

Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 21

PCPs of Proximity

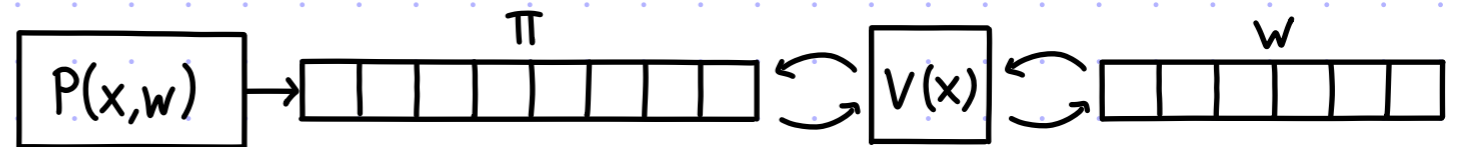


These slides are licensed under the [CC BY-SA 4.0 license](https://creativecommons.org/licenses/by-sa/4.0/).

PCPs of Proximity

In a **PCP of proximity (PCPP)** for a relation R the verifier receives:

- an instance x
- query access to a candidate witness w
- query access to a PCP string π

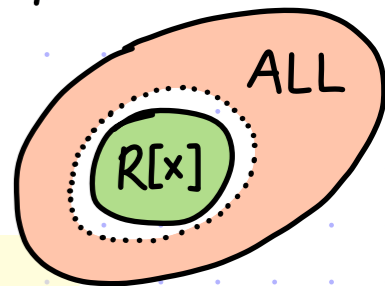


GOAL: convince the verifier that w is **close** to some valid witness in $R[x] := \{w \mid (x,w) \in R\}$.
 if $x \notin L(R)$ then $R[x] = \emptyset$

def: (P,V) is a **PCPP** system for a relation R with **proximity parameter δ** if :

① completeness: $\forall (x,w) \in R \Pr[V^{w,\pi}(x) = 1 \mid \pi \leftarrow P(x,w)] \geq 1 - \epsilon_c$.

② proximity soundness: $\forall (x,w)$ if $\Delta(w, R[x]) \geq \delta$ then $\forall \tilde{\pi} \Pr[V^{w,\tilde{\pi}}(x) = 1 \mid \tilde{\pi} \leftarrow \tilde{P}] \leq \epsilon_s$.



↑ convention $\Delta(w, \emptyset) := 1$

Equivalently:
 $\Delta(w, R[x]) \geq \delta \rightarrow \forall \tilde{\pi} \Pr[V^{w,\tilde{\pi}}(x) = 1] \leq \epsilon_s$

We construct PCPPs in two regimes.

theorem: $\forall \delta > 0 \text{ QESAT}(\mathbb{F}_2) \in \text{PCPP} [\epsilon_c = 0, \epsilon_s = 1/2, \Sigma = \{0,1\}, \ell = \exp(n), q = O(1/\delta), r = \text{poly}(n), \delta]$

theorem: $\forall \delta > 0 \text{ QESAT}(\mathbb{F}_2) \in \text{PCPP} [\epsilon_c = 0, \epsilon_s = 1/2, \Sigma = \{0,1\}, \ell = \text{poly}(n), q = \frac{\text{poly}(\log n)}{\delta}, r = O(\log n), \delta]$

Here $\text{QESAT}(\mathbb{F})$ is the RELATION $\{(p_1, \dots, p_m), a \mid p_1, \dots, p_m \in \mathbb{F}^{\leq 2}[x_1, \dots, x_n], a: [n] \rightarrow \mathbb{F}, p_i(a) = \dots = p_m(a) = 0\}$.

Easy: from PCPP to PCP

lemma: For every proximity parameter δ ,

$$R \in \text{PCPP}[\epsilon_c, \epsilon_s, \Sigma, \ell, q, r, \delta] \rightarrow R \in \text{PCP}[\epsilon_c, \epsilon_s, \Sigma, \ell' = |w| + \ell, q, r]$$

proof: Let (P_{px}, V_{px}) be the PCPP for R . We construct the PCP (P, V) for R as follows.

