Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

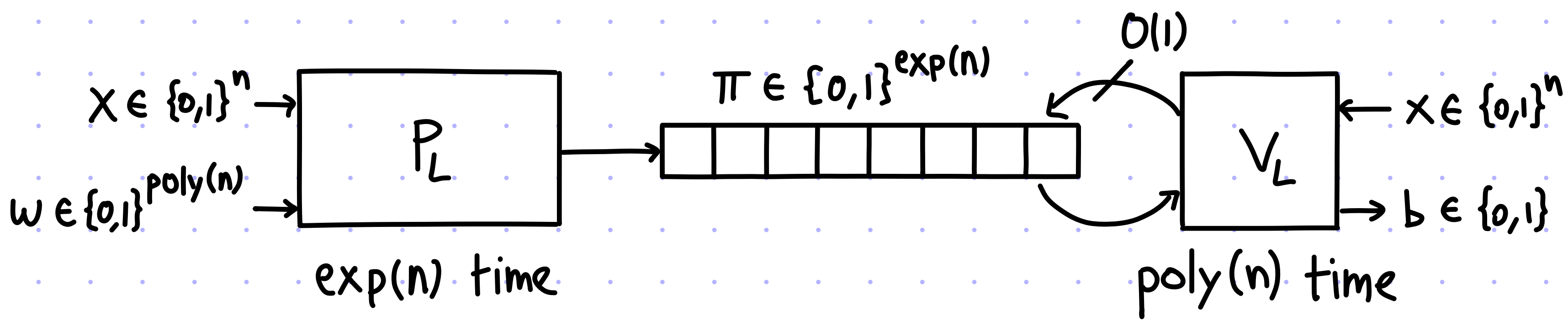
Lecture 08

Exponential-Size PCP

Exponential-Size PCPs for NP

theorem: $NP \subseteq PCP\left[\varepsilon_c = 0,\ \varepsilon_s = 1/2,\ \Sigma = \{0,1\},\ \ell = \exp(n),\ q = O(1),\ r = \mathrm{poly}(n)\right]$

That is, $\forall L \in NP$ $\exists$ PCP system (P_L, V_L) for L that looks like this:



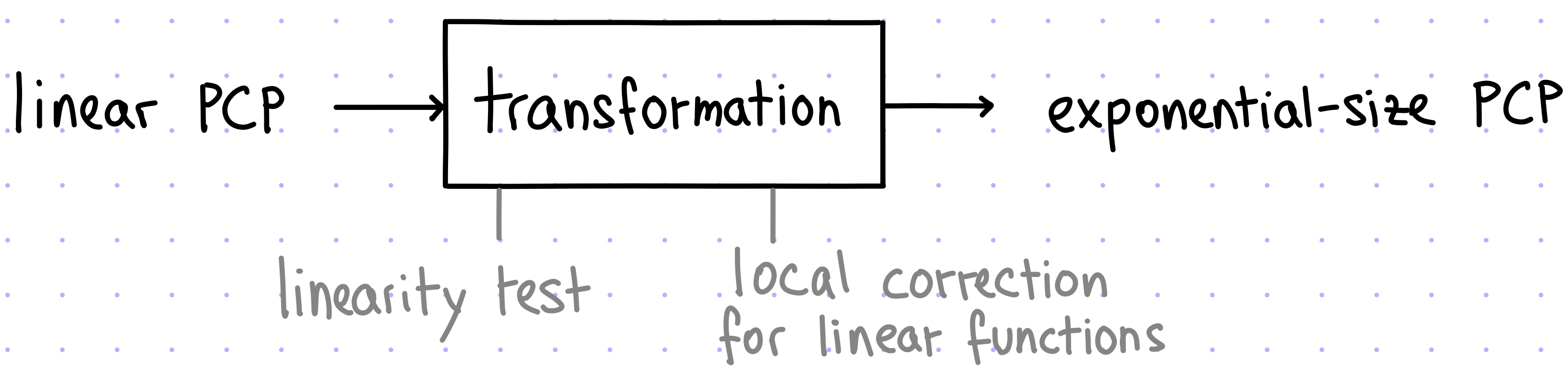
We achieve constant soundness error and constant query complexity.

PROOF STRATEGY:

① define notion of a LINEAR PCP (LPCP)

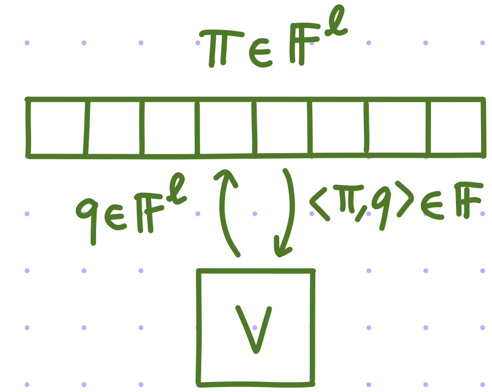
② construct a linear PCP for NP with constant query complexity

③ transform the linear PCP into a (standard) PCP:



Linear PCPs

an LPCP verifier makes linear queries to the proof string



A linear PCP (LPCP) is a PCP where:

(i) the honest PCP string is a linear function

(ii) soundness is relaxed to consider only PCP strings that are linear functions

Given a field $\mathbb{F}$ and vector $\pi \in \mathbb{F}^\ell$, $f_\pi : \mathbb{F}^\ell \to \mathbb{F}$ is the function $f_\pi(x) := \langle \pi, x \rangle$.

<u>def:</u> (P,V) is a LPCP system for a relation R over the field $\mathbb{F}$ with completeness error ε_c and soundness error ε_s if the following holds:

① COMPLETENESS: $\forall (x,w) \in R \quad \Pr\left[V^{f_\pi}(x) = 1 \,\middle|\, \pi \leftarrow P(x,w) \right] \geq 1 - \varepsilon_c$.

