Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 10

Polynomial-Length PCP

Polynomial-Size PCPs for NP

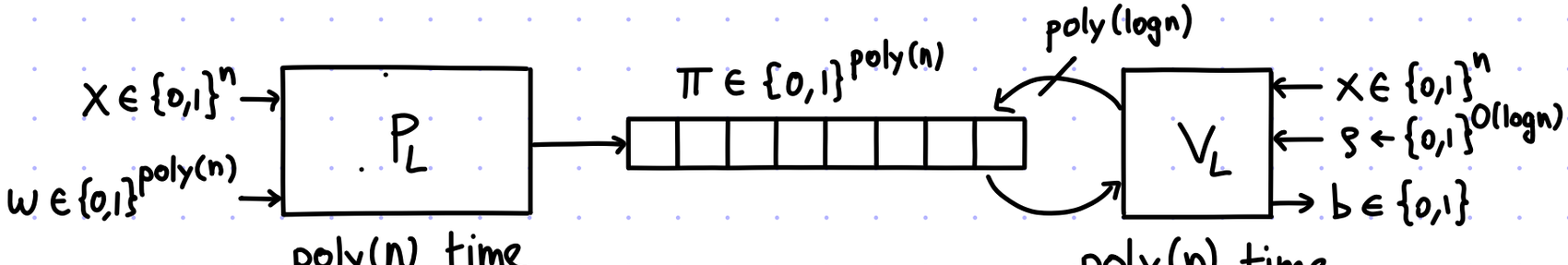
We have proved that $NP \subseteq PCP[\varepsilon_c = 0, \varepsilon_s = 1/2, \Sigma = \{0,1\}, \ell = \exp(n), q = O(1), r = \text{poly}(n)]$.

Today we reduce proof length at the expense of query complexity:

later in the course we reduce this to $q = O(1)$

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

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

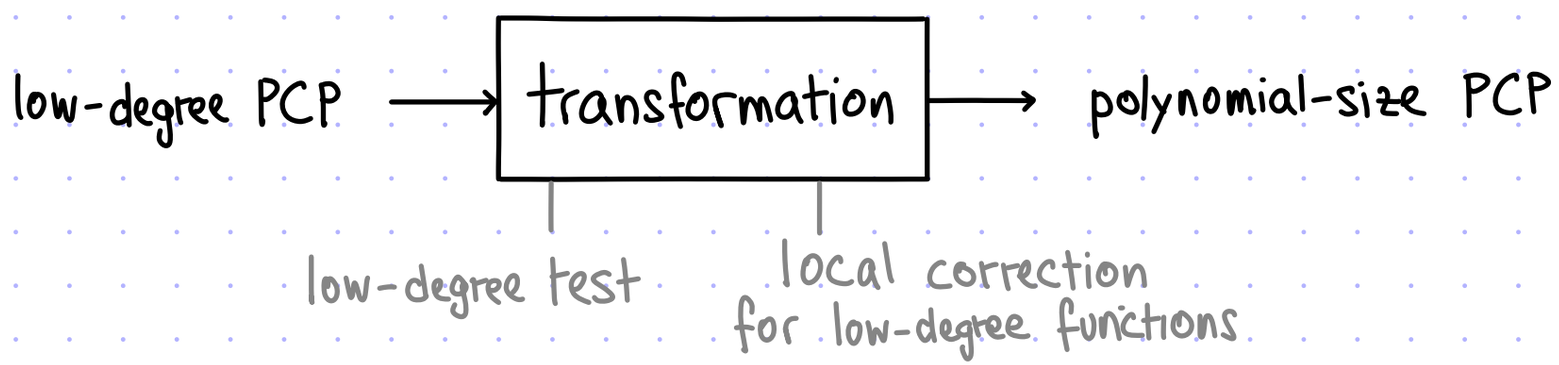


PROOF STRATEGY:

① define notion of a LOW-DEGREE PCP (LDPCP)

② construct a low-degree PCP for NP with polylogarithmic query complexity

③ transform the low-degree PCP into a (standard) PCP:



Polynomial-Size PCP for Quadratic Equations

Recall the following NP-complete problem about quadratic equations over a field $\mathbb{F}$:

$$QESAT(\mathbb{F}) = \left\{ (p_1, \ldots, p_m) \mid \exists\, a_1, \ldots, a_n \in \mathbb{F} \text{ s.t. } \forall j \in [m]\ \ p_j(a_1, \ldots, a_n) = 0 \right\}.$$

We construct a PCP for $QESAT(\mathbb{F})$ with these parameters:

<u>theorem:</u> $QESAT(\mathbb{F}) \subseteq PCP$

		if $\lvert\mathbb{F}\rvert = \text{poly}(\log n)$:
completeness error	$\varepsilon_c = 0$	
soundness error	$\varepsilon_s = O(1) + O\left(\frac{\log^2 n}{\log\log n} \cdot \frac{1}{\lvert\mathbb{F}\rvert}\right)$	$\longrightarrow \varepsilon_s = O(1)$
alphabet	$\Sigma = \mathbb{F}$	
proof length	$\ell = \lvert\mathbb{F}\rvert^{O\left(\frac{\log n}{\log\log n}\right)}$	$\longrightarrow \ell = \text{poly}(n)$
query complexity	$q = \text{poly}(\log n)$	
randomness complexity	$r = O\left(\frac{\log n}{\log\log n} \cdot \log\lvert\mathbb{F}\rvert\right)$	$\longrightarrow r = O(\log n)$

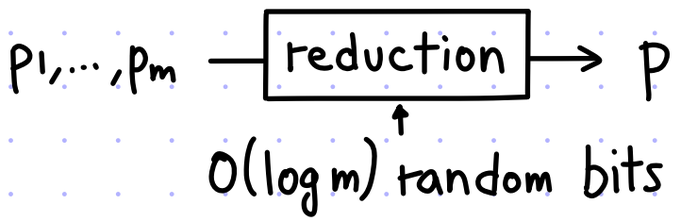
The field must be large enough for soundness and small enough for polynomial proof length.

