Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 20

Robust PCPs

Robust PCPs

We construct robust PCPs for NP.

They are used as "outer PCP" in the proof of the PCP Theorem via proof composition.

We consider non-adaptive verifiers: $V^{\pi}(x;\rho) = \underbrace{D}_{\text{decision algorithm}}(\underbrace{S}_{\text{state algorithm}}(x,\rho), \pi[\underbrace{Q}_{\text{query algorithm}}(x,\rho)])$.

Define $R(V) := \{(s,a) \mid s \in S(x,\rho) \wedge a \in \Sigma^{Q(x,\rho)} \wedge D(s,a)=1\}$ and $R(V)[s] := \{a \mid (s,a) \in R(V)\}$.

<u>def:</u> (P,V) is a PCP system for a relation R with robustness parameter σ if:

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

② <u>robust soundness:</u> $\forall x \notin L(R) \quad \forall \tilde{\pi} \quad \Pr_{\rho}\left[\Delta(\tilde{\pi}[Q(x,\rho)], R(V)[S(x,\rho)]) \leq \sigma\right] \leq \varepsilon_s$.

Robustness $\sigma \in [0, 1/q)$ (wrt Hamming distance over Σ) is trivial.

The challenge is to achieve $\sigma = \Omega(1)$ even if q is super-constant.

We achieve a robust analogue of the poly-length polylog-query PCP:

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

Proof Plan

We prove the theorem in two steps, starting from the "canonical" PCP for NP.

$NP \subseteq PCP[\varepsilon_c = 0,\ \varepsilon_s = \frac{1}{2},\ \Sigma = \{0,1\},\ \ell = poly(n),\ q = poly(\log n),\ r = O(\log n)] \leftarrow$ PCP for QESAT that uses the sumcheck protocol and the low-degree test

Step 1: query bundling reduce query complexity to constant at the expense of alphabet size

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

Step 2: robustification achieve constant robustness (over $\{0,1\}$) at the expense of query complexity

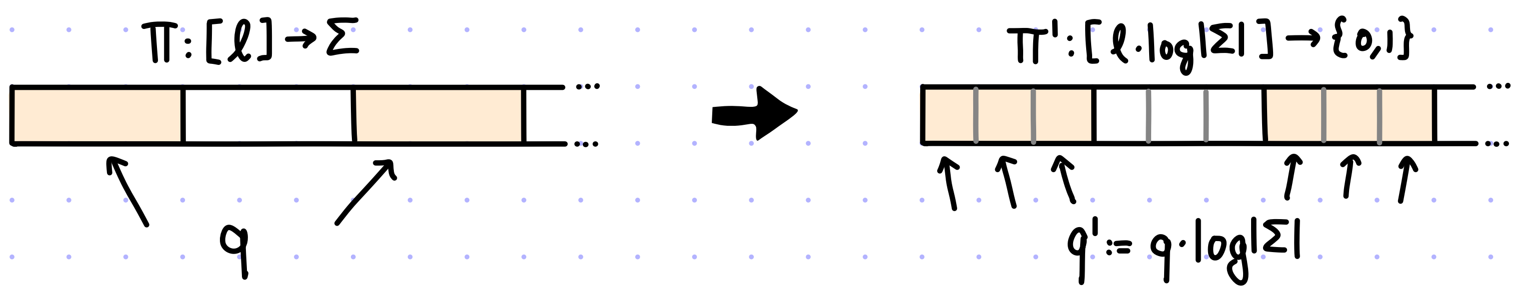
<u>theorem:</u> $NP \subseteq PCP[\varepsilon_c = 0,\ \varepsilon_s = \frac{1}{2},\ \Sigma = \{0,1\},\ \ell = poly(n),\ q = poly(\log n),\ r = O(\log n),\ \sigma = \Omega(1)]$

We study each step.

Robustification

GOAL: achieve good robustness over the binary alphabet, starting from a large-alphabet PCP.

IDEA: break each large-symbol query into multiple bit queries



This preserves completeness and soundness, and reduces the alphabet to binary.

PROBLEM: the resulting PCP may have trivial robustness $\sigma \in \left[0, \frac{1}{q\cdot\log|\Sigma|}\right)$.

Many local views in the large-alphabet PCP may be 1 symbol (out of q) away from accepting.

In the binary-alphabet PCP, each such view may be 1 bit (out of $q\cdot\log|\Sigma|$) away from accepting.