$P(x, w)$

1. Compute proximity proof: $\pi_{px} := P_{px}(x, w)$.
2. Output $\pi := (w, \pi_{px})$.

$$\pi = (\boxed{w} , \boxed{\pi_{px}})$$

$$V^\pi(x): \text{ Check that } V_{px}^{w, \pi_{px}}(x) = 1.$$

Completeness: $\forall (x, w) \in R \quad \Pr[V^\pi(x) = 1 \mid \pi \leftarrow P(x, w)] = \Pr[V_{px}^{w, \pi_{px}}(x) = 1 \mid \pi_{px} \leftarrow P_{px}(x, w)] \geq 1 - \epsilon_c.$

Soundness: $\forall x \notin L(R)$, all candidate witnesses are far from $R[x] = \emptyset$:

$$\forall w \quad \Delta(w, R[x]) = \Delta(w, \emptyset) = 1 \geq \delta \rightarrow \forall \tilde{\pi} = (w, \tilde{\pi}_{px}) \quad \Pr[V^{\tilde{\pi}}(x) = 1] = \Pr[V_{px}^{w, \tilde{\pi}_{px}}(x) = 1] \leq \epsilon_s. \quad \blacksquare$$

Thus PCPPs are "stronger" than PCPs (albeit PCPPs are about proximity rather than satisfiability).

The extra power is when $x \in L(R)$: the PCPP verifier rejects w.h.p. if the given w is far from $R[x]$.

→ We expect to work at least as hard to construct PCPPs as we did for PCPs.

Harder: from PCP to PCPP

[1/2]

RECYCLE: we modify certain PCPs into corresponding PCPPs (for the same relation).

Our recipe to construct PCPPs has been to set $\pi = (\pi_0, \pi_{\text{sat}})$ where

- ① π_0 is (allegedly) a valid encoding of some witness ($\exists w : \pi_0 = \text{Enc}(w)$),
- ② if π_0 is close to $\text{Enc}(w)$ for some w , π_{sat} facilitates checking that w is satisfying.

The soundness analyses for these PCPs in fact tell us something about the encoded assignment:

if $V_{\text{PCP}}^{(\tilde{\pi}_0, \tilde{\pi}_{\text{sat}})}(x) = 1$ with large enough probability then $\tilde{\pi}_0$ is close to $\text{Enc}(w)$ with $(x, w) \in R$.

This motivates the following special property:

def: A PCP $(P_{\text{PCP}}, V_{\text{PCP}})$ is $(\text{Enc}, \epsilon_s, \delta_s)$ -special if:

- $\forall (x, w) \in R$, $P_{\text{PCP}}(x, w)$ outputs a PCP string π of the form $(\text{Enc}(w), \pi_{\text{sat}})$,
- $\forall x \forall \tilde{\pi} = (\tilde{\pi}_0, \tilde{\pi}_{\text{sat}}) \Pr[V_{\text{PCP}}^{(\tilde{\pi}_0, \tilde{\pi}_{\text{sat}})}(x) = 1] > \epsilon_s \rightarrow \exists \tilde{w} \in R[x] : \Delta(\tilde{\pi}_0, \text{Enc}(\tilde{w})) \leq \delta_s$

Harder: from PCP to PCPP

[2/2]

def: A PCP $(P_{\text{PCP}}, V_{\text{PCP}})$ is $(\text{Enc}, \epsilon_s, \delta_s)$ -special if:

- $\forall (x, w) \in R$, $P_{\text{PCP}}(x, w)$ outputs a PCP string π of the form $(\text{Enc}(w), \pi_{\text{sat}})$,
- $\forall x \forall \tilde{\pi} = (\tilde{\pi}_0, \tilde{\pi}_{\text{sat}}) \Pr[V_{\text{PCP}}^{(\tilde{\pi}_0, \tilde{\pi}_{\text{sat}})}(x) = 1] > \epsilon_s \rightarrow \exists \tilde{w} \in R[x]: \Delta(\tilde{\pi}_0, \text{Enc}(\tilde{w})) \leq \delta_s$

Intuition for PCPP constructions:

$V_{\text{PCP}}^{(w, (\pi_0, \pi_{\text{sat}}))}(x)$

1. Check that $V_{\text{PCP}}^{(\pi_0, \pi_{\text{sat}})}(x) = 1$.
2. Test that "Enc⁻¹(π_0) = w".

Suppose that $\Delta(w, R[x]) \geq \delta$.

