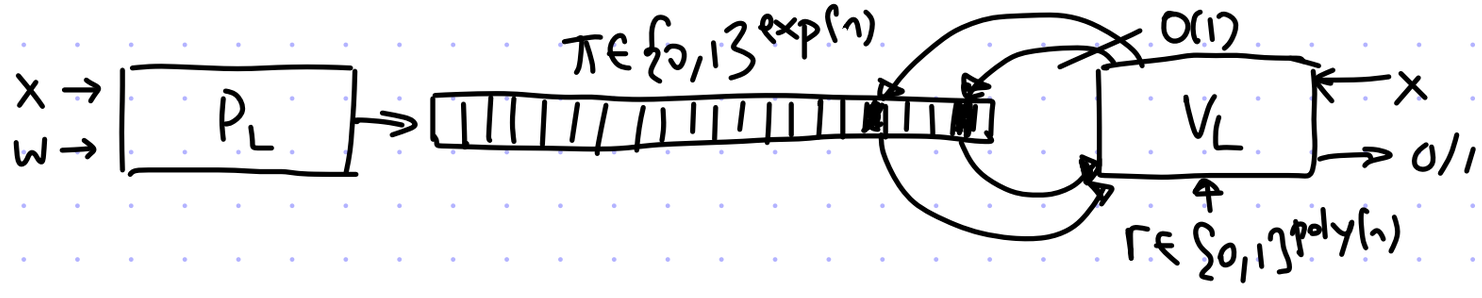
Lecture 09

Foundations of Probabilistic Proofs
Fall 2020
Alessandro Chiesa

Exponential-Size PCPs for NP

theorem: $NP \subseteq PCP[\varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, \ell = \exp(n), q = O(1), r = \text{poly}(n)]$

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



We can achieve soundness error ≤ 0.5 with a constant number of queries!

Proof strategy:

① construct constant-query linear PCP for NP

② construct a linearity test

③ linear PCP + linearity test → exponential-size PCP

Today we discuss ①.

Linear PCPs

A linear PCP is a PCP where:

① the honest proof is a linear function

② we only consider malicious proofs 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 $f_\pi(x) := \langle \pi, x \rangle$.

def: We say that (P,V) is a **LPCP system** for L (over $\mathbb{F}$) if

① completeness: $\forall x \in L$, for $\pi := P(x) \in \mathbb{F}^\ell$, $\Pr_\rho[V^{f_\pi}(x;\rho)=1] \geq 1-\varepsilon_c$

② soundness: $\forall x \notin L \quad \forall \tilde{\pi} \in \mathbb{F}^\ell \quad \Pr_\rho[V^{f_{\tilde{\pi}}}(x;\rho)=1] \leq \varepsilon_s$.

We use similar class notation as for PCP: $\mathsf{LPCP}[\varepsilon_c, \varepsilon_s, \ell, q, r, \dots]$.

theorem: $\mathsf{NP} \subseteq \mathsf{LPCP}[\varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, \ell = O(n^2), q = O(1), r = O(n)]$

Quadratic Equations are NP-Complete

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

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

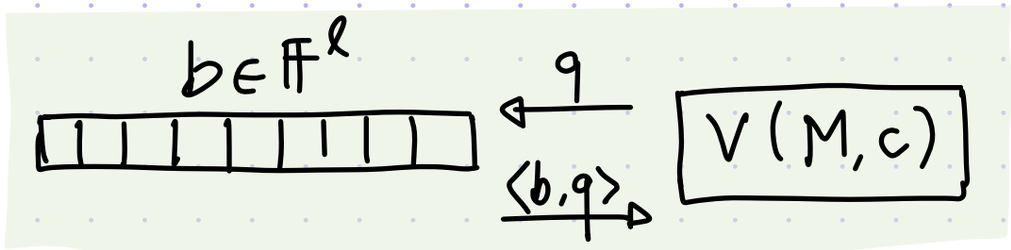
lemma: For any finite field $\mathbb{F}$, $QESAT(\mathbb{F})$ is NP-complete.

proof: Reduce from boolean circuit satisfiability (recall $\{0,1\}$ is a subset of every field):

- assign each wire a variable name: $\underbrace{X_1, \dots, X_{n_{in}}}_{\text{inputs}}, \underbrace{X_{n_{in}+1}, \dots, X_{n-1}}_{\text{internal}}, \underbrace{X_n}_{\text{output}}$
- use equations to enforce gates: $X_k = NAND(X_i, X_j) \mapsto X_k - (1 - X_i \cdot X_j)$
- enforce booleanity: $\forall i \in [n_{in}], \; X_i(1 - X_i) = 0$.