We can switch the alphabet from $\mathbb{F}$ to $\{0,1\}$, incurring a $(\log\lvert\mathbb{F}\rvert)$-factor query increase.

Proof Overview

Theorem: $QESAT(\mathbb{F}) \subseteq PCP\left[\begin{array}{lll} \varepsilon_c = 0 & \Sigma = \mathbb{F} & q = \text{poly}(\log n) \\ \varepsilon_s = O(1) + O\left(\frac{\log^2 n}{\log\log n} \cdot \frac{1}{|\mathbb{F}|}\right) & \ell = |\mathbb{F}|^{O\left(\frac{\log n}{\log\log n}\right)} & r = O\left(\frac{\log n}{\log\log n} \cdot \log|\mathbb{F}|\right) \end{array}\right]$

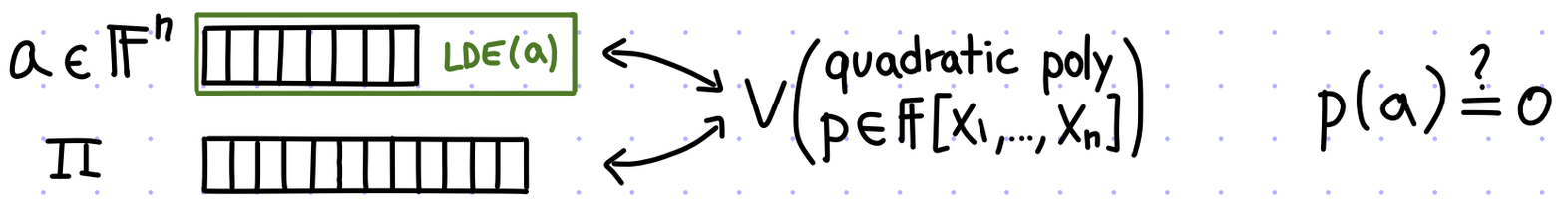
Part 1: small amount of randomness to reduce m equations to 1 equation



- $\forall i \in [m]\ \ p_i(a) = 0 \rightarrow Pr[\,p(a) = 0\,] = 1$
- $\exists i \in [m]\ \ p_i(a) \neq 0 \rightarrow Pr[\,p(a) = 0\,] \leq \varepsilon$

The PCP string will include a substring for each choice of randomness.
So we care about randomness complexity.

Part 2: PCP for evaluation of 1 equation



Conclude: Part 1 + Part 2 + low-degree testing

Part 1: From m Equations to 1 Equation [1/2]

lemma: There is a probabilistic algorithm T s.t. for $|\mathbb{F}| = \text{poly}(\log m)$ ← we will use this to ensure PCP has polynomial length

① $T(p_1,\dots,p_m)$ uses $O(\log m)$ random bits and outputs a quadratic equation $p(X_1,\dots,X_n)$

② $\forall\, a \in \mathbb{F}^n$ if $p_1(a) = \cdots = p_m(a) = 0$ then $\Pr_\sigma[T(p_1,\dots,p_m;\sigma)(a) = 0] = 1$

③ $\forall\, a \in \mathbb{F}^n$ if $\exists\, j \in [m]$ $p_j(a) \neq 0$ then $\Pr_\sigma[T(p_1,\dots,p_m;\sigma)(a) = 0] \leq \varepsilon$

Idea #1: T samples $j \in [m]$ and outputs p_j

This uses little randomness ($\log m$ bits) but the soundness error is large $\left(1 - \frac{1}{m}\right)$.

Idea #2: T samples $\sigma_1,\dots,\sigma_m \in \mathbb{F}$ and outputs $p = \sum_{j\in[m]} \sigma_j \cdot p_j$

This has small soundness error $\left(\frac{1}{|\mathbb{F}|}\right)$ but uses too much randomness (m elts).

[This is essentially what we did inside the LPCP for QESAT($\mathbb{F}$).]

If we sample $\sigma_1,\dots,\sigma_m \in \mathbb{F}_2$ the soundness error is ok $(1/2)$ but not randomness (m bits).

Idea #3: T samples $\sigma \in \mathbb{F}$ and outputs $p = \sum_{j\in[m]} \sigma^j \cdot p_j$

This uses little randomness (1 elt) but now requires the field to be large:

the soundness error is $\frac{m}{|\mathbb{F}|}$ so we need $|\mathbb{F}| \geq \Omega(m)$.