The simple idea can be fixed to achieve this lemma:

lemma: $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r]$

no dependence on Σ

$\subseteq \mathrm{PCP}\left[\varepsilon_c, \varepsilon_s, \Sigma' = \{0,1\}, \ell' = O(\ell\cdot\log|\Sigma|), q' = O(q\cdot\log|\Sigma|), r' = r, \sigma = \Omega\left(\tfrac{1}{q}\right)\right]$

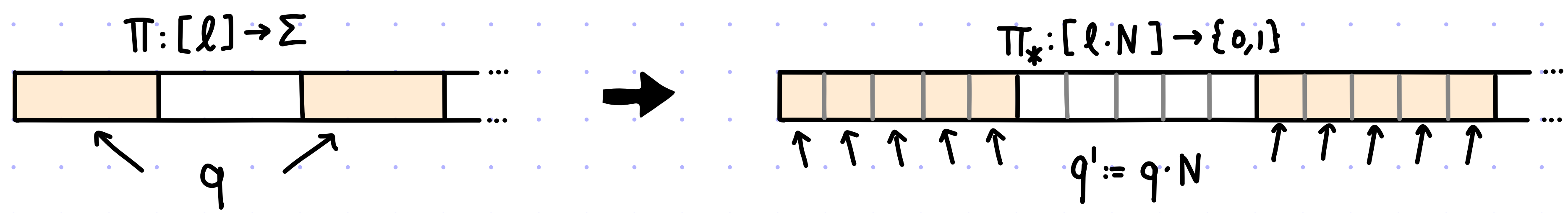
Robustification

IDEA: "sparsify" accepting local views by encoding each proof symbol via an error-correcting code

Let $\mathrm{Enc}: \Sigma \to \{0,1\}^N$ be an injective map with relative distance δ ($\forall$ distinct $a,b \in \Sigma$ $\Delta(\mathrm{Enc}(a), \mathrm{Enc}(b)) \geq \delta$).

lemma: $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r] \subseteq \mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma' = \{0,1\}, \ell' = \ell \cdot N, q' = q \cdot N, r' = r, \sigma = \frac{\delta}{4q}]$

The prior lemma follows from the fact that $\exists$ Enc with $N = O(\log|\Sigma|)$ and $\delta = \Omega(1)$.
standard code construction via code concatenation



$P_*(x,w)$

1. $\Pi := P(x,w) \in \Sigma^\ell$
2. $\forall i \in [\ell]$: $c_i := \mathrm{Enc}(\Pi[i]) \in \{0,1\}^N$
3. Output $\Pi_* := (c_i)_{i \in [\ell]} \in \{0,1\}^{N \cdot \ell}$

$V_*^{\Pi_*}(x)$

Run $V(x)$ by answering each query $i \in [\ell]$:

- make N queries to read $c_i \in \{0,1\}^N$
- return $a_i := \mathrm{Enc}^{-1}(c_i) \in \Sigma$ (reject if $a_i = \perp$)

Completeness: If $(x,w) \in R$ then $\Pr[V^\Pi(x) = 1 \mid \Pi \leftarrow P(x,w)] \geq 1 - \varepsilon_c$. Since $P_*(x,w)$ outputs $\Pi_* = (\mathrm{Enc}(\Pi[i]))_{i \in [\ell]}$, $V_*(x)$ answers each query $i \in [\ell]$ of $V(x)$ with $\mathrm{Enc}^{-1}(\mathrm{Enc}(\Pi[i])) = \Pi[i]$.

Robustification

Robust soundness: Fix $x \notin L(R)$ and $\tilde{\Pi}_* = (\tilde{c}_i)_{i \in [\ell]} \in \{0,1\}^{N \cdot \ell}$.

Define the event E = "local view $\tilde{\Pi}_*[Q_*(x,\rho)]$ contains $\tilde{c}_i$ that is at (relative) distance $\geq \delta/2$ from the code".

