Reed-Muller code (1954)

- Here we view the input as a multivariate polynomial, and consider evaluations.

Defn: Let $\mathbb{F}$ be a finite field; $\ell, d \in \mathbb{N}$ & $d < |\mathbb{F}|$.

- RM code is $RM: \mathbb{F}^{\binom{\ell+d}{d}} \to \mathbb{F}^{|\mathbb{F}|^\ell}$ that maps every ℓ-variate d-deg polynomial P, over $\mathbb{F}$, to all evaluations.

Note: $d=1 \Rightarrow$ WH & $\ell=1 \Rightarrow$ RS

- Thus, $RM: \{ c_{\bar{i}} \in \mathbb{F} \mid |\bar{i}| \le d \} \mapsto \{ P(x_1, \ldots, x_\ell) := \sum_{\bar{i}} c_{\bar{i}} \cdot \bar{x}^{\bar{i}} \mid x_1, \ldots, x_\ell \in \mathbb{F} \}$.

Lemma 3: RM is an ecc of distance $1 - \frac{d}{|\mathbb{F}|}$.

Proof:

- As for RS, we have $\forall a \neq b$,
$$wt(RM(a-b)) = \Delta(RM(a), RM(b)) \cdot \underset{|\mathbb{F}|^\ell}{m}.$$

- By DeMillo et.al.'s lemma on zeros:
$$wt(RM(a-b)) / |\mathbb{F}^\ell| \ge 1 - \frac{d}{|\mathbb{F}|}.$$

□

Concatenated code (Forney 1966)

- WH has a large m, while RS uses a non-binary alphabet. We want to remove both these drawbacks.

So we first apply RS & then WH.
to spread the bits around!

Defn: Let $\mathbb{F}$ be a finite field of size q, $RS: \mathbb{F}^n \to \mathbb{F}^m$, $WH: \{0,1\}^{\lg q} \to \{0,1\}^q$.

Then the concatenated code $WH \circ RS: \{0,1\}^{n \lg q} \to \{0,1\}^{mq}$ is:

1) View RS as a code from $\{0,1\}^{n \lg q}$, & WH as a code from $\mathbb{F}$. (Using a natural binary representation of the elements in $\mathbb{F}$.)

2) $\forall x \in \{0,1\}^{n \cdot \lg q}$,

$$WH \circ RS(x) := \langle WH(RS(x)_i) \mid i \in [m] \rangle,$$

where $RS(x)_i \in \mathbb{F}$ is the ith symbol in $RS(x)$.

▷ $WH \circ RS$ is computable in time poly($|\mathbb{F}|$).

<u>Lemma 4:</u> WH∘RS is an ecc of distance $\frac{1}{2}\cdot\left(1-\frac{n-1}{m}\right)$.

<u>Proof:</u>

- Let $x \neq y \in \{0,1\}^{n \lg q}$. Then we know that the #distinct $\mathbb{F}$-elements in $RS(x), RS(y)$ is $\geqslant \left(1-\frac{n-1}{m}\right)$.
- If $x' \neq y' \in \mathbb{F}$ are in i-th place of $RS(x), RS(y)$, then $\Delta(WH(x'), WH(y')) \geqslant 1/2$.

$$\Rightarrow \Delta(WH\circ RS(x), WH\circ RS(y)) \geqslant \frac{1}{2}\cdot\left(1-\frac{n-1}{m}\right).$$

□

- By the prime number theorems, $\forall k \geqslant 2$, $\exists$ prime $p \in [k, 2k)$. Thus, we can work over the field $\mathbb{F} := \mathbb{F}_p$.

$\Rightarrow$ WH∘RS is an ecc that stretches a $\Theta(k \lg k)$-long message to length, say, $(10k\cdot 2k)$, with distance $\geqslant \frac{1}{2}\cdot\left(1-\frac{k}{10k}\right) = 0.45$.

▷ $\forall n \in \mathbb{N}$, $\exists$ poly-time computable ecc $E: \{0,1\}^n \to \{0,1\}^{20n^2}$ that can sustain 22% errors.

Efficient decoding

- Can we find the unique x given a string y' "close" to $E(x)$?

- Decoding WH is trivial: Since WH length is 2^n, we can afford to scan the full space $\{0,1\}^n$ & find the unique x from y'!

Decoding RS

- Setting: Given a list $(a_1, b_1), \dots, (a_m, b_m) \in \mathbb{F}^2$ for which $\exists$ deg-d polynomial $G: \mathbb{F} \to \mathbb{F}$ s.t. $G(a_i) = b_i$ for t of the pairs.

- Since RS has distance $(1 - \frac{d}{m})$, we are guaranteed the existence of a unique G, if $t > m - \frac{1}{2}\left(1 - \frac{d}{m}\right) \cdot m = \frac{m+d}{2}$ & $m > d$.

- Idea - If t was m then we could have simply interpolated a deg-d G from the linear system $G(a_i) = b_i$, $i \in [m]$.

In the $t < m$ case we introduce an auxiliary error-locator polynomial $\mathcal{E}(X)$ of $\deg = \frac{m-d}{2} = \#$ possible errors, & interpolate polynomials C & $\mathcal{E}$ from:

$$C(a_i) = b_i \cdot \mathcal{E}(a_i) \ , \quad \forall i \in [m],$$

where $\deg(C) = d + \frac{m-d}{2} = \frac{m+d}{2}$.

Theorem (Berlekamp-Welch, 1986): $\exists$ poly$(m, \lg|\mathbb{F}|)$-time algorithm to find G from $\{(a_i, b_i) \mid i\}$.

Proof:

- The algorithm is simply:

1) Find polynomials $C(X), \mathcal{E}(X)$ of degrees $\frac{m+d}{2}$, $\frac{m-d}{2}$ respectively s.t.

$$C(a_i) = b_i \cdot \mathcal{E}(a_i) \ , \quad \forall i \in [m].$$

2) Output $C(X)/\mathcal{E}(X)$.

- The linear system, in Step 1, has m equations & $\left(1+\frac{m+d}{2}\right)+\left(1+\frac{m-d}{2}\right)=m+2$ unknowns.

- It has a nonzero solution because we can take $G(x)\cdot\underbrace{\left(\prod_{G(a_i)\neq b_i}(x-a_i)\right)}_{E(x)}$ as $C(x)$.

- Let C & E be the solutions obtained in Step 1.

$$\Rightarrow \quad C(a_i) - G(a_i)\cdot E(a_i) = 0,$$
$$\text{for } t > \frac{m+d}{2} \text{ of the } i\text{'s}.$$

- But, $\deg\left(C(x) - G(x)\cdot E(x)\right) \leq \frac{m+d}{2} < t$

$$\Rightarrow \quad C = G\cdot E$$
$$\Rightarrow \quad C/E = G(x).$$

- Since we used deg-m polynomial arithmetic over $\mathbb{F}=\mathbb{F}_q$, it can be done in poly$(m, \lg|\mathbb{F}|)$-time. $\square$