# Cyclic additive and quantum stabilizer codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

March 31, 2007

**Abstract**

We develop the theory of additive cyclic codes and of cyclic quantum stabilizer codes.

## Key words

Cyclic codes, additive codes, quantum codes, Galois group, cyclotomic cosets, Kloosterman codes.

## 1 Introduction

**Definition 1.** *A $q$-linear $q^m$-ary code $[n,k]_{q^m}$ is a $km$-dimensional $\mathbb{F}_q$-subspace of $\mathcal{C} \subseteq E^n$, where $E = \mathbb{F}_q^m$. In particular $\mathcal{C}$ has $q^{km}$ codewords.*

This is a generalization of linear codes in the sense that the alphabet is not considered as field $\mathbb{F}_{q^m}$ but only as a vector space over the subfield $\mathbb{F}_q$. These codes are also collectively known as **additive codes** although it may be wiser to reserve this term for the more general case when the alphabet is considered as an abelian group.

In [8, 2, 3] we generalized the classical theory of linear cyclic codes and obtained a description of a large class of additive cyclic codes. This mechanism was then used to obtain constructions of quantum stabilizer codes. Let us call the family of cyclic additive codes as described in [8, 2, 3] **twisted**

**codes.** The theory of twisted codes does not describe the additive cyclic codes in their generality. A small example of a good cyclic code, which is not twisted, is the $[7, 3.5, 4]_4$-code obtained by a computer construction in Blokhuis-Brouwer [6]. In [4] we give a design-theoretic construction of this code.

One of the main objectives of the present paper is to give a general theory of the additive cyclic codes of length coprime to the characteristic. It turns out that the theory of twisted codes is the main ingredient of the general theory. We obtain a parametric description of all those codes and enumerate them. A first construction result is a cyclic $[15, 4.5, 9]_4$-code. The second main objective is the theory of cyclic quantum stabilizer codes. This is the special case of the general theory when the alphabet is $E = \mathbb{F}_q^2$ and the code is self-orthogonal with respect to the symplectic form. We give a parametric description and an enumeration of those quantum stabilizer codes and of the self-dual such quantum codes. The case $q = 2$ of quaternary quantum stabilizer codes is of special interest. In fact the original paper [7] works only with quaternary codes. A justification of the extension to general self-orthogonal symplectic codes is in [1, 11].

# 2 Notation and twisted codes

Let $n \mid q^r - 1$, where $r$ is the order of $q$ mod $n$. Consider the field $F = \mathbb{F}_{q^r}$ and the trace $tr : F \longrightarrow \mathbb{F}_q$. The Galois group $G = Gal(F|\mathbb{F}_q) = \{g_0, g_1, \ldots, g_{r-1}\}$ where $g_i$ maps $x \in F$ to $x^{q^i}$ acts on $Z_n = \mathbb{Z}/n\mathbb{Z}$ in the natural way. The orbits of $G$ on $Z_n$ are the cyclotomic cosets. For a fixed cyclotomic coset $Z$ we denote $s = |Z|$. Let $z \in Z$. The stabilizer $H$ of $z$ in $G$ has order $r/s$ and is generated by $g_s$. The fixed field of $H$ is $L = \mathbb{F}_{q^s}$. Let $W \subset F$ be the subgroup of order $n$, generated by $\alpha$.

A twisted code $\mathcal{C}$ of length $n$ is described by two ingredients,

- a subset $A \subseteq Z_n$ and
- a tuple $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m) \in F^m$ such that the $\gamma_j$ are linearly indendent over $\mathbb{F}_q$ (and consequently $m \leq r$).

The $F$-vector space $\mathcal{P}(A)$ consists of the polynomials with coefficients in $F$ all of whose monomials have degrees in $A$. The codewords of the $F$-linear length $n$ code $(\mathcal{B}(A), \Gamma)$ are the evaluations $ev(v, \Gamma)$ where $v \in \mathcal{P}(A)$, whose entry in coordinate $u \in W$ is the $m$-tuple $(\gamma_1 v, \dots, \gamma_m v)$. Let $\langle , \rangle$ be a nondegenerate bilinear form on the vector space $E = \mathbb{F}_q^m$, extended to $E^n$ in the natural way. The twisted codes are $tr(\mathcal{B}(A), \Gamma)$ and its dual with respect to $\langle , \rangle$. In a traditional coding context it is natural to choose $\langle , \rangle$ as the Euclidean form (the dot product). In the context of quantum codes one chooses $m = 2$ and a symplectic form, giving $E$ the structure of a hyperbolic plane.

