The theory of cyclic codes and a generalization to additive codes

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

September 7, 2000

Abstract

We present a new approach to the theory of cyclic and constacyclic codes and generalize the theory to cover the family of additive (not necessarily linear) cyclic codes. The approach is based on the action of the Galois group (cyclotomic cosets). The conventional representation of cyclic codes as ideals in a factor ring of the polynomial ring is not needed.

1 General facts on linear codes

The construction of many good linear codes involves the following step: one constructs a code $\mathcal{C}$, which is linear over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. A linear q-ary code is then derived either as the trace code or as the subfield code of $\mathcal{C}$.

Definition 1. *Let $F = \mathbb{F}_{q^r}|\mathbb{F}_q$ and let $\mathcal{C}$ be an F-linear code. Denote the trace by $tr = tr : F \longrightarrow \mathbb{F}_q$. The* **trace code** *$tr(\mathcal{C})$ is defined as the set of* *all* $(tr(x_1), tr(x_2), \ldots, tr(x_n))$ *where* $(x_1, x_2, \ldots, x_n) \in \mathcal{C}$*. The* **subfield code** $\mathcal{C}_{F_q}$ *consists of the codewords of* $\mathcal{C}$ *all of whose entries happen to be in* $\mathbb{F}_q$*, formally* $\mathcal{C}_{F_q} = \mathcal{C} \cap \mathbb{F}_q^n$*.*

It is clear that $tr(\mathcal{C})$ and $\mathcal{C}_{F_q}$ are linear q-ary codes. The relationship between them is clarified by the following theorem, which is generally attributed to Delsarte:

Theorem 1 (Delsarte). *In the situation of Definition 1 the following holds:*

$$tr(\mathcal{C})^{\perp} = (\mathcal{C}^{\perp})_{F_q}$$

Proof. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$. Then $\alpha \in tr(\mathcal{C})^{\perp}$ if and only if $\sum_{i=1}^n \alpha_i tr(x_i) = 0$ for all $x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}$. Because of the linearity of the trace this is equivalent with $tr(\sum_{i=1}^n \alpha_i x_i) = 0$. We claim that this is equivalent with $\sum_{i=1}^n \alpha_i x_i = 0$. In fact, if this was not the case, then because of the F-linearity of $\mathcal{C}$ it would follow that tr is the 0-mapping, contradiction. We conclude that $\alpha \in tr(\mathcal{C})^{\perp}$ if and only if $\alpha \in \mathcal{C}^{\perp}$ and all $\alpha_i \in \mathbb{F}_q$. This is our claim. ∎

Definition 2. *Let* $\mathcal{C}$ *be a* q*-ary code of length* n *and dimension* d*. The* **strength** $t = t(\mathcal{C})$ *is the largest number such that the projection from* $\mathcal{C}$ *onto any subset of* t *coordinates is surjective. Equivalently* t *is the largest number such that any* t *columns of a generator matrix of* $\mathcal{C}$ *are linearly independent.*

Theorem 2 (Principle of Duality). *The strength of a linear code and the minimum distance of the dual code (with respect to the dot product) are related by*

$$d(\mathcal{C}^{\perp}) = t(\mathcal{C}) + 1.$$

This is in fact trivial. The principle of duality gives us the opportunity to construct linear q-ary codes as subfield codes $(\mathcal{C}^\perp)_{F_q}$ of the dual code. Knowledge of the minimum distance of this code is equivalent with knowledge of the strength of the corresponding trace-code $tr(\mathcal{C})$. We will apply this construction to codes $\mathcal{C}$, whose codewords are given as evaluations of certain polynomials. A bound on the strength of the trace-code will be an easy consequence of Lagrange interpolation.

Theorem 3 (Lagrange interpolation). *Let $l \geq 0$. If n different elements $x_1, x_2, \ldots, x_n$ in F and n arbitrary elements $\alpha_1, \ldots, \alpha_n$ in F are given, then there is exactly one polynomial $p(X)$ of degree $< n$ with coefficients in F, such that $x_i^l p(x_i) = \alpha_i, i = 1, 2, \ldots, n$.*

We need another basic fact concerning the relation between a code defined over a large field and its subfield and trace codes.

