Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

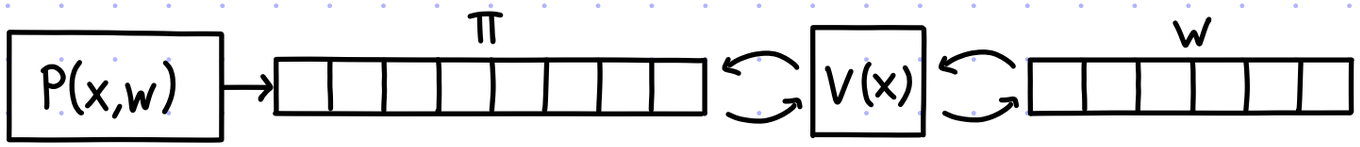
Lecture 21

PCPs of Proximity

PCPs of Proximity

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

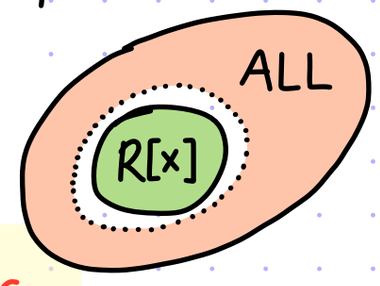
- an instance x
- query access to a candidate witness w
- query access to a PCP string π



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

② **proximity soundness:** $\forall (x,w)$ if $\Delta(w, R[x]) \geq \delta$ then $\forall \tilde{P} \quad \Pr\left[V^{w,\tilde{\pi}}(x) = 1 \;\middle|\; \tilde{\pi} \leftarrow \tilde{P} \right] \leq \varepsilon_s$.

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

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

We construct PCPPs in two regimes.

theorem: $\forall\, \delta > 0 \quad \mathrm{QESAT}(\mathbb{F}_2) \in \mathrm{PCPP}\left[\varepsilon_c = 0,\ \varepsilon_s = 1/2,\ \Sigma = \{0,1\},\ \ell = \exp(n),\ q = O(1/\delta),\ r = \mathrm{poly}(n),\ \delta \right]$

theorem: $\forall\, \delta > 0 \quad \mathrm{QESAT}(\mathbb{F}_2) \in \mathrm{PCPP}\left[\varepsilon_c = 0,\ \varepsilon_s = 1/2,\ \Sigma = \{0,1\},\ \ell = \mathrm{poly}(n),\ q = \frac{\mathrm{poly}(\log n)}{\delta},\ r = O(\log n),\ \delta \right]$

Here $\mathrm{QESAT}(\mathbb{F})$ is the RELATION $\{((p_1,\ldots,p_m), a) \mid p_1,\ldots,p_m \in \mathbb{F}^{\leq 2}[x_1,\ldots,x_n],\ a : [n] \to \mathbb{F},\ p_1(a) = \cdots = p_m(a) = 0\}$.

Easy: from PCPP to PCP

lemma: For every proximity parameter δ,

$$R \in \mathrm{PCPP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell, q, r, \delta] \rightarrow \mathrm{PCP}[\varepsilon_c, \varepsilon_s, \Sigma, \ell' = |w| + \ell, q, r]$$

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

$\pi = ($ [w] , [π_{px}] $)$

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

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

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

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

■

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 PCPs has been to set $\pi = (\pi_0, \pi_{sat})$ where

① π_0 is (allegedly) a valid encoding of some witness ($\exists w : \pi_0 = Enc(w)$),

② if π_0 is close to $Enc(w)$ 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 $V_{PCP}^{(\tilde{\pi}_0, \tilde{\pi}_{sat})}(x) = 1$ with large enough probability then $\tilde{\pi}_0$ is close to $Enc(w)$ with $(x,w) \in R$.

This motivates the following special property:

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

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

Harder: from PCP to PCPP [2/2]

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

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

Intuition for PCPP constructions:

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

1. Check that $V_{PCP}^{(\pi_o,\pi_{sat})}(x) = 1$.
2. Test that "$Enc^{-1}(\pi_o) = w$".

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

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

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

Hence, $\Delta(w, \tilde{w}) \geq \delta$ and $\Delta(\tilde{\pi}_o, Enc(\tilde{w})) \leq \delta_s$. Perhaps there is hope for a test for "$Enc^{-1}(\pi_o) = w$"?

