Some optimization problems in Coding theory

C O N T E N T S

1. Introduction

$\mathbb{F}_q$ $\mathbb{F}_q^n$, *q*-prime power

d(*x*, *y*) $\triangleq$ Hamming distance

C : $(n, M, d)_q$ code

d = d(C) $\triangleq$ min distance

t(C) = $\left\lfloor \frac{d-1}{2} \right\rfloor$

$$\rho(C) = \max_{x \in \mathbb{F}_q^n} \min_{c \in C} d(x, c) \quad \triangleq \text{ covering radius}$$

$\rho(C) = t(C) \Rightarrow$ Perfect code

$\rho(C) = 1 + t(C)$ Quasi-perfect code

If C is a k-dimensional subspace of $\mathbb{F}_q^n$, then

$C : [n, k, d]_q$ code

For linear codes

$d(C) = \{min\ wt\ (c) | c \in C, c \neq 0\}$

$\rho(C) \triangleq max$ weight of a coset leader

The parameters of perfect codes

- $(n, q^n, 1)_q$ - the whole space $\mathbb{F}_q^n$
- $(2l-1, 2, 2l-1)_2$ - the binary repetition code
- $(\frac{q^s-1}{q-1}, q^{\frac{q^s-1}{q-1}-s-1}, 3)_q$ - the Hamming codes
- $(23, 2^{12}, 7)_2$ – the binary Golay code
- $(11, 3^6, 5)_3$ – the ternary Golay code

Classification (up to equivalence)

- Unique linear Hamming code
- Golay codes are unique
- Open: non-linear Hamming codes
- Hamming bound

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

All sets of parameters for which $\exists$ perfect codes are known:

- Van Lint
- Tietäväinen (1973)
- Zinoviev, Leontiev (1972-1973)

Natural question: ? QP codes

2. Covering radius of BCH codes

- Gorenstein, Peterson, Zierler (1960)

  Primitive binary 2-error correcting BCH codes $\Rightarrow$ QP

- MacWilliams, Sloane (1977):

  Research problem (9.4). Show that no other BCH codes are quasi-perfect

- Helleseth (1979):

  No primitive binary t-error-correcting BCH codes are QP when t › 2

  Recall: $n = 2^m - 1$

- Leontiev (1968):

  Partial result for

$$2 < \frac{1}{2}(d-1) < \frac{\sqrt{n}}{\log n}, m \geq 7$$

Binary 3-error correcting BCH codes of length $2^m - 1$, $m \geq 4$

$\rho = 5$

History:

Van der Horst, Berger (1976)

- $m \equiv 0 \ (mod\ 4)$
- $5 \leq m \leq 12$

Assmus, Mattson (1976)

- $m \equiv 1 \text{ or } 3 (mod\ 4), m \geq 5$

Completed by T. Helleseth (1978):

m - even, $m \geq 10$

Long BCH codes

$m_i(x) \in \mathbb{F}_2[x]$

$m_i(x) \triangleq$ min polynomial of α^i, where α is of order $2^m - 1$

Helleseth (1985)

$C = (g(x))$

i) $g(x) = m_{i_1}(x) m_{i_2}(x) \ldots m_{i_t}(x)$

ii) $g(x)$ has no multiple zeros,

iii) D = *max* $\{i_1, i_2, \ldots i_t\}$

If $2^m \geq (D-1)^{4t+2}$, then $\rho(C) \leq 2t + 1$

Tietäväinen (1985)

$\rho(C) \le 2t$ for large enough m.

For t-designed BCH codes of length

$$n = \frac{1}{N}(2^m - 1)$$

$g(x) = m_N(x)m_{3N}(x)\ldots m_{(2t-1)N}(x)$

$2t - 1 \le \rho \le 2t + 1$

3. Quasi-perfect codes

Etzion, Mounits (2005, IT-51) : $q = 2$

$q = 3$

$n = \frac{1}{2}(3^s + 1)$, $k = n - 2s$, $d = 5$, $\rho = 3$

Gashkov, Sidel'nikov (1986)

$n = \frac{1}{2}(3^s - 1)$, $k = n - 2s$, $d = 5$, $\rho = 3$

if $s \geq 3$ - odd

Danev, Dodunekov (2007)

q = 4

Two families:

$n = \frac{1}{3}(4^s - 1)$, k = n – 2s, d = 5

Gevorkjan et al. (1975)

$N = \frac{1}{3}(2^{2s+1} + 1)$, k = n – 2s, d = 5

Dumer, Zinoviev (1978)

Both are quasi-perfect, i.e. $\rho = 3$

D. (1985-86)

Open: ? QP codes for q › 4

In particular, QP codes with d = 5?

