L19

Tuesday, October 18, 2022 10:20 AM

* Decoding of RM(r, m).

$\equiv$ successive majority decoding

* $d_{min} = 2^{m-r}$

suppose the number of error

$$t < \frac{d_{min}}{2} = 2^{m-r-1}$$

$$\vec{m} \cdot G = \vec{x} \qquad G: k \times n$$

* Each message bit is associated to one row of G, $\Rightarrow$ associated to on $S \subseteq \{0, 1, \cdots, m-1\}$ satisfying $|S| \leq r$

* Each coordinate of the codeword $\vec{x}$ is associated to a column of G $\Rightarrow$ associated to a base-2 representation b.

* Let us decode bit m_{S_0} where $|S_0| = r$.

* Because our construction is $\vec{b}$ permutation invariant, it is without loss of generality to

assume $S_0 = \{0, 1, \dots, r-1\}$.

For any $\vec{b} \triangleq \boxed{\vec{b}_{S_0^c} \cdot \vec{b}_{S_0}}$ $\Longleftarrow$ Basically we want to break $\vec{b}$ into $\vec{b}_{S_0}$ & $\vec{b}_{S_0^c}$

* Theorem: for any $|S_0| = r$, and any $\vec{b}_{S_0^c}$,

$$\sum_{\forall \vec{b}_{S_0}} x_{\vec{b}_{S_0^c} \vec{b}_{S_0}} = m_{S_0}.$$

E.g. $m = 3$, $r = 2$

$n = 2^3 = 8$, $k = \binom{3}{0} + \binom{3}{1} + \binom{3}{2} = 7$.

$d_{min} = 2^{3-2} = 2$

$2^3 = 8$

000	001	010	011	100	101	110	111	
1	1	1	1	1	1	1	1	$S = \phi$
	1		1		1		1	$S = \{0\}$
		1	1			1	1	$S = \{1\}$
				1	1	1	1	$S = \{2\}$
			1				1	$S = \{0, 1\}$
					1		1	$S = \{0, 2\}$

					1		1	$S=\{0,2\}$
						1	1	$S=\{1,2\}$

If $S=\{0,1\}$. $\vec{b}_{S_0^c}=b_2$

$b_2=0 \Rightarrow x_0+x_1+x_2+x_3=m_{\{0,1\}}$

$b_2=1 \Rightarrow x_4+x_5+x_6+x_7=m_{\{0,1\}}$.

If $S=\{0,2\}$. $\vec{b}_{S_0^c}=b_1$

$b_1=0 \Rightarrow x_0+x_1+x_4+x_5=m_{\{0,2\}}$.

$b_1=1 \Rightarrow x_2+x_3+x_6+x_7=m_{\{0,2\}}$

If $S=\{1,2\}$. $\vec{b}_{S_0^c}=b_0$

$b_0=0 \Rightarrow x_0+x_2+x_4+x_6=m_{\{1,2\}}$

$b_0=1 \Rightarrow x_1+x_3+x_5+x_7=m_{\{1,2\}}$.

---

proof: Consider any row in $G(r,m)$ with S' index, where $S'\neq S_0$.

Claim: Given any arbitrary $\vec{b}_{S_0^c}$ value.

Among all locations correspond to

$$\left\{ \vec{b} = \boxed{\vec{b}_{S_0^c} \cdot \vec{b}_{S_0}} : \forall \vec{b}_{S_0} \right\}.$$

we have an even number of them being 1.

Proof of Claim: • If $\vec{b}_{S_0^c}$ is not ~~...~~ <u>compatible</u> with $S' \setminus S_0$, then all these locations will be 0. ✓.

• If $\vec{b}_{S_0^c}$ is <u>compatible</u> with $S' \setminus S_0$.

Among 2^r possible ways to choose $\vec{b}_{S_0}$, exactly $2^{r-|S' \cap S_0|}$ of them will have the location of $\vec{b}_{S_0^c} \cdot \vec{b}_{S_0}$ being 1.