Definition 3. *Let $F = \mathbb{F}_{q^r} | \mathbb{F}_q$ and let $\mathcal{C}$ be an F-linear code. We call $\mathcal{C}$* **Galois invariant** *if $\mathcal{C} = \mathcal{C}^q$. This means that $\mathcal{C}$ is mapped onto itself by the Frobenius automorphism.*

Theorem 4. *Let $\mathcal{C}$ be linear code over $F = \mathbb{F}_{q^r}$, which is Galois invariant. Let $tr : F \longrightarrow \mathbb{F}_q$ be the trace. Then the following hold:*

- *$tr(\mathcal{C}) = \mathcal{C}|_{F_q}$.*
- *The $\mathbb{F}_q$-dimension of $tr(\mathcal{C})$ equals the F-dimension of $\mathcal{C}$.*

Proof. The definition of the trace shows that $tr(\mathcal{C}) \subseteq \mathcal{C}|_{F_q}$. Elements of the subfield code, which are linearly independent over $\mathbb{F}_q$, are also linearly independent over F. This shows $dim_{F_q}(\mathcal{C}|_{F_q}) \leq dim_F(\mathcal{C})$. The last link in the chain is provided by Theorem 1. If the length of $\mathcal{C}$ is n, then

$$dim(tr(\mathcal{C})) = dim((C^\perp|_{F_q})^\perp) = n - dim(\mathcal{C}^\perp|_{F_q}) \geq n - dim_F(\mathcal{C}^\perp) = dim_F(\mathcal{C}).$$

It follows that we have equality all along. ∎

Our most important tool is the action of the Galois group.

Definition 4 (cyclotomic cosets). *Consider the Galois group* $G(\mathbb{F}_{q^r}|\mathbb{F}_q) = \langle\sigma\rangle$*, where* σ *is the Frobenius automorphism (*$\sigma(x) = x^q$*), let* $n \mid q^r - 1$*. Then* G *acts as a permutation group on* $\{0, 1, \ldots, n-1\}$ *in the following natural way:*

$$\sigma(i) = iq \ (\ mod\ n).$$

The **cyclotomic cosets** *are the orbits of* G*. Denote by* $Z_n(t)$ *the orbit containing* t*. For* $A \subseteq \mathbb{Z}/n\mathbb{Z}$ *denote by* $\tilde{A}$ *(the Galois closure of* A*) the union of all cyclotomic cosets intersecting* A *nontrivially, and by* $\overline{A}$ *the complement of* A *in* $\mathbb{Z}/n\mathbb{Z}$*.*

The idea behind this action of the Galois group is the following: we apply it in the exponent. Multiplication of the exponent by q ($u^i \mapsto u^{iq}$) is equivalent to application of σ to the field element u^i itself. As we apply this to $u \in W$ we take the exponents mod n.

Observe that the length of a cyclotomic coset is always a divisor of r and that $\{0\}$ is a cyclotomic coset of length 1.

2 Cyclic codes

Definition 5. *Let* $n|q^r - 1$, $A \subseteq \mathbb{Z}/n\mathbb{Z}, F = \mathbb{F}_{q^r}, W$ *the multiplicative subgroup of order* n *of* F*. Denote by* $\mathcal{P}(A)$ *the space of polynomials with coefficients in* F*, whose monomials have degrees in* A*. Consider the array* $\mathcal{B}(A, n, q) = \mathcal{B}(A)$*, whose rows are indexed by* $p(X) \in \mathcal{P}(A)$*, whose columns are indexed by the elements* $u \in W$*, and corresponding entry* $p(u)$*. The* **cyclic code** $\mathcal{C}(A, n, q) = \mathcal{C}(A)$ *is*

$$\mathcal{C}(A) = tr(\mathcal{B}(A))^{\perp}.$$

Call A the **defining set** *of $\mathcal{C}(A)$.*

Theorem 5. *The dimension of the code $\mathcal{C}(A)$ as given in Definition 5 is $n - |\tilde{A}|$, the sum of the lengths of the cyclotomic cosets which intersect A in the empty set.*

Proof. The code $\mathcal{B}(A)$ and the (larger) code $\mathcal{B}(\tilde{A})$ have the same trace-code. As $\mathcal{B}(\tilde{A})$ is Galois invariant, we can use Theorem 4 and conclude that the $\mathbb{F}_q-$dimension of $tr(\mathcal{B}(A))$ agrees with the F-dimension of $\mathcal{B}(\tilde{A})$. This dimension clearly is $|\tilde{A}|$. As $\mathcal{C}(A)$ is the dual of $tr(\mathcal{B}(A))$, its dimension is $n - |\tilde{A}|$.

■

The proof of the following lemma is an easy exercise.

Lemma 1. *If i is not a multiple of n, then* $\sum_{u \in W} u^i = 0$.