$q = 3$, $n = \frac{1}{2}(3^s - 1)$

α – primitive n-th root of unity in an extension field of $\mathbb{F}_3$.

$\langle\beta\rangle = \mathbb{F}_{3^s}^* \Rightarrow \alpha = \beta^2$

The minimal polynomials of α and α^{-1} :

$$g_1(x) = (x - \alpha)(x - \alpha^3) \ldots \left(x - \alpha^{3^{s-1}}\right)$$

$$g_{-1}(x) = (x - \alpha^{-1})(x - \alpha^{-3}) \ldots \left(x - \alpha^{-3^{s-1}}\right)$$

$C_s \triangleq (g(x)),\ g(x) = g_1(x)g_{-1}(x)$

$n = \frac{1}{2}(3^s - 1),\ k = n - 2s,\ s \geq 3$ – odd

$\Rightarrow d = 5$

$\rho(C_s) = 3$

C_s is a BCH code!

Set $\gamma = \alpha^2$. Then $\{\gamma^{\frac{n-3}{2}}, \gamma^{\frac{n-1}{2}}, \gamma^{\frac{n+1}{2}}, \gamma^{\frac{n+3}{2}}\}$

$= \{\alpha^{-3}, \alpha^{-1}, \alpha, \alpha^3,\}$

Hence, infinitely many counterexamples to (9.4)!

C_3 : [13, 7, 5] QR code

Baicheva, D., Kötter (2002)

Open: i) QP BCH codes for

- $q > 4$?

ii) QP BCH codes for $d \geq 7$?

Binary and ternary QP codes with small dimensions

Wagner (1966, 1967)

Computer search, 27 binary QP codes

- $19 \leq n \leq 55$, $\rho = 3$
- One example for each parameter set.

Simonis (2000): the [23, 14, 5] Wagner code is unique up to equivalence.

Recently:

Baicheva, Bouykliev, D., Fack (2007):

A systematic investigation of the possible parameters of QP binary and ternary codes

Results

- Classification up to equivalence of all binary and ternary QP codes of dimensions up to 9 and 6 respectively;
- Partial classification for dimensions up to 14 and 13 respectively

Important observations

- For many sets of parameters $\exists$ more than one QP code:

$[19, 10, 5]_2 \Rightarrow 12$ codes

$[20, 11, 5]_2 \Rightarrow 564$ codes

- Except the extended Golay $[24, 12, 8]_2$ code and the $[8, 1, 8]_2$ repetition code we found 11 $[24, 12, 7]_2$ and 2 $[25, 12, 8]_2$

QP codes with $\rho = 4$

Positive answer to the first open problem of

Etzion, Mounits (2005).

4. Singleton bound, MDS, AMDS, NMDS

Singleton (1964):

C: $[n, k, d]_q$ code $\Rightarrow d \le n - k + 1$

For nonlinear codes: $d \le n - \log_q M + 1$

$s = n - k + 1 \triangleq$ Singleton defect.

$s = 0 \Rightarrow$ MDS codes

An old optimization problem:

$m(k,q) \triangleq \max n: \exists\, [n, k, n - k + 1]_q$ code (MDS code)

Conjecture:

$$m(k,q) = \begin{cases} q+1 & 2 \le k \le q \\ k+1 & q < k \end{cases}$$

except for $m(3,q) = m(q-1, q) = q + 2$

for q =power of 2.

$s = 1 \Rightarrow$ Almost MDS codes (AMDS)

Parameters: $[n, k, n-k]_q$

If C is an AMDS, $C^{\perp}$ is not necessarily AMDS.

D., Landjev (1993): Near MDS codes.

Simplest definition: $d + d^{\perp} = n$

Some properties:

1. If $n \rangle k + q$ every $[n, k, n - k]q$ code is NMDS code.
2. For an AMDS code C: $[n, k, n - k]q$

with $k \geq 2$

i) $n \leq 2q + k$;

ii) C is generated by its codewords of weight $n - k$ and $n - k + 1$; if $n \rangle q + k$, C is generated by its minimum weight vectors.