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

PCPPs from Local Decoders [1/2]

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

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

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

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

lemma: Suppose that $R \in PCP[\varepsilon_c, (Enc, \varepsilon_s, \delta_s), \Sigma, \ell, q, r]$.

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

$$\forall\, \delta > 0 \quad R \in PCPP[\varepsilon_c, \varepsilon_s' = \max\{\varepsilon_s, \underbrace{(1-(1-\varepsilon_{LD})\cdot\delta)^t}_{\leq \varepsilon \text{ for } t := O\left(\frac{\log 1/\varepsilon}{(1-\varepsilon_{LD})\cdot\delta}\right)}\}, \Sigma, \ell, q' = q + t\cdot q_{LD}, r' = r + t\cdot(\log|w| + r_{LD}), \delta].$$

Below is the construction of the PCPP.

$P(x,w)$

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

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

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

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

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

PCPPs from Local Decoders [2/2]

$P(x,w)$

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

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

1. Check that $V_{PCP}^{(\pi_0,\pi_{sat})}(x) = 1$.
2. Sample $i_1, \ldots, i_t \in [|w|]$.
3. Check that $\forall j \in [t]\ D^{\pi_0}(i_j) = w_{i_j}$.

Completeness: Suppose that $(x,w) \in R$. Then $\Pr[V_{PCP}^{(\pi_0,\pi_{sat})}(x)=1] \geq 1-\varepsilon_c$ for $(\pi_0,\pi_{sat}) := P_{PCP}(x,w)$.

Since $\pi_0 = Enc(w)$, $\forall i \in [|w|]\ \Pr[D^{\pi_0}(i) = w_i] = 1$. Hence $\Pr[V^{w,(\pi_0,\pi_{sat})}(x) = 1] \geq 1-\varepsilon_c$.

Soundness: Suppose that w is δ-far from $R[x]$. Fix a proximity proof $\tilde{\pi}_{px} = (\tilde{\pi}_0, \tilde{\pi}_{sat})$.

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

Since V_{PCP} is $(Enc, \varepsilon_s, \delta_s)$-special, $\tilde{\pi}_0$ is δ_s-close to $Enc(\tilde{w})$ for some $\tilde{w} \in R[x]$.

Since $\delta_s \leq \delta_{LD}$, $\forall i \in [|w|]\ \Pr[D^{\tilde{\pi}_0}(i) = \tilde{w}_i] \geq 1-\varepsilon_{LD}$.

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 $\Pr_i[D^{\tilde{\pi}_0}(i) \neq w_i] \geq \Pr_i[D^{\tilde{\pi}_0}(i) = \tilde{w}_i \wedge w_i \neq \tilde{w}_i] \geq (1-\varepsilon_{LD})\cdot\delta$.

Therefore $\Pr_{i_1,\ldots,i_t}[\forall j \in [t]: D^{\tilde{\pi}_0}(i_j) = w_{i_j}] \leq (1-(1-\varepsilon_{LD})\cdot\delta)^t$.

We conclude that $\Pr[V^{w,(\tilde{\pi}_0,\tilde{\pi}_{sat})}(x)=1] \leq \max\{\varepsilon_s, (1-(1-\varepsilon_{LD})\cdot\delta)^t\}$.

Exponential-Size Constant-Query PCPP

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

theorem: $\mathrm{QESAT}(\mathbb{F}) \in \mathrm{PCP}[\,\varepsilon_c = 0,\ \varepsilon_s = 1/2,\ \Sigma = \{0,1\},\ \ell = \exp(n),\ q = O(1),\ r = \mathrm{poly}(n)\,]$

The encoding underlying this PCP is LINEAR EXTENSIONS:

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

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

Moreover, Enc has a local decoder:

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

directly extends to a local corrector:

$\mathrm{plurality}_{j\in[t]}\{\, f(\gamma + r_j) - f(r_j)\,\}$

corrects location $\gamma \in \mathbb{F}^n$

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

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

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

Polynomial-Size Polylog-Query PCPP

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

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

The encoding underlying this PCP is LOW-DEGREE EXTENSIONS:

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

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

Moreover, Enc has a local decoder:

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

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

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

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

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

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

Robustness and Proximity [1/2]

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

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

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

- robust PCP ← RobustificationOf(QueryBundling(PCP))
- PCP of proximity ← Enc-special PCP + local decoder for Enc

Suppose that the PCP (P,V) is $(Enc, \varepsilon_s, \delta_s)$-special.