Part 1: From m Equations to 1 Equation [2/2]

lemma: There is a probabilistic algorithm T s.t. for $|\mathbb{F}| = \text{poly}(\log m)$ ← we will use this to ensure PCP has polynomial length

① $T(p_1,\dots,p_m)$ uses $O(\log m)$ random bits and outputs a quadratic equation $p(X_1,\dots,X_n)$

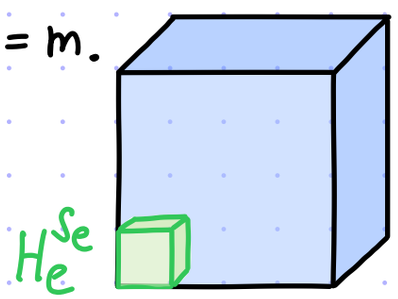
② $\forall\, a\in\mathbb{F}^n$ if $p_1(a)=\cdots=p_m(a)=0$ then $\Pr_\sigma[T(p_1,\dots,p_m;\sigma)(a)=0]=1$

③ $\forall\, a\in\mathbb{F}^n$ if $\exists\, j\in[m]$ $p_j(a)\neq 0$ then $\Pr_\sigma[T(p_1,\dots,p_m;\sigma)(a)=0]\leq\varepsilon$

proof: Identify $[m]$ with $H_e^{s_e}$ for $H_e\subseteq\mathbb{F}$ and $s_e\in\mathbb{N}$ with $|H_e|^{s_e}=m$.

Set $|H_e| = O(\log m)$ and $s_e = \frac{\log m}{\log|H_e|}$.

We can relabel $(p_j)_{j\in[m]}$ as $(p_{j_1,\dots,j_{s_e}})_{j_1,\dots,j_{s_e}\in H_e}$.



The transformation T samples $\sigma_1,\dots,\sigma_{s_e}\in\mathbb{F}$ and outputs

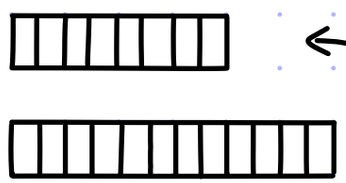
$$p := \sum_{0\leq j_1,\dots,j_{s_e}<|H_e|} \sigma_1^{j_1}\cdots\sigma_{s_e}^{j_{s_e}}\cdot p_{j_1,\dots,j_{s_e}}\,.$$

SOUNDNESS: Fix $a\in\mathbb{F}^n$ and define $q_a(X_1,\dots,X_{s_e}) := \sum_{0\leq j_1,\dots,j_{s_e}<|H_e|} X_1^{j_1}\cdots X_{s_e}^{j_{s_e}}\cdot p_{j_1,\dots,j_{s_e}}(a)$, which is non-zero.

Then $\Pr_\sigma[p(a)=0] = \Pr_\sigma[q_a(\sigma)=0] \leq \frac{s_e\cdot(|H_e|-1)}{|\mathbb{F}|} \leq O\left(\frac{\log^2 m}{\log\log m}\cdot\frac{1}{|\mathbb{F}|}\right) \xrightarrow{|\mathbb{F}|=\Omega\left(\frac{\log^2 m}{\log\log m}\right)} O(1)$

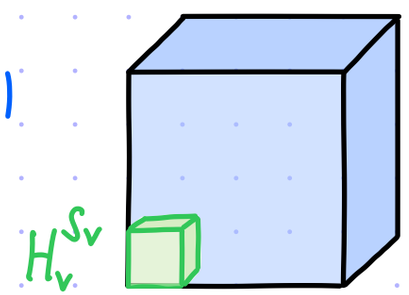
RANDOM BITS: $s_e\cdot\log|\mathbb{F}| = O\left(\frac{\log m}{\log\log m}\cdot\log|\mathbb{F}|\right) \xrightarrow{|\mathbb{F}|=(\log m)^{O(1)}} O(\log m)$ ■

Part 2: Low-Degree PCP for 1 Equation [1/2]

Consider this setting: $a \in \mathbb{F}^n$, Π  V(quadratic poly $p \in \mathbb{F}[X_1,\dots,X_n]$) $\quad p(a) \stackrel{?}{=} 0$

Challenge: the polynomial $p(X_1,\dots,X_n)$ may depend on every variable

Idea: reduce to a sumcheck problem & use the (unrolled) sumcheck protocol



Step 1: arithmetize

- identify $[n]$ with $H_v^{s_v}$ for a subset $H_v \subseteq \mathbb{F}$ with $|H_v| = O(\log n)$ and $s_v := \frac{\log n}{\log |H_v|}$.
- evaluation as a sum:

$$p(a) = \sum_{i,j \in [n]} c_{ij}\, a_i\, a_j = \sum_{\alpha,\beta \in H_v^{s_v}} \hat{c}(\alpha,\beta) \cdot \hat{a}(\alpha) \cdot \hat{a}(\beta)$$

← for simplicity we ignore the linear terms and the constant term

where $\hat{a} : \mathbb{F}^{s_v} \to \mathbb{F}$ is the low-degree extension of $a : [n] \to \mathbb{F}$

$\hat{c} : \mathbb{F}^{2s_v} \to \mathbb{F}$ is the low-degree extension of $c : [n]^2 \to \mathbb{F}$

The addend $q(y,z) := \hat{c}(y,z) \cdot \hat{a}(y) \cdot \hat{a}(z)$ has individual degree $\leq 2 \cdot (|H_v| - 1) \leq 2|H_v|$.