② SOUNDNESS: $\forall x \notin L(R) \ \forall \tilde{P} \quad \Pr\left[V^{f_{\tilde{\pi}}}(x) = 1 \,\middle|\, \tilde{\pi} \leftarrow \tilde{P} \right] \leq \varepsilon_s$.

Equivalently: $\forall x \notin L(R) \ \forall \tilde{\pi} \quad \Pr[V^{f_{\tilde{\pi}}}(x) = 1] \leq \varepsilon_s$

Similar notation to PCPs :

- $V^{f_\pi}(x;\rho)$ makes explicit that ρ is the randomness of V
- $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma = \mathbb{F}, \ell, q, r, \ldots]$ is class notation with parameters

We prove the following theorem:

<u>theorem:</u> $\forall$ finite field $\mathbb{F}$, $\mathrm{NP} \subseteq \mathrm{LPCP}\left[\varepsilon_c = 0,\ \varepsilon_s = \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2},\ \Sigma = \mathbb{F},\ \ell = \mathrm{poly}(n),\ q = O(1),\ r = \mathrm{poly}(n)\right]$

Quadratic Equations are NP-Complete

A system of m quadratic equations in n variables over a field $\mathbb{F}$ is a list of polynomials $p_1,\ldots,p_m \in \mathbb{F}[X_1,\ldots,X_n]$ where each p_i has total degree ≤ 2.

Example: p_1: $X_1X_3 + X_2^2 + X_6$ p_2: $X_1 + X_7 - 1$ p_3: $X_1X_4 + 5X_2X_3 + 7$

def: $\text{QESAT}(\mathbb{F}) := \{(p_1,\ldots,p_m) \mid \exists a_1,\ldots,a_n \in \mathbb{F} \text{ s.t. } \forall i \in [m]\ p_i(a_1,\ldots,a_n) = 0\}$

lemma: For every finite field $\mathbb{F}$, $\text{QESAT}(\mathbb{F})$ is NP-complete.

proof: $\text{QESAT}(\mathbb{F})$ is in $\text{NTIME}(\text{poly}(m,n,\log|\mathbb{F}|))$.

We show NP-hardness by reducing from CSAT (satisfiable boolean circuits).

Given a boolean circuit $C:\{0,1\}^k \to \{0,1\}$:

- assign each wire a variable: $\overbrace{X_1,\ldots,X_k}^{\text{inputs}}, \overbrace{X_{k+1},\ldots,X_{n-1}}^{\text{internal wires}}, \overbrace{X_n}^{\text{output}}$
- enforce booleanity: $\forall i \in [k]$, create the polynomial $X_i \cdot (X_i - 1)$ ($\{0,1\}$ is a subset of every field)
- map each gate to a polynomial: $X_{i_3} = \text{NAND}(X_{i_1}, X_{i_2}) \mapsto X_{i_3} - (1 - X_{i_1} \cdot X_{i_2})$
- output is 1: create the polynomial $X_n - 1$

Overall $n = |C|$, $m = |C| + 1$ (where $|C| = \#$vertices in DAG representing C). ■

Approach for LPCP for QESAT

TOOL 1: linear equations test. LPCP that checks a system of linear equations

PROBLEM: how to extend the approach from linear to quadratic equations?

Example: $p(x_1,x_2,x_3) = x_1 + 2x_2 + 7x_3 + x_1x_2 + 2x_2x_3 + 5x_1x_3 + x_1^2 + 3x_2^2 + x_3^2$

IDEA: linearization. The prover provides the value of each quadratic polynomial

$$\forall\, i,j \in [n] \quad z_{ij} := x_i \cdot x_j$$

PROBLEM: how to check consistency between linear and quadratic terms?

TOOL 2: tensor test. LPCP that checks the expected tensor structure.

REVIEW:

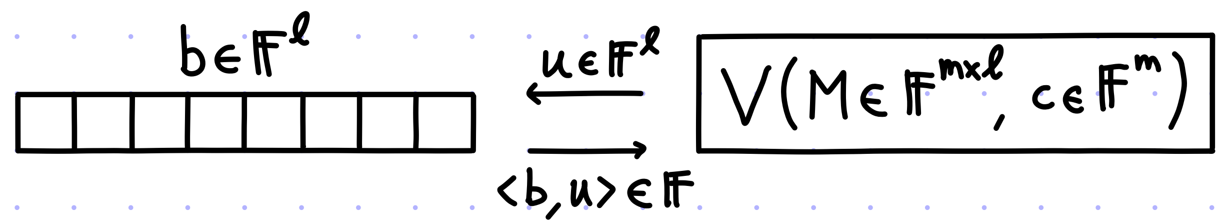
For $a \in \mathbb{F}^n$ and $b \in \mathbb{F}^m$, the tensor product $a \otimes b \in \mathbb{F}^{n \times m}$ is the matrix s.t.

$$\forall\, i \in [n] \quad \forall\, j \in [m] \qquad (a \otimes b)_{i,j} := a_i \cdot b_j .$$

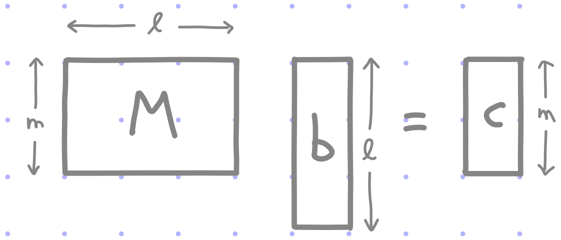
We denote by $\mathrm{flat}(a \otimes b) \in \mathbb{F}^{n \cdot m}$ the concatenation of the rows of $a \otimes b$.

