On the weight distribution of certain trace codes

Yves Edel

Department of Pure Mathematics and Computer Algebra
Ghent University

ALCOMA10
Thurnau, 16 April 2010

The * Construction (MacWilliams Sloane)

Let $\mathcal{A}$ be an irreducible cyclic $[u, r, d_1]_q$ and $\mathcal{B}$ a cyclic $[n, k, d_2]_{q^r}$

Let $\gcd(u, n) = 1$, then $\mathcal{A} * \mathcal{B}$ is a cyclic $[un, rk, d]_q$, $d \geq d_1 d_2$, with codewords:

$$\left(\mathrm{tr}_{r,1}(\zeta^1 c_1), \ldots, \mathrm{tr}_{r,1}(\zeta^u c_1), \ldots, \mathrm{tr}_{r,1}(\zeta^1 c_n), \ldots, \mathrm{tr}_{r,1}(\zeta^u c_n)\right),$$

where $(c_1, ..., c_n) \in \mathcal{B}$ and ζ a primitive u-th root $\in \mathbb{F}_{q^r}$.

This is concatenated code with inner code $\mathcal{A}$ and outer code $\mathcal{B}$.

$$\phi : \mathbb{F}_{q^r} \to \mathcal{A}, \quad c \mapsto \left(\mathrm{tr}_{r,1}(\zeta^1 c), \ldots, \mathrm{tr}_{r,1}(\zeta^u c)\right) \in \mathcal{A}$$

The '* Construction', $\gcd(u, n) > 1$

How to get cyclic codes $\mathcal{A} * \mathcal{B}$, with $\mathcal{A}$ an irreducible cyclic code, if $\gcd(u, n) > 1$?
Answer: $\mathcal{B}$ needs to be a suitable constacyclic code (Jensen 1992).

Applications

- $\Rightarrow$ Use information on $\mathcal{A}, \mathcal{B}$ to obtain information on $\mathcal{A} * \mathcal{B}$
- $\Leftarrow$ Use information on the q-ary cyclic code $\mathcal{A} * \mathcal{B}$ to obtain information on q^r-ary constacyclic code $\mathcal{B}$

Definitions

Let $A \subseteq \mathbb{Z}$, $\{w_1, \ldots, w_n\} = W \subseteq \mathbb{F}_{q^s}^*$

- $\mathcal{P}_s(A) := \{\sum_{i \in A} a_i X^i \mid a_i \in \mathbb{F}_{q^s}\} \subseteq \mathbb{F}_{q^s}[X]$.
- Let $\mathcal{B}(A, W, s)$ the q^s-ary linear code generated by the words

$$(f(w_1), \ldots, f(w_n)), \quad f \in \mathcal{P}_s(A)$$

- Let $r|s$ and $\mathrm{tr}_{s,r} : \mathbb{F}_{q^s} \to \mathbb{F}_{q^r}$ the trace.
  For a $\mathbb{F}_{q^s}$-ary linear code C define its **trace code** $\mathrm{tr}_{s,r}(C)$ as the $\mathbb{F}_{q^r}$-ary linear code generated by the words

$$\mathrm{tr}_{s,r}(c) := (\ldots, \mathrm{tr}_{s,r}(c_i), \ldots), \quad c \in C$$

  Let $\mathcal{T}(A, W, s, r) := \mathrm{tr}_{s,r}(\mathcal{B}(A, W, s))$.

Definitions

Let $\gcd(N, q) = 1$. Define

- The **q-cyclotomic coset** (modulo N) of $i \in \mathbb{Z}$ as:

$$Z_q^N(i) := \{i \cdot q^j \mod N \mid j \in \mathbb{Z}\} \subseteq \mathbb{Z}_N$$

- The **(**q**)-Galois closure** of $A \subseteq \mathbb{Z}_N$ as:

$$\mathrm{gc}_q^N(A) := \bigcup_{i \in A} Z_q^N(i) \subseteq \mathbb{Z}_N$$

  We call A **(**q**)-Galois closed** if $A = \mathrm{gc}_q^N(A)$.

- The **complement** of A in $\mathbb{Z}_N$ ($\mathbb{Z}_N \setminus A$) is denoted as $\overline{A}$.

