Decoding Concatenated Codes

Last time:

Outer code C_{out} $[N, K, D]_{q^k}$ (where $q^k = O(N)$)

Inner code C_{in} $[n, k, d]_q$

Encoding maps $C_{in} : \mathbb{F}_q^k \to \mathbb{F}_q^n$ and $C_{out} : \mathbb{F}_{q^k}^K \to \mathbb{F}_{q^k}^N$

Assume

(1) $D_{C_{out}} : \mathbb{F}_{q^k}^N \to \mathbb{F}_{q^k}^K$ is a polynomial time unique decoding algorithm that can correct up to $\frac{D}{2}$ errors

(2) $D_{C_{in}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is the MLD so, given received word y, it returns a codeword $x = MLD(y) \in C_{in} \subseteq \mathbb{F}_q^n$ in $O(nq^k)$ steps

Algorithm 1 – natural decoder for $C_{out} \circ C_{in}$

Input: received word $y = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N$

Output: message $m \in (\mathbb{F}_q^k)^K$

Step 1: $y' = (y'_1, \ldots, y'_N) \in (\mathbb{F}_q^n)^N$ where $C_{in}(y'_i) = D_{C_{in}}(y_i)$, $1 \leq i \leq N$

Step 2: $m = D_{C_{out}}(y')$

Step 3: return m

The picture is:

$$
\begin{array}{ll}
y = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N & y_i \in \mathbb{F}_q^n \\
\quad \downarrow \ \ldots \ \downarrow D_{C_{in}} & \\
x = (x_1, \ldots, x_N) \in (\mathbb{F}_q^n)^N & x_i = D_{C_{in}}(y_i) \in \mathbb{F}_q^n \\
y' = (y'_1, \ldots, y'_N) \in (\mathbb{F}_{q^k})^N & y'_i \in \mathbb{F}_q^k \cong \mathbb{F}_{q^k} \ \text{ s.t. } \ C_{in}(y'_i) = x_i \\
\downarrow D_{C_{out}} & \\
m \in (\mathbb{F}_{q^k})^K \cong (\mathbb{F}_q^k)^K &
\end{array}
$$

And we proved:

Thm. Algoritm 1 corrects up to $\frac{Dd}{4}$ errors in polynomial time.

Today:

Assume

(1) C_{out} is an $[N, K, D]_{q^k}$ (with $q^k = O(N)$) that can be decoded (by $D_{C_{out}}$) from e errors and s erasures in polynomial time as long as $2e + s < D$

(2) C_{in} is an $[n, k, d]_q$ code, and $D_{C_{in}}$ is the MLD as in algorithm 1

Goal: Decoding algorithm for $C_{out} \circ C_{in}$ that corrects up to $\frac{Dd}{2}$ errors in polynomial time.

Generalized Minimum Distance (GMD) algorithm

Input: received word $y = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N$

Output: message $m \in (\mathbb{F}_q^k)^K$

1. for $1 \leq i \leq N$ do
2. $\quad x_i = D_{C_{in}}(y_i)$
3. $\quad w_i = \min(d_H(x_i, y_i), \frac{d}{2})$
4. $\quad$ with probability $\frac{2w_i}{d}$, set $y_i' =?$,
   otherwise set $y_i' = x'$ where $x_i = C_{in}(x')$
5. $m = D_{C_{out}(y')}$, where $y' = (y_1', \ldots, y_N')$
6. return m

Note that, in step 4, it's a different "randomness" for each i.

The picture is:

$$
\begin{array}{ll}
y = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N & y_i \in \mathbb{F}_q^n \\
\qquad \downarrow \ \ldots \ \downarrow D_{C_{in}} & \\
x = (x_1, \ldots, x_N) \in (\mathbb{F}_q^n)^N & x_i = D_{C_{in}}(y_i) \in \mathbb{F}_q^n \\
y' = (y'_1, \ldots, y'_N) & y'_i \in \mathbb{F}_q^k \cong \mathbb{F}_{q^k} \ \text{ s.t. } \ C_{in}(y'_i) = x_i \text{ or } y'_i = ? \\
\downarrow D_{C_{out}} & \\
m \in (\mathbb{F}_{q^k})^K \cong (\mathbb{F}_q^k)^K &
\end{array}
$$

where $y' \in (\mathbb{F}_{q^k} \cup \{?\})^N$ and **not** $y' \in (\mathbb{F}_{q^k})^N$ as in algorithm 1.

Deterministic GMD algorithm

Input: received word $y = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N$

Output: message $m \in (\mathbb{F}_q^k)^K$

1. for $1 \leq i \leq N$ do
2. $\quad x_i = D_{C_{in}}(y_i)$
3. $\quad w_i = \min(d_H(x_i, y_i), \frac{d}{2})$
4. $P = \{0,1\} \cup \{\frac{2w_1}{d}, \ldots, \frac{2w_N}{d}\}$
5. for $\theta \in P$ do
6. $\quad$ for $1 \leq i \leq N$ do
7. $\quad\quad$ if $\theta < \frac{2w_i}{d}$, set $y_i' =?$, otherwise set $y_i' = x'$ where $x_i = C_{in}(x')$
8. $\quad m_\theta = D_{C_{out}(y')}$, where $y' = (y_1', \ldots, y_N')$
9. return m_{θ^*} for $\theta^* = \arg\min_{\theta \in P} \left(d_H(C_{out} \circ C_{in}(m_\theta), y)\right)$