Let $A = \{z\}$ and $Z$ the cyclotomic coset containing $z$. With the notation introduced above ($|Z| = s, H, L$) denote by $\Gamma^H$ the orbit of $\Gamma$ under $H$ and by $\langle \Gamma^H \rangle_F$ the $F$-vector space generated by $\Gamma^H$. Also, let $\langle \gamma_1, \dots, \gamma_m \rangle_L$ be the $L$-vector space generated by the $\gamma_j$.

**Proposition 1.** *The dimension of $tr((\mathcal{B}(z), \Gamma)$ equals*

$$s \cdot dim_F \langle \Gamma^H \rangle_F = s \cdot dim_L(\langle \gamma_1, \dots, \gamma_m \rangle_L)$$

*Proof.* The first expression is a special case of Theorem 21 of [2]. In order to prove the second expression consider the $\mathbb{F}_q$-linear mapping $a \mapsto tr(ev(aX^z, \Gamma))$ which by definition is surjective : $F \longrightarrow tr((\mathcal{B}(z), \Gamma)$. It has $a$ in the kernel if and only if $a \in (\langle \gamma_1, \dots, \gamma_m \rangle_L)^\perp$, where the dual is with respect to the trace form. □

We consider the ambient space $V_F = F^{mn}$ as the space of $n$-tuples of $m$-tuples: $V_F = \{(v_u) \mid u \in W\}$ where $v_u \in F^m$. For each cyclotomic coset $Z$ let $V_F(Z) = ev(\mathcal{P}(Z)^m)$. Here the typical element $(p_1(X), \dots, p_m(X)) \in \mathcal{P}(Z)^m$ has evaluation $(v_u)$, where $v_u = (p_1(u), \dots, p_m(u))$. We have $dim(V_F(Z)) = m|Z|$ and

$$V_F = \oplus_Z V_F(Z).$$

Also the $\mathbb{F}_q$-dimension of $tr(V_F(Z))$ is $m|Z|$ and

$$\mathbb{F}_q^{mn} = E^n = \oplus_Z tr(V_F(Z)).$$

It follows from the classical theory of linear cyclic codes that the dual of $tr(V_F(Z))$ with respect to $\langle , \rangle$ is $\oplus_{Z' \neq -Z} tr(V_F(Z'))$ (see Theorem 13.6 of [3]).

# 3 Irreducible additive cyclic codes

**Definition 2.** *An additive cyclic code is* **irreducible** *if it does not contain proper nonzero additive cyclic subcodes.*

By Maschke's theorem the cyclic additive codes of length coprime to the characteristic are completely reducible. It suffices therefore, in a sense, to describe the irreducible cyclic codes. The irreducible cyclic codes contained in the twisted codes are easy to describe:

**Proposition 2.** *The irreducible cyclic codes contained in the twisted code* $tr((\mathcal{B}(z),\Gamma))$ *are* $\{tr(ev(r_0 a X^z,\Gamma)) \mid a \in L\}$ *where* $r_0 \in F \setminus \langle\gamma_1,\dots,\gamma_m\rangle_L^\perp$ *is fixed and the dual is with respect to the trace form. The dimension of this irreducible cyclic code is* $s = |Z|$.

*Proof.* Because of irreducibility we can restrict to case $A = \{z\}$. Start from $0 \neq v = tr(ev(r_0X^z))$. The fact that $v \neq 0$ is equivalent with $r_0 \notin (\langle\gamma_1,\dots,\gamma_m\rangle_L)^\perp$. Let $\mathcal{C}$ be the cyclic closure of $v$. The cyclic shift produces $tr(ev(r_0\alpha^z X^z))$ where $W = \langle\alpha\rangle$. This shows that $tr(ev(r_0 L X^z)) \subseteq \mathcal{C}$. As this code is additive and cyclic we have equality. The mapping from $a \in L$ to the generic codeword is $\mathbb{F}_q$-linear, and $a \neq 0$ is in the kernel of the mapping if and only if $r_0 \in \langle\gamma_1,\dots,\gamma_m\rangle_L^\perp$, contradiction. It follows that each of these irreducible codes has dimension $s$. □

Comparison with Proposition 1 shows that the twisted code itself is irreducible if and only if $dim_L(\langle\gamma_1,\dots,\gamma_m\rangle_L) = 1$. This means that all the $\gamma_j$ are $L$-multiples of one another.