Cyclic codes

Let $N \mid (q^s - 1)$. Denote by $\langle \zeta \rangle = W_N$ multiplicative subgroup of order N in $\mathbb{F}_{q^s}^*$. The code $\mathcal{C}(A, N) := \mathcal{T}(A, W_N, s, r)^\perp$ is an cyclic $\mathbb{F}_{q^r}$-linear code, A is called the **defining set** of the cyclic code.

$$\begin{aligned} f = x^a : &\qquad (\zeta^a, \ldots, \zeta^{a(N-1)}, \zeta^{aN}) \\ f = \zeta^a x^a : &\qquad (\zeta^{2a}, \ldots, \zeta^{aN}, \zeta^a) \end{aligned}$$

- $\mathcal{C}(A, N) = \mathcal{C}((A \subset \mathbb{Z}_N), N) = \mathcal{C}(\mathrm{gc}^N_{q^r}(A), N)$
- $|\mathrm{gc}^N_{q^r}(A)| = \dim(\mathcal{T}(A, W_N, s, r)) = N - \dim(\mathcal{C}(A, N))$
- $B = -\overline{\mathrm{gc}^N_{q^r}(A)}$ is the defining set of the dual code.
- $\{\zeta^a \mid a \in \mathrm{gc}^N_{q^r}(A)\}$ are the **zeros** of $\mathcal{C}(A, N)$ and $\{\zeta^{-a} \mid a \in \mathrm{gc}^N_{q^r}(A)\}$ the **nonzeros** of $\mathcal{T}(A, W_N, s, r)$
- ...

Constacyclic codes

A $[n, k, d]_q$ code C is called γ-**constacyclic** if there is a common constant $\gamma \in \mathbb{F}_q$ such that

$$(c_1, \ldots, c_n) \in C \ \Leftrightarrow (c_2, \ldots, c_n, \gamma c_1) \in C$$

If $\gamma^u = 1$, then the following code C' is cyclic:

$$C' = \{(c, \gamma c, \ldots, \gamma^{u-1} c) \mid c \in C\}$$

Especially the weight distribution of C is determined the one of C'.

Characterization (Bierbrauer 2002)

Let $u \mid q - 1$ and $un = N \mid (q^s - 1)$. It is equivalent:

- The class of of q-ary cyclic codes C of length N with the property that **all nonzeros A of C are in the same coset modulo u.**
- The class of q-ary γ-constacyclic codes of length n, for some γ of order u.

Constacyclic codes

Assume that $N = nu$ and the set A has the property that all $a \in A$ equal b modulo u. The code $\mathcal{B}(A, W_N, s)$ is generated by the words

$$(\zeta^{ai} | 0 \leq i < N)$$

Let $\beta := \zeta^n$, a primitive element of W_u.

We have that the entry at coordinate $i + n$ is:

$$\zeta^{a(i+n)} = \zeta^{ai}\zeta^{an} = \zeta^{ai}\zeta^{(b+uv)n} = \zeta^{ai}\zeta^{bn}\zeta^{vN} = \beta^b\zeta^{ai}$$

Let $R_u^N := \{\zeta^i \mid 0 \leq i < n\}$.

$\mathcal{B}(A, R_u^N, s)$ is γ-constacyclic where $\gamma = \beta^b$,

If $u \mid q^r - 1$ for some $r \mid s$ then $\gamma \in \mathbb{F}_{q^r}$ and hence also $\mathcal{T}(A, R_u^N, s, r)$ is γ-constacyclic.

$\mathcal{T}(A, W_N, s, 1)$ for $u \nmid (q-1)$

Assume all elements of A are in the same coset modulo u but $u \nmid (q-1)$, then $\mathcal{T}(A, R_u^N, s, 1) = \ldots$?

Then there is some $r \mid s$, s.t. $u \mid (q^r - 1)$ and

$$\mathrm{tr}_{s,1}\left((c, \gamma c, \ldots, \gamma^{u-1} c)\right) = \mathrm{tr}_{r,1}\left((\mathrm{tr}_{s,r}(c), \gamma \mathrm{tr}_{s,r}(c), \ldots, \gamma^{u-1}\mathrm{tr}_{s,r}(c))\right)$$

$$\mathcal{T}(A, W_N, s, 1) = \mathcal{T}(\{b\}, W_u, r, 1) * \mathcal{T}(A, R_u^N, s, r)$$

If $v = (u, q-1)$

$$\mathcal{T}(A, R_v^N, s, 1) = \mathcal{T}(\{b\}, R_v^u, r, 1) * \mathcal{T}(A, R_u^N, s, r)$$