Tool 1: Linear PCP for Linear Equations

Consider this setting:



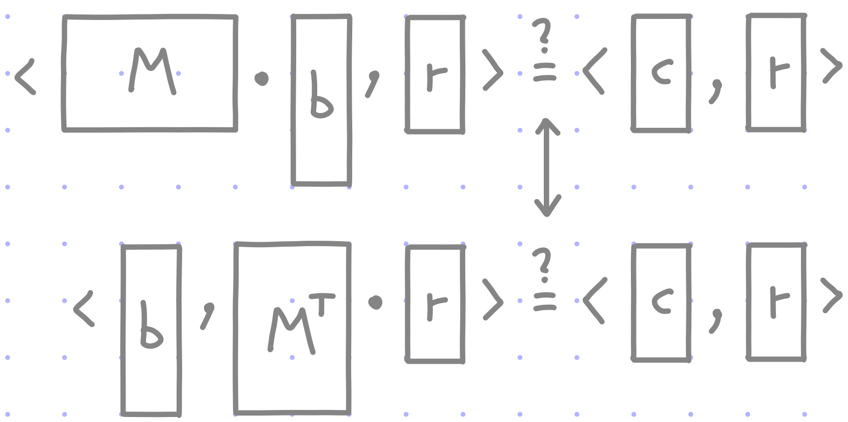
Check that $Mb = c$.



IDEA: random linear combination via a linear query

Observe that for $a, b \in \mathbb{F}^m$: $\begin{cases} \text{if } a=b \text{ then } \Pr_{r \in \mathbb{F}^m}[\langle a,r\rangle = \langle b,r\rangle] = 1 \\ \text{if } a \neq b \text{ then } \Pr_{r \in \mathbb{F}^m}[\langle a,r\rangle = \langle b,r\rangle] \leq \frac{1}{|\mathbb{F}|} \end{cases}$ (by PIL on non-zero $p(X_1,\dots,X_m) := \sum_{i=1}^m (a_i - b_i) X_i$)

This directly leads to an LPCP verifier:



$V^b(M,c)$:
1. Sample $r \in \mathbb{F}^m$.
2. Query $b \in \mathbb{F}^\ell$ at $u := M^T r \in \mathbb{F}^\ell$.
3. Check that $\langle b,u\rangle = \langle c,r\rangle$.

Completeness: $Mb = c \to \forall r \in \mathbb{F}^m \; \langle b,u\rangle \underset{u = M^T r}{=} \langle b, M^T r\rangle \underset{\text{def of inner product}}{=} b^T(M^T r) \underset{\substack{\text{transpose reverses} \\ \text{order in a product}}}{=} (Mb)^T r \underset{\text{def of inner product}}{=} \langle Mb, r\rangle \underset{Mb=c}{=} \langle c, r\rangle$.

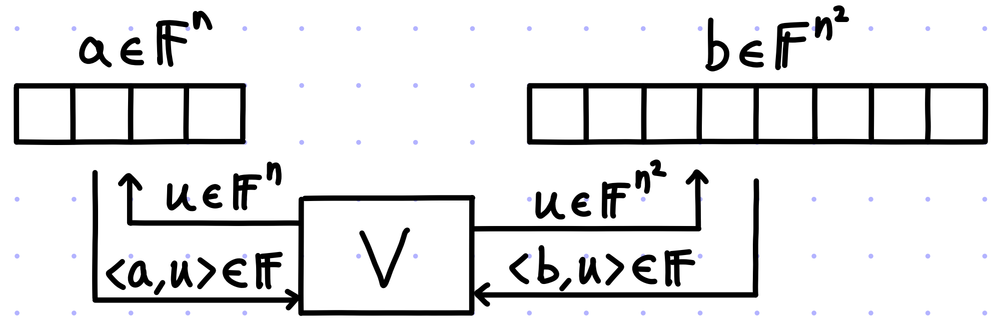
Soundness: $Mb \neq c$ (i.e., $\exists i \in [m]$ s.t. $(Mb)_i \neq c_i$) $\to$

$$\Pr_r[\langle b,u\rangle = \langle c,r\rangle] = \Pr_r[\langle b, M^T r\rangle = \langle c,r\rangle] = \Pr_r[\langle Mb, r\rangle = \langle c,r\rangle] = \Pr_r\left[\sum_{i=1}^m (Mb-c)_i \cdot r_i = 0\right] \leq \frac{1}{|\mathbb{F}|}.$$

Polynomial Identity Lemma applied to (non-zero) polynomial $p(X_1,\dots,X_m) = \sum_{i=1}^m (Mb-c)_i \cdot X_i$

Tool 2: Linear PCP for Tensor Structure

Consider this setting:



Check that $\mathrm{flat}(a \otimes a) = b$.

$V^{a,b}$:
1. Sample $s,t \in \mathbb{F}^n$.
2. Query a at s and t.
3. Query b at $\mathrm{flat}(s \otimes t)$.
4. Check that $\langle b, \mathrm{flat}(s \otimes t) \rangle = \langle a,s \rangle \cdot \langle a,t \rangle$.

Completeness: $b = \mathrm{flat}(a \otimes a) \rightarrow \forall s,t \in \mathbb{F}^n \quad \langle b, \mathrm{flat}(s \otimes t) \rangle = \langle \mathrm{flat}(a \otimes a), \mathrm{flat}(s \otimes t) \rangle$

$$= \sum_{i,j \in [n]} a_i a_j s_i t_j = \Big(\sum_{i \in [n]} a_i s_i\Big) \cdot \Big(\sum_{i \in [n]} a_i t_i\Big) = \langle a,s \rangle \cdot \langle a,t \rangle .$$

Soundness: $b \neq \mathrm{flat}(a \otimes a)$ (i.e., $\exists i^*, j^* \in [n]$ s.t. $b_{i^*j^*} \neq a_{i^*} \cdot a_{j^*}$) $\rightarrow$

$$\Pr_{s,t}\left[\langle b, \mathrm{flat}(s \otimes t) \rangle \neq \langle a,s \rangle \cdot \langle a,t \rangle\right] \overset{\circledast}{=} \Pr_{s,t}\Big[\sum_{i,j} (b_{ij} - a_i a_j) s_i t_j \neq 0\Big] \geq 1 - \frac{2}{|\mathbb{F}|}$$ by Polynomial Identity Lemma.