If $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_0, \tilde{\pi}_{\text{sat}})}(x) = 1] \leq \epsilon_s$ then we are done.

If $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_0, \tilde{\pi}_{\text{sat}})}(x) = 1] > \epsilon_s$ then $\exists \tilde{w} \in R[x] \Delta(\tilde{\pi}_0, \text{Enc}(\tilde{w})) \leq \delta_s$.

Hence, $\Delta(w, \tilde{w}) \geq \delta$ and $\Delta(\tilde{\pi}_0, \text{Enc}(\tilde{w})) \leq \delta_s$. Perhaps there is hope for a test for "Enc⁻¹(π_0) = w"?

IDEA: use LOCAL DECODING of Enc on $\tilde{\pi}_0$ ($\approx \text{Enc}(\tilde{w})$) to compare w and \tilde{w} .

PCPPs from Local Decoders

[1/2]

We construct a PCPP for R from two ingredients: $\begin{cases} \text{a PCP for } R \text{ that uses an encoding } \text{Enc} \\ \text{a local decoder for } \text{Enc} \end{cases}$

def: D is a **local decoder** for Enc with **decoding radius** δ_{LD} and **decoding error** ϵ_{LD} if

① $\forall a \forall i \in [n] \Pr[D^{\text{Enc}(a)}(i) = a_i] = 1$

② if f is δ_{LD} -close to $\text{Enc}(a)$ then $\forall i \in [n] \Pr[D^f(i) \neq a_i] \leq \epsilon_{LD}$

lemma: Suppose that $R \in \text{PCP}[\epsilon_c, (\text{Enc}, \epsilon_s, \delta_s), \Sigma, \ell, q, r]$.

If Enc has a local decoder with decoding radius $\delta_{LD} \geq \delta_s$ and error ϵ_{LD} then $\forall t \in \mathbb{N}$

$\forall \delta > 0 \quad R \in \text{PCPP}[\epsilon_c, \epsilon'_s = \max\{\epsilon_s, (1 - (1 - \epsilon_{LD}) \cdot \delta)^t\}, \Sigma, \ell, q' = q + t \cdot (q_{LD} + 1), r' = r + t \cdot (\log |W| + r_{LD}), \delta]$.

$\leq \epsilon$ for $t := O\left(\frac{\log 1/\epsilon}{(1 - \epsilon_{LD}) \cdot \delta}\right)$

Below is the construction of the PCPP.

$P(x, w)$

1. Compute $(\pi_o, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.
2. Output $\pi_{px} := (\pi_o, \pi_{\text{sat}})$.

$V^{w, (\pi_o, \pi_{\text{sat}})}(x)$

1. Check that $V_{\text{PCP}}^{(\pi_o, \pi_{\text{sat}})}(x) = 1$.
2. Sample $i_1, \dots, i_t \in [|w|]$.
3. Check that $\forall j \in [t] D^{\pi_o}(i_j) = w_{i_j}$.

* Compare with a local corrector C : ① $\forall a \forall i \Pr[C^{\text{Enc}(a)}(i) = \text{Enc}(a)_i] = 1$

② f is δ_{LC} -close to $\text{Enc}(a) \rightarrow \forall i \Pr[C^f(i) \neq \text{Enc}(a)_i] \leq \epsilon_{LC}$

PCPPs from Local Decoders

[2/2]

$P(x, w)$

1. Compute $(\pi_o, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.
2. Output $\pi_{\text{px}} := (\pi_o, \pi_{\text{sat}})$.

