

## Lecture 28: Generalized Minimum Distance Decoding

November 5, 2007

Lecturer: Atri Rudra

Scribe: Sandipan Kundu

**Theorem 0.1.** An  $[n, k]_q$  RS code can be corrected from  $e$  errors (or  $s$  erasures) as long as  $e < \frac{n-k+1}{2}$  (or  $s < n - k + 1$ ) in poly time.

**Theorem 0.2.** An  $[n, k]_q$  RS code can be corrected from  $e$  errors and  $s$  erasures in poly time as long as  $2e + s < (n - k + 1)$ .

*Proof.* Given  $y \in (\mathbb{F}_q^n \cup \{?\})^n$  with erasures and errors, let  $\mathbf{y}'$  be the sub-vector with no erasures. This implies  $\mathbf{y}' \in \mathbb{F}_q^{n-s}$  and we are dealing with  $[n-s, k]_q$  RS code. Now lets run the B-W algorithm on  $\mathbf{y}'$ . It can correct  $\mathbf{y}'$  as long as

$$e < \frac{(n-s) - k + 1}{2}$$

$$\Rightarrow 2e + s < (n - k + 1) \quad (1)$$

So, we proved one can correct  $e$  errors under the stated condition. Now we have to prove that the we can correct the  $s$  erasures under the stated condition in the theorem 0.2. Let  $\mathbf{C}'$  be the output after correcting  $e$  errors. Now we extend  $\mathbf{C}'$  to  $\mathbf{z}' \in (\mathbb{F} \cup \{?\})^n$  with erasures. Run the erasure decoding algorithm on  $\mathbf{z}'$ . This works al long as  $s < (n - k + 1)$ , which in turn is true by (1)  $\square$

# 1 Generalized Minimum Distance Decoding

$C_{out}[N, K, D]_{q^k}$  code such that it can be decoded from  $e$  errors and  $s$  errors and  $s$  erasures in poly time such that  $2e + s < D$ .  $C_{in}[n, k, d]_q$  code with  $k = \mathcal{O}(\log N)$

## 1.1 GMD algorithm (Version 1)

**Input:**  $\mathbf{y} = (y_1, \dots, y_N) \in [q^n]^N$ .

**Step1:**

- (a)  $y'_i = MLD_{c_{in}}(y_i), 1 \leq i \leq N$
- (b)  $w_i = \min(\Delta(y'_i, y_i), \frac{d}{2})$
- (c) With probability  $\frac{2w_i}{d}$ , set  $y'_i \leftarrow \{?\}$

**Step2:** Run errors and erasure algorithm for  $C_{out}$  on  $\mathbf{y}'$ .

**Theorem 1.1.** If exist  $\mathbf{c} \in C_{out} \circ C_{in}$  such that  $\Delta(\mathbf{c}, \mathbf{y}) < \frac{Dd}{2}$  then the GMD algorithm outputs  $\mathbf{c}$  (version 3)

**Lemma 1.2.** If  $\mathbf{y}'$  has  $e'$  errors and  $s'$  erasures after step 1, then

$$\mathbb{E}[2e' + s'] < \frac{D}{2}$$

**Remark 1.3.** Note that if whp  $2e' + s' < \frac{D}{2}$ . Implies get a high probability algorithm.

*Proof.* of lemma 1.2

$e_i \triangleq \Delta(y_i, c_i), 1 \leq i \leq N.$

$$\Rightarrow \sum_i e_i \leq \frac{Dd}{2} \quad (2)$$

$x_i^? = 1$  iff  $y_i' = ?$ ;  $x_i^e = 1$  iff  $y_i' \neq y_i$  and  $y_i' \neq ?$  Done if we can show

$$\mathbb{E}[2x_i^e + x_i^?] < \frac{2e_i}{d} \text{ for every } 1 \leq i \leq N \quad (3)$$

$e' = \sum_i x_i^e, s' = \sum_i x_i^?$  By linearity of expectation using (2)  $\mathbb{E}[2e' + s'] < \frac{2}{d} \sum_i e_i < D$

**Case 1:**  $C_i = y_i'$

$$\mathbb{E}[x_i^?] = Pr[x_i^? = 1] = \frac{2w_i}{d}$$

$$\mathbb{E}[x_i^e] = Pr[x_i^e = 1] = 0$$

Implies (3) is true as

$$\begin{aligned} w_i &= \min(\Delta(y_i', y_i), \frac{d}{2}) \\ &\leq \Delta(y_i', y) \\ &= \Delta(c_i, y) = e_i \end{aligned}$$

**Case 2:**  $C_i \neq y_i'$

$$\mathbb{E}[X_i^?] = \frac{2w_i}{d}$$

$$\mathbb{E}[X_i^e] = Pr[X_i^e = 1] = 1 - \frac{2w_i}{d}$$

$$\Rightarrow \mathbb{E}[2x_i^e + X_i^?] = 2 - \frac{2w_i}{d} \leq \frac{2e_i}{d}$$

(4)

Claim 1: If  $y'_i \neq c_i$ , then  $c_i + w_i \geq d$

**Case 1:**  $w_i = \Delta(y'_i, y_i)$ ,  $e_i = \Delta(y_i, c_i)$

$\Rightarrow$  by triangle inequality

$$\begin{aligned} e_i + w_i &= \Delta(y_i, c_i) + \Delta(y'_i, y_i) \\ &\geq \Delta(c_i, y'_i) \\ &\geq d(y'_i \text{ is in } C_{in}) \end{aligned} \tag{5}$$

**Case 2:**  $w_i = \frac{d}{2} \leq \Delta(y'_i, y_i)$

As  $y'_i$  is obtained from MLD.

$$\begin{aligned} \Delta(y'_i, y_i) &\leq \Delta(c_i, y_i) \\ \Rightarrow e_i = \Delta(c_i, y_i) &\geq \Delta(y'_i, y_i) \geq \frac{d}{2} \\ \Rightarrow e_i + w_i &\geq d \end{aligned} \tag{6}$$

□

**Step 1c:** With probability  $\frac{2w_i}{d}$ ,  $y'_i \leftarrow ?$

(Version 2) Step 1'(c) Pick  $\theta \in [0, 1]$ , at random.

(d) If  $\theta \leq \frac{2w_i}{d}$ , set  $y'_i \leftarrow ?$

$$\begin{aligned} \Pr[y'_i \text{ is an erasure}] &= \frac{2w_i}{d} \\ &= \Pr(\theta \in [0, \frac{2w_i}{d}]) = \frac{2w_i}{d} \end{aligned} \tag{7}$$

Implying even for version 2 of GMD  $\mathbb{E}[2e' + s'] < D$  Possible problem (7) is correlated for different  $i$ . Can pick  $\theta$  from a fixed number of possible values. Can derandomize by going through all possible values of  $\theta$ .