LECTURE 3: CODE CONSTRUCTIONS AND BOUNDS ON CODES

ELISA LORENZO GARCÍA

Contents

1. Code Constructions 1
1.1. Puncturing (or restricted to $\{1,...,n\}/P$) 1
1.2. Extended code 1
1.3. Shortened code 1
1.4. Augmentation code 2
1.5. Direct Sum 2
1.6. Juxtaposition 2
1.7. Plotkin or $(u \mid u+v)$ 2
1.8. The product code 2
1.9. Binary Reed-Muller $RM_2(r,m)$ with $0 \leq r \leq m$. 2
2. Bounds 2
2.1. Singleton bound 2
2.2. Griesmer Bound 2
2.3. Plotkin 3
2.4. Hamming bound 3
2.5. Gilbert bound 3
2.6. Varshamov bound 3
3. Exercises 4

1. Code Constructions

1.1. **Puncturing (or restricted to $\{1,...,n\}/P$).** deleting one or more fixed coordinates $P \subseteq \{1,...,n\}$.

C_P is an $[n-p, k_p, d_p]$-code with $d-p \leq d_P \leq d$ and $k-p \leq k_p \leq k$. If $p < d$ then $k_p = k$.

Example 1.1. $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ is a $[4,3,1]$-code over $\mathbb{F}_2$. We take $P = \{4\}$, then $G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ is a $[3,2,1]$-code.

1.2. **Extended code.** Let us start with C an $[n,k,d]$-code and $v \in \mathbb{F}_q^n$. Then $C^e(v) \subseteq \mathbb{F}_q^{n+1}$ where $c_{n+1} = -\sum v_i c_i$. We get an $[n+1, k, d_e]$-code with $d \leq d_e \leq d+1$.

1.3. **Shortened code.** C, $[n,k,d]$, $S \subseteq \{1,...,n\}$. $C(S) = \{c \in C | c_i = 0 \forall i \in S\}$ and we define by puncturing $C^S = (C(S))_S$. Parameters $[n-s, k_S, d_S]$ with $k-s \leq k_S \leq k$ and $d \leq d_s$.

1.4. **Augmentation code.** C, $[n,k,d]$ and $v \in \mathbb{F}_q^n$.

$$C^a(v) := \{\alpha v + c \mid \alpha \in \mathbb{F}_q, c \in C\}$$

If $v \notin C$ and $w = w(v)$, then $min\{d-w, w\} \leq d(C^a(v)) \leq min\{d, w\}$. In particular $d(C^a(v)) = w$ if $w \leq d/2$

Proposition 1.2. *If we have a code with parameters $[n,k,d]$ with $k \geq 2$ and $n > d \geq 2$ then there exist codes with $[n+1,k,d]$, $[n-1,k-1,d]$, $[n-1,k,d-1]$, $[n,k-1,d]$ and $[n,k,d-1]$.*

1.5. **Direct Sum.** $C_1 \oplus C_2$ with $[n_1+n_2, k_1+k_2, d]$ with $d = min\{d_1, d_2\}$.

1.6. **Juxtaposition.** $G = (G_1 \mid G_2)$ with the same k and $[n_1+n_2, k, d \geq d_1+d_2]$.

1.7. **Plotkin or $(u \mid u+v)$.** $\{(u \mid u+v) \mid u \in C_1, v \in C_2\}$ with same n and $[2n, k_1+k_2, d = min\{2d_1, d_2\}]$.

1.8. **The product code.** $C_1 \otimes C_2$ with $[n_1 n_2, k_1 k_2, d_1 d_2]$

1.9. **Binary Reed-Muller $RM_2(r,m)$ with $0 \leq r \leq m$.** $RM_2(0,m)$ is the repetition code of length 2^m and parameters $[2^m, 1, 2^m]$.
$RM_2(m,m) = \mathbb{F}_2^m$ with $[m,m,1]$.
$RM_2(r+1, m+1)$ is the $(u \mid u+v)$ construction with $RM_2(r+1,m)$ and $RM_2(r,m)$.
$RM_2(r,m)$ has $n = 2^m$, $k = \sum_{i=0}^{r} \binom{m}{i}$ and $d = 2^{m-r}$ and the dual is $RM_2(m-r-1, m)$.

2. Bounds

See the websites: http://www.codetables.de/ and http://codes.se/bounds/.

The smallest case we don't know: binary linear code with $n = 32$, $k = 14$, we have one with $d = 8$, is there anyone with $d = 9$? this would be the maximun.

2.1. **Singleton bound.**

$$d \leq n - k + 1$$

Proof. $rk\, H \leq n-k$ and $rk\, H \geq d-1$. □

$s = n+1-k-d$ is called the Singleton defect or the genus of the code. If $s = 0$, then C is called a maximum distance separable code (MDS). Or almost MDS if genus= 1.

Definition 2.1. Let q be a fixed power of a prime. $\mathcal{C} = \{C_i\}_{i=1}^{\infty}$ a sequence of $\mathbb{F}_q$-linear codes with parameters $[n_i, k_i, d_i]$ is called asymptotic, if $\lim_{i\to\infty} n_i = \infty$ and $R(\mathcal{C}) = \lim_{i\to\infty} \frac{k_i}{n_i}$ and $\delta(\mathcal{C}) = \lim_{i\to\infty} \frac{d_i}{n_i}$ exist. It's good if both are positive.