But we can do better:

$$\overset{\circledast}{=} \Pr_{s,t}\Big[\sum_i \Big(\sum_j (b_{ij} - a_i a_j) t_j\Big) s_i \neq 0\Big] = \Pr_{s,t}\Big[\sum_i p_i(t) s_i \neq 0\Big] \geq \Pr_t\left[p_{i^*}(t) \neq 0\right] \cdot \Pr_{s,t}\Big[\sum_i p_i(t) s_i \neq 0 \,\Big|\, p_{i^*}(t) \neq 0\Big] \geq \Big(1 - \frac{1}{|\mathbb{F}|}\Big)^2 .$$

PIL applied twice

Hence $\Pr_{s,t}\left[\begin{matrix}\langle b, \mathrm{flat}(s \otimes t) \rangle \\ = \langle a,s \rangle \cdot \langle a,t \rangle\end{matrix}\right] \leq 1 - \Big(1 - \frac{1}{|\mathbb{F}|}\Big)^2 = \frac{2|\mathbb{F}| - 1}{|\mathbb{F}|^2}$.

Linear PCP for Quadratic Equations

<u>theorem:</u> $\mathrm{QESAT}(\mathbb{F}) \in \mathrm{LPCP}\left[\, \varepsilon_c = 0,\ \varepsilon_s = \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2},\ \Sigma = \mathbb{F},\ \ell = n+n^2,\ q = 4,\ r = (m+2n)\cdot\log|\mathbb{F}| \,\right]$

Let $(p_1,\dots,p_m)$ be an instance of $\mathrm{QESAT}(\mathbb{F})$ with n variables.

The LPCP verifier expects a proof $\pi = (a,b) \in \mathbb{F}^{n+n^2}$ and works as follows.

$V^{(a,b)}((p_1,\dots,p_m))$: 1. Sample $r \in \mathbb{F}^m$ and $s,t \in \mathbb{F}^n$.

2. Define $M := \begin{bmatrix} \mathrm{coeff}(p_1) \\ \vdots \\ \mathrm{coeff}(p_m) \end{bmatrix} \in \mathbb{F}^{m \times (n+n^2)}$ and $c := \begin{bmatrix} -\mathrm{const}(p_1) \\ \vdots \\ -\mathrm{const}(p_m) \end{bmatrix} \in \mathbb{F}^m$.

$\mathrm{coeff}(p_i) :=$ non-constant coeffs of p_i
$\mathrm{const}(p_i) :=$ constant coeff of p_i

linear equation test → 3. Query (a,b) at $M^T r$ and check that $\langle a \| b, M^T r\rangle = \langle c, r\rangle$.

tensor test → 4. Query b at $\mathrm{flat}(s \otimes t)$, a at s and t, and check that $\langle b, \mathrm{flat}(s\otimes t)\rangle = \langle a,s\rangle \cdot \langle a,t\rangle$.

(a,b) at $(0^n, \mathrm{flat}(s\otimes t))$ (a,b) at $(s,0^{n^2})$ and $(t,0^{n^2})$

<u>Completeness:</u> Suppose $p_1(a) = \dots = p_m(a) = 0$ and set $b := \mathrm{flat}(a \otimes a)$.

Then $\Pr_{s,t}[\langle b, \mathrm{flat}(s\otimes t)\rangle = \langle a,s\rangle\cdot\langle a,t\rangle] = 1$ and $\Pr_r[\langle a\|b, M^T r\rangle = \langle c,r\rangle] = 1$ (since $M\begin{bmatrix} a \\ b\end{bmatrix} = M\begin{bmatrix} a \\ \mathrm{flat}(a\otimes a)\end{bmatrix} = c$).

<u>Soundness:</u> Suppose $\forall a \in \mathbb{F}^n\ \exists i \in [m]\ p_i(a) \neq 0$. Fix any $\pi = (a,b)$.

Either : (i) $b \neq \mathrm{flat}(a\otimes a)$ → tensor test passes w.p. $\leq \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2}$

OR (ii) $b = \mathrm{flat}(a\otimes a)$ and $M\begin{bmatrix} a \\ b\end{bmatrix} \neq c$ → linear equation test passes w.p. $\leq \frac{1}{|\mathbb{F}|}$

From LPCP to PCP

lemma: $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma = \mathbb{F}, \ell, q, r]$
$\leq \mathrm{PCP}[\varepsilon_c, \varepsilon_s' = \max\{\frac{5}{6}, \varepsilon_s + \frac{1}{100}\}, \Sigma = \mathbb{F}, \ell' = \mathbb{F}^{\ell}, q' = O(q \log q), r' = r + O(\ell \cdot \log q \cdot \log|\mathbb{F}|)]$

The lemma enables us to move from LINEAR QUERIES to POINT QUERIES, while preserving query complexity and incurring an exponential blowup in proof length.

This suffices for today's goal:

we proved that $\mathrm{NP} \subseteq \mathrm{LPCP}[\varepsilon_c = 0, \varepsilon_s = 1/2, \Sigma = \{0,1\}, \ell = O(n^2), q = O(1), r = O(n)]$
so the lemma gives $\mathrm{NP} \subseteq \mathrm{PCP}[\varepsilon_c = 0, \varepsilon_s = 1/2, \Sigma = \{0,1\}, \ell = \exp(n), q = O(1), r = \mathrm{poly}(n)]$

(The soundness error is reduced back to $\varepsilon_s = 1/2$ by repeating the verifier $O(1)$ times.)

We are left to prove the lemma.

First Attempt at the Lemma

<u>lemma:</u> $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma = \mathbb{F}, \ell, q, r] \leq \mathrm{PCP}[\varepsilon_c, \varepsilon_s', \Sigma = \mathbb{F}, \ell' = \mathbb{F}^\ell, q', r']$

Let (P_{LPCP}, V_{LPCP}) be an LPCP for a language L. Construct a PCP (P_{PCP}, V_{PCP}) as follows.