Warm Up 1: Linear PCP for Linear Equations

Let $M \in \mathbb{F}^{m \times \ell}$, $b \in \mathbb{F}^{\ell}$, and $c \in \mathbb{F}^{m}$, and consider this setup:



The verifier wishes to check the condition $c \stackrel{?}{=} Mb$ via linear queries.

Idea: use random linear combinations (which are linear queries)

That is: $V(M,c) :=$ sample $r \in \mathbb{F}^m$, query $b \in \mathbb{F}^\ell$ at $q := M^T r \in \mathbb{F}^\ell$ and check that $\langle c, r \rangle = \langle b, q \rangle$

Completeness: if $c = Mb$ then $\forall r \in \mathbb{F}^m \ \langle c, r \rangle = \langle Mb, r \rangle = \langle b, M^T r \rangle = \langle b, q \rangle$.

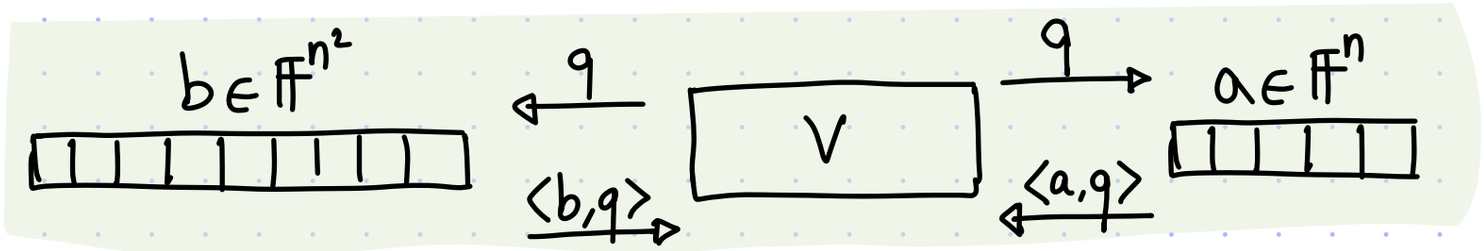
Soundness: if $c \neq Mb$ then

Polynomial Identity Lemma applied to the non-zero poly $p(X_1,..,X_m) := \sum_{i \in [m]} (c-Mb)_i X_i$

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

Warm Up 2: Linear PCP for Tensor Structure

Let $a \in \mathbb{F}^n$ and $b \in \mathbb{F}^{n^2}$ and consider this setup:



The verifier wishes to check the condition $b \stackrel{?}{=} \text{flat}(a \otimes a)$ via linear queries.

$V :=$ sample $s,t \in \mathbb{F}^n$, query b at $\text{flat}(s \otimes t)$, query a at s, t, and check that $\langle b, \text{flat}(s \otimes t) \rangle = \langle a, s \rangle \cdot \langle a, t \rangle$.

Completeness: if $b = \text{flat}(a \otimes a)$ then $\forall\, s,t \in \mathbb{F}^n$

$$\langle b, \text{flat}(s \otimes t) \rangle = \langle \text{flat}(a \otimes a), \text{flat}(s \otimes t) \rangle = \sum_{i,j} a_i a_j s_i t_j = \left(\sum_i a_i s_i\right)\left(\sum_j a_j t_j\right) = \langle a, s \rangle \langle a, t \rangle .$$