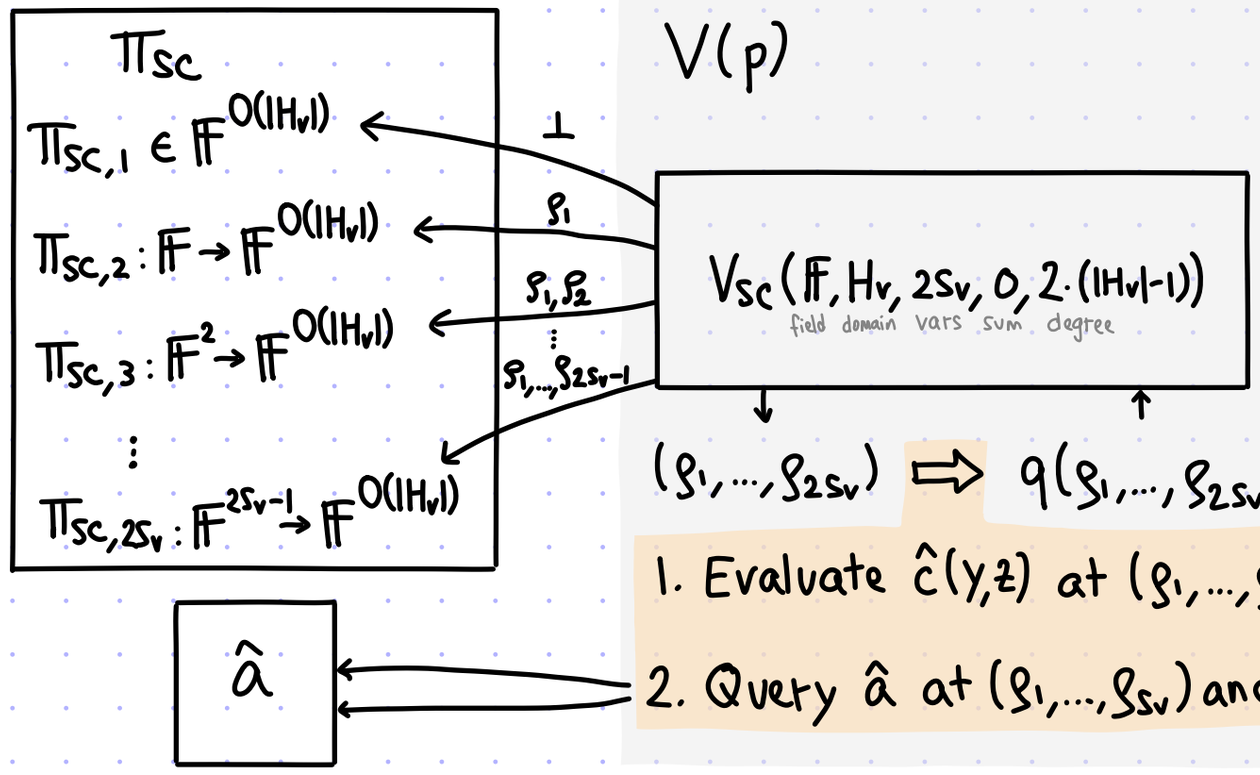
In sum: $p(a) = 0 \iff \sum_{\alpha,\beta \in H_v^{s_v}} q(\alpha,\beta) = 0$ for $q(Y,Z) := \hat{c}(Y,Z) \cdot \hat{a}(Y) \cdot \hat{a}(Z)$

Part 2: Low-Degree PCP for 1 Equation [2/2]

Step 2: probabilistically check the arithmetized statement $\sum_{\alpha,\beta\in H_v^{s_v}} q(\alpha,\beta)=0$

$P(p,a)$

1. Output π_{sc} that is eval table of IP prover for the sumcheck claim $\sum_{\alpha,\beta\in H_v^{s_v}} q(\alpha,\beta)=0$
2. Output $\hat{a}: \mathbb{F}^{s_v}\to\mathbb{F}$. (The LDE of $a:[n]\to\mathbb{F}$.)



proof length:
- $|\pi_{sc}| = O(|\mathbb{F}|^{2s_v}\cdot|H_v|)$
- $|\hat{a}| = |\mathbb{F}|^{s_v}$

query complexity:
- $2s_v$ queries to π_{sc} (each retrieving $O(|H_v|)$ elts)
- 2 queries to $\hat{a}$ (each retrieving 1 elt)

Completeness: if $p(a)=0$ then $\pi=(\text{LDE}(a), \pi_{sc})$ always convinces the verifier

Soundness: $\forall a\in\mathbb{F}^n$ s.t. $p(a)\neq 0$ (so that $\sum_{\alpha,\beta\in H_v^{s_v}} q(\alpha,\beta)\neq 0$) $\forall$ sumcheck PCP string $\tilde{\pi}_{sc}$

