Journal of Algebra 372 (2012) 661–672

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Cyclic additive codes

Jürgen Bierbrauer [1,2]

Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

ARTICLE INFO

Article history:
Received 12 February 2012
Available online 9 October 2012
Communicated by Gerhard Hiss

Keywords:
Cyclic codes
Additive codes
Cyclotomic cosets
Monomial equivalence
Maschke theorem
Galois closure
Duality
Quantum codes

ABSTRACT

We develop the theory of additive cyclic codes.

1. Introduction

We develop the theory of additive cyclic codes in the case when the length of the code is coprime to the characteristic of the field. The definition of an additive code and some basic relations between a code defined over an extension field and its subfield and trace codes are recalled in Section 2. Section 3 discusses the notions of cyclicity of a code. In Section 4 we develop the theory of additive codes which are cyclic in the permutation sense. This contains the classical theory of cyclic linear codes. We discuss when cyclic codes are equivalent and consider the special case of cyclic quantum codes. The general theory of additive codes which are cyclic in the monomial sense is discussed in Section 5. It is proved in Corollary 3 that each quaternary additive code which is cyclic in the monomial sense either is cyclic in the (more restricted) permutation sense or is linear over $\mathbb{F}_4$.

Special cases of this theory were published in earlier work [5,4,1–3].

E-mail address: jbierbra@mtu.edu.
[1] Research partially supported by NSA grant H98230-10-1-0159.
[2] Research supported by the GOA project Incidence Geometry of Ghent University.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2012.08.031

2. Basic facts

Definition 1. A q-linear q^m-ary code $[n,k]_{q^m}$ is a km-dimensional $\mathbb{F}_q$-subspace $\mathcal{C}\subseteq E^n$, 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 a 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**. Observe that the case $m=1$ constitutes the family of **linear codes** (over a field $\mathbb{F}_q$). We will develop the general theory of additive codes which are cyclic in the monomial sense under the general assumption that the characteristic p of the underlying field is coprime to the length n of the code. The main effect of the assumption is that the action of a (cyclic) group of order n on a vector space over a field of characteristic p is completely reducible, by Maschke's theorem (see Definition 5 and Theorem 1). We will make use of basic relations between linear codes over a finite field F and its trace codes and subfield codes over a subfield $K\subset F$. These basic facts and fundamental notions like the Galois group, cyclotomic cosets and Galois closedness are introduced in Chapter 12 of [2]. Recall in particular the Delsarte theorem (Theorem 12.14 of [2]) relating codes over F, their duals, the trace codes and the subfield codes as well as Theorem 12.17 of [2] which states among other things that $\dim_F(U)=\dim_K(tr(U))$ provided the F-linear code U is Galois closed with respect to the subfield K.

3. Code equivalence and cyclicity

Definition 2. Codes $\mathcal{C}$ and $\mathcal{D}$ are **permutation equivalent** if there is a permutation π on n objects such that

$$(x_1,x_2,\ldots,x_n)\in\mathcal{C}\quad\Longleftrightarrow\quad(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(n)})\in\mathcal{D}$$

for all $x=(x_1,\ldots,x_n)\in\mathcal{C}$.

The notion of permutation equivalence can be used for all codes of fixed block length n. It uses the symmetric group S_n as group of motions. Two codes are equivalent if they are in the same orbit under S_n. The stabilizer under S_n is the permutation automorphism group of the code.

In the special case of additive codes, the following more general notion of equivalence is more natural.

Definition 3. q-linear q^m-ary codes $\mathcal{C}$ and $\mathcal{D}$ are **monomially equivalent** if there exist a permutation π on n objects and elements $A_i\in GL(m,q)$ such that

$$(x_0,x_1,\ldots,x_{n-1})\in\mathcal{C}\quad\Longleftrightarrow\quad(A_0x_{\pi(1)},A_1x_{\pi(2)},\ldots,A_{n-1}x_{\pi(n-1)})\in\mathcal{D}$$

for all $x=(x_0,\ldots,x_{n-1})\in\mathcal{C}$.

The group of motions is the wreath product of $GL(m,q)$ and S_n, of order $|GL(m,q)|^n\times n!$ and two additive codes are equivalent in the monomial sense if they are in the same orbit under the action of this larger group. The elements of the wreath product are described by $(n+1)$-tuples $(A_0,\ldots,A_{n-1},\pi)$ where the coefficients $A_i\in GL(m,q)$ and the permutation $\pi\in S_n$. Write the elements of the monomial group as $g(A_0,\ldots,A_{n-1},\pi)$.

Definition 4. A code $\mathcal{C}$ of length n is **cyclic** in the permutation sense if there is an n-cycle $\pi\in S_n$ such that $\pi(\mathcal{C})=\mathcal{C}$.

A q-linear q^m-ary code $\mathcal{C}$ is **cyclic** in the monomial sense if it is invariant under an element $g(A_0,\ldots,A_{n-1},\pi)$ of the monomial group where $\pi\in S_n$ is an n-cycle.

As the n-cycles are conjugate in S_n, it is clear that each code which is cyclic in the permutation sense is permutation equivalent to a code which is invariant under the permutation $\pi = (1, 2, \ldots, n)$.

Proposition 1. *Let $\mathcal{C}$ be q-linear q^m-ary of length n and cyclic in the monomial sense. Then the following hold*:

- *$\mathcal{C}$ is monomially equivalent to a code which is invariant under $g(I, \ldots, I, A'_{n-1}, \pi)$ where $\pi = (0, 1, \ldots, n-1)$.*
- *If $\mathcal{C}$ is invariant under $g(A_0, \ldots, A_{n-1}, (0, \ldots, n-1))$ and $A_0A_1 \ldots A_{n-1} = I$, then $\mathcal{C}$ is cyclic in the permutation sense.*
- *If $\mathcal{C}$ is invariant under $g(I, \ldots, I, A, (0, \ldots, n-1))$ and $ord(A)$ is coprime to n, then $\mathcal{C}$ is cyclic in the permutation sense.*

Proof. We just saw that we can assume $\mathcal{C}$ to be invariant under $g(A_0, A_1, \ldots, A_{n-1}, \pi)$ where $\pi = (0, 1, \ldots, n-1)$. We have that $(x_i) \in \mathcal{C}$ implies $(A_i x_{i+1}) \in \mathcal{C}$. Let now

$$\mathcal{C}' = \left\{ (B_0 x_0, \ldots, B_{n-1} x_{n-1}) \;\middle|\; x = (x_0, \ldots, x_{n-1}) \in \mathcal{C} \right\}.$$