Soundness: if $b \neq \text{flat}(a \otimes a)$ then (there is i^*, j^* s.t. $b_{i^* j^*} \neq a_{i^*} a_{j^*}$ so)

$$\Pr_{s,t}\left[\langle b, \text{flat}(s \otimes t) \rangle \neq \langle a, s \rangle \cdot \langle a, t \rangle\right] = \Pr_{s,t}\left[\sum_{ij} (b_{ij} - a_i a_j) s_i t_j \neq 0\right] = \Pr_{s,t}\left[\sum_i \left(\sum_j (b_{ij} - a_i a_j) t_j\right) s_i \neq 0\right]$$

$$= \Pr_{s,t}\left[\sum_i p_i(t) s_i \neq 0\right] = \Pr_{s,t}\left[\exists\, i \text{ s.t. } p_i(t) \neq 0 \;\&\; \sum_i p_i(t) s_i \neq 0\right] \geq \left(\frac{|\mathbb{F}| - 1}{|\mathbb{F}|}\right)^2 \Rightarrow \text{soundness error} \leq \frac{2|\mathbb{F}| - 1}{|\mathbb{F}|^2} . \quad \square$$

Linear PCP for Quadratic Equations

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

Let $p_1, \ldots, p_m \in \mathbb{F}[X_1, \ldots, X_n]$ be an instance of $\mathrm{QESAT}(\mathbb{F})$.
The LPCP verifier expects a proof $\pi = (a, b) \in \mathbb{F}^{n+n^2}$ and works as follows:

$V^{\pi}(p_1, \ldots, p_m) :=$

1. sample $r \in \mathbb{F}^m$ and $s, t \in \mathbb{F}^n$
2. let $M \in \mathbb{F}^{m \times (n+n^2)}$ and $c \in \mathbb{F}^m$ be $M := \begin{bmatrix} \text{—}\ \mathrm{vec}(p_1)\ \text{—} \\ \text{—}\ \mathrm{vec}(p_2)\ \text{—} \\ \vdots \\ \text{—}\ \mathrm{vec}(p_m)\ \text{—} \end{bmatrix}$ & $c := \begin{bmatrix} \mathrm{const}(p_1) \\ \mathrm{const}(p_2) \\ \vdots \\ \mathrm{const}(p_m) \end{bmatrix}$
   [$\mathrm{vec}(p_i) \in \mathbb{F}^{n+n^2}$ are non-constant coefficients of polynomial p_i]
3. queries: $a \| b$ at $M^T r$, b at $s \otimes t$, and a at $s \| t$.
4. check that $\langle c, r \rangle = \langle a \| b, M^T r \rangle$, $\langle b, s \otimes t \rangle = \langle a, s \rangle \langle a, t \rangle$

Completeness: Suppose $p_1(a) = \cdots = p_m(a) = 0$ and set $b := a \otimes a$. Then:

(i) $b = a \otimes a \Rightarrow$ tensor check passes w.p. 1 (ii) $M \begin{bmatrix} a \\ b \end{bmatrix} = M \begin{bmatrix} a \\ \mathrm{flat}(a \otimes a) \end{bmatrix} = c \Rightarrow$ linear check passes w.p. 1

Soundness: If $p_1, \ldots, p_m$ have no solution then $\forall \pi = (a, b)$ either

(i) $b \neq a \otimes a \Rightarrow$ tensor check passes w.p. $\frac{2|\mathbb{F}|-1}{|\mathbb{F}|^2}$ (ii) $b = a \otimes a$ and $M \begin{bmatrix} a \\ b \end{bmatrix} \neq c$ $\Rightarrow$ linear check passes w.p. $< \frac{1}{|\mathbb{F}|}$

Linear PCP of Linear Size

We have shown that

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

Now we show that

$$RICS(\mathbb{F}) \in LPCP\left[\varepsilon_c = 0,\ \varepsilon_s = \frac{2m}{|\mathbb{F}|},\ \Sigma = \mathbb{F},\ \ell = n+m,\ q = 4,\ r = 1\right]$$

↗

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

The first deployments of cryptographic proofs that leverage PCP-like objects to achieve strong efficiency properties (e.g. crypto proof size is exponentially smaller than the proved computation) were based on LPCPs!

[There is a transformation: LPCP $\vdash$(use crypto)$\rightarrow$ cryptographic proof.]

Improving quadratic proof length to linear proof length as above was an important ingredient to achieve an efficient proving procedure.

RICS has become a de-facto standard for specifying NP-statements.