Then $\Pr_\rho\left[\Delta(\tilde{\Pi}_*[Q_*(x,\rho)], R(V_*)[S_*(x,\rho)]) \underset{⊛}{<} \frac{\delta}{2 \cdot q}\right]$ (any robustness parameter $\sigma < \frac{\delta}{2q}$, e.g. $\sigma = \frac{\delta}{4q}$)

$$\leq \Pr_\rho\left[\Delta(\tilde{\Pi}_*[Q_*(x,\rho)], R(V_*)[S_*(x,\rho)]) < \frac{\delta}{2 \cdot q} \,\middle|\, E\right] + \Pr_\rho\left[\Delta(\tilde{\Pi}_*[Q_*(x,\rho)], R(V_*)[S_*(x,\rho)]) < \frac{\delta}{2 \cdot q} \,\middle|\, \bar{E}\right]$$

$$\leq \underset{(a)}{0} + \underset{(b)}{\varepsilon_s}.$$

(a) Suppose that $\tilde{\Pi}_*[Q_*(x,\rho)]$ contains $\tilde{c}_i$ that is at (relative) distance $\geq \delta/2$ from the code. Then $\tilde{\Pi}_*[Q_*(x,\rho)]$ is at (relative) distance $\geq \delta/2q$ from any accepting local view, because every accepting local view consists of q strings in the code.

(b) Define the "correction" $\bar{\Pi}_* := (\bar{c}_i)_{i \in [\ell]}$ where $\bar{c}_i$ is closest codeword to c_i (break ties arbitrarily).
Define its decoding $\Pi := (\mathrm{Enc}^{-1}(\bar{c}_i))_{i \in [\ell]} \in \Sigma^\ell$.
By the soundness of V, $\Pr[V_*^{\bar{\Pi}_*}(x)] = \Pr[V^{\Pi}(x) = 1] \leq \varepsilon_s$.
If every string in $\tilde{\Pi}_*[Q_*(x,\rho)]$ is at (relative) distance $< \delta/2$ to the code then $\bar{\Pi}_*[Q_*(x,\rho)]$ is the ONLY string of q codewords that is at (relative) distance $< \delta/2q$ to $\tilde{\Pi}_*[Q_*(x,\rho)]$.
So $\Pr_\rho\left[\Delta(\tilde{\Pi}_*[Q_*(x,\rho)], R(V_*)[S_*(x,\rho)]) < \frac{\delta}{2 \cdot q} \,\middle|\, \bar{E}\right] \leq \Pr_\rho\left[\bar{\Pi}_*[Q_*(x,\rho)] \in R(V_*)[S_*(x,\rho)]\right] = \Pr[V_*^{\bar{\Pi}_*}(x) = 1]$. ■

⊛ The bound $\frac{\delta}{2q}$ can be improved to $\lceil qN \frac{\delta}{2q} \rceil / qN = \frac{\lceil N\delta/2 \rceil}{qN}$ ($\frac{\delta}{2q}$ rounded up to the next multiple of $\frac{1}{qN}$) via the same analysis.

Bundling Queries

GOAL: reduce query complexity to constant at the expense of alphabet size

IDEA: provide the answer to each query set (as a large symbol) + consistency test

$P_*(x,w)$

1. $\pi := P(x,w) \in \Sigma^\ell$.
2. For every $\rho \in \{0,1\}^r$:

   $a_\rho := \pi[Q(x,\rho)] \in \Sigma^q$.
3. Output $\pi_* := (\pi, (a_\rho)_{\rho \in \{0,1\}^r})$.

$V_*^{\pi_*}(x)$

1. Sample $\rho \in \{0,1\}^r$ and $i \in [q]$.
2. Read $a_\rho \in \Sigma^q$ and $\pi[Q(x,\rho)[i]]$.
3. Check that $a_\rho[i] = \pi[Q(x,\rho)[i]]$.
4. Check that $V(x;\rho)=1$ when answering j-th query with $a_\rho[j]$.

$$\pi_* := \Big(\underbrace{\square\square\blacksquare\square\square\square\square\square}_{\pi:[\ell]\to\Sigma}, \big(\underbrace{\square\square\square}_{a_\rho:[q]\to\Sigma} \big)_{\rho \in \{0,1\}^r} \Big)$$

lemma: $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r] \subseteq \mathrm{PCP}[\varepsilon_c, \varepsilon_s' = 1 - \frac{1-\varepsilon_s}{q}, \Sigma' = \Sigma^q, \ell' = \ell + 2^r, q' = 2, r' = r + \log q]$

Does NOT suffice for us: we need constant soundness error even when q is super-constant.

Nevertheless, we prove soundness because the analysis is a useful warm-up.