Let $y_i = B_i x_i$. Then $(y_i) \in \mathcal{C}'$ implies $(B_i A_i B_{i+1}^{-1} y_{i+1}) \in \mathcal{C}'$. Choose the B_i such that (for $i = 0$) $B_1 = B_0 A_0$ (for $i = 1$) $B_2 = B_1 A_1 = B_0 A_0 A_1$, up to (for $i = n-2$) $B_{n-1} = B_{n-2} A_{n-2} = B_0 A_0 \ldots A_{n-2}$. It follows that $\mathcal{C}'$ is invariant under $g(I, \ldots, I, A, (0, 1, \ldots, n-1))$ as claimed. Here $A = B_0(A_0 A_1 \ldots A_{n-1}) B_0^{-1}$, a conjugate of $A_0 A_1 \ldots A_{n-1}$. The first statement concerning cyclicity in the permutation sense follows. Let now $\mathcal{C}$ be invariant under $g = g(I, \ldots, I, A, (0, \ldots, n-1))$ and $ord(A) = u$ coprime to n. Then g^u has u of its coefficients equal to A, the others $= I$. The permutation of g^u is an n-cycle. The first statement implies that $\mathcal{C}$ is cyclic in the permutation sense. □

The cyclic group $G = \langle g(A_0, \ldots, A_{n-1}, (0, \ldots, n-1)) \rangle$ has an order a multiple of n and acts on an n-dimensional vector space V over $\mathbb{F}_q$. The cyclic codes are the G-submodules of V. The theory simplifies considerably if the action of G on V is completely reducible.

Definition 5. Let the group G act on a vector space $V = V(n, K)$. An **irreducible submodule** $A \subset V$ is a nonzero G-submodule which does not contain a proper G-submodule (different from 0 and from A itself). The action of G is **completely reducible** if for every G-submodule $A \subset V$ there is a direct complement B of A which is a G-module.

If the action is completely reducible, it suffices in a way to know the irreducibles, as every G-submodule is a direct sum of irreducibles. There is still work to do as the representation of a module as a direct sum of irreducibles may not be unique. However the situation is a lot simpler than in the cases where complete reducibility is not satisfied. This is where Maschke's theorem comes in.

Theorem 1 *(Maschke). In the situation of Definition 5, let the order of G be coprime to the characteristic p of the underlying field. Then the action of G is completely reducible.*

See also [7, p. 666]. This fundamental theorem is the reason why in the theory of cyclic codes it is often assumed that $\gcd(n, p) = 1$.

4. Additive codes which are cyclic in the permutation sense

Recall the situation: W is the cyclic group generated by the permutation $(0, 1, \ldots, n-1)$. It acts on the vector space $V(n, q)$ as a cyclic permutation of the coordinates. The W-submodules are precisely the cyclic linear codes over $\mathbb{F}_q$. We assume $\gcd(n, p) = 1$. Because of Maschke's theorem the action of W on $V(n, q)$ is completely reducible.

Let $r = ord_n(q)$ be the order of q when calculating mod n. Then $n|(q^r - 1)$ and r is the smallest natural number with this property. Let $F = \mathbb{F}_{q^r}$. We find then a cyclic group of order n in F^*. It will be profitable to identify W with this subgroup of F^*. Let $W = \langle\alpha\rangle$.

As we are interested in cyclic **additive** codes, our alphabet is $E = \mathbb{F}_q^m$ and we study the action of W on $V_m = E^n = \mathbb{F}_q^{mn}$. Keep in mind however that we consider the elements of V_m (the codewords) not as nm-tuples over $\mathbb{F}_q$ but rather as n-tuples over E. Refer to the n entries of a codeword as the outer coordinates (in bijection with the elements α^i, $i = 0, \ldots, n-1$, of W) and to the m coordinates of the alphabet E as the inner coordinates. Let $V_{m,F} = V_m \otimes F = (F^m)^n$ be obtained by constant extension with the action of W on outer coordinates. We will relate the codes $C \subset V_m = E^n = \mathbb{F}_q^{nm}$ to their constant extensions $C \otimes F \subset V_{m,F}$ and use basic facts concerning relations between codes defined over a larger field F and a subfield $\mathbb{F}_q$. In particular we associate to each subcode $U \subset V_{m,F}$ its trace code $tr(U) \subset V_m$ obtained by applying the trace $tr = tr_{F|\mathbb{F}_q}$ in each inner coordinate.

Project to one of the m inner coordinates. We obtain then spaces $\mathbb{F}_q^n$ and F^n. The elements of F^n can be uniquely described by univariate polynomials $p(X) \in F[X]$ of degree $< n$, where the codeword defined by $p(X)$ is the evaluation $ev(p(X)) = (p(\alpha^i))$, $i = 0, \ldots, n-1$. Doing this for each inner coordinate we see that the elements of $V_{m,F}$ can be uniquely described by tuples $(p_1(X), \ldots, p_m(X))$ of polynomials $p_j(X) \in F[X]$ of degree $< n$, where the corresponding codeword is the evaluation $ev(p_1(X), \ldots, p_m(X)) = (p_1(\alpha^i), p_2(\alpha^i), \ldots, p_m(\alpha^i))_i$ (an n-tuple of m-tuples, each of the nm entries in F).

Consider the Galois group $G = Gal(F|\mathbb{F}_q)$ (cyclic of order r) and its orbits on $\mathbb{Z}/n\mathbb{Z}$, the cyclotomic cosets. We interpret the elements of $\mathbb{Z}/n\mathbb{Z}$ as the exponents of α in the description of the elements of the cyclic group W. For each polynomial $p(X) \in F[X]$ of degree $< n$, consider the exponents of the monomials occurring in $p(X)$ and how they distribute on the cyclotomic cosets.

Definition 6. Let $\mathcal{P}$ be the space of polynomials in $F[X]$ of degree $< n$. Then $\mathcal{P}$ is an n-dimensional F-vector space. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a set of exponents. The F-vector space $\mathcal{P}(A)$ consists of the polynomials $\in F[X]$ of degree $< n$ all of whose monomials have degrees in A. The **Galois closure** $\tilde{A}$ of A is the union of all cyclotomic cosets that intersect A nontrivially.

Observe that $\mathcal{P}(A)$ is an F-vector space of dimension $|A|$ and it is isomorphic to $ev(\mathcal{P}(A)) \subset V_{1,F}$. The terminology of Definition 6 is justified by the obvious fact that the Galois closure of the code $ev(\mathcal{P}(A)) \subset V_{1,F} = F^n$ is $ev(\mathcal{P}(\tilde{A}))$.

4.1. Linear cyclic codes (case $m = 1$)

We have $\mathcal{P} = \bigoplus_Z \mathcal{P}(Z)$ where Z varies over the cyclotomic cosets and correspondingly $V_{1,F} = F^n = \bigoplus_Z ev(\mathcal{P}(Z))$. As the $ev(\mathcal{P}(Z))$ are Galois closed we also have $V_1 = \mathbb{F}_q^n = \bigoplus tr(ev(\mathcal{P}(Z)))$ and $\dim_{\mathbb{F}_q}(tr(ev(\mathcal{P}(Z)))) = \dim_F(ev(\mathcal{P}(Z))) = |Z|$. Let $V_1(Z) = tr(ev(\mathcal{P}(Z)))$. It is our first task to identify the irreducible W-submodules (the irreducible cyclic codes) in V_1.

