Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 22: Majority Logic Decoding of RM Codes

October 17, 2007

Lecturer: Atri Rudra *Scribe: Sandipan Kundu*

$RM_2(t, v) \longrightarrow$ Evaluations of **v** variable polynomials of degree $\leq$ t.

$$\langle m_s \rangle_S \subseteq [v], |s| \leq t$$
$$P_{\mathbf{m}}(x_1, \ldots, x_v) = \sum_{\substack{S \subseteq [v] \\ |S| \leq t}} C_s \prod_{i \in S} X_i$$
$$RM(\mathbf{m}) = \langle P_{\mathbf{m}}(\alpha_1, \ldots, \alpha_v) \rangle_{(\alpha_1, \ldots \alpha_v) \in \mathbb{F}_2^v}$$

Claim 1: $RM_2(t, v)$ is a $[2^v, \sum_{i=0}^{t} \binom{v}{i}, 2^{v-t}]_2, t \leq v$. (Claim on linearity follows from RS codes.)
Example :
(i) $t = \frac{v}{2}, \Longrightarrow k = 2^{v-1} = \frac{n}{2}, \Longrightarrow R = \frac{1}{2}, d = 2^{\frac{v}{2}} = \sqrt{n}$
(i)$t = 1 \longrightarrow$? (Figure out which code.)

Proposition 0.1. *$RM_2(t, v)$ has distance $2^{(v-t)}$.*

Proof. Show min. weight of non-zero codeword is 2^{vt}.

1. min. wt. $\leq 2^{v-t}$
   $P(x_1, \ldots, x_v) = \prod_{i=1}^{t} x_i$
   $P(\alpha_1, \ldots, \alpha_v) = 1$, iff $\alpha_1 = \alpha_2 = \ldots, \alpha_v = 1$
   No. of such $(\alpha_1 = \alpha_2 = \ldots, \alpha_v) = 2^{v-t}$.

2. min. wt. $\geq 2^{v-t}$
   Proof by induction on v+t.
   <u>Base case</u>: $v = 1, t = 0 \Longrightarrow polynomial = 1$Implies non-zero in all positions.
   Assume true for some$v + t < b$
   Let$v + t = b$
   $$P(x_1, \ldots, x_v) = x_1 \underbrace{Q(x_2, \ldots, x_v)}_{\text{Number of var = v-1, } deg \leq t-1} + \underbrace{R(x_2, \ldots, x_v)}_{\text{No. of var = v-1, } deg \leq t}$$
   Case1 : $R(x_2, \ldots, x_v) \equiv 0$
   Set $X_1 = 1$, by induction, Q is non-zero in $\geq 2^{v-1-(t-1)} = 2^{v-t}$ position.
   Case2 : $R(x_2, \ldots, x_v) \neq 0$
   Set $X_1 \longleftarrow 1$, left with polynomial of deg $\leq t$, $v - 1$ variables.
   $\Longrightarrow$ By induction Q+R has $\geq$ left2^{v-t-1} non-zero values. $X_1 \longleftarrow$ left with R.
   By induction R is non-zero in at least 2^{v-t-1} positions.
   $\Longrightarrow$ p is non-zero $\geq 2 \cdot 2^{v-t-1}$
   $= 2^{v-t}$ positions.

$\square$

Next : Poly time unique decoding algorithm for $RM_2(t, v)$
$\longrightarrow$ can decide up to $< \frac{d}{2} = 2^{v-t-1}$ errors.

Lemma 0.2. *$\forall r \geq 1, s \subseteq [v], st|s| = r$, a polynomial, $p \in \mathbb{F}_2[x_1, \ldots, x_v]$ of degree the following is true.*

For every $\overline{b} \in \mathbb{F}_2^{v-r}$
$\sum_{a \in \mathbb{F}_2^v, a_{\bar{s}=b}} p(a) = C_s$, where $\overline{S} = [v] \backslash S$ for any $T \subseteq [v]$ and $a \in \mathbb{F}_2^v, a_T$ is the projection of a onto T.
Given received word $\overline{y} = \langle y_a \rangle_{a \in \mathbb{F}_2^v}) \leq 2^{v-t-1}$
Find P? (unique P) If we can compute all the coefficients $\{C_c\}_{S \subseteq [v], |s| \leq t}$
Fix $S \subseteq [v], |S| = t$, Compute C_S.
Problem : Donot know the actual values if $P(a)$
$\longrightarrow$ only knows y_a
$\longrightarrow$ donot know the error positions
For every $b \in \mathbb{F}_2^v, T_b \triangleq \{a \in F_2^v \mid a_{\mathbf{a}_s} = b\}, \forall b \neq b', T_b \cap T_{b'} = \emptyset$.
Call T_b to be erroneous if there exists atleast one $a \in T_b$ s.t. $y_a \neq P(a)$.
Obs: If T_b is not erroneous

$$\sum_{y_a \in T_b} y_a = \sum_{a \in T_b} P(\mathbf{a}) = C_s \tag{1}$$

The second equality is by Lemma 1.
Donot know which T_b is erroneous.

$$Total\ number\ of\ errors\ \leq 2^{v-t-1} - 1 \tag{2}$$

$$\text{Total number erroneous } T_b \leq 2^{v-t-1} \tag{3}$$

$$For \geq \frac{1}{2} \text{ fraction of } b \in \mathbb{F}_2^{v-t} \tag{4}$$

T_b is not erroneous.
$\Longrightarrow majority_{b \in \mathbb{F}_2^{v-t}} (\sum_{a \in T_b} y_a) = C_s$. Time do theis step is $= O(n^2)$. Can compute all $C_s, |S| = t$. what about $|S| < t$?.

$$R(x) \triangleq \sum_{\substack{S \subseteq [v] \\ |S|=t}} C_s \prod_{i \in S} X_i \tag{5}$$

Set $P'(x) = P(x) - R(x)$
$\mathbf{y}'_a = \langle y'_a \rangle_{a \in \mathbb{F}_2^v}$s.t.$y'_a = y_a - R(a)$
Note(1): $\Delta(\mathbf{y}', \langle P'(a)_{a \in \mathbb{F}_2^v} \rangle) < 2^{v-t-1} < \frac{2^{v-(t-1)}}{2}$

degree(P')($\in RM_2(t-1,v)$) $\leq t-1$. Reduced problem from to decoding from **y'** for $RM_2(t-1,v)$. Distance of

$$\begin{aligned} RM_2(t-1,v) &= 2^{v-(t-1)} && (6) \\ &= 2^{v-t+1} && (7) \\ &< \frac{2^{v-(t-1)}}{2} && (8) \end{aligned}$$

Implying recursion. Polynomial time computation of each step.