Since $|S'| \leq r = |S_0|$ and $S' \neq S_0$

$\Rightarrow |S' \cap S_0| < r$

$\Rightarrow$ the claim is proven.

Claim: However, for the row corresponding to S_0, exactly one location of $\{\vec{b}_{S_0^c} \vec{b}_{S_0} : \forall \vec{b}_{S_0}\}$ will have value 1.

Together this proves

$$\boxed{\text{Theorem: for any } |S_0| = r, \text{ and any } \vec{b}_{S_0^c}, \quad \sum_{\forall \vec{b}_{S_0}} x_{\vec{b}_{S_0^c} \vec{b}_{S_0}} = m_{S_0}.}$$

Implication #1: There are 2^{m-r} different ways of choosing $\vec{b}_{S_0^c}$, $\Rightarrow$ there ways of choosing $b_{S_0^c}$, $\Rightarrow$ there are 2^{m-r} different ways to find m_{S_0} from $\vec{x}$

Implication #2: If there are at most $t < \frac{d_{min}}{2} = \frac{2^{m-r}}{2}$ errors, then out of all 2^{m-r} ways, strictly less than half is in error.

$\Rightarrow$ strictly more than half are "correct".

Implication #3: We can take the majority vote, out of 2^{m-r} ways of evaluating $m_{S_0} = \sum_{\forall \vec{b}_{S_0}} y_{\vec{b}_{S_0^c} \vec{b}_{S_0}}$ to find m_{S_0} with <u>no error</u>.

Implication #4: Repeat the process, we can find m_S values for all

$|S| = r$ with <u>no error</u>

In practice, the computation / equation of

$$\sum_{\forall \vec{b}_{S_0}} x_{\vec{b}_{S_0} \vec{b}_{S_0^c}} = 0 \quad \text{for all } \vec{b}_{S_0^c}$$

can be written as a "parity-check" matrix

$$H_{S_0} = \overbrace{\boxed{}}^{n=2^m} \left.\vphantom{\begin{matrix}a\\b\\c\\d\end{matrix}}\right\} 2^{m-r}$$

one row for each $\vec{b}_{S_0^c}$ value.

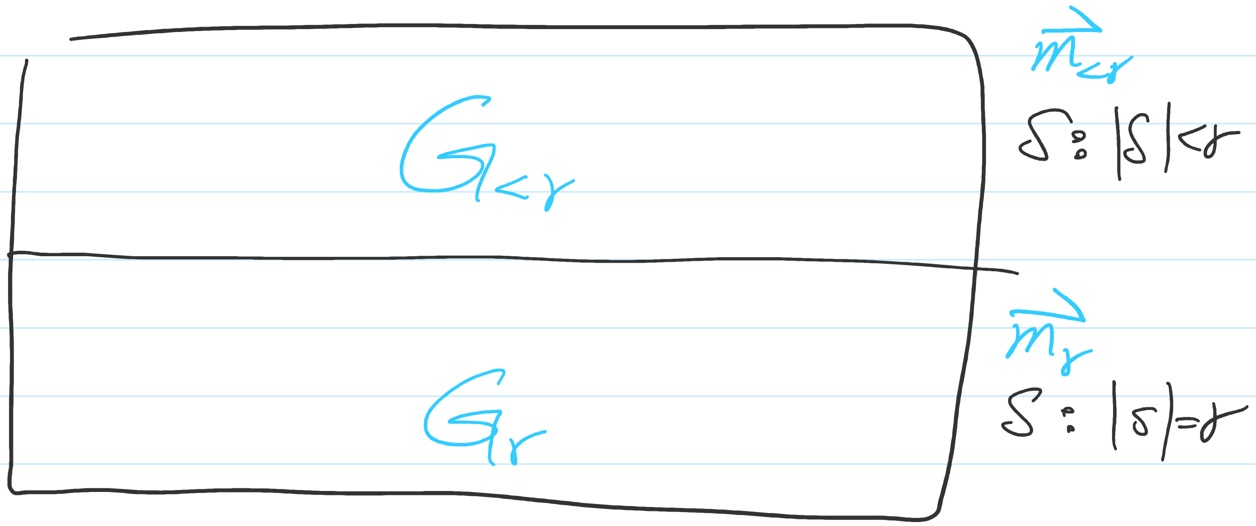
then $\hat{m}_{S_0} = \text{Majority}(H_{S_0} \cdot \vec{y})$

How about those m_S with $|S| < r$?