Theorem 2. *In case $m = 1$, $\gcd(n, p) = 1$ the irreducible cyclic codes in the permutation sense are precisely the $V_1(Z) = tr(ev(\mathcal{P}(Z)))$ of $\mathbb{F}_q$-dimension $|Z|$ where Z is a cyclotomic coset. Each cyclic code can be written as a direct sum of irreducibles in precisely one way. The total number of cyclic codes is 2^u, where u is the number of different cyclotomic cosets.*

Theorem 2 is of course well known in the classical theory of linear cyclic codes. In order to be self-contained we will prove it in the remainder of this subsection.

It follows from basic properties of the trace that in the description of a code $\mathcal{C} \subseteq V_1$ by codewords $tr(ev(p(X)))$ it suffices to use polynomials of the form $p(X) = a_1X^{z_1} + a_2X^{z_2} + \cdots$ where $z_1, z_2, \ldots$ are representatives of different cyclotomic cosets.

Lemma 1. *Let Z be a cyclotomic coset, $z \in Z$, $|Z| = s$, $L = \mathbb{F}_{q^s}$. The $\mathbb{F}_q$-vector space $\langle W^z\rangle$ generated by the u^z where $u \in W$ is L. The codeword $tr(ev(aX^z))$ where $a \in F$ is identically zero if and only if $a \in L^\perp$ where duality is with respect to the trace form.*

Proof. As $ev(\mathcal{P}(Z))$ is F-linear and Galois closed of dimension s, it follows that $tr(ev(\mathcal{P}(Z)))$ is $\mathbb{F}_q$-linear of dimension s. Its generic codeword is $tr(ev(aX^z))$. This codeword is identically zero if and only if $a \in \langle W^z\rangle^\perp$. Comparing dimensions shows $\dim(\langle W^z\rangle) = s$. Let $u \in W$. Then $u^{zq^s} = u^z$ by definition of a cyclotomic coset. This shows $W^z \subset L$. It follows $\langle W^z\rangle = L$. □

Lemma 1 shows that we can assume $a_i \notin L_i^\perp$ for each i. Let us speak of a polynomial in **standard form** in this case, for the moment. Observe that $tr(ev(p(X))) = tr(a_1X^{z_1}) + tr(a_2X^{z_2}) + \cdots$ and the summands $tr(a_iX^{z_i})$ are in different parts of the direct sum decomposition $V_1 = \bigoplus_Z V_1(Z)$.

Lemma 2. *Let $\mathcal{C} \subseteq V_1$ be a cyclic code and $\mathcal{B} \subseteq \mathcal{P}$ the set of all polynomials $p(X)$ of degree $< n$ such that $tr(ev(p(X))) \in \mathcal{C}$. Let $p(X) = a_1X^{z_1} + a_2X^{z_2} + \cdots \in \mathcal{B}$ where $z_1, z_2, \ldots$ are representatives of different cyclotomic cosets. Then $p^{(l)}(X) = a_1\alpha^{lz_1}X^{z_1} + a_2\alpha^{lz_2}X^{z_2} + \cdots \in \mathcal{B}$ for all l. The smallest cyclic code containing $tr(ev(p(X)))$ is the code spanned by the $tr(ev(p^{(l)}(X)))$ for all l.*

Proof. The entry of $tr(ev(p(X)))$ in coordinate α^i is $tr(a_1\alpha^{iz_1} + a_2\alpha^{iz_2} + \cdots)$. After cyclic shift we obtain a codeword whose entry in coordinate α^i is $tr(a_1\alpha^{(i+1)z_1} + a_2\alpha^{(i+1)z_2} + \cdots) = tr(a_1\alpha^{z_1}\alpha^{iz_1} + a_2\alpha^{z_2}\alpha^{iz_2} + \cdots)$ which is the trace of the evaluation of $a_1\alpha^{z_1}X^{z_1} + a_2\alpha^{z_2}X^{z_2} + \cdots$. The first claim follows by repeated application, the second is obvious. □

Let us complete the proof of Theorem 2. Let $\mathcal{C}$ be an irreducible cyclic code and $tr(ev(p(X))) \in \mathcal{C}$ where $p(X)$ is in standard form. Assume $p(X)$ is not a monomial. Let $\mathcal{B}$ be defined as in Lemma 2 and $p(X) = a_1X^{z_1} + a_2X^{z_2} + \cdots \in \mathcal{B}$. Lemma 2 implies that $a_1\alpha^{lz_1}X^{z_1} + a_1\alpha^{lz_2}X^{z_2} \in \mathcal{B}$ for all l. Assume at first $|Z_1| \neq |Z_2|$. Choose l such that $\alpha^{lz_1} = 1$ and $\alpha^{lz_2} \neq 1$. By subtraction we have $a_2(\alpha^{lz_2} - 1)X^{z_2} + \cdots \in \mathcal{B}$. The cyclic code generated by the trace-evaluation of this polynomial has trivial projection to $V_1(Z_1)$. As this is not true of $\mathcal{C}$ it follows from irreducibility that this codeword must be the 0-word, hence $a_2(\alpha^{lz_2} - 1) \in L_2^\perp$. This implies $a_2 \in L_2^\perp$, a contradiction. Assume now $|Z_1| = |Z_2| = s$, let $L = \mathbb{F}_{q^s}$. Use Lemma 2. Let $c_l \in \mathbb{F}_q$ such that $\sum_l c_l\alpha^{lz_1} = 0$. The same argument as above shows that $\sum_l c_l\alpha^{lz_2} = 0$. We have $\beta = \alpha^{z_1} \in L$ and L is the smallest subfield of F containing β. Also $\alpha^{z_2} = \beta^j$ where j is coprime to the order of β. Let $\sum_{l=0}^s c_l\beta^l$ be the minimal polynomial of β. We just saw that $\sum_{l=0}^s c_l\beta^{jl} = 0$. This shows that the mapping $x \mapsto x^j$ is a field automorphism of L. It implies that z_1 and z_2 are in the same cyclotomic coset, a contradiction.

We have seen that a polynomial in standard form whose trace-evaluation generates an irreducible cyclic code is necessarily a monomial aX^z where $a \notin L^\perp$ using the by now standard terminology ($z \in Z$, $|Z| = s$, $L = \mathbb{F}_{q^s}$, $\perp$ with respect to the trace form). Lemma 2 shows that $a\alpha^{lz}X^z \in \mathcal{B}$ for all l. As the α^{lz} generate L (see Lemma 1), it follows that $auX^z \in \mathcal{B}$ for all $u \in L$. By Lemma 2 again we have in fact $\mathcal{C} = tr(ev(aLX^z))$. Consider the mapping $u \mapsto tr(ev(auX^z))$ from L onto $\mathcal{C}$. The kernel of this mapping is 0, so $\mathcal{C}$ has dimension s. As it is contained in $V_1(Z)$ of dimension s, we have equality.