Characterization

Let $N = nu \mid (q^s - 1)$ and $R(b) = \{a \in \mathbb{Z}_N \mid a = b \mod u\}$. $\mathcal{T}(A, W_N, s, 1)$ is decomposable via the $*$ construction in a constacyclic code and a irreducible cyclic code of length u iff there is some b such that

$$Z_q^N(a) \cap R(b) \neq \emptyset \text{ for all } a \in A \tag{1}$$

Then

$$\mathcal{T}(A, W_N, s, 1) = \mathcal{T}(\{b\}, W_u, r, 1) * \mathcal{T}(\mathrm{gc}_q^N(A) \cap R(b), R_u^N, s, r)$$

An alternative characterization of Equation 1 is that every q-cyclotomic coset of $\mathrm{gc}_q^N(A)$ has to contain one q^r-cyclotomic coset of $R(b)$.

$N = un$, $\gcd(u,n) = 1$

R_u^N is a representative system of W_N modulo W_u, i.e.

$$W_N = W_u R_u^N := \{wa | w \in W_u, a \in R_u^N\} \text{ and } W_u \cap R_u^N = \{1\}$$

If $\gcd(u,n) = 1$ then also

$$W_N = W_u W_n := \{wa | w \in W_u, a \in W_n\} \text{ and } W_u \cap W_n = \{1\}$$

and hence up to permutation of coordinates, we have

$$\begin{aligned} & \mathcal{T}(\{b\}, W_u, r, 1) * \mathcal{T}(A, R_u^N, s, r) \\ = \; & \mathcal{T}(A, W_N, s, 1) \\ = \; & \mathcal{T}(\{b\}, W_u, r, 1) * \mathcal{T}(A, W_n, s, r) \end{aligned}$$

so this code can be decomposed also in cyclic codes which gives the original $*$-construction.

Let $N = un \mid (q^s - 1)$, $u \mid (q^r - 1)$, r minimal with $r \mid s$.
Let $A \subset \mathbb{Z}_N$ with $b = a \mod u$ for all $a \in A$.

$$a_i = |\{c \in \mathcal{T}(A, W_N, s, 1) \mid wt(c) = i\}|$$

$$A_i = |\{c \in \mathcal{T}(A, R_u^N, s, r) \mid wt(c) = i\}|$$

Lemma

Let $\gcd(q-1, (q^r-1)/(q-1)) = 1$, $v := \gcd(q-1, u)$ and $u = v(q^r-1)/(q-1)$. Let $\gcd(b, q^r-1) = 1$. It is

$$A_i = a_{ivq^{r-1}}$$

For binary cyclic codes the condition simplifies to $u = 2^r - 1$, $\gcd(b, q^r - 1) = 1$.

This holds e.g for every quaternary constacyclic code where the common modulus $b \neq 0$.

Under the conditions of the corollary the inner code of the concatenation, $\mathcal{T}(\{b\}, W_u, r, 1)$, consists of v copies of the Simplex code.

The condition ensures 1. that the Simplex code is cyclic and 2. that the inner code consists of v copies of the Simplex code.

The simplex code is the constacyclic code $\mathcal{T}(\{1\}, R_{q-1}^{q^r-1}, r, 1)$.
If $\gcd(b, q^r-1) = 1$ this code is equivalent to $\mathcal{T}(\{b\}, R_{q-1}^{q^r-1}, r, 1)$.
As $\gcd(q-1, (q^r-1)/(q-1)) = 1$ this code is isomorphic to the cyclic code $\mathcal{T}(\{b\}, W_{\frac{q^r-1}{q-1}}, r, 1)$.

As $u = v\frac{q^r-1}{q-1}$ with $v \mid (q-1)$ The inner code $\mathcal{T}(\{b\}, W_u, r, 1)$ equals $\mathcal{T}(\{*\}, W_v, 1, 1) * \mathcal{T}(\{b\}, R_v^u, r, 1)$

Now $\gcd(v, \frac{q^r-1}{q-1}) = 1$ as $\gcd(q-1, (q^r-1)/(q-1)) = 1$ by assumption. Hence $\mathcal{T}(\{b\}, R_v^u, r, 1)$ is isomorphic to the cyclic code, which is isomorphic to the simplex code $\mathcal{T}(\{b\}, W_{\frac{q^r-1}{q-1}}, r, 1)$

Conclusion the inner code is a copy of v simplex codes.

