Combinatorics, 2017 Fall, USTC

Week 13 Note 1

2017.12.12, Tuesday

1 Reed-Muller codes(RM codes)

$m > 0$, q is a prime power, $0 \leq t < q$, $k = \binom{m+t}{t}$, $n = q^m$. Let $\alpha_1, \cdots, \alpha_n$ be distinct points in $\mathbb{F}_q^m$.

Messages: $\omega = (\omega_1, \ldots, \omega_k) \in \mathbb{F}_q^k$. List and order all monomials $x_1^{t_1} x_2^{t_2} \cdots x_m^{t_m}$ with $t_1 + t_2 + \cdots + t_m \leq t$. We have $\binom{m+t}{t}$ such monomials.

Then associate message ω with a multivariable polynomial $P_\omega(x_1, x_2, \ldots x_m)$ =sum of monomials of degree at most t and coefficients ω_i.

Let $X_\omega = (P_\omega(\alpha_1), \ldots, P_\omega(\alpha_n))$, and $\mathcal{C} = \{X_\omega : \omega \in \mathbb{F}_q^k\}$.

Note: If we let

$$B = \{x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m} : e_1 + \ldots + e_m \leq t\},$$

then it's easy to see that $\mathcal{C}$ is spanned by $\{(f(\alpha_1), \ldots, f(\alpha_n)) : f \in B\}$. And for any $f \neq f' \in B$, we can check $(f(\alpha_1), \ldots, f(\alpha_n)) \neq (f'(\alpha_1), \ldots, f'(\alpha_n))$, and $\{(f(\alpha_1), \ldots, f(\alpha_n)) : f \in B\}$ is linearly independent over $\mathbb{F}_q$(**see GTM84, p.143, lemma 1**)

Therefore, $\mathcal{C}$ is a q-ary code of length $n = q^m$ and size $q^k = q^{\binom{m+t}{t}}$.

Since a multivariable polynomial of degree t can have at most tq^{m-1} roots in $\mathbb{F}_q^m$, we have $dist(\mathcal{C}) \geq q^m - tq^{m-1} = n(1 - \frac{t}{q})$.

• Binary RM codes

$q = 2$, $t = 1$, $n = 2^m$, $\mathcal{C} = 2^{m+1}$, $dist(\mathcal{C}) = \frac{n}{2}$. It's a Hadamard code from H-matrix of order 2^m.

2 Some bounds of the size of a code $\mathcal{C}$

Question: Given minimum distance d, how large can $|\mathcal{C}|$ be?

Let $|A| = q$, we have $|B_t(x)| = |B_t(y)|$ for any $x \neq y \in A^n$. In fact

$$|B_t(x)| = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j.$$

Denote $V(n,t) = |B_t(x)|$.

Theorem 1 (**Gilbert-Varshmov Bound**). *Let $A_q(n,d)$ be the maximum possible size of a q-ary code $\mathcal{C}$ with length n and $dist(\mathcal{C}) = d$. Then*

$$A_q(n,d) \geq \frac{q^n}{V(n,d-1)}.$$

Proof. *Let $\mathcal{C}$ be a code having maximum size $A_q(n,d)$. Then $\forall x \in A^n$, $\exists$ at least one codeword $C_x \in \mathcal{C}$ such that $d_H(x, C_x) \leq d-1$, since otherwise we can add x to $\mathcal{C}$, i.e. $\{x\} \cup \mathcal{C}$ is also a code of minimum distance d, which contradicts to the maximality of $\mathcal{C}$. Hence $A^n = \bigcup_{c \in \mathcal{C}} B_{d-1}(c)$, then*

$$q^n = |A^n| \leq \sum_{c \in \mathcal{C}} |B_{d-1}(c)| = |\mathcal{C}| \cdot V(n,d-1) \Longrightarrow |\mathcal{C}| \geq \frac{q^n}{V(n,d-1)}. \quad \square$$

Theorem 2 (**Hamming Bound**). *$A_q(n,d) \leq \frac{q^n}{V(n,t)}$, where $2t+1 \leq d$.*

Proof. *By the fact that $B_t(x) \cap B_t(y) = \emptyset$ for all $x \neq y \in \mathcal{C}$.* $\square$

Lemma 3. *If $x_1, \ldots, x_m \in \mathbb{R}^n$ are nonzero and satisfy $< x_i, x_j > \leq 0$ for all $i \neq j$, then $m \leq 2n$.*

Proof. *See the reference book.* $\square$

Theorem 4 (**Plotkin Bound**). *If $\mathcal{C} \subseteq \{0,1\}^n$, $dist(\mathcal{C}) = d$, and $2d \leq n$, then $|\mathcal{C}| \leq d2^{n-2d+2}$.*

Proof. *Firstly, consider the case $2d = n$. Let $C_1, \ldots, C_m$ be the codewords of $\mathcal{C}$. For each $i \in [m]$, let x_i be the vector in $\mathbb{R}^n$ obtained from C_i by changing $0 \to 1$ and $1 \to -1$. Then $< x_i, x_j > \leq n - 2d = 0$, $\forall i \neq j$. By **Lemma 3**, we have $|\mathcal{C}| = m \leq 2n = 4d = d2^{n-2d+2}$.*