This completes the proof of Theorem 2. As a result we obtain an algorithmic description of all codewords of all cyclic linear codes in the permutation sense of length n, where $\gcd(n, p) = 1$. The codes are in bijection with sets of cyclotomic cosets. Let $Z_1 \cup \cdots \cup Z_t$ be such a set. Let $z_k \in Z_k$, $s_k = |Z_k|$, $L_k = \mathbb{F}_{q^{s_k}}$. The dimension of the code is $\sum_k s_k$. Its generic codeword $w(x_1, \ldots, x_t)$ where $x_k \in L_k$ has entry

$$\sum_k tr_{L_k|\mathbb{F}_q}\left(x_k\alpha^{iz_k}\right)$$

in coordinate i where $i = 0, \ldots, n-1$. The cyclic shift of codeword $w((x_k)_k)$ is $w((x_k\alpha^{z_k})_k)$.

4.2. Cyclic additive codes

Let now $m \geqslant 1$ arbitrary. This is the case of additive not necessarily linear cyclic codes in the permutation sense. Recall that we still assume $\gcd(n, p) = 1$. We want to determine the irreducible

cyclic codes in this case. The fact that we have dealt with case $m = 1$ already will be helpful. Let $\mathcal{C}$ be an irreducible cyclic code and π_j, $j = 1, \ldots, m$, the projections to the inner coordinates. If $\pi_j(\mathcal{C})$ is not identically zero, then $\pi_j(\mathcal{C})$ is a linear irreducible cyclic code. It is therefore described by a cyclotomic coset (see Theorem 2). It can be assumed that this happens for all j (otherwise we are dealing with a smaller value of m). Let $Z_1, \ldots, Z_m$ be the corresponding cyclotomic cosets. At first we show that they are identical.

Lemma 3. *Let $\mathcal{C}$ be an irreducible cyclic code. The cyclotomic cosets determined by the irreducible linear cyclic codes $\pi_j(\mathcal{C})$ are all identical.*

Proof. We can assume $m = 2$ and $tr(ev(p_1(X), p_2(X))) \in \mathcal{C}$ where $p_1(X) = a_1X^{z_1}$, $p_2(X) = a_2X^{z_2}$ and $a_i \notin L_i^{\perp}$ with the notation used in the previous subsection. Assume z_1, z_2 are in different cyclotomic cosets. The proof is similar to the main portion of the proof of Theorem 2. Lemma 2 shows $(a_1\alpha^{lz_1}X^{z_1}, a_2\alpha^{lz_2}X^{z_2}) \in \mathcal{B}$ for all l, where $\mathcal{B}$ is the $\mathbb{F}_q$-linear space of tuples of polynomials whose trace-evaluation is in $\mathcal{C}$. Assume z_1, z_2 are in different cyclotomic cosets Z_1, Z_2, of lengths s_1, s_2. If $s_1 \neq s_2$, the same argument applies as in the proof of Theorem 2. If $s_1 = s_2$, the argument used in the proof of Theorem 2 shows $Z_1 = Z_2$, another contradiction. □

Theorem 3. *Let Z be a cyclotomic coset. Each nonzero codeword in $V_m(Z) = tr(ev(\mathcal{P}(Z), \ldots, \mathcal{P}(Z)))$ generates an irreducible cyclic code of dimension $s = |Z|$.*

Proof. Such a codeword can be written as $tr(ev(a_1X^z, a_2X^z, \ldots, a_mX^z))$. The entry in outer coordinate i and inner coordinate j is $tr(a_j\alpha^{iz})$. Lemma 2 shows that the cyclic code $\mathcal{C}$ generated by this codeword is the span of the codewords with entry $tr(a_j\alpha^{lz}\alpha^{iz})$ in the same position. As the α^{lz} generate $L = \mathbb{F}_{q^s}$ (see Lemma 1) it follows that $\mathcal{C}$ consists of the codewords with entry $tr(a_ju\alpha^{iz})$ in the (i, j)-coordinate, where $u \in L$. It is now clear that this code is the cyclic code generated by any of its nonzero codewords, in other words $\mathcal{C}$ is irreducible. By the transitivity of the trace we have $tr(a_ju\alpha^{iz}) = tr_{L|\mathbb{F}_q}(b_ju\alpha^{iz})$ where $b_j = tr_{F|L}(a_j)$. The fact that the code is nonzero means that not all the b_j vanish. The mapping $u \mapsto tr(ev(a_1uX^z, \ldots, a_muX^z))$ is injective, so $\dim(\mathcal{C}) = s$. □

Corollary 1. *The total number of irreducible permutation cyclic q-linear q^m-ary codes of length n coprime to the characteristic is $\sum_Z (q^{ms} - 1)/(q^s - 1)$ where Z varies over the cyclotomic cosets and $s = |Z|$.*

Proof. In fact, $V_m(Z)$ has $\mathbb{F}_q$-dimension ms, and each of the irreducible subcodes has $q^s - 1$ nonzero codewords. □

Observe that this is true also in the linear case $m = 1$: the number of irreducible cyclic codes is the number of cyclotomic cosets in this case (see Theorem 2). More importantly we obtain a parametric description of the irreducible codes. Such a code is described by the following data:

1. A cyclotomic coset Z. Let $s = |Z|$, $L = \mathbb{F}_{q^s}$, choose $z \in Z$.
2. A point $P = (b_1 : \ldots : b_m) \in PG(m - 1, L)$.

The codewords are then parametrized by $x \in L$. The entry in outer coordinate i and inner coordinate j is $tr_{L|\mathbb{F}_q}(b_jx\alpha^{iz})$. Denote this code by $\mathcal{C}(z, P)$. This leads to a parametric description of all cyclic additive codes, not just the irreducible ones.

Definition 7. Let Z be a cyclotomic coset of length $s, z \in Z$, $L = \mathbb{F}_{q^s}$ and $U \subset V(m, L)$ a k-dimensional vector subspace (equivalently: a $PG(k - 1, L) \subset PG(m - 1, L)$). Let $P_1, \ldots, P_k$ be the projective points determined by a basis of U. Define $\mathcal{C}(z, U) = \mathcal{C}(z, P_1) \oplus \cdots \oplus \mathcal{C}(z, P_k)$.