Bundling Queries

<u>lemma:</u> $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r] \subseteq \mathrm{PCP}[\varepsilon_c, \varepsilon_s' = 1 - \frac{1-\varepsilon_s}{q}, \Sigma' = \Sigma^q, \ell' = \ell + 2^r, q' = 2, r' = r + \log q]$

<u>Proof of soundness.</u>

Fix $x \notin L(R)$ and $\pi_* = (\pi, (a_\rho)_{\rho \in \{0,1\}^r})$.

$$\Pr[V_*^{\pi_*}(x)=1] = \Pr[V_*^{\pi_*}(x)=1 \mid V^\pi(x)=1] \cdot \Pr[V^\pi(x)=1] + \Pr[V_*^{\pi_*}(x)=1 \mid V^\pi(x)=0] \cdot \Pr[V^\pi(x)=0]$$

$$\leq 1 \cdot \Pr[V^\pi(x)=1] + \Pr[V_*^{\pi_*}(x)=1 \mid V^\pi(x)=0] \cdot (1 - \Pr[V^\pi(x)=1])$$

$$\leq 1 \cdot \Pr[V^\pi(x)=1] + (1-\tfrac{1}{q}) \cdot (1 - \Pr[V^\pi(x)=1])$$

$$= \tfrac{1}{q} \cdot \Pr[V^\pi(x)=1] + 1 - \tfrac{1}{q} \leq \tfrac{1}{q} \cdot \varepsilon_s + 1 - \tfrac{1}{q} = 1 - \frac{1-\varepsilon_s}{q}.$$

We are left to show the inequality highlighted in green:

$$\Pr[V_*^{\pi_*}(x)=1 \mid V^\pi(x)=0] \leq \Pr_{\rho,\gamma}\left[V_*^{\pi_*}(x;(\rho,\gamma))=1 \;\middle|\; \begin{array}{l} a_\rho \neq \pi[Q(x,\rho)] \\ \vee \; V^{[Q(x,\rho),a_\rho]}(x;\rho)=0 \end{array} \right]$$

$$\leq \Pr_{\rho,\gamma}\left[V_*^{\pi_*}(x;(\rho,\gamma))=1 \mid a_\rho \neq \pi[Q(x,\rho)] \right]$$

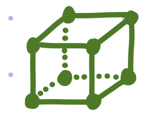
$$\leq \Pr_{\rho,\gamma}\left[a_\rho[\gamma] = \pi[Q(x,\rho)[\gamma]] \mid a_\rho \neq \pi[Q(x,\rho)] \right]$$

$$\leq 1 - \tfrac{1}{q}. \quad \blacksquare$$

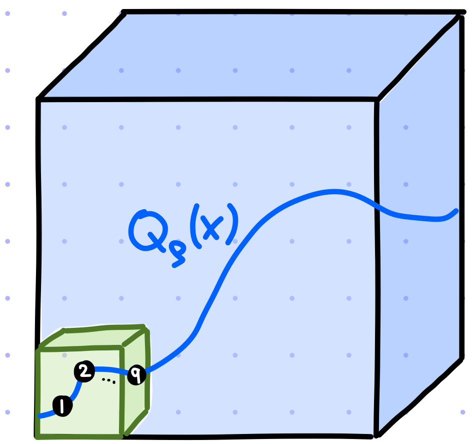
Bundling Queries

Fix a field $\mathbb{F}$, subset $H \subseteq \mathbb{F}$, and number of variables $m \in \mathbb{N}$. Assume that $|\mathbb{F}| \geq \max\{|\Sigma|, q\}$.

for convenience

Identify $[\ell]$ with H^m by setting $m := \frac{\log \ell}{\log |H|}$. $\cdots\cdots \leftrightarrow$ 

View a query set $Q(x,\rho) \subseteq [\ell]$ as q elements in H^m.



Changes from prior approach:

- replace $\pi : [\ell] \to \Sigma$ with its $(\mathbb{F}, H, m)$-extension $\hat{\pi} : \mathbb{F}^m \to \mathbb{F}$
- replace $a_\rho : [q] \to \Sigma$ with $\hat{a}_\rho(z) := \hat{\pi}(Q_\rho(z)) \in \mathbb{F}^{<q \cdot m \cdot |H|}[z]$ where $Q_\rho : \mathbb{F} \to \mathbb{F}^m$ is m polynomials of degree $<q$ s.t. $\forall j \in [q]$ $Q_\rho(j) := Q(x,\rho)[j] \in H^m$.

(We use $1,2,\dots,q$ to denote any q distinct elements in $\mathbb{F}$.)

