6.440 Essential Coding Theory Spring 2013

Lecture 7 - February 27, 2013

Lecturer: Madhu Sudan *Scribe: Pasin Manurangsi*

1 Overview

This lecture includes the following topics.

- Wozencraft Enzemble of Codes
- BCH Codes
- Working towards explicit answer of Binary Codes (Forney codes and Justesen Codes)

2 Finite Field

Recall from last time that three different ways that we can represent finite filed $\mathbb{F}_{p^t}$ are

1. Via Polynomials : $\mathbb{F}_{p^t} \cong \mathbb{F}_p[x]/q$ where $q \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree t.
2. Via Vector Space : $\mathbb{F}_{p^t} \cong \mathbb{F}_p^t$, a linear isomorphism. That is, $\beta \in \mathbb{F}_{p^t}$, $\beta \mapsto V_\beta$, a vector in $\mathbb{F}_p^t$. In this isomorphism, we have $V_\beta + \gamma V_\beta = V_{\beta+\gamma\beta}$ where $\alpha, beta \in \mathbb{F}_{p^t}$ and $\gamma \in \mathbb{F}_p$.
3. Via Matrices : There exists a map from $\mathbb{F}_{p^t}$ to $\mathbb{F}_p^{t\times t}$ which each element of $\mathbb{F}_{p^t}$ gets represented by a $t \times t$ matrix. That is $\alpha \mapsto M_\alpha$. In this isomorphism, $M_{\alpha+\beta} = M_\alpha + M_\beta$ and $M_\alpha M_\beta = M_{\alpha\beta}$.

The second and third representations will be mainly used in this lecture.

3 Wozencraft Ensemble

3.1 Overview

Wozencraft ensemble is a collection of codes, all with rates $\frac{1}{2}$ and most of them have a good distance.

Definition 1 *Wozencraft Ensemble is a collection of codes* $\{C_\alpha\}_\alpha$ *where* $C_\alpha : m \to (m, M_\alpha m)$ *for all* $\mathbb{F}_{2^k}$ *for each* $\alpha \in \mathbb{F}_{2^k}$.

We can see that each code C_α is a $[2k, k, d]_2$ code where d varies from code to code and the generator matrix for C_α is $[I_k|M_\alpha]$. In the next section, we will next show the bound for d.

3.2 Properties

We begin by proving the following claim.

Claim 2 *For any $\langle a, b\rangle \in \mathbb{F}_2^{2k}$ such that $a \neq 0$, there exists at most one $\alpha \in \mathbb{F}_{2^k}$ such that $\langle v_a, v_b\rangle \in C_\alpha$.*

Proof If $\langle v_a, v_b\rangle$ is an element of C_α, then there exists $m \in \mathbb{F}_2^k$ such that $mM_\alpha = v_a M_\alpha = v_b$. This implies that $\alpha = ba^{-1}$. ■

We will next obtain the bound for distances of codes.

Claim 3 *The number of codes C_α of distance $\geq d$ is at least $2^k - Vol(d-1, n)$.*

Proof First, recall that since C_α is a linear code, we have $\triangle(C_\alpha) = \min_{c\in C, c\neq 0}\{wt(x)\}$. As a result, C_α is of distance less than d if and only if there exists $w \in \mathbb{F}_2^{2k}$ such that $w \neq 0, wt(w) \leq d-1$ and $w \in C_\alpha$.

From Claim 2, we have, for any $w \in \mathbb{F}_2^{2k}$ such that $wt(w) < d$, w belongs to at most one C_α; there are $Vol(d-1, n)$ such w s. As a result, there are at least $2^k - Vol(d-1, n)$ such C_α s that are of distance at least d. ■

Observation 4 *If $Vol(d-1, n) < 2^k$, Claim 3 also implies that at least one of the code has distance at least d. Since $Vol(d-1, n) \approx 2^{nH(\frac{d}{n})}$, the inequality can be translated approximately to $1 - R > H(\delta)$. This is approximately the Gilbert-Varshamov bound.*

3.3 Exercise

The following exercises are intended for students to test their thorough understanding of Wozencraft Ensemble.

1. Entend Wozencraft to codes of rate $\frac{1}{l}$ for a positive integer l.
2. Entend Wozencraft to codes of rate $1 - \frac{1}{l}$ for a positive integer l.
3. Let us consider ensemble $\{C_\alpha^*\}$ where $C_\alpha^* : m \mapsto (m, m + \alpha)$. Are these good codes? Why or why not?

4 Binary Linear Codes from Reed-Solomon Codes

Let $n = q = 2^l$. Consider any Reed-Solomon $[n, n-d, d]_q$ code $C \subseteq \mathbb{F}_q^n$.

Define a map from $\mathbb{F}_q^n \to F_q^{nl}$ by $w \to v$ by writing out the binary expansion of each coordinate of w. Suppose that C gets mapped to $\tilde{C} \subseteq \mathbb{F}_q^{nl}$. It is easy to see that $\tilde{C}$ is a $[nl, (n-d)l, d]_2 = [n \log n, (n-d) \log n, d]_2$ code.

