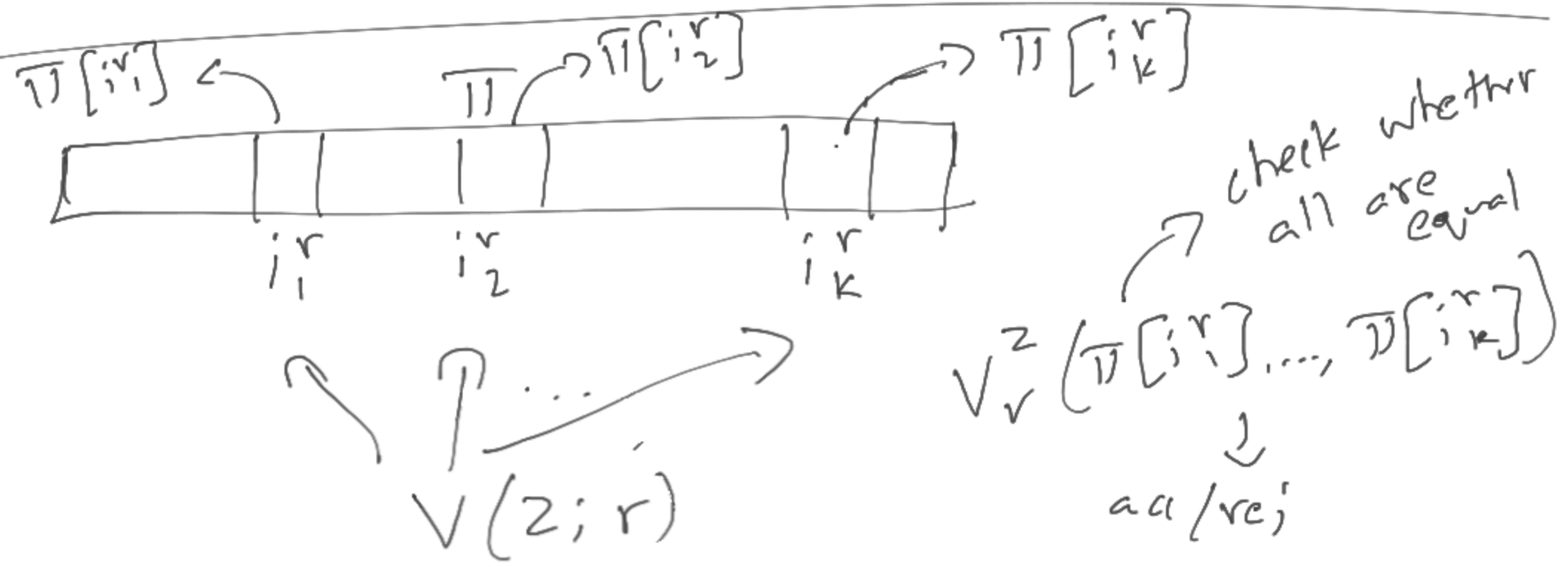
$R(z)$:- Variables $x_1, \ldots, x_m$

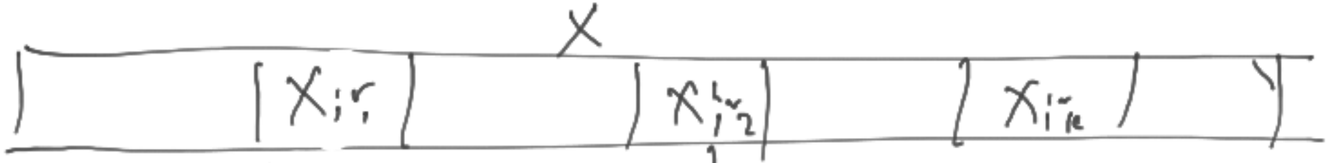
- $\emptyset = (\emptyset_1, \ldots, \emptyset_t)$: $\emptyset_r = V_r^z(x_{i_1^r}, \ldots, x_{i_k^r})$

$t = 2^{c\log n}$ $\quad r \in [t]$

$= n^c$

$$R(z) = \left\{ V_r^z\left(x_{i_1^r}, \ldots, x_{i_k^r}\right) \right\}_{r \in \{0,1\}^{c\log(n)}} \quad \text{over } (x_1, \ldots, x_m),\ m = |\Pi|$$





$$V_r^z(\cdot, \ldots, \cdot) = (x_{i_1^r} = x_{i_2^r} = \cdots = x_{i_k^r})$$

$z \in L$: completeness of PCP

$\Rightarrow \exists \Pi : \Pr_r [V^{\Pi}(z; r) \text{ accepts}] = 1$

$\Rightarrow \exists \Pi : \forall r \in \{0,1\}^{c \log n} : V_r^z(\Pi[i_1^r], \ldots, \Pi[i_k^r])$ accepts

$\Rightarrow \exists$ assignment to $(x_1, \ldots, x_m)$ s.t.