WARM UP: $\pi_* := \Big(\overbrace{\square\square\square\square\square\square\square\square\square\square}^{\hat{\pi} : \mathbb{F}^m \to \mathbb{F}}, \big(\overbrace{\square\square\square\square}^{\hat{a}_\rho(z)} \big)_{\rho \in \{0,1\}^r} \Big)$

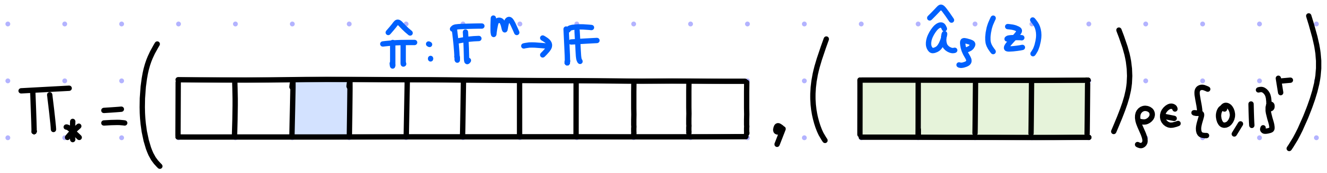
$P_*(x,w)$

1. $\pi := P(x,w) \in \Sigma^\ell \subseteq \mathbb{F}^{H^m}$.
2. $\hat{\pi} : \mathbb{F}^m \to \mathbb{F}$ is $(\mathbb{F},H,m)$-extension of π.
3. $\forall \rho \in \{0,1\}^r$: $\hat{a}_\rho(z) := \hat{\pi}(Q_\rho(z))$.
4. Output $\pi_* := (\hat{\pi}, (\hat{a}_\rho)_{\rho \in \{0,1\}^r})$.

$V_*^{\pi_*}(x)$

1. Sample $\rho \in \{0,1\}^r$ and $\gamma \in \mathbb{F}$.
2. Read $\hat{a}_\rho \in \mathbb{F}[z]$ and $\hat{\pi}(Q_\rho(\gamma))$.
3. Check that $\hat{a}_\rho(\gamma) = \hat{\pi}(Q_\rho(\gamma))$.
4. Check that $V(x;\rho) = 1$ when answering j-th query with $\hat{a}_\rho(j)$.

Bundling Queries



$V_*^{\Pi_*}(x)$

1. Sample $\rho \in \{0,1\}^r$ and $\gamma \in \mathbb{F}$.
2. Read $\hat{a}_\rho \in \mathbb{F}[z]$ and $\hat{\pi}(Q_\rho(\gamma))$.
3. Check that $\hat{a}_\rho(\gamma) = \hat{\pi}(Q_\rho(\gamma))$.
4. Check that $V(x;\rho) = 1$ when answering j-th query with $\hat{a}_\rho(j)$.

For this warm-up case, we assume that $\hat{\pi}$ is an $(\mathbb{F}, H, m)$-extension of (some) $\pi : [\ell] \to \Sigma$.

claim: the soundness error is $\leq 1 - (1-\varepsilon_s)\cdot\left(1 - \frac{q \cdot m \cdot |H|}{|\mathbb{F}|}\right)$. [this improves on $1 - (1-\varepsilon_s)\cdot\frac{1}{q}$]

proof: Suppose that $x \notin L(R)$ and fix a PCP $\Pi_* := (\hat{\pi}, (\hat{a}_\rho)_{\rho \in \{0,1\}^r})$.

It suffices to show that $\Pr[V_*^{\Pi_*}(x) = 1 \mid V^{\pi}(x) = 0] \leq \frac{q \cdot m \cdot |H|}{|\mathbb{F}|}$ (by a similar analysis as the prior construction).

$$
\begin{aligned}
\Pr[V_*^{\Pi_*}(x)=1 \mid V^{\pi}(x)=0] &\leq \Pr_{\rho,\gamma}\left[V_*^{\Pi_*}(x;(\rho,\gamma)) = 1 \;\middle|\; \begin{array}{l} \hat{a}_\rho \neq \hat{\pi}[Q_\rho] \\ \vee\; V^{[Q_\rho([q]), \hat{a}_\rho([q])]}(x;\rho) = 0 \end{array} \right] \\
&\leq \Pr_{\rho,\gamma}\left[V_*^{\Pi_*}(x;(\rho,\gamma)) = 1 \;\middle|\; \hat{a}_\rho \neq \hat{\pi}[Q_\rho] \right] \\
&\leq \Pr_{\rho,\gamma}\left[\hat{a}_\rho[\gamma] = \hat{\pi}[Q_\rho(\gamma)] \;\middle|\; \hat{a}_\rho \neq \hat{\pi}[Q_\rho] \right] \\
&\leq \frac{q \cdot m \cdot |H|}{|\mathbb{F}|}.
\end{aligned}
$$

∎

Bundling Queries

Q: how to handle the noisy case?