Refer to the $\mathcal{C}(z, U)$ as **constituent codes**. Here $\mathcal{C}(z, U)$ has dimension ks if $U \subseteq L^m$ has dimension k. Use an **encoding matrix** $B = (b_{lj})$, a (k, m)-matrix with entries from L. The rows z_l of B form

a basis of U. The codewords $w(x)$ are parametrized by $x = (x_l) \in L^k$. The entry of codeword $w(x)$ in outer coordinate i and inner coordinate $j = 1, \ldots, m$ is

$$tr_{L|\mathbb{F}_q}\big((x \cdot s_j)\alpha^{iz}\big) \tag{1}$$

where s_j is column j of B. The image of $w(x)$ under one cyclic shift is $w(\alpha^z x)$. What happens if we use a different basis (z'_l) for the same subspace U? Then $z'_l = \sum_{r=1}^k a_{lr} z_r$ and $A = (a_{lr})$ is invertible. The image of $w(x)$ under this operation (replacing z_l by z'_l) has (i, j)-entry $tr_{L|\mathbb{F}_q}(\sum_{l=1}^k x_l \sum_{r=1}^k a_{lr} b_{rj} \alpha^{iz})$. This describes $w(x')$ where $x'_l = \sum_{r=1}^k x_r a_{rl}$, in other words $x' = xA \in L^k$. We have seen that $\mathcal{C}(z, U)$ is indeed independent of the choice of an encoding matrix. Basic properties of the trace show that the dependence on the choice of representative $z \in Z$ is given by $\mathcal{C}(qz, U^q) = \mathcal{C}(z, U)$.

Here is a concrete expression for the weights of constituent codes: Codeword $w(x)$ has entry $w(x)_i = 0$ in outer coordinate i if and only if $x \cdot s_j \in (\alpha^{iz})^\perp$ for all j, with respect to the $tr_{L|\mathbb{F}_q}$-form.

Finally each cyclic code can be written in a unique way as the direct sum of its constituent codes: $\mathcal{C} = \bigoplus_Z \mathcal{C}(z, U_Z)$ where Z varies over the cyclotomic cosets and z is a fixed representative of Z.

Definition 8. Let $N(m, q)$ be the total number of subspaces of the vector space $\mathbb{F}_q^m$.

In particular $N(1, q) = 2$, $N(2, q) = q + 3$, $N(3, q) = 2(q^2 + q + 2)$.

Corollary 2. *The total number of permutation cyclic q-linear q^m-ary codes of length n coprime to the characteristic is $\prod_Z N(m, q^{|Z|})$.*

Example 1. Let $q = 2$, $m = 2$, $n = 7$. The cyclotomic cosets have lengths $1, 3, 3$ (representatives $0, 1, -1$). There are $3 + 9 + 9 = 21$ irreducible cyclic, $5 \times 11 \times 11 = 605$ cyclic codes altogether. A $[7, 3.5, 4]_4$-code is obtained as $\mathcal{C}(1, (1, 0)\mathbb{F}_8) \oplus \mathcal{C}(-1, (0, 1)\mathbb{F}_8) \oplus \mathcal{C}(0, (1, 1)\mathbb{F}_2)$, where $\mathcal{C}(0, (1, 1)\mathbb{F}_2)$ simply is the repetition code $\langle (11)^7 \rangle$. In the language of Definition 1 we have $km = 2k = 7$ and the quaternary dimension is therefore $k = 3.5$. It may be checked that the minimum distance is indeed 4.

Example 2. Let $q = 2$, $m = 2$, $n = 15$. 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. A $[15, 4.5, 9]_4$-code is obtained as $\mathcal{C}(1, (\epsilon, 1)\mathbb{F}_{16}) \oplus \mathcal{C}(3, (1, \epsilon^2)\mathbb{F}_{16}) \oplus \mathcal{C}(0, (1, 1)\mathbb{F}_2)$, see [3]. Here $F = \mathbb{F}_{16} = \mathbb{F}_2(\epsilon)$ and $\epsilon^4 = \epsilon + 1$.

Equivalence

When are two additive cyclic codes $\bigoplus_Z \mathcal{C}(z, U_Z)$ and $\bigoplus_z \mathcal{C}(z, U'_Z)$ equivalent? Two such situations are easy to see. Here is the first.

Proposition 2. *Let $C = (c_{uj}) \in GL(m, q)$. Then the additive cyclic code $\mathcal{C} = \bigoplus_Z \mathcal{C}(z, U_Z)$ is monomially equivalent to $\bigoplus_Z \mathcal{C}(z, U_Z C)$.*

Proof. Use the GL-part of monomial equivalence. An equivalent code is obtained if we apply the matrix C to each entry of $\mathcal{C}$. This means that for each constituent Z the entry $w(x)_i(j) = tr_{L|\mathbb{F}_q}((x \cdot s_j)\alpha^{iz})$ is replaced by $\sum_{u=1}^m c_{uj} w(x)_i(u)$. As $c_{uj} \in \mathbb{F}_q$ this amounts to replacing the encoding matrix B_Z by $B_Z C$, and therefore the subspace U_Z by $U_Z C$. □

As a special case of Proposition 2 consider the case of irreducible codes for $m = 2$. We have a fixed cyclotomic coset Z of length $s = |Z|$ and $U = (b_1 : b_2)$ is a point of the projective line $PG(1, L)$. Multiplication by C from the right amounts to apply a Möbius transformation, an element of $PGL(2, q)$. The number of non-equivalent irreducible codes belonging to cyclotomic coset Z with respect to the

equivalence described by Proposition 2 equals the number of orbits of $PGL(2,q)$ on the projective line $PG(1,q^s)$.

Here is the second such situation.

Proposition 3. *Let* $\gcd(t,n)=1$. *The additive permutation cyclic code* $\mathcal{C}=\bigoplus_Z \mathcal{C}(z,U_Z)$ *is permutation equivalent to* $\bigoplus_Z \mathcal{C}(tz,U_Z)$.

Proof. The generic codeword $w(x)$ of the second code above has entry $tr_{L|\mathbb{F}_q}((x\cdot s_j)\alpha^{itz})$ in outer coordinate i, inner coordinate j (see Eq. (1)). This is the entry of the first code in outer coordinate i/t mod n and inner coordinate j. □

Proposition 3 describes an action of the group of units in $\mathbb{Z}/n\mathbb{Z}$. Here is an example.

Example 3. There are precisely three non-equivalent length 7 irreducible additive quaternary codes which are cyclic in the permutation sense.

Proof. This is case $q=2$, $m=2$, $n=7$. The total number of irreducible cyclic codes is $3+9+9=21$ (once $PG(1,2)$ and twice $PG(1,8)$). The number of inequivalent such codes is at most $1+2=3$. In fact, the three codes $\mathcal{C}(0,U)$ where $U\in PG(1,2)$ are all equivalent by Proposition 2. By Proposition 3 it suffices to consider $Z(1)$ for the remaining irreducible codes. The number of possibly inequivalent such irreducible codes is the number of orbits of $GL(2,2)$ on $PG(1,8)$. There are two such orbits. The corresponding codes are $\mathcal{C}(1,(0,1))$ and $\mathcal{C}(1,(1,\epsilon))$ where $\epsilon\notin\mathbb{F}_2$. It is in fact obvious that those irreducible codes are pairwise non-equivalent. Clearly the first one is inequivalent to the others as it has binary dimension 1 (the repetition code $\langle(11)^7\rangle$). The second code has $w(x)_i=(0,tr(x\epsilon^i))$, of constant weight 4. The third of those irreducible codes has $w(x)_i=(tr(x\epsilon^i),tr(x\epsilon^{i+1}))$, clearly not of constant weights. □

4.3. Duality and quantum codes

Fix a nondegenerate bilinear form $\langle\,,\rangle$ on the vector space $E=\mathbb{F}_q^m$, extend it to $V_m=E^n$, to F^m and to $V_{m,F}=(F^m)^n$ in the natural way. In coordinates this means that $\langle\,\rangle$ is described by coefficients $a_{kl}\in\mathbb{F}_q$ where $k,l=1,\ldots,m$ such that $\langle(x_k),(y_l)\rangle=\sum_{k,l}a_{kl}x_ky_l$. Duality will be with respect to this bilinear form. Basic information is derived from the following fact:

Lemma 4. *Let* $W=\langle\alpha\rangle\subset F=\mathbb{F}_{q^r}$ *be the cyclic subgroup of order n, and the integer l not a multiple of n. Then* $\sum_{i=0}^{n-1}\alpha^{il}=0$.

