- [Lots of pairwise-independent points]

$\forall\, \phi \neq T \subseteq [k]$, $\underline{s_T} := \bigoplus_{i \in T} s_i$ (bit-wise XOR)

& $\underline{\sigma_T} := \bigoplus_{i \in T} \sigma_i$.

- Compute $\forall i \in [n]$, $x_i = \underset{T}{\mathrm{maj}} \{\sigma_T \oplus f(s_T + e_i)\}$, where e_i is all 0's except 1 at the i-th position.

- OUTPUT $x_1 \cdots x_n$ [Hope: it is in $\mathcal{L}_f$.]
- Repeat the above $1000n/\varepsilon^4$ times.

<u>Analysis</u>: Let us consider a <u>fixed</u> $x \in \mathcal{L}_f$ & compute the probability of outputing it.

- $\Pr[\forall i \in [k],\ \sigma_i = x \odot s_i] = 2^{-k} \geqslant 1/2m$.

- We now <u>assume</u> $\forall i \in [k]$, $\underline{\sigma_i = x \odot s_i}$.
- Define $\forall\, \phi \neq T \subseteq [k]$, $\forall j \in [n]$,

$$\underline{Z_{T,j}} := \begin{cases} 1, & \text{if } f(s_T + e_j) = x \odot (s_T + e_j). \\ 0, & \text{else.} \end{cases}$$

• Define $Z_j := \sum_{\phi \neq T \subseteq [k]} Z_{T,j}$, $\forall j \in [n]$.

$\Rightarrow E[Z_j] = \sum_T Pr[f(s_T + e_j) = x \odot (s_T + e_j)]$
$\geq m \cdot \left(\frac{1}{2} + \frac{\varepsilon}{2}\right)$. [linearity of expectation]

• For a fixed j: $Z_{T,j}$'s are not indepen-dent but are pairwise independent.

So, instead of Chernoff, we apply the Chebychev's inequality:

$$Pr[|R - E(R)|^2 \geq k^2 \cdot var(R)] \leq 1/k^2.$$

$\Rightarrow Pr[Z_j \leq m/2] = Pr[|Z_j - E[Z_j]| \geq m\varepsilon/2]$

$\leq var(Z_j) / \left(\frac{m\varepsilon}{2}\right)^2 \underset{*}{=} \sum_T var(Z_{T,j}) / \left(\frac{m\varepsilon}{2}\right)^2$

* needs pairwise-independence

$\leq m / \left(\frac{m\varepsilon}{2}\right)^2 = 4/m\varepsilon^2 \leq 1/50n$.

• Overall, $Pr["x_1 \cdots x_n" = x] \geq \frac{1}{2m} \cdot \left(1 - \frac{1}{50n}\right)^n$
$> e^{-1/50}/m$.

output in L_f

$\Rightarrow$ Repeating the above algorithm $2m$ times would yield the x whp.

Further, repeating it $(2m \cdot 2/\varepsilon^2)$ times would yield the list $\mathcal{L}_f$ with probability $\geq 2/3$. $\square$

Local list decoding RM

- Recall that RM "maps" $\binom{\ell+d}{d}$ evaluations of a d-deg ℓ-variate polynomial $P(\bar{x})$ to all $|\mathbb{F}|^\ell$ evaluations.

Our goal is to output $P(x)$, given an $x \in \mathbb{F}^\ell$, an oracle to a corrupted $RM \circ P$ & an advice. Let $q := |\mathbb{F}|$.

Theorem 2 (Sudan, Trevisan, Vadhan, 1999): RM has a local list decoder handling $1-10\sqrt{d/q}$ errors.

(Compare: RS list decoder handled $1-\sqrt{d/q}$ errors.)

Proof: • Idea — Given $x \in \mathbb{F}^{\ell}$ & an oracle f to a corrupted RMoP, randomly pick an $r \in \mathbb{F}$.

The advice is $(x_0, y_0) \in \mathbb{F}^{\ell+1}$ s.t. $P(x_0) = y_0$.

Let L_{x,x_0} be a random cubic curve passing through $(0, x)$ & $(r, x_0) \in \mathbb{F}^{\ell+1}$.

(L_{x,x_0} has the points $\{q(t) := (q_1(t), \ldots, q_\ell(t)) \mid t \in \mathbb{F}\}$ in $\mathbb{F}^{\ell}$, where q_i's are cubics.)

