## Theorem 3: $\exists\ O(q_1 q_2 \cdot \lg q_1 \cdot \lg|\Sigma|)$-query $Ld_{\rho_1\rho_2}$ for the ecc $E := E_2 \circ E_1 : \{0,1\}^n \to \{0,1\}^{mk}$.

**Proof:**

- Idea – Break $y$ into blocks of size $k$. On a block call $E_2$'s $Ld_{\rho_2}$ ($\lg|\Sigma|$)-times. Finally, call $E_1$'s $Ld_{\rho_1}$ on several decoded blocks.

- Input: Index $i \in [n]$ & oracle access to $y \in \{0,1\}^{mk}$ s.t. $\exists x \in \{0,1\}^n$, $\Delta(y, E_2 \circ E_1(x)) < \rho_1\rho_2$.
- Output: $b \in \{0,1\}$ (whp $b = x_i$).
- Decoder:
  1) View $y$ as $m$ blocks each of $k$-bits. [It is a corrupted $\langle E_2(E_1(x)_j) \mid j \in [m] \rangle$.]
  2) To find the $j$-th symbol $E_1(x)_j$ we call $E_2$'s $Ld_{\rho_2}$ on the $j$-th block of $y$.
     We do this $\lg|\Sigma|$ times to recover the full $E_1(x)_j$.
  3) We repeat this $(50 \cdot \lg q_1)$ times so that the probability of not decoding $E_1(x)_j$ is

$< 1/10q_1$ [Hint: Chernoff bound & then the union bound yields $1/q_1^2 \times \lg|\Sigma| < \frac{1}{10q_1}$, as $q_1 \geq |\Sigma|$.]

4) Since $< \rho_1$ of the blocks in $y$ can be at distance $> \rho_2$ from the respective true block, we use $E_1$'s $Ld_{\rho_1}$ to query $q_1$ blocks.

With probability $> 1 - \frac{1}{10q_1} \times q_1 = 0.9$

the $q_1$ answers to $E_1$'s $Ld_{\rho_1}$ are consistent with that of a string that is $\rho_1$-close to $E(x)$.

$\Rightarrow$ $E_1$'s $Ld_{\rho_1}$ outputs $x_j$ with probability

$\geq 0.9 - 1/3 > 1/2$

& queries $= O(q_2 \cdot \lg|\Sigma| \cdot \lg q_1 \cdot q_1)$. $\square$

Corollary: For WHoRM local decoder the #queries is $O(q \cdot \lg^2 q)$ handling up to $\frac{1}{6} \cdot \left(1 - \frac{d+5}{q-1}\right) \cdot \frac{1}{4}$ errors, where $q = |\mathbb{F}|$.

- Our final goal is to show: If $f$ is a worst-case hard function & $E$ a locally decodable code, then $E \circ tt(f)$ is the truth-table of an average-case hard function $g$.

- For average-case hardness of $g$ we would need an $E$ that is locally decodable up to $(1/2 - \delta)$ errors!

  This type of decodability cannot be unique.

- So, we relax unique decodability to that of finding a list.


Theorem (Johnson bound 1962): If $E: \{0,1\}^n \to \{0,1\}^m$ is an ecc with distance $\geq (\frac{1}{2} - \varepsilon)$ then $\forall x \in \{0,1\}^m$ & $\overset{>0}{\delta} \geq \sqrt{\varepsilon}$, $\exists \leq 1/2\delta^2$ codewords $y_1, \ldots, y_\ell$ s.t. $\Delta(x, y_i) \leq 1/2 - \delta$, $\forall i \in [\ell]$.

<u>Proof:</u> • Idea – We reduce the notion of distance to that of inner-product & use linear algebra.

• Let $\Delta(x, y_i) \leq 1/2 - \delta$, $\forall i \in [\ell]$.

• Define $z_1, \ldots, z_\ell \in \{-1, 1\}^m$ s.t.

$$\underline{z_{i,k}} = \begin{cases} 1, & \text{if } x_k = y_{i,k} \\ -1, & \text{else.} \end{cases}$$

• $\Delta(x, y_i) \leq 1/2 - \delta \Rightarrow$

(1) --- $$\sum_{k \in [m]} z_{i,k} \geq \left(\tfrac{1}{2}+\delta\right)m - \left(\tfrac{1}{2}-\delta\right)m = 2\delta m.$$

counting 1's   -1's

• $\Delta(y_i, y_j) \geq 1/2 - \varepsilon \Rightarrow$

(2) --- $$\langle z_i, z_j \rangle = \sum_k z_{i,k} \cdot z_{j,k} \leq \left(\tfrac{1}{2}+\varepsilon\right)m - \left(\tfrac{1}{2}-\varepsilon\right)m$$

$$= 2\varepsilon m \leq 2\delta^2 m.$$

• Let $w := \sum_{i \in [\ell]} z_i$.

$$\Rightarrow \langle w, w \rangle = \sum_{i \in [\ell]} \langle z_i, z_i \rangle + \sum_{i \neq j} \langle z_i, z_j \rangle$$

By (2)

(3) --- $$\leq \sum_i m + \sum_{i \neq j} 2\delta^2 m \leq \ell m + 2\delta^2 \ell^2 m.$$

• Also, by (1): $\sum_{k=1}^{m} w_k = \sum_{\substack{k\in[m]\\ i\in[\ell]}} z_{i,k} \geqslant 2\delta\ell m$.

By Cauchy-Schwarz's, $\sum w_k^2 \geqslant (\sum w_k)^2/m$,
$\Rightarrow \langle w,w\rangle \geqslant (2\delta m\ell)^2/m = 4\delta^2\ell^2 m$.

• This means, by (3), that:
$4\delta^2\ell^2 m \leq \langle w,w\rangle \leq \ell m + 2\delta^2\ell^2 m$
$\Rightarrow \quad 2\delta^2\ell \leq 1$
$\because \delta > 0 \quad \Rightarrow \quad \ell \leq 1/2\delta^2 \leq 1/2\varepsilon$. $\square$

– Thus, there are not too many codewords $(\frac{1}{2}-\sqrt{\varepsilon})$-close to $x$ if the distance of the code is $(\frac{1}{2}-\varepsilon)$.

Can we compute this list efficiently? & locally?

– We will see that both the answers are yes!