Kloosterman Codes

The Kloosterman code or dual Mélas code is the binary primitive cyclic code of length $2^s - 1$ and dimension $2s$ and nonzeros $\{-1, 1\}$, i.e. $\mathcal{T}(\{-1,1\}, W_{2^s-1}, s, 1)$.

The code is a composition if there is some $r \mid s$ such that $(Z_2(-1) \mod (2^r-1)) \cap (Z_2(1) \mod (2^r-1)) \neq \{0\}$

So if $(2^r - 1) \mid (2^j + 1) \Leftrightarrow (2^r - 1) \mid (2^{(j \mod r)} + 1)$ for some j, i.e. it has to be $r = 2, j = 1 \mod 2$.

I.e. the Kloosterman Code decomposes ("only") in a quaternary constacyclic code with $A = \{-2, 1\}$ and $s = 2t$.

This constacyclic code is the dual of the two-error correcting code of Dumer Zinoviev (1978).

The distance of the Kloosterman code is $2 \cdot 4^{t-1} - 2^t$

Corollary

$\mathcal{T}(\{-2,1\}, R_3^{2^{2t}-1}, 2t, 2)$, the dual of the two-error correcting code of Dumer Zinoviev is a

$$[\frac{(2^t-1)(2^t+1)}{3}, 2t, 4^{t-1} - 2^{t-1}]_4$$

The smallest cases are $[21, 6, 12]_4$, $[85, 8, 56]_4$, $[341, 10, 240]_4$.

The dual Zetterberg code

The dual Zetterberg code is a binary irreducible cyclic code of length 2^t+1, with nonzero $\{1\}$ i.e. $\mathcal{T}(\{1\}, W_{2^t+1}, s, 1)$. The 2^t+1-roots of unity are in $\mathbb{F}_2^s$ with $s = 2t$.

The "common modulus condition" is empty. The code is decomposeable if there is some $r|s$, s.t. $2^r - 1 \mid 2^t + 1$. As before this implies $r = 2$ and $t \mod 2 = 1$.

The dual Zetterberg code decomposes ("only") for t odd in a quaternary constacyclic code: $\mathcal{T}(\{1\}, R_3^{2^t+1}, s, 1)$, this is the dual of the two error correcting code of Gevorkyan, Avetisyan and Tigranyan (1975)

The distance d of the dual Zetterberg code is $d = \lceil \frac{q+1}{2} - \sqrt{q} \rceil$.

Lemma

$\mathcal{T}(\{1\}, R_3^{2^t+1}, s, 2)$, the dual of the two error correcting code of Gevorkyan, Avetisyan and Tigranyan, is a

$$[(2^t+1)/3, t, d]_4, \text{ where } d = \lceil \frac{q+1-2\sqrt{q}}{4} \rceil$$

The smallest cases are $[11, 5, 6]_4$, $[43, 7, 27]_4$, $[171, 9, 117]_4$.

On the weight distribution of the Kloosterman and dual Zetterberg Code

The weight distribution of both codes were determined (using the Hecke-operator) by Schoof and v.d.Vlugt (91) (see also E.B. (04)).

Definition

Let $q = 2^s$. For $v \in \mathbb{F}_q^*$ let p_v be the number of $x \in \mathbb{F}_q^*$ such that

$$\mathrm{tr}_{s,1}(x) = \mathrm{tr}_{s,1}(v/x) = 1.$$

Also let m_i be the number of v such that $p_v = i$.

Consider the curve

$$y^2 + y = x + \frac{v}{x}$$

defined over $\mathbb{F}_q$. The homogeneous equation is

$$F(X, Y, Z) = XY^2 + XYZ + X^2Z + vZ^3 = 0.$$

The curve is smooth. As the homogeneous polynomial has degree 3 the genus is $\binom{3-1}{2} = 1$, so we do have an elliptic curve.

$F(X, Y, 0) = XY^2$. So there are two points at infinity, $(1:0:0)$ and $(0:1:0)$. Point $(0:1:0)$ is the only one with $X = 0$.

For the other points work with the affine equation. Each x such that $\mathrm{tr}_{s,1}(x + v/x) = 0$ yields precisely two rational points of the curve.