$P_{PCP}(x)$: 1. Compute $\pi := P_{LPCP}(x) \in \mathbb{F}^\ell$.

2. Output $\Pi := (\langle \pi, a \rangle)_{a \in \mathbb{F}^\ell} \in \mathbb{F}^{\mathbb{F}^\ell}$.

$V_{PCP}^{\tilde{\Pi}}(x)$: Simulate $V_{LPCP}(x)$ by answering $a \in \mathbb{F}^\ell$ with $\tilde{\Pi}(a)$.

<u>Completeness:</u> $x \in L \rightarrow V_{PCP}^{\Pi}(x) = V_{PCP}^{(\langle \pi, a \rangle)_{a \in \mathbb{F}^\ell}}(x) = V_{LPCP}^{f_\pi}(x)$ accepts w.p. $\geq 1 - \varepsilon_c$.

<u>Soundness:</u> $x \notin L \rightarrow \forall \tilde{\Pi} \in \mathbb{F}^{\mathbb{F}^\ell}$ $\Pr[V_{PCP}^{\tilde{\Pi}}(x) = 1] \leq ?$

PROBLEM: $\tilde{\Pi}$ may not equal $(\langle \tilde{\pi}, a \rangle)_{a \in \mathbb{F}^\ell}$ for some $\tilde{\pi} \in \mathbb{F}^\ell$.
And we cannot test that $\tilde{\Pi}$ has this form using few queries.

<u>IDEA:</u> augment the PCP verifier with the BLR linearity test to ensure that $\tilde{\Pi}$ is close to $\mathrm{LIN} = \{ f : \mathbb{F}^\ell \rightarrow \mathbb{F} \mid f \text{ is } \mathbb{F}\text{-linear} \}$.

Realizing this idea requires some care...

Second Attempt at the Lemma

lemma: $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma=\mathbb{F}, \ell, q, r] \le \mathrm{PCP}[\varepsilon_c, \varepsilon_s', \Sigma=\mathbb{F}, \ell'=\mathbb{F}^{\ell}, q', r']$

Let (P_{LPCP}, V_{LPCP}) be an LPCP for a language L. Construct a PCP (P_{PCP}, V_{PCP}) as follows.

$P_{PCP}(x)$: 1. Compute $\pi := P_{LPCP}(x) \in \mathbb{F}^{\ell}$.

SAME AS BEFORE 2. Output $\Pi := (\langle \pi, a\rangle)_{a\in\mathbb{F}^{\ell}} \in \mathbb{F}^{\mathbb{F}^{\ell}}$.

$V_{PCP}^{\tilde{\Pi}}(x)$: Check that $V_{BLR}^{\tilde{\Pi}}(x)=1$ and then simulate $V_{LPCP}(x)$ by answering $a\in\mathbb{F}^{\ell}$ with $\tilde{\Pi}(a)$.

Completeness: $x \in L \to V_{PCP}^{\Pi}(x) = V_{BLR}^{(\langle\pi,a\rangle)_{a\in\mathbb{F}^{\ell}}} \wedge V_{LPCP}^{(\langle\pi,a\rangle)_{a\in\mathbb{F}^{\ell}}}(x) = 1 \wedge V_{LPCP}^{f_\pi}(x)$ accepts w.p. $\ge 1-\varepsilon_c$.

Soundness: $x \notin L \to$ Fix any $\tilde{\Pi} \in \mathbb{F}^{\mathbb{F}^{\ell}}$. Fix a parameter $\delta < \overbrace{\frac{1}{2}\cdot\left(1-\frac{1}{|\mathbb{F}|}\right)}^{\text{unique decoding radius}}$.

- Case 1: $\tilde{\Pi}$ is δ-far from LIN. $\Pr[V_{BLR}^{\tilde{\Pi}}=1] \le 1-\Delta(\tilde{\Pi}, \mathrm{LIN}) \le 1-\delta$.
- Case 2: $\tilde{\Pi}$ is δ-close to LIN.

LIN has relative distance $\ge 1-\frac{1}{|\mathbb{F}|}$

Let $\hat{\Pi} = (\langle\pi,a\rangle)_{a\in\mathbb{F}^{\ell}} \in \mathrm{LIN}$ be the unique linear function that is closest to $\tilde{\Pi}$.

$$\Pr\left[V_{LPCP}^{\boxed{\tilde{\Pi}}}(x)=1\right] \le \Pr\left[V_{LPCP}^{\pi}(x)=1 \,\middle|\, \begin{array}{l}\text{all queries by } V_{LPCP} \text{ are}\\ \text{answered with } \hat{\Pi}=(\langle\pi,a\rangle)_{a\in\mathbb{F}^{\ell}}\end{array}\right] + \Pr\left[\begin{array}{l}\exists \text{ query } a \text{ by } V_{LPCP}\\ \text{s.t. } \tilde{\Pi}(a)\neq\hat{\Pi}(a)\end{array}\right]$$

$$\le \varepsilon_s + q\cdot\delta$$ ← Assumes that each LPCP query is random in $\mathbb{F}^{\ell}$.

PROBLEM: This may NOT be the case. In fact, NONE of the queries in our LPCP are!

The Lemma via Linearity Testing and Local Correction

lemma: $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma = \mathbb{F}, \ell, q, r]$

$$\leq \mathrm{PCP}\left[\varepsilon_c, \varepsilon_s' = \max\left\{\tfrac{7}{8}, \varepsilon_s + q \cdot \exp(-t)\right\}, \Sigma = \mathbb{F}, \ell' = \mathbb{F}^{\ell}, q' = 3 + 2t \cdot q, r' = r + (2\ell + t \cdot \ell) \cdot \log|\mathbb{F}|\right]$$

Let $(P_{\mathrm{LPCP}}, V_{\mathrm{LPCP}})$ be an LPCP for a language L. Construct a PCP $(P_{\mathrm{PCP}}, V_{\mathrm{PCP}})$ as follows.

