Coding Theory

(Bounds on Code Parameters)

Lector: Nikolai L. Manev

Institute of Mathematics and Informatics, Sofia, Bulgaria

Modified linear codes

- *Extending*: Increasing the length of (n, M) code by adding an additional redundant coordinates without changing the number of codewords:

$$\widehat{\mathcal{C}} \stackrel{\text{def}}{=} \{(c_0, c_1 \ldots, c_n) \mid (c_1 \ldots, c_n) \in \mathcal{C},\ c_0 + \cdots + c_n = 0\}$$

For linear codes this operation corresponds to adding a column to G, and respectively, column and row to the parity-check matrix:

$$\widehat{\mathbf{H}}_m = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & & & & \\ \vdots & & & \mathbf{H}_m & \\ 0 & & & & \end{pmatrix}.$$

Definition. The code generating by $\widehat{\mathbf{H}}_m$ is called *first-order Reed-Muller code*, written $\mathcal{R}(1, m)$.

Modified linear codes 2

- *Puncturing*: Decreasing the length of the code by deleting one of its parity-check positions. The resulting code is $(n-1, M)$ with minimum distance at least $d-1$. For linear codes the operation corresponds to deleting such a column of $\mathbf{G}$ that its rank not to be decreased. The effect on $\mathbf{H}$ is deleting a column and a row.

Modified linear codes 2

- *Puncturing*: Decreasing the length of the code by deleting one of its parity-check positions. The resulting code is $(n-1, M)$ with minimum distance at least $d-1$. For linear codes the operation corresponds to deleting such a column of $\mathbf{G}$ that its rank not to be decreased. The effect on $\mathbf{H}$ is deleting a column and a row.
- *Augmenting*: A $[n,k]_q$ code is augmented by adding new codewords to become $[n,k+1]_q$ code. The operation is carried out by adding a new row (linearly independent from the others) to $\mathbf{G}$, and by deleting a row in $\mathbf{H}$. If all-one vector $\mathbf{1} \notin \mathcal{C}$, a binary code $\mathcal{C}$ is often augmented to $\tilde{\mathcal{C}} = \mathcal{C} \cup (\mathbf{1} + \mathcal{C})$. In this case

$$d(\tilde{\mathcal{C}}) = \min\{d,\ n - d_{max}\}.$$

Modified linear codes 3

- *Expurgating*: An $[n, k]_q$ code is expurgated to $[n, k-1]_q$ code by deleting suitable codewords. The operation corresponds to a decrease in the number of rows of $\mathbf{G}$ and adding a row in $\mathbf{H}$ with increasing its rank.

Modified linear codes 3

- *Expurgating*: An $[n,k]_q$ code is expurgated to $[n,k-1]_q$ code by deleting suitable codewords. The operation corresponds to a decrease in the number of rows of $\mathbf{G}$ and adding a row in $\mathbf{H}$ with increasing its rank.
- *Lengthening*: Adding an information coordinate. An $[n,k]_q$ code becomes $[n+1,k+1]_q$ code. The operation is a combination of extending and augmenting.

$$\begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & \mathbf{G} \end{pmatrix}.$$

Modified linear codes

- *Expurgating*: An $[n,k]_q$ code is expurgated to $[n,k-1]_q$ code by deleting suitable codewords. The operation corresponds to a decrease in the number of rows of $\mathbf{G}$ and adding a row in $\mathbf{H}$ with increasing its rank.
- *Lengthening*: Adding an information coordinate. An $[n,k]_q$ code becomes $[n+1,k+1]_q$ code. The operation is a combination of extending and augmenting.

$$\begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & \mathbf{G} \end{pmatrix}.$$

- *Shortening*: Deleting an information coordinate. An $[n,k]_q$ code becomes $[n-1,k-1]_q$ code. Usually it is carried out by taking only codewords which have a given value in a fixed coordinate, that is $c_i = a$.

Definition. Let $\mathcal{C}$ be an $[n,k]_q$ code and $\mathbf{u}$ is a codeword with weight w. *Residual code of $\mathcal{C}$ with respect to $\mathbf{u}$* is called the code $Res(\mathcal{C},\mathbf{u})$ which is obtained by deleting all coordinates where $\mathbf{u}$ has non-zero entries.

Let $\mathbf{G}$ be a generator matrix of $\mathcal{C}$ whose first row is u. Then $Res(\mathcal{C},u)$ has $\mathbf{G}_0$ as a generator matrix, where

$$\mathbf{G} = \begin{pmatrix} 0\,0\ldots0 & \overbrace{*\,*\ldots*}^{w} \\ \mathbf{G}_0 & \mathbf{G}_1 \end{pmatrix}$$

Several coding bounds

- Sphere packing (Hamming) bound.
- Plotkin bound.
- Singleton bound.
- Gilbert-Varshamov bound.
- Griesmer bound.