Let $N = n \log n$. The code $\tilde{C}$ above is approximately a $[N, N - d \log N, d]_2$ code. In the case that d is a constant and N is large, it is not hard to check that this code approximately the Gilbert-Varshamov bound.

5 BCH Codes

5.1 Overview and Construction

Named after Bose, Chaudhuri and Hocquenghem, BCH codes achieve $[n, n - \lceil \frac{d-2}{2} \log n - 1 \rceil, d]_2$. The idea is also to expanding Reed-Solomon code.

In order to construct, we start by a Reed-Solomon code $C \subseteq \mathbb{F}_2^q$ which is a $[n, n-d, d]_q$ code with $n = q = 2^l$. Let $C_{BCH} = C \cap \mathbb{F}_2^q$.

It is not hard to see that linearlity holds for C_{BCH} and the distance is at least d. Next, we will show that the dimension is at least $n - \lceil (d-2) \log n \rceil - 1$.

The parity check matrix for C is shown below.

$$H = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{d-2} \end{bmatrix}$$

We can also conclude that the parity check matrix is:

$$H_{BCH} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{d-2} \end{bmatrix}$$

where $V_a \in \mathbb{F}_2^l$ is a binary representation of a.

We have

$$\begin{aligned} \text{Dimension} &\geq n - \text{number of columns} \\ &= n - \lceil (d-2) \log n \rceil - 1. \end{aligned}$$

This is still not the bound that we promised. In order to get that bound, first observe the following which is easily check by binomial theorem.

Observation 5 *Over* $\mathbb{F}_{p^t}$, $(x+y)^p = x^p + y^p$.

Next, we will show that we can ignore the even power columns in the matrix H_{BCH}. This is because

$$\begin{aligned}\sum x_i \alpha_i^{2j} &= \sum x_i^{2j} x^{2j} \\ \text{(From Observation 5)} &= (\sum x_i^j y_i^j)^2.\end{aligned}$$

As a result, the parity check matrix below is enough.

$$H'_{BCH} = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^3 & \cdots & \alpha_1^{2\lceil \frac{d-2}{2} \rceil - 1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^3 & \cdots & \alpha_n^{2\lceil \frac{d-2}{2} \rceil - 1} \end{bmatrix}$$

As a result, we get a code C_{BCH} with $k \geq n - \lceil \frac{d-2}{2} \rceil \log n - 1$ as intended.

5.2 Comparison to Hamming Bound and Gilbert-Varsharmov Bound

Now, we will compare BCH codes to the Hamming Bound and Gilbert-Varsharmov Bound when d is small.

Let $Vol_q(d,n) \triangleq$ Volume of ball of radius d in $|\Sigma|^n$ where $|\Sigma| = q$. The Hamming Bound and G-V Bound can be written as

- Hamming : If C is $(n,k,d)_q$ code then, $q^n \geq q^k Vol_q(\frac{d-1}{2}, n)$.
- G-V : If $q^n \leq q^k Vol(d-1,n)$, then there exists a code $(n,k,d)_q$.

As we have shown before, $Vol_q(d,n) \approx \binom{n}{d}(q+1)^d \approx \left(\frac{en}{d}\right)^d (q-1)^d$. Using this, the bounds become:

- Hamming : $n \geq k + \frac{d-1}{2}\log n - \frac{d-1}{2}\log d$
- G-V : $n \leq k + d\log n - d\log d$

This means that if $d = o(n^{1/2-\epsilon})$, then BCH is asymtotically better than G-V or random code.

6 Forney Codes

Now, we turn to Forney codes which use concatenating technique.

Suppose that we have C_1, a $[n_1, k_1, d_1]_q$ code and C_2, a $[n_2, k_2, d_2]$ code where $n_1 = q = 2^{k_2}$. We can find define a code $C_1 \circ C_2$ by a composition of the

C_1 and C_2. In this way, it is not hard to see that $[n_1 n_2, k_1 k_2, d_1 d_2]$.

This impliess that if C_1 is of rate R_1 and relative distance δ_1 and C_1 is of rate R_2 and relative distance δ_2, then $C_1 \circ C_2$ is of rate $R_1 R_2$ and relative distance $\delta_1 \delta_2$. As a result, if C_1 and C_2 are asymtotically good then so is C_3.

We can use Reed-Soloman code as C_1 and G-V as C_2. Even though C_2 cannot be found in polynomial time of the size of C_2, it can be found in polynomial time of the size of C_1 since $n_1 = q = 2^{k_2}$. Thus, the whole code can be computed in polynomial time of q.

However, this is still somewhat not explicit enough in the sense that given i, j we cannot find the i, j entry of the generator matrix G fast enough.

7 Justensen Codes

Consider the Forney code. In the second step, we use all the same codes. Why don't we use different codes?

If in the second step, we use different codes and we can gaurantee that most of these codes have high distances, then we get a code with high distance. Yes, we can use Wozencraft ensemble in the second step! One advantage of using this is that we do not need to find a good code for the second step but instead just use Wozencraft ensemble which can be found in a better runtime.