$V^{w, (\pi_o, \pi_{\text{sat}})}(x)$

1. Check that $V_{\text{PCP}}^{(\pi_o, \pi_{\text{sat}})}(x) = 1$.
2. Sample $i_1, \dots, i_t \in [|w|]$.
3. Check that $\forall j \in [t] D^{\pi_o}(i_j) = w_{i_j}$.

Completeness: Suppose that $(x, w) \in R$. Then $\Pr[V_{\text{PCP}}^{(\pi_o, \pi_{\text{sat}})}(x) = 1] \geq 1 - \epsilon_c$ for $(\pi_o, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.

Since $\pi_o = \text{Enc}(w)$, $\forall i \in [|w|] \Pr[D^{\pi_o}(i) = w_i] = 1$. Hence $\Pr[V^{w, (\pi_o, \pi_{\text{sat}})}(x) = 1] \geq 1 - \epsilon_c$.

Soundness: Suppose that w is δ -far from $R[x]$. Fix a proximity proof $\tilde{\pi}_{\text{px}} = (\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})$.

If $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})}(x) = 1] \leq \epsilon_s$ then we are done. So suppose that $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})}(x) = 1] > \epsilon_s$.

Since V_{PCP} is $(\text{Enc}, \epsilon_s, \delta_s)$ -special, $\tilde{\pi}_o$ is δ_s -close to $\text{Enc}(\tilde{w})$ for some $\tilde{w} \in R[x]$.

Since $\delta_s \leq \delta_{\text{LD}}$, $\forall i \in [|w|] \Pr[D^{\tilde{\pi}_o}(i) = \tilde{w}_i] \geq 1 - \epsilon_{\text{LD}}$.

Since w is δ -far from $R[x]$, w is δ -far from $\tilde{w} \in R[x]$, so $\Pr_i[w_i \neq \tilde{w}_i] \geq \delta$.

Hence $\Pr_i[D^{\tilde{\pi}_o}(i) \neq w_i] \geq \Pr_i[D^{\tilde{\pi}_o}(i) = \tilde{w}_i \wedge w_i \neq \tilde{w}_i] \geq (1 - \epsilon_{\text{LD}}) \cdot \delta$.

Therefore $\Pr_{i_1, \dots, i_t}[\forall j \in [t]: D^{\tilde{\pi}_o}(i_j) = w_{i_j}] \leq (1 - (1 - \epsilon_{\text{LD}}) \cdot \delta)^t$.

We conclude that $\Pr[V^{w, (\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})}(x) = 1] \leq \max\{\epsilon_s, (1 - (1 - \epsilon_{\text{LD}}) \cdot \delta)^t\}$.

Exponential-Size Constant-Query PCPP

We constructed a PCP for QESAT(\mathbb{F}) with proof length $\exp(n)$ and query complexity $O(1)$.

theorem: QESAT(\mathbb{F}) \in PCP [$\epsilon_c = 0$, $\epsilon_s = 1/2$, $\Sigma = \{0,1\}$, $l = \exp(n)$, $q = O(1)$, $r = \text{poly}(n)$]

The encoding underlying this PCP is **LINEAR EXTENSIONS**:

Enc: $\mathbb{F}^n \rightarrow \mathbb{F}^{\mathbb{F}^n}$ where $\text{Enc}(a) := \{ \langle \gamma, a \rangle \}_{\gamma \in \mathbb{F}^n}$.

The soundness analysis shows that, $\forall \delta_s < \frac{1}{2} \cdot (1 - \frac{1}{|\mathbb{F}|})$, the PCP is $(\epsilon_s = O(1), \delta_s, \text{Enc})$ -special.

Moreover, Enc has a **local decoder**:

$D^f(i) :=$

1. Sample $r_1, \dots, r_t \in \mathbb{F}^n$.
2. Query f at $\{e_i + r_j\}_{j \in [t]} \cup \{r_j\}_{j \in [t]}$.
3. Output plurality $_{j \in [t]} \{ f(e_i + r_j) - f(r_j) \}$.

directly extends to a local corrector:

plurality $_{j \in [t]} \{ f(\gamma + r_j) - f(r_j) \}$
corrects location $\gamma \in \mathbb{F}^n$

If f is δ_{LD} -close to Enc(a) then $\Pr [D^f(i) \neq a_i] \leq \exp(- (1 - 2\delta_{LD}) \cdot t) \leq \epsilon_{LD}$ for $t = O(\frac{\log 1/\epsilon_{LD}}{1 - 2\delta_{LD}})$.