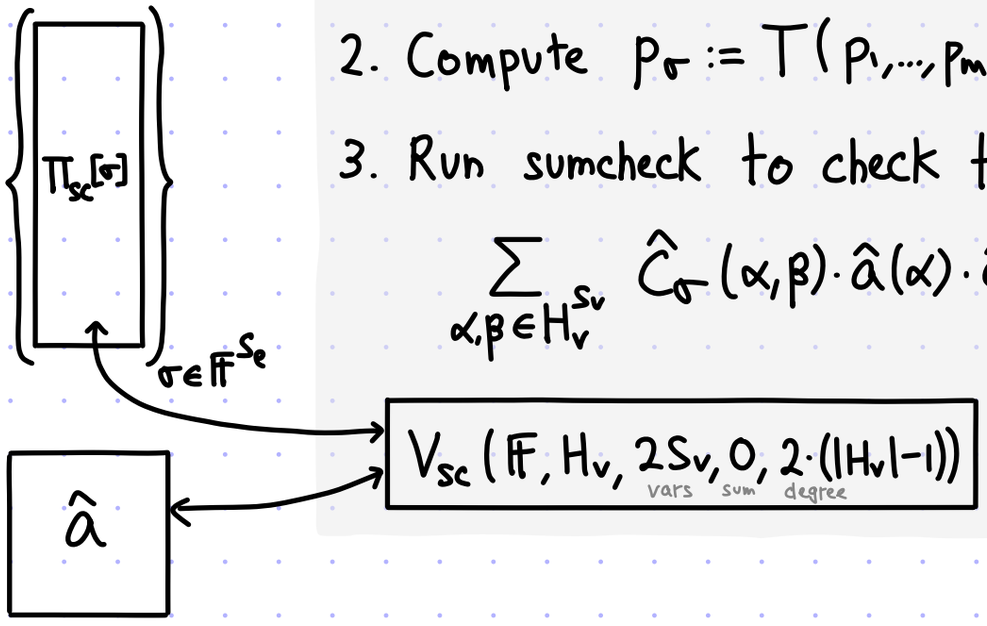
$$\Pr\left[V^{(\text{LDE}(a),\tilde{\pi}_{sc})}(p)=1\right] \le \frac{(2s_v)\cdot(2\cdot(|H_v|-1))}{|\mathbb{F}|} \le O\left(\frac{\log^2 n}{\log\log n}\cdot\frac{1}{|\mathbb{F}|}\right)$$

Low-Degree PCP for Quadratic Equations [1/2]

We combine Part 1 and Part 2:

$P((p_1,\dots,p_m),a)$

1. For every $\sigma \in \mathbb{F}^{S_e}$:
   - $p_\sigma := T(p_1,\dots,p_m;\sigma)$
   - $\Pi_{sc}[\sigma]$:= eval table for sumcheck claim "$p_\sigma(a)=0$"
   - output $\Pi_{sc}[\sigma]$
2. Output $\hat{a}:\mathbb{F}^{S_v}\to\mathbb{F}$.
   (The LDE of $a:[n]\to\mathbb{F}$.)



$V((p_1,\dots,p_m))$

1. Sample $\sigma \in \mathbb{F}^{S_e}$.
2. Compute $p_\sigma := T(p_1,\dots,p_m;\sigma)$.
3. Run sumcheck to check that $p_\sigma(a)=0$:

$$\sum_{\alpha,\beta\in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\cdot\hat{a}(\alpha)\cdot\hat{a}(\beta) = 0$$

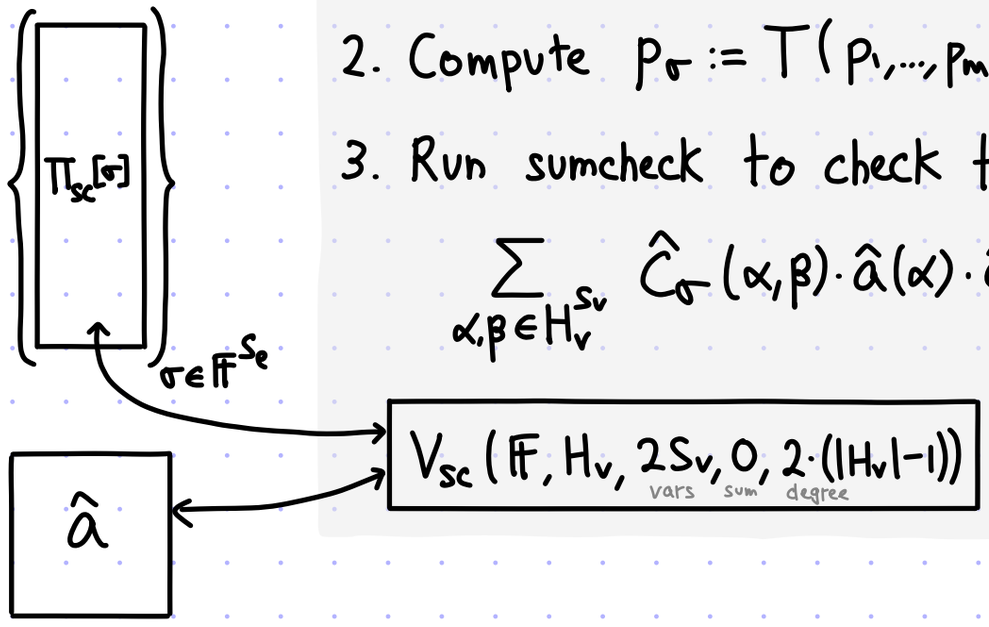
- proof length: $|\mathbb{F}|^{S_e}\cdot\left(|\mathbb{F}|^{2S_v}\cdot O(|H_v|)\right)+|\mathbb{F}|^{S_v} = |\mathbb{F}|^{O(S_e+S_v)} = |\mathbb{F}|^{O\left(\frac{\log m}{\log\log m}+\frac{\log n}{\log\log n}\right)}$
- query complexity: $2S_v$ queries to Π_{sc}, each retrieving $O(|H_v|)$ elements; 2 queries to $\hat{a}$, each retrieving 1 element. $O(S_v\cdot|H_v|)$ elements $= O\left(\frac{\log n}{\log|H_v|}\cdot|H_v|\right) = O\left(\frac{\log^2 n}{\log\log n}\right)$.
- randomness complexity: $S_e\cdot\log|\mathbb{F}| + 2S_v\cdot\log|\mathbb{F}| = O\left(\frac{\log m}{\log|H_e|}+\frac{\log n}{\log|H_v|}\right)\cdot\log|\mathbb{F}| = O\left(\frac{\log m}{\log\log m}+\frac{\log n}{\log\log n}\right)\cdot\log|\mathbb{F}|$