Consider the robust PCP $(P_*, V_*) := \mathrm{RobustificationOf}(\mathrm{QueryBundling}((P,V)))$.

The robust soundness analysis establishes that (P_*, V_*) has robustness $\sigma = \Omega(1)$ and ALSO that (P_*, V_*) is $(Enc', \varepsilon_s', \delta_s')$-special for

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

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

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

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

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 $f(a\mu + b) = \hat{g}_{a,b}(\mu)$.

Robustness and Proximity [2/2]

Recall the definition of a robust PCPP.

We consider non-adaptive verifiers: $V^{w,\pi}(x;s) = D(S(x,\rho),(w,\pi)[Q(x,s)])$.

decision algorithm; state algorithm; query algorithm

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

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

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

② <u>soundness:</u> $\forall (x,w)$ if $\Delta(w,R[x]) \geq \delta$ then $\forall \tilde{\pi} \quad \Pr_s\left[\Delta\left((w,\tilde{\pi})[Q(x,s)], R(V)[S(x,s)]\right) \leq \sigma\right] \leq \varepsilon_s$.

<u>PROBLEM:</u> 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: $((f(e_i+\lambda_1 r_j),\ldots,f(e_i+\lambda_{d+1} r_j)))_{j\in[t]}$.

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 $\text{plurality}_{j\in[t]}\{p_j(0)\}$.

PCPPs from Decoding Consistency Tests [1/2]

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

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

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

② $\forall\, a, \tilde{a}, \tilde{c} \quad \Delta(a, \tilde{a}) \geq \delta \;\wedge\; \Delta(\tilde{c}, Enc(\tilde{a})) \leq \delta_D \;\rightarrow\; \forall\, \tilde{\pi}_D \quad \Pr\left[V_D^{a, \tilde{c}, \tilde{\pi}_D} = 1 \right] \leq \varepsilon_D(\delta)$.

$P(x, w)$

1. Compute $(\pi_0, \pi_{sat}) := P_{PCP}(x, w)$.
2. Compute $\pi_D := P_D(w, \pi_0)$.
3. Output $\pi_{Px} := (\pi_0, \pi_{sat}, \pi_D)$.

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

1. Check that $V_{PCP}^{(\pi_0, \pi_{sat})}(x) = 1$.
2. Check that $V_D^{w, \pi_0, \pi_D} = 1$.

lemma: Suppose that (P_{PCP}, V_{PCP}) is $(Enc, \varepsilon_S, \delta_S)$-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 $\max\{\varepsilon_S, \varepsilon_D(\delta)\}$.

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

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

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

$\delta_D := \delta_{LD}$

$\varepsilon_D(\delta) := (1 - (1 - \varepsilon_{LD}) \cdot \delta)^t$

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

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

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

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

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

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

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

Since V_{PCP} is $(Enc, \varepsilon_s, \delta_s)$-special, $\tilde{\pi}_o$ is δ_s-close to $Enc(\tilde{w})$ 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 $\delta_s \leq \delta_D$, $\Pr[V_D^{w,\tilde{\pi}_o,\tilde{\pi}_D}=1] \leq \varepsilon_D(\delta)$.

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

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

Deciding Consistency Test with Robustness

We are left to construct a decoding consistency test for $(\mathbb{F},H,m)$-extensions with robustness $\sigma := \Omega(1)$.

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

$V_D^{a,c,\perp}$

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

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

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 $Enc(\tilde{c})|_{\ell_{i,r}}$. 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 $\Delta(\tilde{c},Enc(\tilde{a})) \le \delta_D$, $\Pr_r[\,\Delta(\tilde{c}|_{\ell_{i,r}\setminus\{0\}}, Enc(\tilde{a})|_{\ell_{i,r}\setminus\{0\}}) \ge \frac{1}{4}\,] \ge 1-4\delta_D$.

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

Overall w.p. $\ge \delta\cdot(1-4\delta_0) = \Omega(\delta)$, either must change a_i or a constant fraction of the read line.