We apply the **PCPP lemma** to this PCP and local decoder to obtain this result:

theorem: $\forall \delta > 0$ QESAT(\mathbb{F}) \in PCPP [$\epsilon_c = 0$, $\epsilon_s = 1/2$, $\Sigma = \{0,1\}$, $l = \exp(n)$, $q = O(1/\delta)$, $r = \text{poly}(n)$, δ]

Polynomial-Size Polylog-Query PCPP

We constructed a PCP for QESAT (\mathbb{F}_2) with proof length $\text{poly}(n)$ and query complexity $\text{poly}(\log n)$.

theorem: QESAT (\mathbb{F}_2) \in PCP [$\epsilon_c = 0$, $\epsilon_s = 1/2$, $\Sigma = \{0,1\}$, $\ell = \text{poly}(n)$, $q = \text{poly}(\log n)$, $r = O(\log n)$]

The encoding underlying this PCP is **LOW-DEGREE EXTENSIONS**:

Enc: $\mathbb{F}^n \rightarrow \mathbb{F}^{\mathbb{F}^{\frac{\log n}{\log |H|}}}$ where Enc(a) := " $(\mathbb{F}, H, \frac{\log n}{\log |H|})$ -extension of a" $\frac{\log n}{\log |H|} \cdot |H|$

The soundness analysis shows that, $\forall \delta_s < \frac{1}{2} \cdot (1 - \frac{d}{|F|})$, the PCP is $(\epsilon_s = O(1), \delta_s, \text{Enc})$ -special.

Moreover, Enc has a local decoder:

$D^f(i) :=$

1. Sample $r_1, \dots, r_t \leftarrow \mathbb{F}^{\frac{\log n}{\log |H|}}$.
2. For $j=1, \dots, t$: query f at $\{e_i + \lambda_1 r_j, \dots, e_i + \lambda_{d+1} r_j\}$.
3. For $j=1, \dots, t$: let $p_j(x)$ be the interpolation of $\{(e_i + \lambda_1 r_j, f(e_i + \lambda_1 r_j)), \dots, (e_i + \lambda_{d+1} r_j, f(e_i + \lambda_{d+1} r_j))\}$.
4. Output plurality $\gamma_{j \in [t]} \{p_j(0)\}$.

Here e_i is i -th point in $H^{\frac{\log n}{\log |H|}}$ and $\lambda_1, \dots, \lambda_{d+1} \in \mathbb{F}$ are distinct and $\neq 0$.

directly extends to a local corrector:
 $\{(\gamma + \lambda_1 r_j, f(\gamma + \lambda_1 r_j)), \dots, (\gamma + \lambda_{d+1} r_j, f(\gamma + \lambda_{d+1} r_j))\}$
 corrects location $\gamma \in \mathbb{F}^{\frac{\log n}{\log |H|}}$

If f is δ_{LD} -close to Enc(a) then $\Pr[D^f(i) \neq a_i] \leq \exp(-(1-(d+1)\delta_{LD}) \cdot t) \leq \epsilon_{LD}$ for $t = O(\frac{\log 1/\epsilon_{LD}}{1-(d+1)\delta_{LD}})$.

We apply the **PCPP lemma** to this PCP and local decoder to obtain this result:

theorem: $\forall \delta > 0$ QESAT (\mathbb{F}_2) \in PCPP [$\epsilon_c = 0$, $\epsilon_s = 1/2$, $\Sigma = \{0,1\}$, $\ell = \text{poly}(n)$, $q = \frac{\text{poly}(\log n)}{\delta}$, $r = O(\log n)$, δ]

Robustness and Proximity

[1/2]

In the proof of the PCP Theorem via proof composition we also need a PCPP that is robust.