3. C: $[n, k]_q$ – NMDS code with weight distribution $\{Ai, i = 0, ..., n\}$ then:

$$A_{n-k+s} =$$

$$\binom{n}{k-s}\sum_{s=0}^{s-1}(-1)^j\binom{n-k+s}{j}(q^{s-j}-1)+(-1)^s\binom{k}{s}A_{n-k}$$

4. $A_{n-k} \leq \binom{n}{k-1}\dfrac{q-1}{k}$

An optimization problem

Define

$m'(k, q) = max\, n : \exists$ a NMDS code with parameters $[n, k, n\text{-}k]_q$

What is known?

1. $m'(k, q) \leq 2q+k$.

   In the case of equality $A_{\text{n-k+1}} = 0$.

2. $m'(k, q) = k + 1$ for every $k > 2q$.

3. $\forall$ integer α, $0 \leq \alpha \leq k$

$m'(k, q) \leq m'(k\text{-}\alpha, q) + \alpha$

4. If $q > 3$, then

$m'(k, q) \leq 2q + k - 2$

5. Tsfasman, Vladut (1991): NMDS AG codes for every

$$n \le \begin{cases} q + [2\sqrt{q}] & \mathit{if}\ p\ \mathit{divides} [2\sqrt{q}], q = p^m, m \ge 3 - \mathit{odd} \\ q + [2\sqrt{q}] + 1 & \mathit{otherwise} \end{cases}$$

Conjecture: $m'(k, q) \approx q + 2\sqrt{q}$

5. Grey – Rankin bound

Grey (1956), Rankin(1962)

C : $(n, M, d)_2$ code, (1, 1,…1) $C. \in$

C $\triangleq$ self-complementary

Then $M \leq \dfrac{8d(n-d)}{n-(n-2d)^2}$

provided $\dfrac{1}{2}(n-\sqrt{n}) < d < \dfrac{1}{2}(n+\sqrt{n})$

Constructions of codes meeting the Grey-Rankin bound

Gary Mc Guire (1997)

Suppose $n-\sqrt{n} < 2d < n$. Then

A. i) *n*-odd; $\exists$ a self-complementary code meeting the Grey-Rankin bound $\Leftrightarrow$ $\exists$ a Hadamard matrix of size $n + 1$;

ii) *n*-even; ∃ a self-complementary code meeting the Grey-Rankin bound ⇔ ∃ a quasi-symmetric 2 – (*n*, *d*, λ) design with

block intersection sizes $\frac{d}{2}$ and $\frac{1}{2}(3d-n)$

$$\lambda = \frac{d(d-1)}{n-(n-2n)^2}$$

Remark

A code is said to form an orthogonal array of strength t

$$\Updownarrow$$

The projection of the code on to any t coordinates contains every t-tuple the same number of times

Equality in $M \leq \dfrac{8d(n-d)}{n-(n-2d)^2}$ holds

$$\Updownarrow$$

The distance between codewords in *C* are all in $\{0, d, n-d, n\}$ and the codewords form an orthogonal array of strength 2.

B. In the linear case

i) n-odd; the parameters of C are

$[2^s - 1,\ s + 1,\ 2^{s-1} - 1]$, $s \geq 2$

and the corresponding Hadamard matrix is

of Sylvester type.

ii) n-even; the parameters are

$[2^{2m-1} - 2^{m-1},\ 2m + 1,\ 2^{2m-2} - 2^{m-1}]$ $C_1 \triangleq$, or

$[2^{2m-1} + 2^{m-1},\ 2m + 1,\ 2^{2m-2}]$ $C_2 \triangleq$.

Remark

Put C_1 and C_2 side by side:

$RM(1, 2m) = (C_1 | C_2)$

$$\Downarrow$$

\# of nonequivalent codes of both types is equal.

Remark

$\exists$ nonlinear codes meeting

$$M \leq \frac{8d(n-d)}{n-(n-2d)^2}$$

Bracken, Mc Guire, Ward (2006)

$u \in N$, even

i) Suppose $\exists$ a $2u$ x $2u$ Hadamard matrix and $u-2$ mutually orthogonal $2u$ x $2u$ Latin squares.

Then there exists a quasi-symmetric

2-$(2u^2 - u, u^2 - u, u^2 - u - 1)$ design with

block intersection sizes

$\frac{1}{2}(u-1)u$ and $\frac{1}{2}(u-2)u$

ii) Suppose $\exists$ a $2u$ x $2u$ Hadamard matrix and $u-1$ mutually orthogonal Latin squares.