Asymptotic bound: $R(\mathcal{C}) + \delta(\mathcal{C}) \leq 1$

2.2. **Griesmer Bound.**

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$$

Proof. See exercise 3.3. □

2.3. **Plotkin.** C is an $[n, M, d]$ code over $\mathbb{F}_q$ such that $qd > (q-1)n$. Then $M \leq \lfloor \frac{qd}{qd-(q-1)n} \rfloor$.

Equality holds iff C is equidistant code of minimum distance d with $M(q-1)dn = (M-1)q$.

Proof. We count in two different ways:

$$M(M-1)d \leq S = \sum_{x \in C} \sum_{y \in C} d(x,y) \leq n \frac{q-1}{q} M^2.$$

Last inequality a bit more difficult. □

Asymptotic If $\delta(\mathcal{C}) \leq \frac{q-1}{q}$ then $R(\mathcal{C}) + \frac{q}{q-1}\delta(\mathcal{C}) \leq 1$.

2.4. **Hamming bound.** $A_q(n,d) = max\#C/\mathbb{F}_q$ with fixed n and d. $B_q(n,d)$ same thing but linear. Then

$$B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{V_q(n,t)}$$

with $t = \lfloor \frac{d-1}{2} \rfloor$ and $V_q(n,t) = \#B_t(x) = \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$.

Asymptotic bound: $R(\mathcal{C}) \leq 1 - H_q(\delta(\mathcal{C})/2)$ with $H_q(x) = log_q \frac{(q-1)^x}{x^x(1-x)^{1-x}}$.

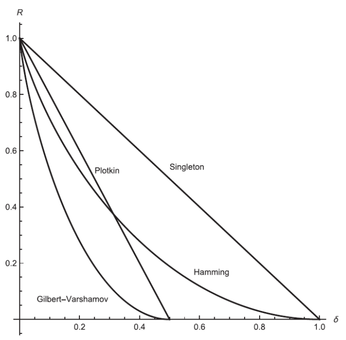
2.5. **Gilbert bound.** $a_q(n,d) = log_q A_q(n,d) \geq n - log_q V_q(n, d-1)$

Proof. Again, looking at the balls the result follows. □

2.6. **Varshamov bound.** $b_q(n,d) = log_q B_q(n,d) \geq n - \lceil log_q V_q(n,d-1) \rceil$

Proof. Again, looking at the balls the result follows. □

Asymptotic: There exists a good $\mathcal{C}$ such that $R(\mathcal{C}) = 1 - H_q(\delta(\mathcal{C}))$.



Example 2.2. Let us take $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$ over $\mathbb{F}_5$. We have $q = 5$, $n = 5$, $k = 2$, $d = 4$, $A_0 = 1$, $A_1 = A_2 = A_3 = 0$, $A_4 = 20$ and $A_5 = 4$.

Singleton bound: $4 \leq 5 - 2 + 1$ then genus 0 and MDS.

Griesmer bound: $5 \geq \lceil \frac{4}{1} \rceil + \lceil \frac{4}{5} \rceil = 5$

Plotkin bound: $M = 5^2 \leq \lfloor \frac{5^4}{5 \cdot 4 - 4 \cdot 5}$. Condition not hold!

Hamming bound: $5^2 \leq B_5(5,4) \leq A_5(5,4) \leq \frac{5^5}{V_5(5,1)}$ where $V_5(5,1) = 1 + 5 \cdot 4$.

Gilbert bound: $2 \leq a_5(5,4) \geq 5 - log_5 V_5(5,3) = 5 - log_5(1 + 5 \cdot 4 + 10 \cdot 4^2 + 10 \cdot 4^3) = 1, ...$

3. Exercises

Exercise 3.1. Compute the parameters of the following codes:

(1) Puncturing (or restricted to $\{1, ..., n\}/P$) deleting one or more fixed coordinates $P \subseteq \{1, ..., n\}$. C_P is an $[n-p, k_p, d_p]$-code with $d-p \leq d_P \leq d$ and $k-p \leq k_p \leq k$. If $p < d$ then $k_p = k$.

(2) Extended code Let C be an $[n, k, d]$-code and $v \in \mathbb{F}_q^n$. Then $C^e(v) \subseteq \mathbb{F}_q^{n+1}$ where $c_{n+1} = -\sum v_i c_i$. We get an $[n+1, k, d_e]$-code with $d \leq d_e \leq d+1$.

(3) Direct Sum $C_1 \oplus C_2$ with $[n_1 + n_2, k_1 + k_2, d]$ and $d = min\{d_1, d_2\}$.

(4) Juxtaposition $G = (G_1 \mid G_2)$ with the same k and $[n_1 + n_2, k, d \geq d_1 + d_2]$.

`ex:vandermonde`

Exercise 3.2. Let $n \leq q$. Let $a = (a_1, .., a_n)$ be an n-tuple of mutually distinct elements of $\mathbb{F}_q$. Let k be an integer $0 \leq k \leq n$. Define

$$G_k(a) = \begin{pmatrix} 1 & ... & 1 \\ a_1 & ... & a_n \\ ... & ... & ... \\ a_1^{k-1} & ... & a_n^{k-1} \end{pmatrix}.$$

The code with generator matrix $G_k(a)$ is a MDS code.

`ex:Griesmer`

Exercise 3.3. Prove the Griesmer bound by induction on k and by considering the puntured code C_P with $P = \mathrm{supp}(c)$ for a $c \in C$ with $w(c) = d$.

Elisa Lorenzo García, Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.

Email address: elisa.lorenzogarcia@univ-rennes1.fr