Next we want to study how twisted codes $tr((\mathcal{B}(z),\Gamma)$ and $tr((\mathcal{B}(z),\Gamma')$ intersect. Let $v = tr(ev(aX^z,\Gamma))$. Then $v$ is in the intersection if there exists $a'$ such that $v = tr(ev(a'X^z,\Gamma')$. This is equivalent with $a\Gamma - a'\Gamma'$ having all its components in $L^\perp$.

**Definition 3.** *Let* $c_s(\Gamma,\Gamma')$ *be the* $L$*-dimension of the space* $A \subseteq F$ *of all* $a$ *such that there exists* $a'$ *satisfying* $a\Gamma - a'\Gamma' \in (L^\perp)^m$. *Here the dual is with respect to the trace form.*

Clearly $A$ is an $L$-vector space and $A \supseteq (\langle\gamma_1,\dots,\gamma_m\rangle_L)^\perp$.

**Proposition 3.** *The dimension of* $tr((\mathcal{B}(z),\Gamma) \cap tr((\mathcal{B}(z),\Gamma')$ *is*

$$s \cdot (c_s(\Gamma,\Gamma') - dim_L(\langle\gamma_1,\dots,\gamma_m\rangle_L^\perp)).$$

*Proof.* The elements of the intersection are parametrized by the elements $a$ of the $s \cdot c_s(\Gamma,\Gamma')$-dimensional space defined above, and $a$ is in the kernel if it is orthogonal to the $L$-vector space generated by the $\gamma_j$. □

Comparison with Proposition 1 shows that $tr((\mathcal{B}(z),\Gamma)\subseteq tr((\mathcal{B}(z),\Gamma')$ if and only if $c_s(\Gamma,\Gamma')=r/s$ and $tr((\mathcal{B}(z),\Gamma)\subseteq tr((\mathcal{B}(z),\Gamma')$ if and only if $c_s(\Gamma,\Gamma')=c_s(\Gamma',\Gamma)=r/s$.

A central result is the following:

**Theorem 1.** *Let $\mathcal{C}$ be an irreducible cyclic additive $q^m$-ary $q$-linear code of length $n$ where $gcd(n,q)=1$ such that the projection to each of the $m$ coordinates is nonzero. Then $\mathcal{C}$ is contained in a twisted code.*

*Proof.* Let $\pi_j$ be the projection from $\mathbb{F}_q^m$ onto coordinate $j$, where $j=1,\dots,m$. By assumption $\pi_j(\mathcal{C})$ is not the 0-code. As it is a $q$-ary linear cyclic code it can be described by a nonempty union $Z_j$ of cyclotomic cosets. Because of irreducibility each $Z_j$ is a cyclotomic coset. Choose $z_j\in Z_j$ and consider the stabilizers $H_j$ and fixed fields $L_j$. Let $\mathcal{B}$ be the set of all $m$-tuples $(v_1,\dots,v_m)$ of polynomials whose trace-evaluations are in $\mathcal{C}$. By definition and basic properties of the trace we can choose $v_j=b_jX^{z_j}$. Without restriction there is some $(aX^{z_1},bX^{z_2},\dots)\in\mathcal{B}$ where $a\notin L_1^{\perp},b\notin L_2^{\perp}$. Let $\alpha$ be a generator of $W$. The cyclicity shows that some $(a\alpha^{z_1}X^{z_1},b\alpha^{z_2}X^{z_2},\dots)\in\mathcal{B}$, by induction $(a\alpha^{iz_1}X^{z_1},b\alpha^{iz_2}X^{z_2},\dots)\in\mathcal{B}$ for all $i=0,1,\dots$. Assume $ord(\alpha^{z_1})\neq ord(\alpha^{z_2})$. Without restriction there is some $i$ such that $\alpha^{iz_1}=1,\alpha^{iz_2}\neq 1$. After subtraction this yields $(0,b(\alpha^{iz_2}-1)(X^{z_2},\dots)\in\mathcal{B}$. This contradicts the irreducibility. It follows $ord(\alpha^{z_1})=ord(\alpha^{z_2})$ and therefore $|Z_1|=|Z_2|=s$. Let $\beta=\alpha^{z_1}$. Then $\alpha^{z_2}=\beta^j$ for a $j$ coprime with the order of $\beta$. The smallest field containing $\beta$ is $L=GF(q^s)$. The irreducibility shows that $\sum c_i\beta^i=0$ with coefficients $c_i\in\mathbb{F}_q$ if and only if $\sum c_i\beta^{ij}=0$. This shows that raising to the $j$-th power is a field automorphism of $L$. It follows that $z_2$ and $z_1$ are in the same cyclotomic coset. $\square$