$P_{\mathrm{PCP}}(x)$: 1. Compute $\pi := P_{\mathrm{LPCP}}(x) \in \mathbb{F}^{\ell}$.

SAME AS BEFORE 2. Output $\Pi := (\langle \pi, a \rangle)_{a \in \mathbb{F}^{\ell}} \in \mathbb{F}^{\mathbb{F}^{\ell}}$.

$V_{\mathrm{PCP}}^{\tilde{\Pi}}(x)$: Check that $V_{\mathrm{BLR}}^{\tilde{\Pi}}(x) = 1$.

locally correct every answer

Sample $r_1, \ldots, r_t \in \mathbb{F}^{\ell}$.

Simulate $V_{\mathrm{LPCP}}(x)$ by answering $a \in \mathbb{F}^{\ell}$ with $\mathrm{plurality}\{\tilde{\Pi}(a + r_i) - \tilde{\Pi}(a)\}_{i \in [t]}$.

Completeness: $x \in L \rightarrow V_{\mathrm{PCP}}^{\Pi}(x) = V_{\mathrm{BLR}}^{(\langle \pi, a \rangle)_{a \in \mathbb{F}^{\ell}}} \wedge V_{\mathrm{LPCP}}^{\ell c[(\langle \pi, a \rangle)_{a \in \mathbb{F}^{\ell}}]}(x)$

$$= V_{\mathrm{BLR}}^{(\langle \pi, a \rangle)_{a \in \mathbb{F}^{\ell}}} \wedge V_{\mathrm{LPCP}}^{(\langle \pi, a \rangle)_{a \in \mathbb{F}^{\ell}}}(x)$$

$$= 1 \wedge V_{\mathrm{LPCP}}^{f_{\pi}}(x)$$, which accepts w.p. $\geq 1 - \varepsilon_c$.

The Lemma via Linearity Testing and Local Correction

<u>lemma:</u> $\mathrm{LPCP}[\varepsilon_c, \varepsilon_s, \Sigma=\mathbb{F}, \ell, q, r]$

$\leq \mathrm{PCP}[\varepsilon_c, \varepsilon_s' = \max\{\frac{7}{8}, \varepsilon_s + q\cdot\exp(-t)\}, \Sigma=\mathbb{F}, \ell'=\mathbb{F}^{\ell}, q' = 3 + 2t\cdot q, r' = r + (2\ell + t\cdot\ell)\cdot\log|\mathbb{F}|]$

Let $(P_{\mathrm{LPCP}}, V_{\mathrm{LPCP}})$ be an LPCP for a language L. Construct a PCP $(P_{\mathrm{PCP}}, V_{\mathrm{PCP}})$ as follows.

$P_{\mathrm{PCP}}(x)$: 1. Compute $\pi := P_{\mathrm{LPCP}}(x) \in \mathbb{F}^{\ell}$.

SAME AS BEFORE 2. Output $\Pi := (\langle\pi, a\rangle)_{a\in\mathbb{F}^{\ell}} \in \mathbb{F}^{\mathbb{F}^{\ell}}$.

$V_{\mathrm{PCP}}^{\tilde{\Pi}}(x)$: Check that $V_{\mathrm{BLR}}^{\tilde{\Pi}}(x) = 1$.

locally correct every answer

Sample $r_1, \ldots, r_t \in \mathbb{F}^{\ell}$.

Simulate $V_{\mathrm{LPCP}}(x)$ by answering $a \in \mathbb{F}^{\ell}$

with plurality$\{\tilde{\Pi}(a+r_i) - \tilde{\Pi}(a)\}_{i\in[t]}$.

<u>Soundness:</u> $x \notin L \rightarrow$ Fix any $\tilde{\Pi} \in \mathbb{F}^{\mathbb{F}^{\ell}}$. Fix a parameter $\delta < \min\{\frac{1}{4}, \overbrace{\frac{1}{2}\cdot(1-\frac{1}{|\mathbb{F}|})}^{\text{unique decoding radius}}\} = \frac{1}{4}$.

- Case 1: $\tilde{\Pi}$ is δ-far from LIN. $\Pr[V_{\mathrm{BLR}}^{\tilde{\Pi}} = 1] \leq 1 - \Delta(\tilde{\Pi}, \mathrm{LIN}) \leq 1 - \delta \leq 7/8$.

fix $\delta := \frac{1}{8}$

- Case 2: $\tilde{\Pi}$ is δ-close to LIN.

LIN has relative distance $\geq 1 - \frac{1}{|\mathbb{F}|}$

Let $\hat{\Pi} = (\langle\pi, a\rangle)_{a\in\mathbb{F}^{\ell}} \in \mathrm{LIN}$ be the unique linear function that is closest to $\tilde{\Pi}$.

$$\Pr\left[V_{\mathrm{LPCP}}^{\boxed{\tilde{\Pi}}}(x) = 1\right] \leq \Pr\left[V_{\mathrm{LPCP}}^{\pi}(x) = 1 \,\middle|\, \begin{array}{l}\text{all queries by } V_{\mathrm{LPCP}} \text{ are} \\ \text{answered with } \hat{\Pi} = (\langle\pi,a\rangle)_{a\in\mathbb{F}^{\ell}}\end{array}\right] + \Pr\left[\begin{array}{l}\exists \text{ query } a \text{ by } V_{\mathrm{LPCP}} \\ \text{s.t. } lc[\tilde{\Pi}](a) \neq \hat{\Pi}(a)\end{array}\right]$$

$$\leq \varepsilon_s + q\cdot\exp(-t) \circledast.$$

$\leftarrow$ Can set $t := O(\log q)$.

$\circledast$ $\forall \hat{\Pi} \in \mathrm{LIN}\ \forall a \in \mathbb{F}^{\ell}\ \Pr_r[\tilde{\Pi}(a+r) - \tilde{\Pi}(r) \neq \hat{\Pi}(a)] \leq 2\cdot\Delta(\tilde{\Pi}, \hat{\Pi})$.