Sphere packing (Hamming) bound

Let $\mathbb{F} = GF(q)$.

Definition. The *Hamming sphere of radius r and center c* is the set of all vectors of $\mathbb{F}^n$ which are at a Hamming distance $\leq r$ from c, that is,

$$S(c,r) \stackrel{\text{def}}{=} \{v \in \mathbb{F}^n \mid d(c,v) \leq r\}$$

Its volume (i.e., the number of vectors in it) does not depend on c and it is

$$V_q(n,r) = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j.$$

Definition. The *packing radius* of $\mathcal{C}$ is the largest integer $t(\mathcal{C})$ such that the spheres of radius t with centers at each of the codewords do not overlap, i.e. they form $|\mathcal{C}|$ pairwise disjoint subsets of $\mathbb{F}^n$.

Sphere packing (Hamming) bound

Theorem. If $\mathcal{C}$ is an $(n, M, d)_q$ code with packing radius t, then

$$M(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t) \leq q^n.$$

If $\mathcal{C}$ is a linear $[(n, k, d]_q$ code, then

$$\sum_{i=0}^{t} \binom{n}{i}(q-1)^i \leq q^{n-k},$$

where $t = \lfloor (d-1)/2 \rfloor$. It can be rewritten into the form

$$n - k \geq \log_q V_q(n, t).$$

Definition. A *perfect code* is one which achieves the Hamming bound, that is, $MV_q(n, t) = q^n$.

The Hamming codes are perfect codes.

Plotkin and Singleton bounds

Let $A_q(n,d)$ denote the maximum number of codewords of q-ary code of block length n and minimum distance d.

Theorem. If n, d, q are integers, $n \geq d,\ q \geq 2$, and $d > \frac{q-1}{q}n$, then

$$A_q(n,d) \leq \frac{qd}{qd-(q-1)n}.$$

Plotkin and Singleton bounds

Let $A_q(n,d)$ denote the maximum number of codewords of q-ary code of block length n and minimum distance d.

Theorem. If n, d, q are integers, $n \geq d,\ q \geq 2$, and $d > \frac{q-1}{q}n$, then

$$A_q(n,d) \leq \frac{qd}{qd-(q-1)n}.$$

Theorem. For any integers n, d, q such that $n \geq d,\ q \geq 2$:

$$A_q(n,d) \leq q^{n-d+1}.$$

For linear codes we get $k \leq n-d+1.$

Gilbert-Varshamov bound

Theorem. If the integers n, d satisfy

$$1+\binom{n-1}{1}(q-1)+\binom{n-1}{2}(q-1)^2+\cdots+\binom{n-1}{d-2}(q-1)^{d-2} < q^{n-k},$$

then there exists an $[n,k,d]_q$ code.

Corollary. There exists an $[n,k,d]_q$ code whose parameters satisfy

$$\sum_{i=0}^{d-2}\binom{n}{i}(q-1)^i \geq q^{n-k}.$$

Taking logarithm we obtain $\log_q \sum_{i=0}^{d-2}\binom{n}{i}(q-1)^i \geq n-k$. It can be proved that

$$\lim_{n\to\infty}\frac{\log_q \sum_{i=0}^{d-2}\binom{n}{i}(q-1)^i}{n} = H_q\left(\frac{d}{n}\right),$$

Gilbert-Varshamov bound 2

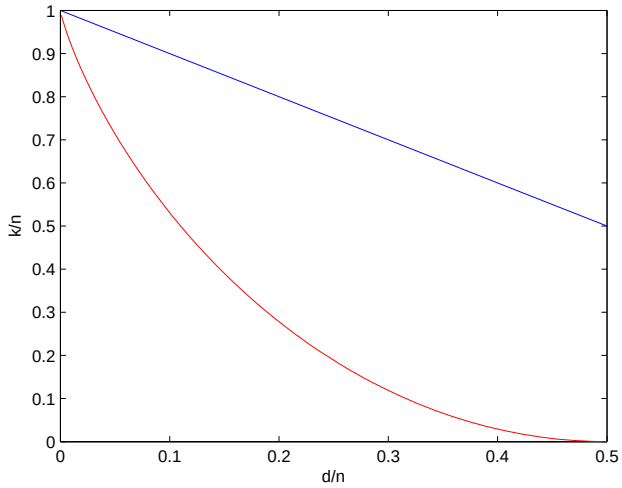
where $H_q(x) = x \log_q(q-1) - x \log_q x - (1-x)\log_q(1-x)$.