theorem: $\forall \delta > 0$ QESAT $(\mathbb{F}_2) \in \text{PCPP}[\epsilon_c = 0, \epsilon_s = 1/2, \Sigma = \{0,1\}, \ell = \text{poly}(n), q = \frac{\text{poly}(\log n)}{\delta}, r = O(\log n), \delta, \sigma = \Omega(1)]$

We have seen how to separately achieve robust PCPs and PCPs of proximity:

- Robust PCP \leftarrow ROBUSTIFICATION(QUERY BUNDLING(PCP))
- PCP of proximity \leftarrow Enc-special PCP + local decoder for Enc

Suppose that the PCP (P, V) is $(\text{Enc}, \epsilon_s, \delta_s)$ -special.

Consider the robust PCP $(P_*, V_*) := \text{ROBUSTIFICATION}(\text{QUERY BUNDLING}((P, V)))$.

The robust soundness analysis establishes that (P_*, V_*) has

robustness $\sigma = \Omega(1)$ and ALSO that (P_*, V_*) is $(\text{Enc}', \epsilon_s', \delta_s')$ -special for

- $\text{Enc}' := \text{LDE}_{\mathbb{F}, H, m} \circ \text{Enc}$
- $\epsilon_s' := \max \left\{ \epsilon_{\text{LPT}}(\delta), 1 - (1 - \epsilon_s) \cdot \left(1 - \frac{qm|H|}{|F|-q} - \delta \right) \right\}$
- $\delta_s' := \min \left\{ \frac{1}{2} \cdot \left(1 - \frac{qm|H|}{|F|-q} \right), \delta_s \right\}$.

$$\pi_* = \left(\left[\text{array of } q \text{ cells} \right]_{f: \mathbb{F}^m \rightarrow \mathbb{F}}, \left(\left[\text{array of } r \text{ cells} \right]_{\hat{a}_{g,v}(z)} \right)_{\substack{g \in \{0,1\}^r \\ v \in \mathbb{F}^m}}, \left(\left[\text{array of } m \text{ cells} \right]_{\hat{a}_{a,b}} \right)_{a,b \in \mathbb{F}^m} \right)$$

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

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

Q: what if we construct a PCPP via a local decoder for Enc' ?

Robustness and Proximity

[2/2]

Recall the definition of a **robust PCPP**.

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

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

def: (P,V) is a **PCPP** system for a relation R with **proximity parameter δ** & **robustness parameter σ** if:

① completeness: $\forall (x,w) \in R \quad \Pr[V^{w,\pi}(x) = 1 \mid \pi \leftarrow P(x,w)] \geq 1 - \epsilon_c$.

② soundness: $\forall (x,w)$ if $\Delta(w, R[x]) \geq \delta$ then $\forall \tilde{\pi} \quad \Pr_{\tilde{\pi}}[\Delta((w,\tilde{\pi})[Q(x,g)], R(V)[S(x,g)]) \leq \sigma] \leq \epsilon_s$.

PROBLEM: the local decoder for (\mathbb{F}, m, H) -extensions is **NOT** robust.

The local view of the local decoder consists of $t \cdot (d+1)$ values: $((f(e_i + \lambda_1 r_j), \dots, f(e_i + \lambda_{d+1} r_j)))_{j \in [t]}$.

It suffices to change t of these (a $\frac{1}{d+1} = o(1)$ fraction) to change the local decoder's output.

E.g. one can change $(f(e_i + \lambda_1 r_j))_{j \in [t]}$ to consistently change $(p_j(0))_{j \in [t]}$, and thus plurality $\text{plurality}_{j \in [t]} \{p_j(0)\}$.