By a Chernoff bound, if $\Delta(\tilde{\Pi}, \hat{\Pi}) < \frac{1}{4}$ then

$\Pr_{r_1,\ldots,r_t}[\text{plurality}\{\tilde{\Pi}(a+r_i) - \tilde{\Pi}(a)\}_{i\in[t]} \neq \hat{\Pi}(a)] \leq \exp(-t)$.

Exponential-Size PCP for QESAT [no abstractions]

$V_{PCP}^{\tilde{\pi}}((p_1,\dots,p_m))$:

1. Sample $x,y \leftarrow \mathbb{F}^{n^2+n}$ and check that $\tilde{\pi}(x)+\tilde{\pi}(y)=\tilde{\pi}(x+y)$.
2. Sample $r \leftarrow \mathbb{F}^m$ and $s_1,s_2 \leftarrow \mathbb{F}^n$.
3. Sample $u_1,\dots,u_t \leftarrow \mathbb{F}^{n^2+n}$.
4. Define $M := \begin{bmatrix} \mathrm{coeff}(p_1) \\ \vdots \\ \mathrm{coeff}(p_m) \end{bmatrix} \in \mathbb{F}^{m\times(n+n^2)}$ and $c := \begin{bmatrix} -\mathrm{const}(p_1) \\ \vdots \\ -\mathrm{const}(p_m) \end{bmatrix} \in \mathbb{F}^m$.
5. Set $v_{LC} := \mathrm{plurality}\{\tilde{\pi}(M^T \cdot r + u_i) - \tilde{\pi}(u_i)\}_{i\in[t]}$ and check that $v_{LC} = \langle c, r\rangle$.
6. Set $v_{TC1} := \mathrm{plurality}\{\tilde{\pi}(\mathrm{flat}(s_1 \otimes s_2) \| 0^n + u_i) - \tilde{\pi}(u_i)\}_{i\in[t]}$ and check that $v_{TC1} = v_{TC2} \cdot v_{TC3}$.

   $v_{TC2} := \mathrm{plurality}\{\tilde{\pi}(0^{n^2} \| s_1 + u_i) - \tilde{\pi}(u_i)\}_{i\in[t]}$

   $v_{TC3} := \mathrm{plurality}\{\tilde{\pi}(0^{n^2} \| s_2 + u_i) - \tilde{\pi}(u_i)\}_{i\in[t]}$

improved analysis of BLR test
(compared to $\max\{5/6, 1-\delta/2\}$)

The soundness error is $\min_{\delta\in[0,1/4)} \max\left\{1-\delta,\ \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2} + 4\cdot 2\cdot e^{-\frac{t}{4}\cdot(1/2-2\delta)^2}\right\}$.

Fix $\delta = 1/8$. Then $\max\left\{7/8,\ \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2} + 8\cdot e^{-t/64}\right\} \underset{|\mathbb{F}|\geq 2}{\leq} \max\left\{7/8,\ 3/4 + 8\cdot e^{-t/64}\right\} \leq 7/8$ for $t \geq 5\cdot 64 = 320$.

$8\cdot e^{-5} \leq \frac{1}{8} = \frac{7}{8} - \frac{3}{4}$

The query complexity is $3+5\cdot t = 1603$.

Additional Slides:
LPCP with Linear Proof Length

Linear PCP of Linear Size

We have shown that

theorem: $\mathrm{QESAT}(\mathbb{F}) \in \mathrm{LPCP}\left[\varepsilon_c = 0,\ \varepsilon_s = \frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2},\ \Sigma = \mathbb{F},\ \ell = n^2+n,\ q = 4,\ r = (m+2n)\cdot\log|\mathbb{F}|\right]$

Next we show that

theorem: $\mathrm{R1CS}(\mathbb{F}) \in \mathrm{LPCP}\left[\varepsilon_c = 0,\ \varepsilon_s = \frac{2m}{|\mathbb{F}|},\ \Sigma = \mathbb{F},\ \ell = n+m,\ q = 4,\ r = \log|\mathbb{F}|\right]$

↑ A restriction of QESAT($\mathbb{F}$) that is still NP-complete.

The first real-world deployments of succinct cryptographic proofs were based on LPCPs.
(Here "succinct" means "proof verification is exponentially faster than the proved computation".)

These are obtained via a transformation:

$$\boxed{\text{LPCP}} \xrightarrow{\text{transformation based on linear-only encodings}} \boxed{\text{succinct cryptographic proof}}$$

Improving the proof length from quadratic to linear enabled an efficient LPCP prover.
R1CS has become a popular standard for specifying NP statements.

Rank-1 Constraint Satisfiability

$\{\langle a_i,z\rangle\cdot\langle b_i,z\rangle=\langle c_i,z\rangle\}_{i\in[m]}$

def: $\mathrm{R1CS}(\mathbb{F})=\Big\{(\underbrace{A,B,C}_{m\times n\text{ matrices}},u)\ \Big|\ \exists w\in\mathbb{F}^{n-|u|}\text{ s.t. } Az\circ Bz=Cz \text{ for } z:=(u,w)\Big\}.$

Rank 1 Constraint Systems

$$\begin{bmatrix}-a_1-\\-a_2-\\\vdots\\-a_m-\end{bmatrix}\cdot\begin{bmatrix}|\\z\\|\end{bmatrix}\circ\begin{bmatrix}-b_1-\\-b_2-\\\vdots\\-b_m-\end{bmatrix}\cdot\begin{bmatrix}|\\z\\|\end{bmatrix}=\begin{bmatrix}-c_1-\\-c_2-\\\vdots\\-c_m-\end{bmatrix}\cdot\begin{bmatrix}|\\z\\|\end{bmatrix}$$

R1CS($\mathbb{F}$) restricts QESAT($\mathbb{F}$) to quadratic equations of the form $\langle a_i,z\rangle\cdot\langle b_i,z\rangle=\langle c_i,z\rangle$.