That is $\pi_* = (f, (\hat{a}_\varsigma)_{\varsigma \in \{0,1\}^r})$ where $f: \mathbb{F}^m \to \mathbb{F}$ is arbitrary. We no longer require that f is the $(\mathbb{F}, H, m)$-extension $\hat{\pi}$ of some $\pi: [\ell] \to \Sigma$.

PROBLEM 1: The Rubinfeld–Sudan LDT that we studied makes $\omega(1)$ queries to f.

In fact, every LDT makes $d+2 = \omega(1)$ queries to f.

Fix 1: We use a large-alphabet constant-query PCPP for low-degreeness.

The LINE VS. POINT TEST is such a PCPP.

$$P_{LPT}(f) := \left(\hat{g}_{a,b} := f(ax+b) \in \mathbb{F}^{\leq d}[x]\right)_{a,b \in \mathbb{F}^m}$$

$V_{LPT}^{f, (\hat{g}_{a,b})_{a,b \in \mathbb{F}^m}}$

1. Sample $a, b \in \mathbb{F}^m$ and $\mu \in \mathbb{F}$.
2. Check that $f(a\mu + b) = \hat{g}_{a,b}(\mu)$.

Completeness: $\forall f: \mathbb{F}^m \to \mathbb{F}$ of total degree $\leq d$ for, $\pi_{px} := P_{LPT}(f)$, $\Pr[V_{LPT}^{f, \pi_{px}} = 1] = 1$.

Soundness: $\forall f: \mathbb{F}^m \to \mathbb{F}$ $\forall \tilde{\pi}_{px} = (\hat{g}_{a,b} \in \mathbb{F}^{\leq d}[x])$, f is δ-far from total degree d $\to$ $\Pr[V_{LPT}^{f, \tilde{\pi}_{px}} = 1] \leq \varepsilon_{LPT}(\delta)$.

Fact [that we do not prove]: $\exists\, \delta_0, \varepsilon_0 \in (0,1)$ s.t. $\delta \geq \delta_0 \to \varepsilon_{LPT}(\delta) \leq \varepsilon_0$.

Bundling Queries

Q: how to handle the noisy case?

That is $\pi_* = (f, (\hat{a}_\varsigma)_{\varsigma \in \{0,1\}^r})$ where $f : \mathbb{F}^m \to \mathbb{F}$ is arbitrary.

We no longer require that f is the $(\mathbb{F}, H, m)$-extension $\hat{\pi}$ of some $\pi : [\ell] \to \Sigma$.

PROBLEM 2: The query $Q_\varsigma(\gamma)$ to f is NOT uniformly random in $\mathbb{F}^m$.

Indeed,
$$Q_\varsigma(\gamma) := \sum_{j \in [q]} Q(x, \varsigma)[j] \cdot L_{[q],j}(\gamma)$$
where $\{L_{[q],j}(X)\}_{j \in [q]}$ are the Lagrange polynomials for $[q]$.

The degree of each $L_{[q],j}(X)$ is $q-1$, and $L_{[q],j}(\gamma)$ is (typically) NOT uniformly random for random $\gamma \leftarrow \mathbb{F}$.

E.g. the distribution $\{\gamma^2 \mid \gamma \leftarrow \mathbb{F}\}$ is supported only on squares of $\mathbb{F}$. (Approx half the elements if $\mathrm{char}(\mathbb{F}) \neq 2$.)

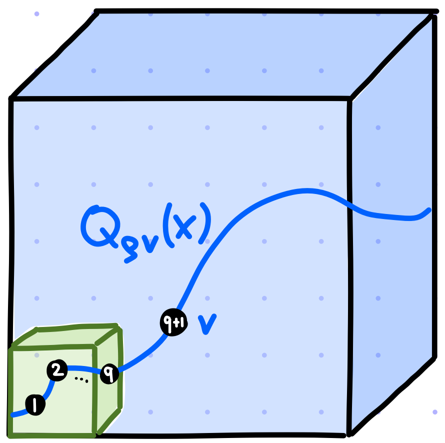
Fix 2: We randomize the query to f.