Rank-1 Constraint Satisfiability

def: $\mathrm{RICS}(\mathbb{F}) = \{ (v, \underbrace{A, B, C}_{m \times n \text{ matrices}}) \mid \exists z \in \mathbb{F}^n \text{ s.t. } Az \circ Bz = Cz \ \& \ z = (v, w) \text{ for some } w \}$.

$$\begin{bmatrix} — a_1 — \\ — a_2 — \\ \vdots \\ — a_m — \end{bmatrix} \begin{bmatrix} 1 \\ z \\ 1 \end{bmatrix} \circ \begin{bmatrix} — b_1 — \\ — b_2 — \\ \vdots \\ — b_m — \end{bmatrix} \begin{bmatrix} 1 \\ z \\ 1 \end{bmatrix} = \begin{bmatrix} — c_1 — \\ — c_2 — \\ \vdots \\ — c_m — \end{bmatrix} \begin{bmatrix} 1 \\ z \\ 1 \end{bmatrix} \quad \text{i.e.} \quad \{ \langle a_i, z \rangle \langle b_i, z \rangle = \langle c_i, z \rangle \}_{i \in [m]}$$

[these are special case of quadratic equations]

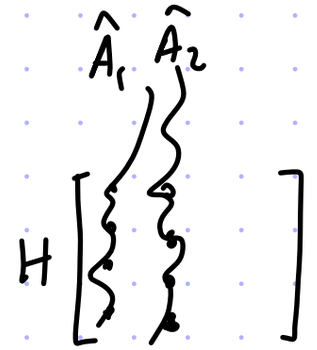
lemma: $\mathrm{RICS}(\mathbb{F})$ is NP-complete

proof: Again reduce from boolean circuit satisfiability.

- assign each wire a variable name: $\underbrace{x_1, \dots, x_{n_{in}}}_{\text{inputs}}, \underbrace{x_{n_{in}+1}, \dots, x_{n-1}}_{\text{internal}}, \underbrace{x_n}_{\text{output}}$
- use rank-1 equations to enforce gates: $x_k = \mathrm{NAND}(x_i, x_j) \mapsto (1 - x_i)(1 - x_j) = 1 - x_k$
- enforce booleanity: $\forall i \in [n_{in}], \ x_i(1 - x_i) = 0$.

The RICS instance considers $z = (1, x_1, \dots, x_n) \in \mathbb{F}^{n+1}$ and matrices $A, B, C \in \mathbb{F}^{n \times (n+1)}$ where $\forall i \in [n_{in}]$ a_i, b_i, c_i are for booleanity and $\forall i = n_{in}+1, \dots, n$ a_i, b_i, c_i are for gate i.

Linear PCP of Linear Length for R1CS



First we arithmetize the R1CS condition:

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

low-degree extend each column

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

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

$$\Leftrightarrow \exists \underset{[\text{of deg} \le m-2]}{\text{quotient } Q(X)} \text{ s.t. } Q(X)\prod_{i\in H}(X-i) = \left(\sum_{j\in[n]} \hat{A}_j(X) z_j\right)\left(\sum_{j\in[n]} \hat{B}_j(X) z_j\right) - \left(\sum_{j\in[n]} \hat{C}_j(X) z_j\right)$$

Next we write the LPCP: the verifier expects a proof $\pi = (z, Q) \in \mathbb{F}^{n+(m-1)}$ and

$V^{f_\pi}(v, A, B, C) :=$

1. sample $r \in \mathbb{F}$
2. queries: z at $(\hat{A}_1(r), \ldots, \hat{A}_n(r)), (\hat{B}_1(r), \ldots, \hat{B}_n(r)), (\hat{C}_1(r), \ldots, \hat{C}_n(r))$
   Q at $(1, r, r^2, \ldots, r^{m-2})$
3. check that $Q(r)\prod_{i\in H}(r-i) = \left(\sum_{j\in[n]} \hat{A}_j(r) z_j\right)\left(\sum_{j\in[n]} \hat{B}_j(r) z_j\right) - \left(\sum_{j\in[n]} \hat{C}_j(r) z_j\right)$
4. check that z consistent with v with 1 more query

can avoid by asking for $\pi = (w, Q)$ and add in V