Proof. Let $S=\sum_{i=0}^{n-1}\alpha^{il}$. Then $\alpha^lS=S$ and $\alpha^l\neq1$. It follows $(1-\alpha^l)S=0$ which implies $S=0$. □

Proposition 4. $V_{m,F}(Z)^\perp=\bigoplus_{Z'\neq-Z}V_{m,F}(Z')$. $V_m(Z)^\perp=\bigoplus_{Z'\neq-Z}V_m(Z')$.

Proof. As the dimensions are right, it suffices to show that $V_{m,F}(Z)$ is orthogonal, with respect to $\langle\,\rangle$, to $V_{m,F}(Z')$ when $Z'\neq-Z$ (an analogous statement holds for the second equality). Concretely this means $\sum_{k,l=1}^m a_{kl}\sum_{i=0}^{n-1}p_k(\alpha^i)q_l(\alpha^i)=0$ where $p_k(X)\in\mathcal{P}(Z)$, $q_l(X)\in\mathcal{P}(Z')$. By bilinearity it suffices to prove this for fixed k,l and $p_k(X)=X^z$, $q_l(X)=X^{z'}$ where $z\in Z$, $z'\in Z'$. Let $j=z+z'$. Then j is not a multiple of n. We need to show $\sum_{i=0}^{n-1}\alpha^{iz+iz'}=0$. This follows from Lemma 4. This proves the first equality. The proof of the second equality is analogous, using the definition of the trace. □

Observe that the result of Proposition 4 is independent of the bilinear form $\langle\,,\rangle$. The information contained in the bilinear form will determine the duality relations between subspaces of $V_{m,F}(Z)$ and $V_{m,F}(-Z)$ as well as between subspaces of $V_m(Z)$ and $V_m(-Z)$. In order to decide self-orthogonality, the following formula is helpful (see Lemma 17.26 of [2]):

Lemma 5. $\sum_{u\in W} tr(au^z)tr(bu^{-z}) = n \times tr(atr_{F|L}(b))$.

Proof. Let S be the sum on the left. Write out the definition of the trace: $S = \sum_{j,k=0}^{r-1} a^{q^j} b^{q^j} \times \sum_{u\in W} u^{(q^i-q^j)z}$. The inner sum vanishes if $(q^i - q^j)z$ is not divisible by n. In the contrary case the inner sum is n. The latter case occurs if and only if $i = j + \rho s$ where $s = |L|$ and $\rho = 0, \ldots, s-1$. It follows $S = n\sum_i a^{q^i} \sum_\rho b^{q^i q^{\rho s}} = ntr(atr_{F|L}(b))$. □

An interesting special case concerns the cyclic quantum stabilizer codes, over an arbitrary ground field $\mathbb{F}_q$. In this case $m = 2$ and the bilinear form is the symplectic form $\langle (x_1, x_2), (y_1, y_2)\rangle = x_1y_2 - x_2y_1$ (in particular $\langle x, x\rangle = 0$ always). By definition such a code is a (cyclic) q-ary quantum stabilizer code if it is self-orthogonal with respect to the symplectic form. The basic lemma to decide self-orthogonality is the following:

Proposition 5. *In the situation considered here* ($m = 2$ *and the symplectic form,* $\gcd(n, p) = 1$) *irreducible codes* $\mathcal{C}(z, P)$ *and* $\mathcal{C}(-z, P')$ *are orthogonal if and only if* $P = P'$.

Proof. Observe that Z and $-Z$ have the same length $s, L = \mathbb{F}_{q^s}$ and $P, P' \in PG(1, L)$. It suffices to show that $\mathcal{C}(z, P)$ and $\mathcal{C}(-z, P)$ are orthogonal. Let $P = (v_1 : v_2)$. Writing out the symplectic product of typical vectors we need to show

$$\sum_{u\in W} tr\big(av_1u^z\big)tr\big(bv_2u^{-z}\big) = \sum_{u\in W} tr\big(av_2u^z\big)tr\big(bv_1u^{-z}\big)$$

for $a, b \in F$. Lemma 5 shows that the sum on the left equals $n \times tr(av_1tr_{F|L}(bv_2)) = n \times tr(av_1v_2tr_{F|L}(b)) = n \times tr_{L|\mathbb{F}_q}(v_1v_2tr_{F|L}(a)tr_{F|L}(b))$ which by symmetry coincides with the sum on the right. □

Theorem 4. *The number of additive cyclic* q^2*-ary quantum stabilizer codes is*

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

The number of self-dual such codes is

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

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

Proof. Let $\mathcal{C} = \sum_Z S_Z$ where $S_Z = \mathcal{C}(z, U_Z)$. This 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 S_Z or S_{-Z} is 0, then there is no restriction on the other. If $S_Z = \mathcal{C}(z, L^2)$, then $S_{-Z} = 0$.

Consider case $Z = -Z, s > 1$. Then $s = 2i$. Either $S_Z = 0$ or $S_Z = \mathcal{C}(z, P)$ is a self-orthogonal irreducible code where $P \in PG(1, L)$. The dual of S_Z in its constituent is $\mathcal{C}(-z, P)$ by Proposition 5. As $-z = z^{q^i}$, we have $\mathcal{C}(-z, P) = \mathcal{C}(z, P^{q^i})$. This equals S_Z if and only if $P \in PG(1, L')$ where $L' = \mathbb{F}_{q^i}$. There are $q^i + 1$ choices for P. Case $Z = -Z$, $s = 1$ contributes $q+2$ self-orthogonal and $q+1$ self-dual codes. □

Example 4. In case $n = 7$ we obtain $4 \times 30 = 120$ quantum codes altogether and $3 \times 11 = 33$ self-dual ones.

Example 5. 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.

