Decoding WH∘RS

Theorem: For $WH \circ RS : \{0,1\}^{n \lg q} \to \{0,1\}^{mq}$,
$\exists$ poly(q)-time decoder, if the fraction of errors $< \frac{1}{4} \cdot \left(\frac{1}{2} - \frac{n-1}{2m}\right)$.

* Notice the fall from RS by 1/4-th.

Proof:

- Let y' be "close" to $y = \langle WH(RS(x)_i) \mid i \in [m] \rangle$.
- The hypothesis implies that
$\#\{i \mid WH(RS(x)_i) \text{ has } \geq q/4 \text{ errors}\} < \frac{m-n+1}{2}$.

$\Rightarrow$ WH-decoding will yield $\langle \tilde{y}_1, \dots, \tilde{y}_m \rangle =: \tilde{y}$
with $\tilde{y}_i = RS(x)_i$ for $> \underbrace{\frac{m+n-1}{2}}_{= m - \frac{m-n+1}{2}}$ of the i's.

$\Rightarrow$ RS-decoding of $\tilde{y}$ yields the unique x.

$\square$

- Thus, WH∘RS is a practical ecc that handles up to 11% of errors.

- For hardness amplification we need an even stronger kind of decoding:

Local Decoding

Defn: Let $E: \{0,1\}^n \to \{0,1\}^m$ be an ecc & $\rho \in (0,1)$.

Short: Ld_ρ → A local decoder for E handling ρ errors is an algorithm that:

Given $j \in [n]$ & oracle to y s.t. $\Delta(y, E(x)) < \rho$,

Outputs x_j with probability $\geq 2/3$

& poly($\lg m$)-time.

(Thus, when m is large, very few bits of y are needed to guess x_j!)

Theorem 1: $\forall \rho < 1/4$, WH-code has a Ld_ρ.

Proof:

- Idea - Querying the two positions - z & $z+e_j$ - suffices to guess x_j.

n-bit

the j-th bit 1 while others 0

- <u>Input</u>: $j \in [n]$, oracle $f: \{0,1\}^n \to \{0,1\}$ s.t.
$$\Pr_z [f(z) \neq x \odot z] \leq \rho.$$
[x is the unknown plaintext, $tt(f)$ is corrupted $E(x)$.]
- <u>Output</u>: $b \in \{0,1\}$ (Whp $b = x_j$).
- <u>Decoder</u>:
  1) Randomly pick $z \in \{0,1\}^n$.
  2) Let $e_j \in \{0,1\}^n$ be the string with 1 at the j-th place & 0 in the rest.
  3) Output $f(z) + f(z+e_j) \bmod 2$.

- Clearly, the time complexity is $poly(n) = poly(\lg m)$, as $m = 2^n$.

- <u>Analysis</u>: $\Pr_z [f(z) = x \odot z \wedge f(z+e_j) = x \odot (z+e_j)]$
$$\geq 1 - 2\rho > 1/2.$$
$\Rightarrow \Pr_z [f(z) + f(z+e_j) = x \odot e_j \bmod 2] > 1/2.$
$\Rightarrow \Pr_z [b = x_j] > 1/2.$
- This can be further boosted. $\square$

Local decoder for RM

- Recall RM: $\mathbb{F}^{\binom{\ell+d}{d}} \to \mathbb{F}^{|\mathbb{F}|^\ell}$ is of distance $\left(1-\frac{d}{|\mathbb{F}|}\right)$, $d < |\mathbb{F}| < \infty$.

- For local decoding it will be convenient to view RM as mapping $\binom{\ell+d}{d}$ evaluations of a polynomial f to its $|\mathbb{F}|^\ell$ evaluations.

Theorem 2: $\forall \rho \leq \frac{1}{6}\left(1-\frac{d+5}{|\mathbb{F}|-1}\right)$, RM-code has a LD_ρ.

Proof:

- Idea – The degree-d polynomial f is unknown & we want to evaluate it at, say, $x \in \mathbb{F}^\ell$.

  Pick a random line L_x through x, evaluate f on each point in L_x, & use RS-decoder to learn $f|_{L_x}$.

  (This is a generalization of WH local decoder)

- Input: $x \in \mathbb{F}^n$, oracle $\tilde{f} : \mathbb{F}^\ell \to \mathbb{F}$ that agrees with some ℓ-variate d-deg f on $\geq 1-\rho$ points.

- <u>Output</u>: $\alpha \in \mathbb{F}$ [whp $\alpha = f(x)$].
- <u>Decoder</u>:
  1) Pick a random $z \in \mathbb{F}^{\ell}$ & define "line" $L_x := \{ x + tz \mid t \in \mathbb{F} \}$.
  2) Query $\tilde{f}$ on L_x, i.e. collect the pairs $\{ (t, f(x+tz)) \mid t \in \mathbb{F} \} =: \tilde{f}(L_x)$.
  3) Via RS-decoder, on $\tilde{f}(L_x)$, find a degree $\leq d$ polynomial $\tilde{Q} : \mathbb{F} \to \mathbb{F}$ s.t.
     $\tilde{Q}(t) = \tilde{f}(x+tz)$ for the largest number of t's.
  4) Output $\tilde{Q}(0)$.

- Clearly, the time complexity is $\mathrm{poly}(\ell, d, |\mathbb{F}|)$.
- <u>Analysis</u>:
  - RS decoder tries to reconstruct $f(x+tz) =: Q(t)$, which has deg $\leq d$ & is univariate.
  - For the decoder to find Q we need the guarantee, $\Pr_z\left[\#t, \text{with } Q(t) \neq \tilde{f}(x+tz), \text{ is} < \frac{|\mathbb{F}|-d}{2} \right] \geq 2/3$.

- For that we compute the expectation:

$$\mathop{\mathrm{Exp}}_{z}\left[\#\{t\in\mathbb{F} \mid f(x+tz)\neq\tilde{f}(x+tz)\}\right] \leq$$

$$1+\sum_{t\in\mathbb{F}^*}\Pr_{z}\left[f(x+tz)\neq\tilde{f}(x+tz)\right]\leq 1+\rho\cdot(|\mathbb{F}|-1).$$

- Thus, by Markov's inequality:

$$\Pr_{z}\left[\#\{t\in\mathbb{F} \mid Q(t)\neq\tilde{Q}(t)\}\geq\frac{|\mathbb{F}|-d}{2}\right]$$

$$\leq 1+\rho\cdot(|\mathbb{F}|-1)\Big/\frac{|\mathbb{F}|-d}{2} \leq \frac{1+\frac{1}{6}\cdot(|\mathbb{F}|-d-6)}{(|\mathbb{F}|-d)/2}=\frac{1}{3}.$$

- Thus, with $\mathrm{prob}_z\geq\frac{2}{3}$, Step-3 produces

$$\tilde{Q}(t)=Q(t)=f(x+tz).$$

$$\Rightarrow\ \tilde{Q}(0)=f(x).$$

$\square$

<u>Local decoder for concatenated codes</u>

- Let $E_1:\{0,1\}^n\to\Sigma^m$ resp. $E_2:\Sigma\to\{0,1\}^k$ be ecc's with local decoders of q_1 resp. q_2 queries handling ρ_1 resp. ρ_2 errors.

[Like RM we assume that $q_1\geq|\Sigma|$.]