The number N of rational points is

$$N = 2 + 2(2p_v - 1) = 4p_v.$$

By the Hasse inequality

$$q + 1 - 2\sqrt{q} < 4p_v < q + 1 + 2\sqrt{q}$$

(the inequality is strict as, if f is odd the bounds are not integer, if f even they are $1 \mod (2)$), hence

$$\frac{q + 1 - 2\sqrt{q}}{4} < p_v < \frac{q + 1 + 2\sqrt{q}}{4}.$$

Kloosterman codes

The codeword $c(a, b)$ where $a, b \in \mathbb{F}_q$, of the Kloosterman code has entry

$$c(a, b)_x = \mathrm{tr}_{s,1}(ax + b/x)$$

$wt(c(a, 0)) = wt(c(0, b)) = q/2$ and $wt(c(a, b)) = wt(c(1, ab))$. So:

$$wt(c(1, v)) = q - 2p_v.$$

All codewords of the Kloosterman code have even weight. The weight distribution for nonzero weights is given by

$$\begin{aligned} a_{2j} &= (q-1)m_{q/2-j}, \text{ for } j \neq q/4, \text{ and} \\ a_{q/2} &= (q-1)(m_{q/4}+2). \end{aligned}$$

The (even) minimum distance d is bounded by $d > \frac{q-1}{2} - \sqrt{q}$.

Dual Zetterberg codes

Lemma

Let $s = 2t$ and $q = 2^t$. Let $0 \neq \alpha \in \mathbb{F}_q$. The following are equivalent:

- *There exists $x \in W_{q+1} \setminus \{1\}$ such that $\mathrm{tr}_{s,t}(x) = \alpha$*
- $\mathrm{tr}_{t,1}(1/\alpha) = 1$.

A word of the dual Zetterberg code $\mathcal{T}(\{1\}, W_{q+1}, s, 1)$ is $c(u) = (\mathrm{tr}_{s,1}(ux) \mid x \in W_{q+1})$ where $u \in \mathbb{F}_{q^2}$.

$W_{q+1} \cap \mathbb{F}_q = 1$, so any $v \in \mathbb{F}_{q^2}^*$ can be written uniquely in the form $v = ux$, with $u \in \mathbb{F}_q^*$ and $x \in W_{q+1}$.

$$wt(c(v)) = wt(c(ux)) = wt(c(u))$$

As $u \in \mathbb{F}_q^*$ it is $\mathrm{tr}_{s,1}(ux) = \mathrm{tr}_{t,1}(u\alpha)$, where $\alpha = \mathrm{tr}_{s,t}(x)$.
For $x = 1$ the entry $c(u)_x = \mathrm{tr}_{s,1}(ux) = 0$.

So $wt(c(u))$ equals the number of $x \in W_{q+1} \setminus \{1\}$ with $\mathrm{tr}_{t,1}(u\alpha) = 1$. By the lemma then $\mathrm{tr}_{t,1}(1/\alpha) = 1$.

There are $p_{1/u}$ elements $\alpha \in \mathbb{F}_q$ with $\mathrm{tr}_{t,1}(1/\alpha) = \mathrm{tr}_{t,1}(u\alpha) = 1$. Each such α contributes 2 coordinates x. We conclude that for $v = x/u$ the weight $wt(c(v)) = 2p_u$.

All weights of the dual Zetterberg code are even, and its nonzero weights are

$$a_{2i} = (q+1)m_i \text{ for } i > 0.$$

The (even) minimum distance d is bounded by $d > \frac{q+1}{2} - \sqrt{q}$.

References

J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Designs, Codes and Cryptography*, 25:189–206, 2002.

I. Dumer. Nonbinary double-error-correcting codes designed by means of algebraic verieties. *IEEE Transactions on Information Theory*, 41:1657–1666, 1995.

I. Dumer and V. A. Zinoviev. Some new maximal codes over $GF(4)$. *Probl. Peredach.Inform (in Russian)*, 14(3):24–34, 1978. English translation in *Problems of Information Transmission*, 14(3):174–181, 1978.

Y. Edel and J. Bierbrauer. Caps of order $3q^2$ in affine 4-space in characteristic 2. *Finite Fields and their Applications*, 10:168–182, 2004.

References

D. Gevorkyan, A. Avetisyan, and G. Tigranyan. On the structure of two-error-correcting in Hamming metric over Galois fields. *Computational Techniques, Kuibyshev (in Russian)*, 3:19–21, 1975.

J. M. Jensen. Cyclic concatenated codes with constacyclic outer codes. *IEEE Trans. Inf. Theory*, 38(3):950–959, 1992.

F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing Co., Amsterdam, 1977.

R. Schoof and M. van der Vlugt. Hecke operators and the weight distribution of certain codes. *Journal of Combinatorial Theory A*, 57(2):163–186, 1991.