all of the $V_r^z(x_{i_1^r}, \ldots, x_{i_k^r})$

are satisfied

$z \notin L$: soundness of PCP

$\Rightarrow \forall \pi^* : \Pr_r [V^{\pi^*}(z; r) \text{ accepts}] \leq 1/2$

$\Rightarrow \forall \pi^* :$ fraction of r on which $V_r^z(\pi^*[i_1^r], \ldots, \pi^*[i_k^r])$ accepts $\leq 1/2$

$\Rightarrow \forall$ any assignment to $(x_1, \ldots, x_m)$:

fraction of $V_r^z(x_{i_1^r}, \ldots, x_{i_k^r})$ satisfied $\leq \frac{1}{2}$

$z \in L \Rightarrow \phi \leftarrow R(z), \quad OPT(\phi) = 1$

$z \notin L \Rightarrow \phi \leftarrow R(z), \quad OPT(\phi) \leq 1/2$

0.51 - approximate Max-kCSP in poly time $\Rightarrow$ can distinguish det. $OPT(\phi) = 1$ and $OPT(\phi) \leq 0.5$ in poly time $\Rightarrow$ Decide L in poly time

L is NP-hard $\Rightarrow$ 0.51-approximating is NP-hard Max-kCSP

$NP \subseteq PCP[a, p]$ $\rightarrow$ instance of Max-q-CSP with 2^p constraints

A Simple PCP Theorem

$NP \subseteq PCP[O(1), poly]$

ML: Instance is $A \in F_2^{m \times n}$, $b \in F_2^m$

Does there exist $u \in F_2^n$ s.t. $Au = b$?

$$A = \begin{bmatrix} — & a_1 & — \\ & \vdots & \\ — & a_m & — \end{bmatrix} \qquad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

$a_i \in F_2^n$

Assumption:

A - full rank

$a_1, \ldots, a_m$ Span all of F_2^n

π: $\pi \in \mathbb{F}_2^{2^n}$ for $a \in \mathbb{F}_2^n$: $\pi[a] = \langle a, u \rangle$

H_u = | $\langle 0^n, u \rangle$ | $\langle 0^{n-1}1, u \rangle$ | ... | $\langle a_i, u \rangle$ | ... | $\langle 1^n, u \rangle$ |

b_i^n if $Au = b$

$V^{\pi}(A, b)$:

1. Check that π is actually H_u for some $u \in \mathbb{F}_2^n$] later
2. Check that this u satisfies $Au = b$] now

Simple check for setup 2: For all $i \in [m]$, query $\Pi[a_i]$, and check that $\Pi[a_i] = b_i$

$$A = \begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} \quad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Needs m queries

$$H_u[a] = \langle a, u \rangle = \ell_u(a) = \sum_{j \in [n]} u[j] \cdot a[j]$$

$a \in F_2^n$

$$\ell_u : F_2^n \longrightarrow F_2$$

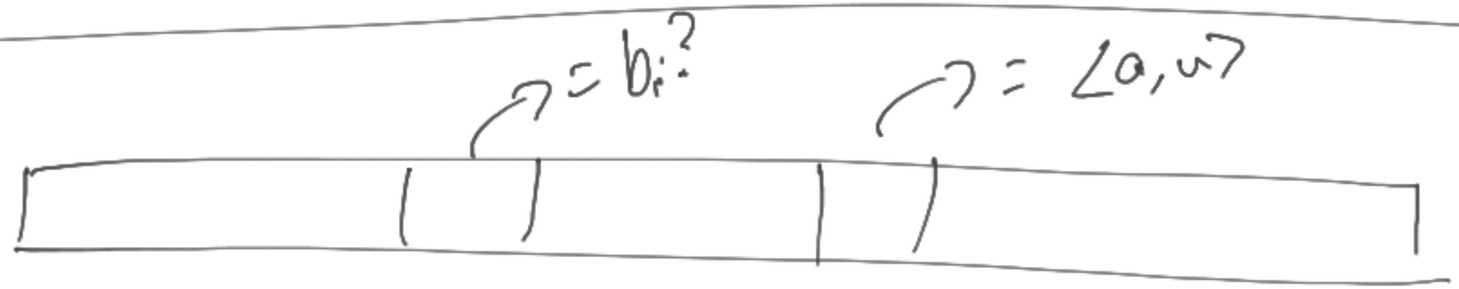
$$\ell(a[1], \ldots, a[n])$$

$$\ell(y_1, \ldots, y_n) = \sum_j u[j] \cdot y_j$$

Thm: for any distinct $u, v \in \mathbb{F}_2^n$:

$$\Pr_{a \leftarrow \mathbb{F}_2^n}\left[\langle u,a\rangle = \langle v,a\rangle\right] = \frac{1}{2}$$

$\pi = H_v$:



H_u :

$c_i \in \mathbb{F}_2$

$Au = b$

$$a = \sum c_i a_i$$

$$H_u(a) = H_u\left[\textstyle\sum c_i a_i\right] = \sum c_i H_u[a_i] = \sum c_i b_i$$