Low-Degree PCP for Quadratic Equations [2/2]

We combine Part 1 and Part 2:

$P((p_1,\dots,p_m),a)$

1. For every $\sigma \in \mathbb{F}^{S_e}$:
   - $p_\sigma := T(p_1,\dots,p_m;\sigma)$
   - $\Pi_{sc}[\sigma]$:= eval table for sumcheck claim "$p_\sigma(a)=0$"
   - output $\Pi_{sc}[\sigma]$
2. Output $\hat{a}:\mathbb{F}^{S_v}\to\mathbb{F}$.
   (The LDE of $a:[n]\to\mathbb{F}$.)



$V((p_1,\dots,p_m))$

1. Sample $\sigma \in \mathbb{F}^{S_e}$.
2. Compute $p_\sigma := T(p_1,\dots,p_m;\sigma)$.
3. Run sumcheck to check that $p_\sigma(a)=0$:

$$\sum_{\alpha,\beta\in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\cdot\hat{a}(\alpha)\cdot\hat{a}(\beta) = 0$$

Completeness: if $p_1(a)=\dots=p_m(a)=0$ then $\forall \sigma\in\mathbb{F}^{S_e}$ $p_\sigma(a)=0$, so $\sum_{\alpha,\beta\in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\hat{a}(\alpha)\hat{a}(\beta)=0$

Soundness: if $(p_1,\dots,p_m)\notin QESAT(\mathbb{F})$ then, $\forall a$ and $\forall \tilde{\pi}_{sc}=\{\tilde{\pi}_{sc}[\sigma]\}_\sigma$,

- $p_\sigma(a)=\sum_{\alpha,\beta\in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\hat{a}(\alpha)\hat{a}(\beta)\neq 0$ except w.p. $\leq O\left(\frac{S_e\cdot|H_e|}{|\mathbb{F}|}\right) = O\left(\frac{\log^2 m}{\log\log m}\cdot\frac{1}{|\mathbb{F}|}\right)$
- if so then sumcheck accepts w.p. $\leq O\left(\frac{S_v\cdot|H_v|}{|\mathbb{F}|}\right) = O\left(\frac{\log^2 n}{\log\log n}\cdot\frac{1}{|\mathbb{F}|}\right)$

Recall: Low-Degree Testing

For multivariate polynomials there are two notions of degree:

- total degree : $LD[\mathbb{F}, n, \text{tot} \leq d]$
- individual degree : $LD[\mathbb{F}, n, \text{ind} \leq d]$

A low-degree test V_{LDT} for $LD[\mathbb{F}, n, \text{tot/ind} \leq d]$ works as follows:

① COMPLETENESS: if $f: \mathbb{F}^n \to \mathbb{F} \in LD[\mathbb{F}, n, \text{tot/ind} \leq d]$ then $\Pr[V_{LDT}^f = 1] = 1$.

② SOUNDNESS: if $f: \mathbb{F}^n \to \mathbb{F}$ is δ-far from $LD[\mathbb{F}, n, \text{tot/ind} \leq d]$ then $\Pr[V_{LDT}^f = 1] \leq \varepsilon_{LDT}(\delta)$.

The RS test is a total low-degree test with $\begin{cases} q_{LDT} = O(d^3) \\ r_{LDT} = O(d^2 \cdot n \cdot \log|\mathbb{F}|) \end{cases}$ ← TOO LARGE (to achieve PCP with log randomness)

A slightly different total low-degree test achieves $q_{LDT} = O(d)$ and $r_{LDT} = O(n \cdot \log|\mathbb{F}|)$.

Today we assume an individual low-degree test with $\begin{cases} q_{LDT} = O(n \cdot d) \\ r_{LDT} = O(n \cdot \log|\mathbb{F}|) \end{cases}$

This is ok because a total low-degree test can be augmented to test individual degree.

(That said, we COULD use a total degree test, incurring a minor degradation in parameters.)

REMARK: we evaluate polynomials on $\mathbb{F}^n$ because the low-degree test expects this.

(Relaxing to D^n for certain $D \subseteq \mathbb{F}$ is sometimes possible but it's not easy.)