PCPPs from Decoding Consistency Tests

[1/2]

We construct a PCPP for R from two ingredients: $\begin{cases} \text{a PCP for } R \text{ that uses an encoding } \text{Enc} \\ \text{a decoding consistency test for } \text{Enc} \end{cases}$

def: (P_D, V_D) is a **decoding consistency test** for Enc with **decoding radius** δ_D and **decoding error** ϵ_D if:

$$\textcircled{1} \forall a \Pr[V_D^{a, \text{Enc}(a), \pi_D} = 1 \mid \pi_D \leftarrow P_D(a, \text{Enc}(a))] = 1.$$

$$\textcircled{2} \forall a, \tilde{a}, \tilde{c} \Delta(a, \tilde{a}) \geq \delta \wedge \Delta(\tilde{c}, \text{Enc}(\tilde{a})) \leq \delta_D \rightarrow \forall \tilde{\pi}_D \Pr[V_D^{a, \tilde{c}, \tilde{\pi}_D} = 1] \leq \epsilon_D(\delta).$$

$P(x, w)$

1. Compute $(\pi_0, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.

2. Compute $\pi_D := P_D(w, \pi_0)$.

3. Output $\pi_{Px} := (\pi_0, \pi_{\text{sat}}, \pi_D)$.

$V^{w, (\pi_0, \pi_{\text{sat}}, \pi_D)}(x)$

1. Check that $V_{\text{PCP}}^{(\pi_0, \pi_{\text{sat}})}(x) = 1$.

2. Check that $V_D^{w, \pi_0, \pi_D} = 1$.

lemma: Suppose that $(P_{\text{PCP}}, V_{\text{PCP}})$ is $(\text{Enc}, \epsilon_S, \delta_S)$ -special and (P_D, V_D) is a decoding consistency test with decoding radius $\delta_D \geq \delta_S$ and decoding error ϵ_D .

Then $\forall \delta > 0$ (P, V) is a PCPP for R with proximity parameter δ and soundness error $\max\{\epsilon_S, \epsilon_D(\delta)\}$.

Note: A local decoder D for Enc directly implies a decoding consistency test (P_D, V_D) for Enc .

$P_D(a, \text{Enc}(a)) := \perp$
(the proof π_D is empty)

$V_D^{a, \tilde{c}, \perp} :=$ 1. Sample $i_1, \dots, i_t \in [l(a)]$.
2. Check that $\forall j \in [t] D^{\tilde{c}}(i_j) = a_{i_j}$.

$\delta_D := \delta_{\text{LD}}$
 $\epsilon_D(\delta) := (1 - (1 - \epsilon_{\text{LD}}) \cdot \delta)^t$

In this case, the above PCPP is the PCPP based on D from before.

PCPPs from Decoding Consistency Tests

[2/2]

$P(x, w)$

1. Compute $(\pi_o, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.
2. Compute $\pi_D := P_D(w, \pi_o)$.
3. Output $\pi_{px} := (\pi_o, \pi_{\text{sat}}, \pi_D)$.

$V^{w, (\pi_o, \pi_{\text{sat}}, \pi_D)}(x)$

1. Check that $V_{\text{PCP}}^{(\pi_o, \pi_{\text{sat}})}(x) = 1$.
2. Check that $V_D^{w, \pi_o, \pi_D} = 1$.

Completeness: Suppose that $(x, w) \in R$. Then $\Pr[V_{\text{PCP}}^{(\pi_o, \pi_{\text{sat}})}(x) = 1] \geq 1 - \epsilon_c$ for $(\pi_o, \pi_{\text{sat}}) := P_{\text{PCP}}(x, w)$.

Since $\pi_o = \text{Enc}(w)$, $\forall i \in [|w|]$ $\Pr[V_D^{w, \pi_o, \pi_D} = 1] = 1$. Hence $\Pr[V^{w, (\pi_o, \pi_{\text{sat}}, \pi_D)}(x) = 1] \geq 1 - \epsilon_c$.

Soundness: Suppose that w is δ -far from $R[x]$. Fix a proximity proof $\tilde{\pi}_{px} = (\tilde{\pi}_o, \tilde{\pi}_{\text{sat}}, \tilde{\pi}_D)$.

If $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})}(x) = 1] \leq \epsilon_s$ then we are done. So suppose that $\Pr[V_{\text{PCP}}^{(\tilde{\pi}_o, \tilde{\pi}_{\text{sat}})}(x) = 1] > \epsilon_s$.