# 4 The additive cyclic codes

By Theorem 1 each irreducible additive cyclic code is contained in a twisted code provided all its $m$ coordinate projections are nonzero. By Proposition 2 we know the irreducible cyclic codes contained in twisted codes. If some of the coordinate projections of our irreducible cyclic code vanish, then we should forget them. The code is then contained in a twisted code for a smaller value of $m$. It follows that an irreducible cyclic additive code $\mathcal{C}$ is determined by the following ingredients:

- the support consisting of the coordinates $j \in \{1, 2, \ldots, m\}$ such that $\pi_j(\mathcal{C}) \neq 0$,
- an $m$-tuple $\Gamma$ with 0-entries outside of the support and nonzero entries in the support,
- a cyclotomic coset and,
- in the case when the corresponding twisted code is not irreducible, a coset (see Proposition 2).

The first two ingredients can be combined into one: a nonzero tuple $\Gamma \in F^m$. We specialize to case $m = 2$ now.

**Theorem 2.** *The irreducible cyclic additive codes in case $m = 2$ are the twisted codes $tr((\mathcal{B}(z), \Gamma)$, where $z$ varies over representatives $z$ of cyclotomic cosets and $\Gamma$ varies over representatives of points in $PG(1, L)$, where $L = GF(q^s)$ and $s = |Z|$.*

*Proof.* We know that all those codes are indeed irreducible, and they are precisely the twisted codes (with $m = 2$ or $m = 1$) which are irreducible cyclic codes. Consider now a code $tr((\mathcal{B}(z), \Gamma')$ where $\Gamma' = (1, \gamma')$ and $\gamma \notin L$. Let $\Gamma = (1, \gamma)$ where $\gamma \in L$. We claim that $tr((\mathcal{B}(z), \Gamma) \subset tr((\mathcal{B}(z), \Gamma')$. In order to show this it suffices by Proposition 3 to show that for each $a \in F$ we can find $a'$ such that $a(1, \gamma) - a'(1, \gamma') \in (L^{\perp})^2$, in other words $tr_L(\gamma')$ and $tr_L(a'\gamma')$ are prescribed, where $tr_L$ is the trace : $F \longrightarrow L$. As $\gamma' \notin L$ this is possible. The same proof works when $\Gamma = (0, 1)$. We see that the nonzero elements of the $2s$-dimensional code $tr((\mathcal{B}(z), \Gamma')$ are partitioned into the nonzero elements of those irreducible twisted subcodes. $\square$