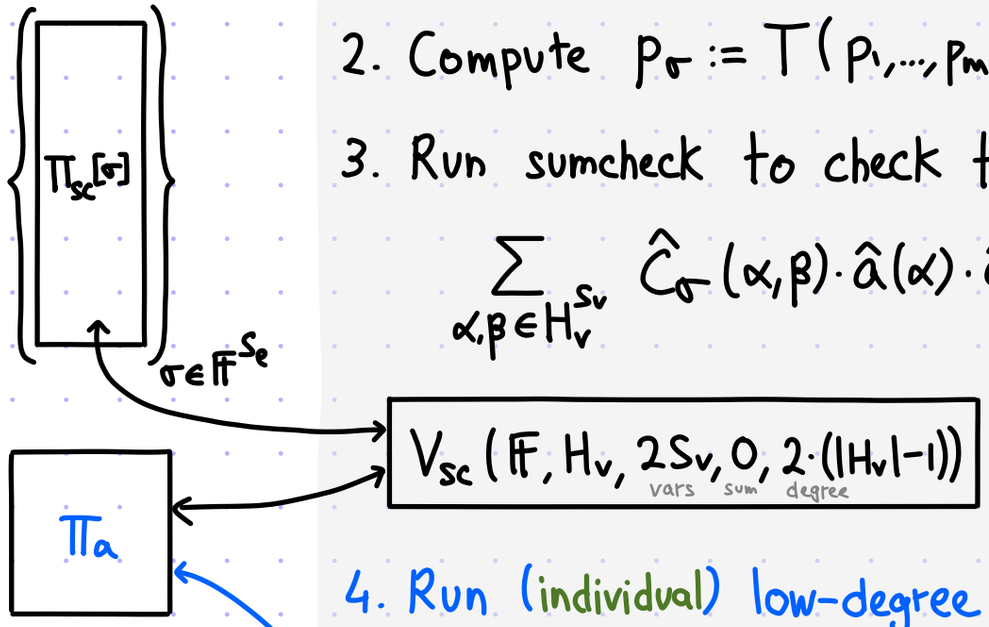
PCP for Quadratic Equations

> **Remark:**
> If instead we ran a total LDT with $d = S_v \cdot (|H_v|-1)$, the sumcheck error would increase from $O\left(\frac{S_v \cdot |H_v|}{|\mathbb{F}|}\right)$ to $O\left(\frac{S_v^2 \cdot |H_v|}{|\mathbb{F}|}\right)$.

Add an individual low-degree test:

$P((p_1,\ldots,p_m),a)$

1. For every $\sigma \in \mathbb{F}^{S_c}$:
   - $p_\sigma := T(p_1,\ldots,p_m;\sigma)$
   - $\Pi_{sc}[\sigma]$:= eval table for sumcheck claim "$p_\sigma(a)=0$"
   - output $\Pi_{sc}[\sigma]$
2. Output $\hat{a}:\mathbb{F}^{S_v}\to\mathbb{F}$ as π_a. (The LDE of $a:[n]\to\mathbb{F}$.)



$V((p_1,\ldots,p_m))$

1. Sample $\sigma \in \mathbb{F}^{S_c}$.
2. Compute $p_\sigma := T(p_1,\ldots,p_m;\sigma)$.
3. Run sumcheck to check that $p_\sigma(a)=0$:

$$\sum_{\alpha,\beta \in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\cdot\hat{a}(\alpha)\cdot\hat{a}(\beta) = 0$$

4. Run (individual) low-degree test on π_a:

If π_a is δ-far from $LD[\mathbb{F}, S_v, \text{ind} \le |H_v|-1]$ then $\Pr[V_{LDT}^{\pi_a}=1] \le \varepsilon_{LDT}(\delta)$.

If π_a is δ-close to $\hat{a} \in LD[\mathbb{F}, S_v, \text{ind} \le |H_v|-1]$ then, except w.p. $\le 2\delta$, both queries to π_a see $\hat{a}$.

Here there is no need for self-correction because both queries are random.

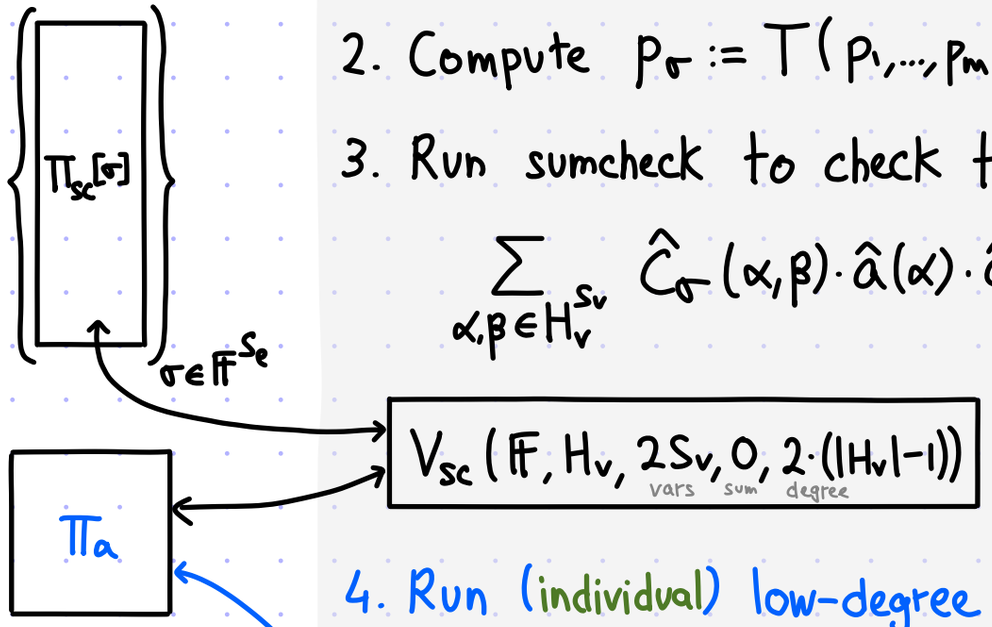
The soundness error is $\max\left\{\varepsilon_{LDT}(\delta), O\left(\left(\frac{\log^2 m}{\log\log m}+\frac{\log^2 n}{\log\log n}\right)\cdot\frac{1}{|\mathbb{F}|}\right)+2\delta\right\}$.