Since V_{PCP} is $(\text{Enc}, \epsilon_s, \delta_s)$ -special, $\tilde{\pi}_o$ is δ_s -close to $\text{Enc}(\tilde{w})$ for some $\tilde{w} \in R[x]$.

Since w is δ -far from $R[x]$, w is δ -far from $\tilde{w} \in R[x]$.

Since $\delta_s \leq \delta_D$, $\Pr[V_D^{w, \tilde{\pi}_o, \tilde{\pi}_D} = 1] \leq \epsilon_D(\delta)$.

We conclude that $\Pr[V^{w, (\tilde{\pi}_o, \tilde{\pi}_{\text{sat}}, \tilde{\pi}_D)}(x) = 1] \leq \max\{\epsilon_s, \epsilon_D(\delta)\}$.

OBSERVATION: if $(P_{\text{PCP}}, V_{\text{PCP}})$ has robustness parameter σ_{PCP} and (P_D, V_D) has robustness parameter σ_D then (P, V) has robustness parameter $\sigma := \min\{\sigma_{\text{PCP}}, \sigma_D\}$.

Decoding Consistency Test with Robustness

We are left to construct a decoding consistency test for (\mathbb{F}, H, m) -extensions with robustness $\sigma := \Omega(\delta)$.

IDEA: apply "bespoke" robustification to the local decoder for (\mathbb{F}, H, m) -extensions.

$V_D^{a, c, t}$

1. Sample $i_1, \dots, i_t \in [|\mathbb{A}|]$ and $r_1, \dots, r_t \in \mathbb{F}^m$.
2. For every $j \in [t]$:
 - query c on the line $\ell_{i_j, r_j}(z) := (1-z) \cdot i_j + z \cdot r_j$.
 - interpolate $\{(1-\lambda) \cdot i_j + \lambda \cdot r_j, c((1-\lambda) \cdot i_j + \lambda \cdot r_j)\}_{\lambda \in \mathbb{F} \setminus \{0\}}$ to obtain a polynomial $p_j(z)$.
 - check that $\deg(p_j) \leq m \cdot (|H| - 1)$.
 - check that $p_j(0) = a_{i_j}$.

Soundness: Suppose that $\exists \tilde{a}$ s.t. $\Delta(a, \tilde{a}) \geq \delta$ and $\Delta(\tilde{c}, \text{Enc}(\tilde{a})) \leq \delta_D$.

Fix i s.t. $\tilde{a}_i \neq a_i$. To make a local view accepting one must change a_i or change $c|_{\ell_{i, r}}$ to a polynomial (of degree $< m \cdot (|H| - 1)$) other than $\text{Enc}(\tilde{c})|_{\ell_{i, r}}$. Since $\ell_{i, r}$ is a random line through i , $\forall \lambda \in \mathbb{F} \setminus \{0\}$ $\ell_{i, r}(\lambda)$ is random in \mathbb{F}^m . Since $\Delta(\tilde{c}, \text{Enc}(\tilde{a})) \leq \delta_D$, $\Pr[\Delta(\tilde{c}|_{\ell_{i, r} \setminus \{0\}}, \text{Enc}(\tilde{a})|_{\ell_{i, r} \setminus \{0\}}) \geq \frac{1}{4}] \geq 1 - 4\delta_D$.

Hence, w.p. $\geq 1 - 4\delta_D$, if $\tilde{c}|_{\ell_{i, r} \setminus \{0\}}$ has degree $\leq m \cdot (|H| - 1)$ then $\tilde{c}|_{\ell_{i, r} \setminus \{0\}} \equiv \text{Enc}(\tilde{a})|_{\ell_{i, r} \setminus \{0\}}$.

Overall w.p. $\geq \delta \cdot (1 - 4\delta_D) = \Omega(\delta)$, either must change a_i or a constant fraction of the read line.

Bibliography

PCPs of Proximity

- [BGHSV 2005]: [Robust PCPs of proximity, shorter PCPs and applications to coding](#), by Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, Salil Vadan.
- [DR 2006]: [Assignment testers: towards a combinatorial proof of the PCP theorem](#), by Irit Dinur, Omer Reingold.