Lower Bounds for the Minimum Distance of an AG-Code

Peter Beelen

Danish Technical University
Copenhagen

19th September 2005

ECC 2005

Summary:

- Introduction in coding theory
- Some AG-codes
- The order bound
- The generalized order bound

Notation:

- $\mathbb{F}_q$ a field with q elements.

- Hamming weight of $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$

$$w_H(c) := \#\{i \mid c_i \neq 0\}.$$

- A q-ary code C of length n

a linear subspace of $\mathbb{F}_q^n$.

- Minimum distance of C

$$d(C) := \min\{w_H(c) \mid c \in C \backslash \{0\}\}.$$

- An $[n, k, d]_q$ code

a code $C \subset \mathbb{F}_q^n$ with $\dim(C) = k$ and $d(C) = d$.

- Rate of a code: R=k/n.

The Hamming code C_H:

$C_H \subset \mathbb{F}_2^7$. For any $c = (c_1, \ldots, c_7) \in C_H$ one has:

$$c_5 = c_1 + c_2 + c_4,$$

$$c_6 = c_1 + c_2 + c_3,$$

$$c_7 = c_1 + c_3 + c_4.$$

Repetition code

$$C_R := \{(0, \ldots, 0), (1, \ldots, 1)\} \subset \mathbb{F}_2^n.$$

$$d(C_R) = n$$

C_R corrects up to $\lfloor (n-1)/2 \rfloor$ errors.

$$R = \frac{1}{n}$$

Have good codes low rate?

Shannon's theorem:

Theorem 1 *There exists a positive number CAP, such that information transmission at any rate* $R < CAP$ *is possible.*

The proof is NOT constructive!

RS-codes:

$$L_{RS}(i) := \{f(X) \in \mathbb{F}_q[X] \mid \deg f(X) < i\},$$

$$\mathrm{Ev} : L_{RS}(i) \longrightarrow (\mathbb{F}_q)^{q-1},$$

$$\mathrm{Ev}(f(X)) = (f(\alpha_1), \ldots, f(\alpha_{q-1})),$$

$$\alpha_j \neq 0.$$

$[n, k, d]_q$ RS-codes:

$E_{RS}(i) := \mathrm{Ev}(L_{RS}(i))$ and

$C_{RS}(i) := E_{RS}(i)^{\perp}$.

Then $d \geq n - k + 1$.

Hermitian codes:

$$L_{Her}(i) := \{f(X,Y) \in \mathbb{F}_{q^2}[X,Y] \mid \deg_Y f(X,Y) < q,$$
$$\mathrm{wdeg} f(X,Y) < i\},$$

with $\mathrm{wdeg}(X) = q$ and $\mathrm{wdeg}(Y) = q+1$.

$$\mathrm{Ev} : L_{Her}(i) \longrightarrow (\mathbb{F}_{q^2})^{q^3}$$

$$\mathrm{Ev}(f(X,Y)) = (f(\alpha_1, \beta_1), \ldots, f(\alpha_{q^3}, \beta_{q^3})),$$
$$\beta_j^q + \beta_j = \alpha_j^{q+1}.$$

$[n,k,d]_{q^2}$ Hermitian codes:

$E_{Her}(i) := \mathrm{Ev}(L_{Her}(i))$ and

$C_{Her}(i) := E_{Her}(i)^{\perp}$.

Then $d \geq n - k + 1 - q(q-1)/2$.

General one-point AG-codes

Let $\mathcal{C}$ be an algebraic curve over $\mathbb{F}_q$, with

$$\mathcal{C}(\mathbb{F}_q) = \{P, P_1, \ldots, P_N\}.$$

$$L_{\mathcal{C}}(i) := L(iP).$$

$$\mathrm{Ev} : L_{\mathcal{C}}(i) \longrightarrow (\mathbb{F}_q)^N,$$

$$\mathrm{Ev}(f) = (f(P_1), \ldots, f(P_N)).$$

$[n, k, d]_q$ codes:

$E_{\mathcal{C}}(i) := \mathrm{Ev}(L_{\mathcal{C}}(i))$ and

$C_{\mathcal{C}}(i) := E_{\mathcal{C}}(i)^{\perp}$.