For every $v \in \mathbb{F}^m$,

$Q_{\varsigma v} : \mathbb{F} \to \mathbb{F}^m$ is m polynomials of degree $\leq q$ s.t.
$$\begin{cases} \forall j \in [q] \; Q_{\varsigma v}(j) := Q(x, \varsigma)[j] \in H^m \\ Q_{\varsigma v}(q+1) := v \end{cases}.$$

Note that, for random $v \in \mathbb{F}^m$, $\forall \gamma \in \mathbb{F} \setminus [q]$ $Q_{\varsigma v}(\gamma)$ is random in $\mathbb{F}^m$.

Indeed,
$$Q_\varsigma(\gamma) := \sum_{j \in [q]} Q(x, \varsigma)[j] \cdot L_{[q+1],j}(\gamma) + v \cdot L_{[q+1],q+1}(\gamma)$$
and $L_{[q+1],q+1}(\gamma) \neq 0$ for $\gamma \in \mathbb{F} \setminus [q]$.



Bundling Queries

The final construction.

lines oracle of degree $d < m \cdot |H|$

$$\Pi_* = \left(\overset{f:\mathbb{F}^m \to \mathbb{F}}{\boxed{}},\ \left(\overset{\hat{a}_{gv}(z)}{\boxed{}} \right)_{\substack{g \in \{0,1\}^r \\ v \in \mathbb{F}^m}},\ \left(\overset{\hat{g}_{a,b}}{\boxed{}} \right)_{a,b \in \mathbb{F}^m} \right)$$

$P_*(x,w)$

1. $\pi := P(x,w) \in \Sigma^\ell \subseteq \mathbb{F}^{H^m}$.
2. $\hat{\pi} : \mathbb{F}^m \to \mathbb{F}$ is $(\mathbb{F},H,m)$-extension of π.
3. $\forall\, g \in \{0,1\}^r,\ v \in \mathbb{F}^m$: $\hat{a}_{gv}(z) := \hat{\pi}(Q_{gv}(z))$.
4. $\forall\, a,b \in \mathbb{F}^m$: $\hat{g}_{a,b}(z) := \hat{\pi}(az+b)$.
5. Output $\pi_* := \left(\hat{\pi},\ (\hat{a}_{gv})_{\substack{g \in \{0,1\}^r \\ v \in \mathbb{F}^m}},\ (\hat{g}_{a,b})_{a,b \in \mathbb{F}^m}\right)$.

$V_*^{\pi_*}(x)$

1. Sample $g \in \{0,1\}^r$, $\gamma \in \mathbb{F} \setminus [q]$, $v \in \mathbb{F}^m$.
2. Read $\hat{a}_{gv} \in \mathbb{F}[z]$ and $f(Q_{gv}(\gamma))$.
3. Check that $\hat{a}_{gv}(\gamma) = f(Q_{gv}(\gamma))$.
4. Check that $V(x;g) = 1$ when answering j-th query with $\hat{a}_{gv}(j)$.
5. Sample $a,b \in \mathbb{F}^m$ and $\mu \in \mathbb{F}$, and check that $f(a\mu+b) = \hat{g}_{a,b}(\mu)$.

<u>lemma:</u> $\mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r] \subseteq \mathrm{PCP}\begin{bmatrix} \varepsilon_c & \varepsilon_s' = \max\left\{ \varepsilon_{LPT}(\delta),\ 1-(1-\varepsilon_s)\cdot\left(1 - \frac{qm|H|}{|\mathbb{F}|-q} - \delta\right) \right\} \\ \Sigma' = \Sigma^{qm|H|} & \ell' = |\mathbb{F}|^m + 2^r |\mathbb{F}|^m + |\mathbb{F}|^{2m} \\ q' = 4 & r' = r + O(m \cdot \log |\mathbb{F}|) \end{bmatrix}$

We can then set $|H| = \log \ell$, $m = \frac{\log \ell}{\log |H|} = \frac{\log \ell}{\log\log \ell}$, $|\mathbb{F}| = O(qm|H|)$.

Bibliography

Robust PCPs

- [DR 2006]: Assignment testers: towards a combinatorial proof of the PCP theorem, by Irit Dinur, Omer Reingold.
- [ALMSS 1998]: Proof verification and the hardness of approximation problems, by Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, Mario Szegedy.

Section 7.2 on O(1) query tests