Therefore,

$$\lim_{n\to\infty} \frac{k}{n} \geq 1 - H_q\left(\frac{d}{n}\right),$$

Consider BSC with error rate p. If block length is n the code has to correct pn error in a codeword. Hence, a good class of codes is one with

$$\lim_{n\to\infty} \frac{d}{n} = \text{const} \quad \text{and} \quad \lim_{n\to\infty} \frac{k}{n} = \text{const}.$$



The red graph depicts $y = 1 - H_2(x)$ that presents the Gilbert-Varshamov bound. The blue graph ($y = 1 - x$) presents the Singleton bound. Good classes of codes are between them.

Griesmer bound

Theorem. Let $n_q(k,d)$ denote the minimal integer n for which a q-ary $[n,\ k,\ d]_q$ code exists. The following inequality holds:

$$n_q(k,d) \geq g_q(k,d) \ = \ \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil ,$$

where $\lceil x \rceil$ is the smallest integer $\geq x$.

Definition. $[n_q(k,d),\ k,\ d]_q$ codes are called *optimal*. Optimal codes of length $n_q(k,d) = g_q(k,d)$ are called *Griesmer codes*.

Griesmer bound

Theorem. Let $n_q(k,d)$ denote the minimal integer n for which a q-ary $[n,\ k,\ d]_q$ code exists. The following inequality holds:

$$n_q(k,d) \geq g_q(k,d) \ = \ \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil ,$$

where $\lceil x \rceil$ is the smallest integer $\geq x$.

Definition. $[n_q(k,d),\ k,\ d]_q$ codes are called *optimal*. Optimal codes of length $n_q(k,d) = g_q(k,d)$ are called *Griesmer codes*.

Lemma. If a q-ary $[n,\ k,\ d]_q$ code exists, then an $[n-d,\ k-1,\ d_0]_q$ code also exists.

Griesmer bound

Theorem. Let $n_q(k,d)$ denote the minimal integer n for which a q-ary $[n,\ k,\ d]_q$ code exists. The following inequality holds:

$$n_q(k,d) \geq g_q(k,d) = \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil,$$

where $\lceil x \rceil$ is the smallest integer $\geq x$.

Definition. $[n_q(k,d),\ k,\ d]_q$ codes are called *optimal*. Optimal codes of length $n_q(k,d) = g_q(k,d)$ are called *Griesmer codes*.

Lemma. If a q-ary $[n,\ k,\ d]_q$ code exists, then an $[n-d,\ k-1,\ d_0]_q$ code also exists.

For example, $g_2(6,3) = 9$, but $n_2(6,3) = 10$ since $[9,6,3]$ code does not exist. $[10,6,3]$ code can be obtained by shortening 5 times the $[15,11,3]$ Hamming code.

The MacWilliams identities

Definition. Let $\mathcal{C}$ be a q-ary $[n,\, k,\, d]_q$ code with weight distribution $A_0, A_1, \ldots, A_d, \ldots, A_n$. The polynomial $W_C(x) = A_0 + A_1 x + \cdots + A_d x^d + \cdots + A_n x^n$ is called the *weight enumerator* of $\mathcal{C}$. Obviously $W_C(x) = 1 + x^d b(x)$.

Example. The 3-ary $[4, 2]$ code:

$$\mathcal{C} = \{0000, 1110, 2220, 2102, 1201, 0212, 0121, 2011, 1022\}$$

has weight enumerator $W_C(x) = 1 + 8x^3$.

Theorem. If $\mathcal{C}$ is an $[n,\, k]$ code over $\mathbb{F} = GF(q)$ with the weight enumerator $W_C(x)$, then the weight enumerator, $W_{C^\perp}(x)$, of its dual code is given by

$$W_{C^\perp}(x) = \frac{1}{q^k}\,(1 + (q-1)x)^n\, W_C\left(\frac{1-x}{1+(q-1)x}\right).$$

Corollary. If $\{A_i\}_1^n$ and $\{B_i\}_1^n$, are the weight distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively, then

$$B_m = \frac{1}{q^k} \sum_{i=0}^{n} A_i P_m(i),$$

where

$$P_m(t) = \sum_{j=0}^{m} (-1)^j \binom{t}{j} \binom{n-t}{m-j} (q-1)^{m-j}, \ m = 0, 1 \ldots n.$$

The above polynomials are called *Krawtchouk polynomials*.

In the case $q = 2$:

$$P_0(t) = 1; \qquad P_2(t) = \binom{n}{2} - 2nt + 2t^2;$$
$$P_1(t) = n - 2t; \quad P_3(t) = \binom{n}{3} - (n^2 - n + 2/3)t + 2nt^2 - \tfrac{4}{3}t^3.$$

The end of the part

Thank You for Attention!