**Proposition 4.** *The number of nonzero irreducible cyclic additive codes in case $m = 2$ is $\sum_Z (q^{|Z|} + 1)$.*

We also obtain a complete picture of the additive cyclic codes, at least in case $m = 2$. Recall that the ambient space $E^n = \mathbb{F}_q^{2n}$ is written as the direct sum of the $tr(V_F(Z))$, where $Z$ varies over the cyclotomic cosets and $dim(tr(V_F(Z))) = 2|Z| = 2s$. Each $\Gamma \in F \times F$ generates a point $P \in PG(1, F)$. Choose a representative $z$ for each cyclotomic coset $Z$. The irreducible cyclic codes are precisely the $tr(\mathcal{B}(z), \Gamma)$ where $z$ varies over the representatives of cyclotomic cosets and $\Gamma$ varies over representatives of points in $PG(1,q^s)$ (and $|Z|=s$). Each $Z$ therefore yields $q^s+1$ irreducible cyclic codes, each of $\mathbb{F}_q$-dimension $s$. Their nonzero elements partition the $2s$-dimensional space $tr(V_F(Z))$, and $tr((\mathcal{B}(z),\Gamma)=tr(V_F(Z))$ whenever $\Gamma$ generates a point of $PG(1,F)$ which is not in $PG(1,L)$.

**Theorem 3.** *The number of cyclic additive codes in case $m=2$ is $\prod_Z(q^{|Z|}+3)$.*

*Proof.* In order to describe a cyclic code we have to decide the contribution of each cyclotomic coset $Z$. If $|Z|=s$ there are $q^s+3$ possibilities: the summand is either one of the $q^s+1$ irreducible codes (dimension $s$ each) or the 0-code or is $tr(V_F(Z))$. □

## Lengths 7 and 15

As illustrative examples consider the quaternary length 7 and 15 cases. In the first case ($q=2, m=2, n=7$) we have cyclotomic cosets of lengths $1,3,3$ (representatives $0,1,-1$) and therefore $3+9+9=21$ irreducible cyclic, $5\times 11\times 11=605$ cyclic codes alltogether. A $[7,3.5,4]_4$-code is obtained as the sum of the irreducible codes $tr((\mathcal{B}(1),1,0)$, $tr((\mathcal{B}(-1),0,1)$, $tr((\mathcal{B}(0),1,1)$. It is self-dual with respect to the dot product but not self-dual with respect to the symplectic form. In fact, there is no additive code with these parameters which is self-dual in the symplectic sense, as this would generate a quantum code $[[7,0,4]]_4$ which cannot exist (see [10]).

In length 15 we use the primitive equation $\epsilon^4=\epsilon+1$ for $F=GF(16)=\mathbb{F}_2(\epsilon)$. Representatives of the cyclotomic cosets are 0 (length 1), 5 (length 2) and $1,3,14$ (length 4 each). There are $3+5+3\times 17=59$ irreducible cyclic codes and a total of $5\times 7\times 19^3$ cyclic codes. Define

$$\mathcal{C}=tr((\mathcal{B}(1),\epsilon,1)\oplus tr((\mathcal{B}(3),1,\epsilon^2)\oplus tr((\mathcal{B}(0),1,1).$$

Then $\mathcal{C}$ is a $[15,4.5,9]_4$-code. These are new parameters. In fact a linear $[15,5,9]_4$ cannot exist. Here is a concrete representation of its subcode $\mathcal{D}=tr((\mathcal{B}(1),\epsilon,1)\oplus tr((\mathcal{B}(3),1,\epsilon^2)$. The codewords are parametrized by pairs $a,b\in F=GF(16)$, the coordinates by $0\neq x\in F$ and the corresponding entry is the pair

$$c_{a,b}(x)=(tr(\epsilon ax+bx^3), tr(ax+\epsilon^2bx^3)).$$

Cases $b=0$ and $a=0$ describe the two irreducible subcodes. $\mathcal{C}$ is the direct sum of $\mathcal{D}$ and $11^{15}$.

# 5 Cyclic quantum stabilizer codes

This corresponds to the case when $m = 2$ and the bilinear form $\langle , \rangle$ on $E = \mathbb{F}_q^2$ is symplectic. Such a cyclic $q^2$-ary code $\mathcal{C}$ of length $n$ coprime to the characteristic is a **quantum stabilizer code** if it contains its dual. If $\mathcal{C} \supseteq \mathcal{C}^\perp$ has dimension $k$ and all codewords in $\mathcal{C} \setminus \mathcal{C}^\perp$ have weight $\geq d$, then the quantum parameters are written as $[[n, 2k - n, d]]_{q^2}$. The code is **pure** if all nonzero codewords of $\mathcal{C}$ have weight $\geq d$.