Secondly, consider the case $n > 2d$. Write $n = 2d + k$. Consider the first k coordinates of $\mathcal{C}$, and group the codewords together if their first k coordinates are the same. By average principle, there exists a group of codewords of size$\geq \frac{|\mathcal{C}|}{2^k}$. By deleting the first k coordinates of this group, we obtain a set $\mathcal{C}' \subseteq \{0,1\}^{2d}$ of size $|\mathcal{C}'| \geq \frac{|\mathcal{C}|}{2^k}$, and minimum distance d. By the first case, $|\mathcal{C}'| \leq 4d$, we have $|\mathcal{C}| \leq |\mathcal{C}'| \cdot 2^k \leq 4d \cdot 2^{n-2d} = d2^{n-2d+2}$. $\square$

Note: For the case $2d > n$, see ***Fundamentals of Error-Correcting Codes*(p.58)**.

3 Binary Linear Codes

If $\mathcal{C} \subseteq \{0,1\}^n$ forms a subspace of $\mathbb{F}_2^n$ over $\mathbb{F}_2$(i.e. if $x, y \in \mathcal{C}$, then $x + y \in \mathcal{C}$), then $\mathcal{C}$ is called a **linear code**.

Note:

(1) Reed-Solomon codes and Reed-Muller codes are linear codes over $\mathbb{F}_q$.

(2) Linear codes that achieve Singleton's Bound are called **MDS**(maximum distance separable) codes.

Suppose $\dim \mathcal{C} = k$, $|\mathcal{C}| = 2^k$. k basis vectors (regard them as row vectors) of $\mathcal{C}$ form a $k \times n$ matrix G, which is called the **generating matrix** of $\mathcal{C}$, i.e.

$$\mathcal{C} = \{x^{\mathrm{T}} G \in \mathbb{F}_2^n : \ x \in \mathbb{F}_2^k\}.$$

The **dual code** $\mathcal{C}^{\perp} = \{y \in \mathbb{F}_2^n : \ < x, y >= 0, \text{ for all } x \in \mathcal{C}\}$.
Let H be the $(n-k) \times n$ generating matrix of $\mathcal{C}^{\perp}$, then H is called the **parity check matrix** of $\mathcal{C}$. It's easy to see $\mathcal{C} = \{x \in \mathbb{F}_2^n : \ Hx = 0\}$.

• **Syndrome decoding:** send a message $u \in \mathbb{F}_2^k$, first encode u to $x = u^{\mathrm{T}} G$ and send x. Suppose x' is received, and $d_H(x, x') \leq t$. How to find this x with $Hx = 0$? It is equivalent to finding a unique vector $a \in B_t(0) \subset \mathbb{F}_2^n$ for which $Ha = Hx'$, then $x = x' + a$ since $H(x' + a) = 0$.

The **weight** $w(x)$ of a vector x is #of nonzero coordinates of x. For a code $\mathcal{C}$, let $w(\mathcal{C}) = \min\{w(x) : \ x \in \mathcal{C}, x \neq 0\}$.

Fact: If $\mathcal{C}$ is a binary linear code, then $dist(\mathcal{C}) = w(\mathcal{C})$.

Proof. *$\forall x \neq y \in \mathcal{C}$, $d_H(x, y) = w(x + y) \geq w(\mathcal{C})$. $\Longrightarrow dist(\mathcal{C}) \geq w(\mathcal{C})$. Let $0 \neq z \in \mathcal{C}$, s.t. $w(z) = w(\mathcal{C})$, then $w(\mathcal{C}) = w(z) = d_H(z, 0) \geq dist(\mathcal{C})$.* □

Theorem 5. *Let $\mathcal{C}$ be a binary linear code with parity check matrix H. Then $dist(\mathcal{C}) = d$ if and only if every set of $d-1$ columns of H are linearly independent, but some d columns are linearly dependent.*

Proof. *$dist(\mathcal{C}) = w(\mathcal{C})$.*

Since $x \in \mathcal{C}$ if and only if $Hx = 0$, if $x \neq 0$, this means the columns of H corresponding to the 1-positions of x are linearly dependent. So if $dist(\mathcal{C}) = d$, then exists d columns of H are linearly dependent, since $\mathcal{C}$ has a codeword of weight d. But all $d-1$ columns of H are linearly independent since $\mathcal{C}$ doesn't have a codeword of weight $d-1$. □

Theorem 6. *A binary linear code $\mathcal{C} \subseteq \{0,1\}^n$ of dimension k and minimum distance d exists provided that*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} < 2^{n-k}.$$

Proof. *Construct an* $(n-k) \times n$ *matrix* H *s.t no* $d-1$ *columns are linearly dependent.*

Choose successive columns so that each new columns is not a linear combination of any $d-2$ *or fewer previous columns. If we try to choose the* i^{th} *column, then vectors of length* $n-k$ *which can't be chosen is at most* $N(i) = \sum_{j=0}^{d-2} \binom{i-1}{j}$. *So if* $N(i) < 2^{n-k}$, *then an* i^{th} *can be added to the matrix. Thus if* $N(n) < 2^{n-k}$, *then we can obtain a matrix having* n *columns.* □