5. Cyclic additive codes in the monomial sense

Let $\mathcal{C}$ be a q^m-ary q-linear code of length n, which is cyclic in the monomial sense. Let $\gcd(n, p) = 1$, $m \geqslant 1$ and $A \in GL(m, q)$ of order u, where $\gcd(u, p) = 1$. Let $r = ord_n(q)$, $r' = ord_{un}(q)$ and $F = \mathbb{F}_{q^r} \subseteq F' = \mathbb{F}_{q^{r'}}$ be the corresponding fields. Consider cyclotomic cosets $Z \subset \mathbb{Z}/un\mathbb{Z}$. For fixed Z of length s let $z \in Z$, $L = \mathbb{F}_{q^s}$. Also, let $\kappa = ord_u(q)$ and $K = \mathbb{F}_{q^\kappa}$. It follows from Proposition 1 that by monomial equivalence it suffices to consider cyclic codes in the monomial sense fixed under the action of $g = g(I, \ldots, I, A, (0, 1, \ldots, n-1))$ of order un. Such codes are also known as **constacyclic** codes. Here the matrix A plays the role of a constant factor. Let $G = \langle g \rangle$. Also, let β be a generator of the group of order un in F' and $\alpha = \beta^u \in F$. Let $\gamma = \beta^n$ be of order u. Then $\gamma \in K = \mathbb{F}_{q^\kappa}$.

Definition 9. Let $A \in GL(m, q)$, $A^u = 1$. Define the **inflation** $I_A : \mathbb{F}_q^{mn} \longrightarrow \mathbb{F}_q^{umn}$ by

$$I_A(\underbrace{x_0, \ldots, x_{n-1}}_{x}) = \left(x|Ax \ldots |A^{u-1}x\right).$$

The mapping $contr : (x|Ax \ldots |A^{u-1}x) \mapsto x \in \mathbb{F}_q^{mn}$ is the **contraction** : $I_A(\mathbb{F}_q^{mn}) \longrightarrow \mathbb{F}_q^{mn}$.

Lemma 6. *In the situation of Definition 9, the q-linear q^m-ary code $\mathcal{C}$ of length n is invariant under the (monomial) action of the cyclic group G of order un generated by $g(I, \ldots, I, A, (0, 1, \ldots, n-1))$ if and only if $I_A(\mathcal{C})$ is cyclic in the permutation sense under the permutation $(0, 1, \ldots, un-1)$. The contraction $contr(\mathcal{C})$ is irreducible under the action of G if and only if the cyclic length un code $\mathcal{C}$ is irreducible.*

Proof. Observe that $\mathcal{C}$ and $I_A(\mathcal{C})$ have the same dimension and $\mathcal{C}$ is recovered from $I_A(\mathcal{C})$ as the projection to the first n coordinates. The claims are by now obvious. □

5.1. The linear case $m = 1$

In this special case we have $g = g(1, \ldots, 1, \gamma, (0, 1, \ldots, n-1))$ where the matrix A now is a constant $\gamma \in \mathbb{F}_q^*$ of order u where $u|q-1$. Let $u = ord(\gamma)$. Write the elements of the ambient space $\mathbb{F}_q^{un}$ as (x_i) where $i \in \mathbb{Z}/un\mathbb{Z}$. Then $x \in \mathbb{F}_q^{un}$ is in $I_\gamma(\mathbb{F}_q^n)$ if and only if $x_{i+n} = \gamma x_i$ always holds.

Theorem 5. *Let $\gcd(n, p) = 1$ and $\gamma \in \mathbb{F}_q^*$, $ord(\gamma) = u$. The codes which are invariant under the group generated by $g = g(1, \ldots, 1, \gamma, (0, 1, \ldots, n-1))$ are the contractions of the cyclic codes of length un in the permutation sense defined by cyclotomic cosets consisting of numbers which are $1 \bmod u$. If there are a such cyclotomic cosets in $\mathbb{Z}/un\mathbb{Z}$, then the number of codes invariant under g is 2^a.*

Proof. Observe $\gcd(un, p) = 1$. By Lemma 6 the codes in question are the contractions of the length un cyclic codes all of whose codewords (x_i) satisfy $x_{i+n} = \gamma x_i$ for all i. Let Z be a cyclotomic coset, $z \in Z$, $|Z| = s$, $L = \mathbb{F}_{q^s}$. A typical codeword of the irreducible cyclic code defined by Z has entry $x_i = tr_{L|\mathbb{F}_q}(a\beta^{iz})$, where $a \in L$. It follows $x_{i+n} = tr_{L|\mathbb{F}_q}(a\beta^{(i+n)z}) = \gamma^z x_i$. We must have $z = 1 \bmod u$. □

Here is an algorithmic view concerning linear length n q-ary codes which are invariant under $g = g(1, \ldots, 1, \gamma, (0, 1, \ldots, n-1))$ where $ord(\gamma) = u$: Let $r' = ord_{un}(q)$ and $F' = \mathbb{F}_{q^{r'}}$. Let $ord(\beta) = un$ such that $\gamma = \beta^n$. Let $\alpha = \beta^u$. Consider the cyclotomic cosets $Z_1, \ldots, Z_a$ in $\mathbb{Z}/un\mathbb{Z}$ whose elements are 1 mod u. Observe that $|Z_1 \cup \cdots \cup Z_a| = n$. Let $s_k = |Z_k|$, $L_k = \mathbb{F}_{q^{s_k}} \subseteq F'$. Then $\mathcal{C} \subseteq \bigoplus \mathcal{C}_k$ where the $\mathcal{C}_k$ are the irreducible γ-constacyclic codes of length n. We have $\dim(\mathcal{C}_k) = s_k$. The codewords of $\mathcal{C}_k$ are $w(x)$ where $x \in L_k$. The entry of $w(x)$ in coordinate i is $tr_{L_k|\mathbb{F}_q}(x\beta^{iz_k})$. The image of $w(x)$ under

the monomial operation $g(1,\dots,1,\gamma,(0,1,\dots,n-1))$ is $w(\beta^{z_k}x)$. After n applications this leads to $w(\gamma^{z_k}x)=w(\gamma x)=\gamma w(x)$, as expected.

Example 6. Consider $q=4$, $u=3$, $n=15$. Then $F=\mathbb{F}_{16}$ whereas $F'=\mathbb{F}_{4^6}$. The cyclotomic cosets in $\mathbb{Z}/45\mathbb{Z}$ consisting of numbers divisible by 3 are in bijection with the 9 cyclotomic cosets mod 15. The contractions of the cyclic length 45 codes defined by Z-cosets all of whose elements are divisible by 3 reproduce precisely the length 15 cyclic codes in the permutation sense. There are only three cyclotomic cosets all of whose elements are 1 mod 3. They are

$$\{1,4,16,19,31,34\},\ \{7,13,22,28,37,43\},\ \{10,25,40\}.$$

It follows that there are $2^3=8$ constacyclic quaternary linear codes with constant $\gamma=\beta^{15}$ of order 3.