Ans: Successive decoding.

First solve m_S for all $|S| = r$.

then remove the <u>impact</u> of those m_S.



$$y' = y - \vec{m}_r \cdot G_r$$

Since $\vec{m}_r$ are free-of-error. || assuming $t < 2^{m-r}$

$\Rightarrow$ the same $t < \frac{2^{m-r}}{2}$ errors remain in y'. but $G_{<r}$ is essentially $G(r-1, m)$, another RM code.

the new code has $d_{min} = 2^{m-r+1}$ which is larger than $2 \cdot t$ again.

$\Rightarrow$ We can then repeat the process to decode m_S w. $|S| = r-1$.

In practice

$$H_S = \left.\overbrace{\begin{bmatrix} \quad & \quad & \quad & \quad \\ & & & \\ & & & \end{bmatrix}}^{2^m}\right\} 2^{m-|S|}$$

$$\hat{m}_S = \text{Majority}\left(\left[H_S \underline{\left(y' - (m_r G_r) \right)} \right]^T \right)$$

iterative/successive decoding.

---

* Iteratively applying this successive decoding for $|S| = r, r-1, r-2, \ldots, 1$

$\Rightarrow$ Perfect decoding if $t < 2^{m-r}/2$

* If $t \geq 2^{m-r}/2$, then sometimes the decoding may fail.

say for some $|S_0| = r$, if the t errors are fully spread

$\geq 2^{m-r}/2$

the t errors are fully spread $\geq 2^{m-r}/2$

in all $\sum_{\forall \vec{b}_{S_0}} x_{\vec{b}_{S_0} \vec{b}_{S_0^c}} = 0$ for all $\vec{b}_{S_0^c}$

then the majority decoding fails for that particular m_{S_0}.

$\Rightarrow$ The error will <u>propagate</u> under successive decoding

---

However, sometimes decoding can still be successful.

For example $m=5$, $r=1$

$d_{min} = 2^{5-1} = 16$

$t < d_{min}/2 = 8 \Rightarrow$ successful decoding is guaranteed.

What if $t=8$ and the 8 error locations are

① 0 0 0 0 0

② 0 0 0 0 1

③ 0 0 0 1 0

④ 0 0 1 0 1

⑤ 0 1 0 1 0

⑥ 1 0 1 0 1

⑦ arbitrary / does not impact the example

⑧ arbitrary

For any $|S_0| = r = 1 \Rightarrow |S_0^c| = 4$.

If $S_0^c = \{0,1,2,3\}$ then $x_④$ and $x_⑥$ participate in the same equation when $\vec{b}_{S_0^c} = -0101$

If $S_0^c = \{0,1,2,4\}$. then $x_③$ and $x_⑤$ participate in the same equation when $\vec{b}_{S_0^c} = 0-010$

If $S_0^c = \{0,1,3,4\}$, then $x_⑤$ and $x_④$ participate in the same equation when $\vec{b}_{S_0^c} = 00-01$

If $S_0^c = \{0,2,3,4\}$. then $x_①$ and $x_③$

participate in the same equation when

$\vec{b}_{S_6^c} = 000-0$

If $S_6^c = \{1,2,3,4\}$, then $x_{①}$ and $x_{②}$

participate in the same equation when

$\vec{b}_{S_6^c} = 0000-$

$\Longrightarrow$ Majority decoding is successful

for $|S|=1$. ✓

We have the first example that

decoding beyond $\lfloor \frac{d_{min}}{2} \rfloor$ is sometimes

possible.