PCP for Quadratic Equations [2/2]

Add an individual low-degree test:

$P((p_1,\dots,p_m),a)$

1. For every $\sigma \in \mathbb{F}^{S_c}$:
   - $p_\sigma := T(p_1,\dots,p_m;\sigma)$
   - $\Pi_{sc}[\sigma]$:= eval table for sumcheck claim "$p_\sigma(a)=0$"
   - output $\Pi_{sc}[\sigma]$
2. Output $\hat{a}:\mathbb{F}^{S_v}\to\mathbb{F}$ as π_a. (The LDE of $a:[n]\to\mathbb{F}$.)



$V((p_1,\dots,p_m))$

1. Sample $\sigma \in \mathbb{F}^{S_c}$.
2. Compute $p_\sigma := T(p_1,\dots,p_m;\sigma)$.
3. Run sumcheck to check that $p_\sigma(a)=0$:

$$\sum_{\alpha,\beta\in H_v^{S_v}} \hat{C}_\sigma(\alpha,\beta)\cdot\hat{a}(\alpha)\cdot\hat{a}(\beta) = 0$$

4. Run (individual) low-degree test on π_a:

Theorem:

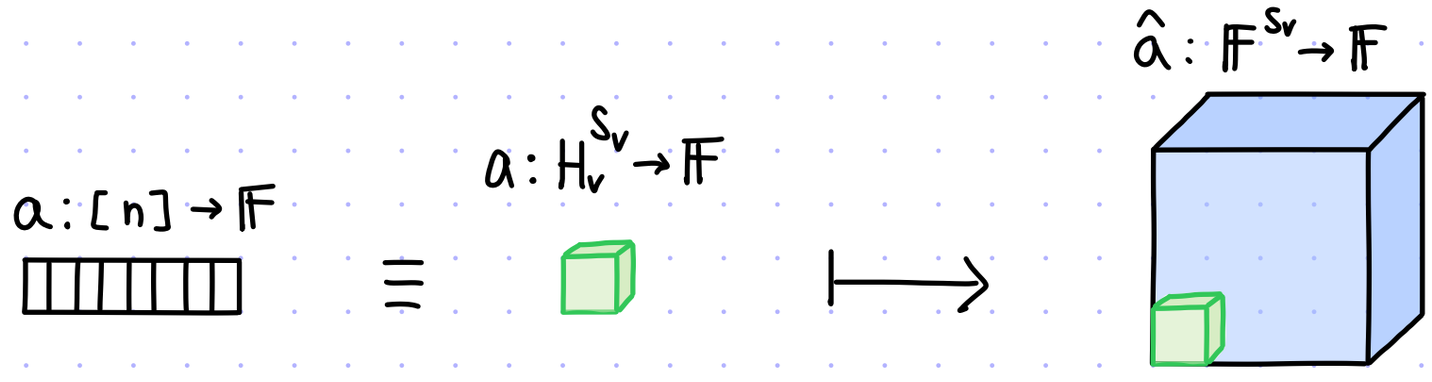
$$\mathrm{QESAT}(\mathbb{F}) \subseteq \mathrm{PCP}\left[\begin{array}{l} \varepsilon_c = 0 \\ \varepsilon_s = \max\left\{\varepsilon_{LDT}(\delta), O\left(\left(\frac{\log^2 m}{\log\log m}+\frac{\log^2 n}{\log\log n}\right)\cdot\frac{1}{|\mathbb{F}|}\right)+2\delta\right\} \end{array}\quad \begin{array}{l} \Sigma = \mathbb{F} \\ \ell = |\mathbb{F}|^{O\left(\frac{\log n}{\log\log n}\right)} \end{array}\quad \begin{array}{l} q = O\left(\frac{\log^2 n}{\log\log n}\right)+q_{LDT} \\ r = O\left(\frac{\log n}{\log\log n}\cdot\log|\mathbb{F}|\right)+r_{LDT} \end{array}\right]$$

For the LDT we use: $q_{LDT} = \mathrm{poly}(S_v, |H_v|) = \mathrm{poly}(\log n)$ and $r_{LDT} = O(S_v\cdot\log|\mathbb{F}|) = O\left(\frac{\log n}{\log\log n}\cdot\log|\mathbb{F}|\right)$.

Digest: Low-Degree Polynomials in PCP

We constructed a PCP for the NP-complete problem QESAT with $\ell = \text{poly}(n)$ & $q = \text{poly}(\log n)$.

The PCP string includes a Reed-Muller encoding of a satisfying assignment:



We used the structure of low-degree (multivariate) polynomials to:

- reduce m equations to 1 equation using a "pseudorandom" linear combination
- check an equation via the sumcheck protocol
- locally test the encoding via a low-degree test

Bibliography

Polynomial size PCPs

- [BFL 1991]: Non-deterministic exponential time has two-prover interactive protocols, by László Babai, Lance Fortnow, Carsten Lund.
- [BFLS 1991]: Checking computations in polylogarithmic time, by László Babai, Lance Fortnow, Leonid Levin, Mario Szegedy.
- [AS 1992]: Probabilistic checking of proofs; a new characterization of NP, by Sanjeev Arora, Madhu Sudan.
- [GS 2002]: Locally testable codes and PCPs of almost-linear length, by Oded Goldreich, Madhu Sudan.
- [RS 1997]: A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP, by Ran Raz, Shmuel Safra.
- [GR 2015]: Non-interactive proofs of proximity, by Tom Gur, Ron D. Rothblum.

See Section A.8 for a LDT for individual degree from an LDT for total degree.