**Theorem 4.** *A cyclic additive $q^2$-ary quantum code is equivalent with a cyclic additive code in case $m = 2$ which is contained in its dual with respect to the symplectic form $\langle , \rangle$.*

Our first objective is to give a parametrized description of the self-orthogonal codes $\mathcal{B}$ as in Theorem 4. Write $\mathcal{B} = \sum_Z S_Z$. Recall from the introduction and [3] that

$$tr(V_F(Z))^\perp = \sum_{Z' \neq Z} tr(V_F(Z')).$$

It follows that $\mathcal{B}$ is self-orthogonal if and only if $S_Z$ and $S_{-Z}$ are orthogonal for each $Z$. Consider at first the generic case $Z \neq -Z$. If one of the $S_Z$ or $S_{-Z}$ is 0, then there is no restriction on the other. If $S_Z = tr(V_F(Z))$, then $S_{-Z} = 0$.

We use Lemma 17.26 of [3]:

**Lemma 1.** $\sum_{u \in W} tr(\alpha u^{z_0}) tr(\beta u^{-z_0}) = n \times tr(\alpha Tr(\beta))$, *where $Tr$ is the trace $: F \longrightarrow \mathbb{F}_{q^s}$.*

**Proposition 5.** *Let $\Gamma = (\gamma_1, \gamma_2), \Gamma' = (\gamma_1', \gamma_2') \in L \times L$. The irreducible cyclic codes $tr((\mathcal{B}(z), \Gamma)$ and $tr((\mathcal{B}(-z), \Gamma')$ are orthogonal if and only if $\Gamma$ and $\Gamma'$ generate the same point in $PG(1, L)$.*

*Proof.* Writing out the symplectic product of typical vectors we obtain the condition

$$\sum_{u \in W} tr(\gamma_1 a u^z) tr(\gamma_2' b u^{-z}) - tr(\gamma_2 a u^z) tr(\gamma_1' b u^{-z}) = 0$$

for all $a, b \in F$. Because of Lemma 1 and the $L$-linearity of $Tr$ an equivalent condition is $\gamma_1 \gamma_2' = \gamma_2 \gamma_1'$. $\square$

This shows what the self-orthogonality condition is: if $S_Z = tr((\mathcal{B}(z), \Gamma)$ for $\Gamma \in PG(1, q^s)$, then either $S_{-Z} = 0$ or $S_{-Z} = tr((\mathcal{B}(-z), \Gamma)$.

Consider case $Z = -Z, s > 1$. Then either $S_Z = 0$ or $S_Z$ is a self-orthogonal irreducible code $tr((\mathcal{B}(z), \Gamma)$. By Proposition 5 this must coincide with $tr((\mathcal{B}(-z), \Gamma)$. We have $s = 2i$ and $zq^i = -z$. It follows $tr((\mathcal{B}(-z), \Gamma) = tr((\mathcal{B}(z), \Gamma^{q^i})$ and the condition is that $\Gamma$ and $\Gamma^{q^i}$ generate the same projective point, which means that $\Gamma \in PG(1, q^i)$. There are $q^i + 1$ choices for $\Gamma$. As $Z = \{0\}$ contributes $q + 2$ self-orthogonal and $q + 1$ self-dual codes we arrive at the following enumeration result:

**Theorem 5.** *The number of additive cyclic $q^2$-ary quantum stabilizer codes is*

$$\prod_{Z=-Z, s=1} (q+2) \prod_{Z=-Z, s>1} (q^{s/2}+2) \prod_{Z \neq -Z} (3q^s+6).$$

*The number of self-dual such codes is*

$$\prod_{Z=-Z, s=1} (q+1) \prod_{Z=-Z, s>1} (q^{s/2}+1) \prod_{Z \neq -Z} (q^s+3).$$

*Here $s = |Z|$ and the last product is over all pairs $\{Z, -Z\}$ of cyclotomic cosets such that $Z \neq -Z$.*

In case $n = 7$ we obtain $4 \times 30 = 120$ quantum codes alltogether and $3 \times 11 = 33$ self-dual ones, for $n = 15$ the number of quantum codes is $4 \times 4 \times 6 \times 54$ and there are $3 \times 3 \times 5 \times 19$ self-dual codes.