Query f on L_{x,x_0} & run RS list decoder to find a unique $g(t) = P \circ q(t)$ s.t. $g(r) = y_0$.

Output $g(0)$ $(= P(x)$ whp$)$.

• We will give a decoder that works for "most" of the input $x \in \mathbb{F}^{\ell}$.

This suffices as one can later use the "querying on a line" idea (of the RM local decoder) to make the above work $\forall x \in \mathbb{F}^{\ell}$.

Input: 1) Oracle f s.t. $\Pr_{x \in \mathbb{F}^{\ell}}[f(x) = P(x)] > 10\sqrt{d/q}$,

unknown poly. d-deg ℓ-var.

and $|\mathbb{F}| > d^4$.

2) advice $\underline{(x_0, y_0)} \in \mathbb{F}^\ell \times \mathbb{F}$. $[\, P(x_0) = y_0 \,]$

3) $x \in \mathbb{F}^\ell$.

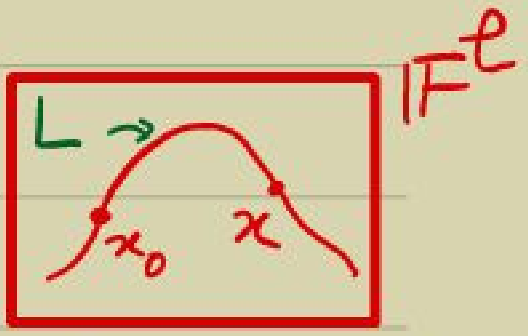
<u>Output</u>: $y \in \mathbb{F}$ [whp $\exists!\, P$ s.t. $P(x) = y$.]

<u>Decoder</u>:

1) Pick a random $r \in \mathbb{F}$ & cubics $q_i(t)$, $i \in [\ell]$, s.t. $\underline{q(t)} := (q_1(t), \ldots, q_\ell(t))$ satisfies:

$$q(0) = x \ \& \ q(r) = x_0.$$

Define $L = L_{x, x_0} := \{ q(t) \mid t \in \mathbb{F} \}$.



2) Query $\underline{f}$ on L to obtain $S := \{ (t, f \circ q(t)) \mid t \in \mathbb{F} \}$.

3) Run RS list decoder on S to find the <u>list</u> $g_1, \ldots, g_k$ of all deg-$3d$ polynomials that agree on $\geq 8\sqrt{dq}$ pairs in S.

4) If $\exists$ unique i s.t. $g_i(r) = y_0$ then OUTPUT $g_i(0)$. Else FAIL.

<u>Analysis</u>: • Hypothesis on f implies that f agrees with a P on $\geq 8\sqrt{dq}$ points in L with probability ≥ 0.99.

[Hint: Since points other than $\{x, x_0\}$ on the <u>random</u> L are pairwise independent, we can use Chebyshev's inequality.]

• Assuming this agreement of f with P on L: the list-size $k \leq 8\sqrt{dq}/3d$.

$$\Rightarrow \Pr_r[\exists!\, i,\ g_i(r) = y_0] > 1 - k \cdot \Pr_r[g_i(r) = g_j(r)]$$
$$\geq 1 - k \cdot 3d/q \geq 1 - 8\sqrt{d/q} > 0.99$$

$\Rightarrow$ Overall, the decoder has success probability $> 0.99^2 > 0.98$ & the time-complexity is $\mathrm{poly}(q, \ell)$. $\square$

<u>Remark</u>: The above shows that "most" (x_0, y_0) are an advice for x. Thus, $\exists (x_0, y_0)$ that works for "most" x.

Local list decoding WH∘RM

Theorem 3 (STV '99): $E_1 : \{0,1\}^n \to \Sigma^m$ resp. $E_2 : \Sigma \to \{0,1\}^k$ are ecc with local list decoders using advice from index-sets I_1 resp. I_2 & handling $1-\varepsilon_1$ errors resp. $1/2 - \varepsilon_2$ errors.

Then $E_2 \circ E_1$ has a local list decoder using advice from $I_1 \times I_2$ that handles $(1-\varepsilon_1 |I_2|) \cdot (\frac{1}{2} - \varepsilon_2)$ errors.

Proof sketch:

- Idea – Similar to that of their local decoder.

$\square$

– From this we now deduce that for a worst-case hard f, WH∘RM∘tt(f) is the truth-table of an average-case hard function.