Then $\exists$ a quasi-symmetric

2-$(2u^2 + u, u^2, u^2 - u)$ design with block

intersection sizes

$$\frac{1}{2}(u-1)u \quad \text{and} \quad \frac{1}{2}u^2$$

The associated codes have parameters

($n = 2u^2 - u$, $M = 8u^2$, $d = u^2 - u$)

($n = 2u^2 + u$, $M = 8u^2$, $d = u^2$)

$u = 6$

($n = 66$, $M = 288$, $d = 30$)

$\Downarrow$ $\leftarrow$ Open ? 30 years

Meeting $M \le \dfrac{8d(n-d)}{n-(n-2d)^2}$

Nonbinary version of GR-bound

Fu, Kløve, Shen (1999)

C: $(n, M, d)_q$ - code, for which

1) $$d_{up} - \frac{1}{2q}\sqrt{(q-2)^2 + 4(q-1)n} < d$$

$$d \le d_{up} = n\frac{q-1}{q} - \frac{q-2}{2q}$$

2) $\forall\ a, b \in C \Rightarrow d(a, b) \leq 2\,\mathrm{dup} - d.$

Then

$$M \leq \frac{q^2 d(2d_{up} - d)}{q^2 d\left(2d_{up} - d\right) - (q-1)^2 n(n-1)}$$

Construction of codes meeting FKS bound

The general concatenation construction

A: $(n_a, M_a, d_a)_{q_a}$ code $\Rightarrow$ outer code

B: $(n_b, M_b, d_b)_{q_b}$ code $\Rightarrow$ inner code

Assume: $q_a = M_b$

$B = \{b_{(i)}, i = 0,1\ldots, M_b - 1\}$

The alphabet of A:

$E_a = \{0, 1, \ldots, q_a - 1\}$

The construction:

$\forall\, a \in A,\quad a = (a_1, a_2, \ldots, a_{n_a}),\ a_i \in E_a$

$\Downarrow$

$C(a) = (b(a_1), b(a_2), \ldots, b(a_{n_a}))$

$\Downarrow$

$C = \{c(a) : a \in A\}$

$C : (n, M, d)_q$ code with parameters

$n = n_a n_b,\ M = M_a,\ d \geq d_a d_b,\ q = q_b$

D., Helleseth, Zinoviev (2004)

Take

$$B: \ (n_b = \frac{q^m - 1}{q - 1}, M_b = q^m, d_b = q^{m-1})_q$$

$q = p^h$, p – prime

A : an MDS code with $d_a = n_a - 1$, $M_a = q^{2m}$

Take $n_a = \frac{1}{2}(q^m - q) + 1$

The general concatenated construction:

C : *(n, M, d)*$_q$ with

$$n = \frac{q^m - 1}{q - 1}\left(\frac{\mathrm{q^m - q}}{2} + 1\right)$$

$$M = q^{2m}, \mathrm{d} = \frac{1}{2}\mathrm{q^{m-1}(q^m - q)}$$

C meets the FKS bound

Something more:

1) in terms of n:

$$n^2 - (3q^m - q + 1)n + q^m(q^m - q + 2) \dot{<} 0$$

n_1, n_2 - the roots, $n_1 < n_2$

$$0 < n_1 < n_{max} = \frac{1}{2}(q^m - q) + 1 < n_2$$

$\Downarrow$

The construction gives codes satisfying FKS bound for $\forall\, n,\ n_1 < n \le n_{max}$ and with equality for $n = n_{max}$

n-simplex in the *n*-dimensional *q*-ary Hamming space

$\triangleq$

A set of *q* vectors with Hamming distance *n* between any two distinct vectors.

$\Downarrow$

$M \leq \dfrac{8d(n-d)}{n-(n-2d)^2}$ ≈an upper bound on the size of a family of binary *n*-simplices with pairwize distance ≥ *d*.

$S_q(n, d) \triangleq$ *max* # of n-simplices in the q-ary Hamming n-space with distance $\geq d$.

$$\Downarrow$$

$$S_2(n, d) \leq \frac{4d(n-d)}{n-(n-2d)^2}$$

Bassalygo, D., Helleseth, Zinoviev (2006)

$$S_{\mathrm{q}}(n,d) \le \frac{q[qd-(q-2)n](n-d)}{n-[(q-1)n-qd]^2}$$

provided that the denominator is positive.

The codes meeting the bound

have strength 2.

6. Conclusions

- Optimality with respect to the length, distance, dimension is not a necessary condition for the existence of a QP code;
- The classification of all parameters for which $\exists$ QP codes would be much more difficult than the similar one for perfect codes.

Open (and more optimistic):

- Are there QP codes with $\rho \geq 5$?
- Is there an upper bound on the minimum distance of QP codes?

THANK YOU!