# 6 Codes of Kloosterman type

The self-dual $[7, 3.5, 4]_4$-code of Section 4 is generated by the all-1-word and a code whose words are indexed by a pair $a, b$ of elements of $\mathbb{F}_8$, with entry $(tr(ax), tr(b/x))$ in coordinate $x \in \mathbb{F}_8^*$. This is very much remeniscent of the Kloosterman or dual Mélas codes.

**Definition 4.** *Let $q = 2^f$. The Kloosterman code is a $2f$-dimensional length $q - 1$ binary code whose codewords are $c(a, b)$, where $a, b \in \mathbb{F}_q$, with entry $tr(ax + b/x)$ in coordinate $0 \neq x \in \mathbb{F}_q$.*

**Definition 5.** *For $0 \neq v \in \mathbb{F}_q$ let $p_v$ be the number of $0 \neq x \in \mathbb{F}_q$ such that $tr(x) = tr(v/x) = 1$. Here $tr$ is the absolute trace.*

The determination of the minimum distance of the Kloosterman codes is equivalent with the determination of the largest number $p_v$. A close relation with elliptic curves shows that this number is the largest integer less than $(q+1+2\sqrt{q})/4$. Schoof-van der Vlugt [12] have indeed determined the weight distribution of the Kloosterman codes. In [9] we made use of this information to determine the weight distribution of certain extremal caps in $AG(4,q)$.

We may consider $tr((\mathcal{B}(1),1,0)\oplus tr((\mathcal{B}(-1),0,1)$ and its direct sum with $tr((\mathcal{B}(0),1,1)$ in case $q=2, m=2, n=2^r-1$ as additive versions of Kloosterman codes. Unfortunately we cannot expect good code parameters in general as the irreducible subcodes themselves have minimum distance $2^{r-1}$. Consider instead the codes

$$tr((\mathcal{B}(1),1,\gamma_1)\oplus tr((\mathcal{B}(-1),1,\gamma_2)$$

where the $\gamma_i$ are different and not in $\mathbb{F}_2$. In this case the irreducible summands have minimum weights $2^r-2^{r-2}$. The general codeword $v(a,b)$ (where $a,b\in F=GF(2^r)$) has entry

$$v(a,b)_x=(tr((ax+b/x),tr(a\gamma_1x+b\gamma_2/x))$$

in coordinate $x\neq 0$. We can assume $ab\neq 0$. Let $v=ab$ and replace $x$ by $vx$. In order to determine the minimum distance one has to count the $x\neq 0$ such that

$$tr(x+v/x)=tr(\gamma_1x+\gamma_2v/x)=0.$$

# References


[1] A. Ashikhmin and E. Knill: *Nonbinary quantum stabilizer codes, IEEE Transactions on Information Theory* **47** (2001), 3065-3072.

[2] J.Bierbrauer: *The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography* **25** (2002), 189-206.

[3] J.Bierbrauer: *Introduction to Coding Theory, Chapman and Hall/CRC Press*, 2004.

[4] J. Bierbrauer, G. Faina, S. Marcugini, F. Pambianco: *Additive quaternary codes of small length, Proceedings ACCT, Zvenigorod (Russia) September 2006*, 15-18.

[5] J. Bierbrauer and Y. Edel: Quantum twisted codes, *Journal of Combinatorial Designs* **8** (2000), 174-188.

[6] A. Blokhuis and A. E. Brouwer, *Small additive quaternary codes, European Journal of Combinatorics* **25** (2004), 161-167.

[7] A.R.Calderbank,E.M.Rains,P.W.Shor and N.J.A.Sloane: *Quantum error correction via codes over GF(4), IEEE Transactions on Information Theory* **44** (1998),1369-1387.

[8] Y.Edel and J.Bierbrauer:*Twisted BCH-codes, Journal of Combinatorial Designs* **5** (1997), 377-389.

[9] Y.Edel and J.Bierbrauer: Caps of order $3q^2$ in affine 4-space in characteristic 2, *Finite Fields and Their Applications* **10** (2004), 168-182.

[10] M. Grassl: Tables on http://iaks-www.ira.uka.de/home/grassl/

[11] E.M.Rains: *Nonbinary quantum codes, IEEE Transactions on Information Theory* **45** (1999),1827-1832.

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