Example 7. Consider $q=8$, $n=21$. Then $F'=\mathbb{F}_{2^{42}}=\mathbb{F}_{8^{14}}$. The constant is $\gamma=\beta^7$ of order 7. We have $un=7\times 21=147$ and we have to consider the action of $q=8$ (the Galois group of order 14) on the 21 elements which are 1 mod 7. The corresponding cyclotomic cosets are

$$Z(1)=\{1,8,64,71,-20,-13,43,50,-41,-34,22,29,85,-55\}$$

of length 14 and

$$Z(15)=\{15,-27,78,36,-6,-48,57\}$$

of length 7. It follows that there are precisely two irreducible γ-constacyclic $\mathbb{F}_8$-linear codes of length 21, of dimensions 14 and 7.

Here are some more interesting and well-known examples.

Example 8. Let $q=4$, $u=3$, $Q=2^f$ where f is odd, and $n=(Q^f+1)/3$, $F=\mathbb{F}_{4^f}$. The irreducible constacyclic quaternary code defined by the cyclotomic coset generated by 1 has dimension f and dual distance 5. Its dual is therefore a linear $[(2^f+1)/3,(2^f+1)/3-f,5]_4$-code. This is the first family from [6], see also Section 13.4 of [2].

Example 9. The second family of constacyclic quaternary codes from [6] occurs in case $u=3$, $n=(4^f-1)/3$ for arbitrary f where the cyclotomic cosets are those generated by 1 and -2. This yields a $2f$-dimensional quaternary code of dual distance 5 and therefore $[(4^f-1)/3,(4^f-1)/3-2f,5]_4$-codes for arbitrary f.

5.2. The general case $m\geqslant 1$

Theorem 6. *With notation as introduced above, choose a representative z for each cyclotomic coset Z and U_Z the Eigenspace of the Eigenvalue γ^z of A in its action on L^m. Then each code stabilized by G is contained in $\bigoplus_Z contr(\mathcal{C}(z,U_Z))$.*

Proof. The additive cyclic length un codes are direct sums over cyclotomic cosets Z of codes parametrized by subspaces $U_Z\subset L^m$, using the customary terminology. Such a code is in $I_A(\mathbb{F}_q^{mn})$ if and only if each codeword $x=(x_i)$ (where $i=0,\dots,un-1$ and $x_i\in\mathbb{F}_q^m$) satisfies $x_{i+n}=Ax_i$. Fix Z and ask for which subspace U this is satisfied. Let $A=(a_{jj'})\in GL(m,q)$ and $U=P=(b_1:\dots:b_m)\in PG(m-1,L)$ be a point. Let $tr=tr_{L|\mathbb{F}_q}$. The condition is

$$tr\big(xb_j\beta^{(i+n)z}\big)=\sum_{j'}a_{jj'}tr\big(xb_{j'}\beta^{iz}\big)$$

for all i, all j and $x \in L$. As $\beta^n = \alpha$ an equivalent condition is

$$tr\left(x\beta^{iz}\left(\gamma^z b_j - \sum_{j'} a_{jj'} b_{j'}\right)\right) = 0$$

which is equivalent to $\gamma^z b_j = \sum_{j'} a_{jj'} b_{j'}$, in other words b (written as a column vector) is an Eigenvector for the Eigenvalue γ^z of A. □

Here is an algorithmic view again. The constacyclic length n additive codes are direct sums of their constituents, where the constituents correspond to cyclotomic cosets in $\mathbb{Z}/un\mathbb{Z}$. Let Z be such a cyclotomic coset, $z \in Z$, $|Z| = s$, $L = \mathbb{F}_{q^s}$ and $\beta, \alpha, \gamma = \beta^n$ as usual. The irreducible subcodes are the contractions of $\mathcal{C}(z, P)$ where $P = (b_1, \ldots, b_m) \in L^m$ has to satisfy $AP = \gamma^z P$ (and we write P as a column vector). This irreducible length n constacyclic code $contr(\mathcal{C}(z, P))$ has dimension s. Its codewords are $w(x), x \in L$. The entry of $w(x)$ in outer coordinate $i = 0, 1, \ldots, n-1$ and inner coordinate j is $tr_{L|\mathbb{F}_q}(xb_j\beta^{iz})$. The effect of the generator $g = g(I, \ldots, I, A, (0, \ldots, n-1))$ of the cyclic group G is $g(w(x)) = w(\beta^z x)$.

Proposition 6. *Let $\mathcal{C}$ be a q-linear q^m-ary length n code, which is invariant under $g(I, \ldots, I, A, (0, 1, \ldots, n-1))$, where $\gcd(n, p) = 1$ and A of order $u = q^m - 1$ represents multiplication by a primitive element γ in $\mathbb{F}_{q^m}$. Then $\mathcal{C}$ is $\mathbb{F}_{q^m}$-linear.*

Proof. It suffices to prove this for irreducible constacyclic codes $contr(\mathcal{C}(z, P))$. The generic codeword $w(x)$ has been described above. Applying matrix A in each outer coordinate $i = 0, \ldots, n-1$ yields the codeword $w(\gamma^z x)$ which is still in the code. □

Proposition 6 applies in particular in cases $q = 2$, $m = 2$, $u = 3$ and $q = 2$, $m = 3$, $u = 7$.

Corollary 3. *Each quaternary additive code, which is cyclic in the monomial sense, either is quaternary linear or is equivalent to cyclic in the permutation sense.*

Proof. Use Proposition 1 to obtain a code which is invariant under $g = (I, \ldots, I, A, (0, \ldots, n-1))$ where $A \in GL(2, 2)$ and $u = \det(A)$. If $u = 1$ or $u = 2$ or when $u = 3$ and n not divisible by 3, then the additive code is cyclic in the permutation sense (see Proposition 1). In the case when $u = 3$, Proposition 6 shows that the code is a quaternary linear constacyclic code. □

This shows that in the quaternary case the full theory of additive constacyclic codes does not produce anything useful as in each case we are reduced to a more elementary theory, either quaternary linear constacyclic or additive and cyclic in the permutation sense.

References

[1] J. Bierbrauer, The theory of cyclic codes and a generalization to additive codes, Des. Codes Cryptogr. 25 (2002) 189–206.
[2] J. Bierbrauer, Introduction to Coding Theory, Chapman and Hall/CRC Press, 2004.
[3] J. Bierbrauer, Cyclic additive and quantum stabilizer codes, in: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields WAIFI, Madrid, 2007, in: Lecture Notes in Comput. Sci., vol. 4547, 2007, pp. 276–283.
[4] J. Bierbrauer, Y. Edel, Quantum twisted codes, J. Combin. Des. 8 (2000) 174–188.
[5] Y. Edel, J. Bierbrauer, Twisted BCH-codes, J. Combin. Des. 5 (1997) 377–389.
[6] D.N. Gevorkyan, A.M. Avetisyan, G.A. Tigranyan, On the structure of two-error-correcting in Hamming metric over Galois fields, in: Computational Techniques, vol. 3, Kuibyshev, 1975, pp. 19–21 (in Russian).
[7] S. Lang, Algebra, revised 3rd ed., Springer, New York, 2002.