Then $d \geq n - k + 1 - g$.

AG-codes in practice

- How to find curves $\mathcal{C}$?
- How to find a basis of $L_{\mathcal{C}}(i)$?
- How to decode?
- What is the performance?

The order bound

$$H(P) := \{i \in \mathbb{N} \,|\, L_{\mathcal{C}}(i-1) \neq L_{\mathcal{C}}(i)\}$$

$$\nu(i) := \#\{(k,l) \in H(P)^2 \,|\, k + l = i + 1\}.$$

Theorem 2 *For any* $c \in C_{\mathcal{C}}(i) \backslash C_{\mathcal{C}}(i+1)$*:*

$$w_H(c) \geq \nu(i).$$

$$d_{ord}(i) := \min\{\nu(j) \,|\, j \geq i, C_{\mathcal{C}}(j) \neq C_{\mathcal{C}}(j+1)\}.$$

Theorem 3

$$d(C_{\mathcal{C}}(i)) \geq d_{ord}(i).$$

The Hermitian curve for $q = 4$

$H = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \dots\}$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
$\nu(i)$	0	0	0	2	2	0	0	3	4	3	0	4	6
$d_{ord}(i)$	2	2	2	2	2	3	3	3	3	3	4	4	4

i	13	14	15	16	17	18	19	20	21	22	23
$\nu(i)$	6	4	5	8	9	8	9	10	12	12	13
$d_{ord}(i)$	4	4	5	8	8	8	9	10	12	12	13

In fact we have $d(C_{Her}(i)) = d_{ord}(i)$.

Generalized order bound

As before $\mathcal{C}$ is an algebraic curve over $\mathbb{F}_q$. Let G be a rational divisor and $P \in \mathcal{C}(\mathbb{F}_q)$.

$C_{\mathcal{C}}(G) := \mathrm{Ev}(L(G))$.

$H(P, G) := -v_P(L(G + P))$.

$\nu(P, G) :=$
$\#\{(i, j) \in H(P, G) \times H(P) \mid i + j = v_P(G) + 1\}$

Theorem 4 *For any* $c \in C_{\mathcal{C}}(G) \backslash C_{\mathcal{C}}(G + P)$*:*

$$w_H(c) \geq \nu(P, G).$$

A more-dimensional theory for codes $C_{\mathcal{C}}(G)$ exists!

9		10		11		12		13	
·	10	·	10	·	11	·	12	·	13
9		9		10		11		12	
·	9	·	9	·	10	·	11	·	12
8		9		10		11		12	
·	8	·	9	·	9	·	10	·	11
6		7		8		9		10	
·	8	·	9	·	8	·	9	·	10
5		6		7		8		9	
·	7	·	8	·	7	·	8	·	9
6		6		6		7		8	
·	6	·	7	·	6	·	7	·	8
6		6		7		8		9	
●	5	·	6	·	6	·	6	·	7
4		5		6		7		8	
·	4	·	6	·	6	·	5	·	6
1		2		3		4		5	
·	4	·	6	·	6	·	4	·	5
3		3		3		3		4	
·	3	·	5	·	5	·	3	·	4
4		4		4		5		6	
·	2	·	4	·	4	·	3	·	3
3		3		4		5		6	
·	1	·	3	·	4	·	3	·	2
0		1		2		3		4	
·	0	·	3	·	4	·	3	·	1
0		0		0		0		0	
·	0	·	3	·	4	·	3	·	0

Theorem 5 *We have*

$$d(C_{Her}(iP + jQ)) = d_{genord}(iP + jQ).$$

Similarly as in the case of one-point codes

$$d_{genord}(iP + jQ)$$

does not always give the minimum distance.

Future work:

- Integrate the generalized order bound and other existing lower bounds.

Concluding remarks

• AG-codes are promising good long codes.

• The explicit description of AG-codes is incomplete.

• The knowledge of the parameters of AG-codes is improving.

Thank you for your attention!