(Some quadratic equations are "far" from this form, e.g., $\sum_{i=1}^n x_i^2=0$.)

A quadratic equation is $x^TAx+Bx+c$.
A rank-1 constraint is $x^T(a\otimes b)x-c^Tx$.

lemma: For every finite field $\mathbb{F}$, R1CS($\mathbb{F}$) is NP-complete.

proof: R1CS($\mathbb{F}$) is in NTIME(poly($m,n,\log|\mathbb{F}|$)).

We show NP-hardness by reducing from CSAT (satisfiable boolean circuits).

Given a boolean circuit $C:\{0,1\}^k\to\{0,1\}$:

- assign each wire a variable $\underbrace{x_1,\dots,x_k}_{\text{inputs}},\underbrace{x_{k+1},\dots,x_{n-1}}_{\text{internal wires}},\underbrace{x_n}_{\text{output}}$ and allocate a variable x_0 for constants
- enforce booleanity: $\forall i\in[k]$, create the constraint $x_i\cdot(x_i-x_0)=0$
- map each gate to a constraint: $x_{i_3}=\mathrm{NAND}(x_{i_1},x_{i_2})\mapsto x_{i_1}\cdot x_{i_2}=x_0-x_{i_3}$
- output is 1: create the constraint $x_0\cdot x_n=x_0$

each constraint induces corresponding rows in the matrices A,B,C

Hence $n=|C|+1$, $m=|C|+1$ (where $|C|=\#$vertices in DAG representing C). Finally, set $u:=(1)$. ■

Linear PCP of Linear Length for R1CS

Arithmetize the R1CS condition via univariate polynomials:

$$Az \circ Bz = Cz \leftrightarrow \left\{\Big(\sum_{j\in[n]} A_{ij} z_j\Big)\cdot\Big(\sum_{j\in[n]} B_{ij} z_j\Big) - \Big(\sum_{j\in[n]} C_{ij} z_j\Big) = 0\right\}_{i\in[m]}$$

$$\leftrightarrow \left\{\Big(\sum_{j\in[n]} \hat{A}_j(i) z_j\Big)\cdot\Big(\sum_{j\in[n]} \hat{B}_j(i) z_j\Big) - \Big(\sum_{j\in[n]} \hat{C}_j(i) z_j\Big) = 0\right\}_{i\in H}$$

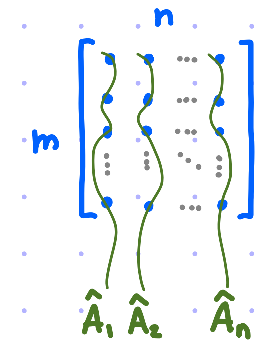
$$\leftrightarrow \prod_{i\in H}(X-i) \text{ divides } \Big(\sum_{j\in[n]} \hat{A}_j(X) z_j\Big)\cdot\Big(\sum_{j\in[n]} \hat{B}_j(X) z_j\Big) - \Big(\sum_{j\in[n]} \hat{C}_j(X) z_j\Big)$$

$$\leftrightarrow \exists \text{ quotient } \hat{Q}(X) \text{ (of degree } \leq m-2) \text{ s.t. } \hat{Q}(X)\prod_{i\in H}(X-i) = \Big(\sum_{j\in[n]} \hat{A}_j(X) z_j\Big)\cdot\Big(\sum_{j\in[n]} \hat{B}_j(X) z_j\Big) - \Big(\sum_{j\in[n]} \hat{C}_j(X) z_j\Big)$$

low-degree extend each column:

$\hat{A}_j \in \mathbb{F}^{<m}[X]$ is LDE of

$A_j : H \to \mathbb{F}$ where $A_j(i) := A_{ij}$



The LPCP verifier expects a proof $\pi = (w, \hat{Q}) \in \mathbb{F}^{(n-k)+m-1}$ and works as follows.

$V^{(w,\hat{Q})}((A,B,C,u))$:

1. Sample $r \leftarrow \mathbb{F}$.
2. Query w at $(\hat{A}_j(r))_{j=k+1}^{n}, (\hat{B}_j(r))_{j=k+1}^{n}, (\hat{C}_j(r))_{j=k+1}^{n}$ to obtain a, b, c.
3. Query $\hat{Q}$ at $(r^i)_{i=0}^{m-2}$ to obtain d.
4. Check that $\hat{Q}(r)\prod_{i\in H}(r-i) = \Big(\sum_{j\in[n]} \hat{A}_j(r) z_j\Big)\cdot\Big(\sum_{j\in[n]} \hat{B}_j(r) z_j\Big) - \Big(\sum_{j\in[n]} \hat{C}_j(r) z_j\Big)$

   by checking that $d \cdot \prod_{i\in H}(r-i) = \big(\sum_{j=1}^{k} \hat{A}_j(r) u_j + a\big)\cdot\big(\sum_{j=1}^{k} \hat{B}_j(r) u_j + b\big) - \big(\sum_{j=1}^{k} \hat{C}_j(r) u_j + c\big)$.

Bibliography

Exponential size PCPs

- [ALMSS 1998]: Proof verification and the hardness of approximation problems, by Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, Mario Szegedy.

Arguments from linear PCPs

- [IKO 2007]: Efficient arguments without short PCPs, by Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky.
- [BCIOP 2013]: Succinct non-interactive arguments via linear interactive proofs, by Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, Omer Paneth.

Contains a linear size linear PCP

- [SBVBPW 2013]: Resolving the conflict between generality and plausibility in verified computation, by Srinath Setty, Benjamin Braun, Victor Vu, Andrew Blumberg, Bryan Parno, Michael Walfish.
- [GGPR 2013]: Quadratic span programs and succinct NIZKs without PCPs, by Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova.
- [Groth 2016]: On the size of pairing-based non-interactive arguments, by Jens Groth. (▸Video)

Widely deployed!