Lemma 1 together with Theorems 1 and 4 yield the following:

Theorem 6. *We have $\mathcal{B}(A)^\perp = \mathcal{B}(-\overline{A})$, $\mathcal{C}(A) = \mathcal{B}(-\overline{\tilde{A}})_{F_q}$ and*

$$\mathcal{C}(A)^\perp = tr(\mathcal{B}(A)) = tr(\mathcal{B}(\tilde{A})) = \mathcal{B}(\tilde{A})_{F_q} = \mathcal{C}(-\overline{\tilde{A}})$$

Theorem 6 can be used in order to obtain a representation of the codewords of cyclic codes, which is almost canonical (see Subsection 2.1). As a first application, let A be such that $0 \notin A$. Then $\mathcal{C}(A) = \mathcal{C}(-\overline{\tilde{A}})^\perp = \mathcal{B}(-\overline{\tilde{A}})_{F_q}$ contains $\mathcal{B}(\{0\})_{F_q}$, which is generated by the all-1-word.

Lemma 2. *If $0 \notin A$, then the cyclic code $\mathcal{C}(A)$ contains the all-1-word and hence the repetition code.*

Theorem 7. *Let A and B be unions of cyclotomic cosets. Then the following hold:*

$$\mathcal{C}(A) \cap \mathcal{C}(B) = \mathcal{C}(A \cup B)$$

$$\langle \mathcal{C}(A), \mathcal{C}(B) \rangle = \mathcal{C}(A \cap B)$$

Proof. $\mathcal{C}(A)\cap\mathcal{C}(B) = tr(\mathcal{B}(A))^{\perp}\cap tr(\mathcal{B}(A))^{\perp} = tr(\langle\mathcal{B}(A),\mathcal{B}(B)\rangle)^{\perp} = tr(\mathcal{B}(A\cup B))^{\perp} = \mathcal{C}(A\cup B)$. The second equality can be reduced to the first one. Show that the dual codes agree and use Theorem 6. We leave this as an exercise.

■

Consider the minimum distance of the cyclic code $\mathcal{C}(A) = \mathcal{C}(\tilde{A})$. If A contains a set of t consecutive numbers, then it follows from Theorem 3 that $tr(\mathcal{B}(A))$ has strength $\geq t$. It follows that $\mathcal{C}(A)$ has minimum distance $\geq t+1$. We formalize this argument and generalize it slightly:

Definition 6 (intervals). *$A \subseteq \mathbb{Z}/n\mathbb{Z}$ is an* **interval** *if there is a generator of $\mathbb{Z}/n\mathbb{Z}$ (equivalently: an integer j, coprime with n), such that $A = \{jl, j(l+1), \ldots, j(l+i-1)\}$, for some l (mod n). We will abbreviate the interval $A = \{i, i+1, \ldots, j\}$ as $A = [i, j]$.*

As we are free to replace the generator of our cyclic group by some other generator it is clear that our argument is valid in this situation. We have proved the following:

Theorem 8 (BCH-bound). *If $\tilde{A}$ contains an interval of length t, then $d(\mathcal{C}(A, n, q)) \geq t+1$.*

This is known as the BCH-bound. If we wish to guarantee a certain minimum distance, then it suffices by the BCH-bound to choose as defining set an interval A of a certain size. The resulting cyclic codes are known as $BCH-$codes.

Example 1. *Let $q = 3, r$ odd, $n = (3^r-1)/2, A = \{1, -1\}$. We have $Z_n(1) = \{3^i \mid i = 1, 3, \ldots 3^{r-1}\}$ and of course $Z_n(-1) = -Z_n(1)$. It follows that $\tilde{A} = Z_n(1) \cup Z_n(-1)$ has $2r$ elements. The cyclic code $\mathcal{C}(A)$ has dimension $n - 2r$ (see Theorem 5). As $\{-3, -1, 1, 3\} \subset \tilde{A}$ is an interval, we see that $\mathcal{C}(A)$ has parameters*

$$[(3^r-1)/2, (3^r-1)/2 - 2r, 5]_3 \text{ for odd } r \geq 3.$$

The smallest members of this family are $[13, 7, 5]_3, [121, 111, 5]_3$.

2.1 Generator matrices of cyclic codes

The dimension formula suggests that every cyclotomic coset of length s avoiding $\tilde{A}$ should contribute precisely s rows to a generator matrix of the cyclic code $\mathcal{C}(A)$. This is made precise in the following theorem.

Theorem 9. *Let $\mathcal{C}(A) = \mathcal{C}(A, n, q)$ be a q-ary cyclic code of length n, and $F = \mathbb{F}_{q^r} = \mathbb{F}_q(\epsilon)$. Let further $Z = Z(i)$ be a cyclotomic coset of length s satisfying $Z \cap \tilde{A} = \emptyset$. Define $v(j, -i) \in \mathbb{F}_q^n, j = 0, 1, \ldots, r-1$ as the n-tuple with entry $tr(\epsilon^j \beta^{-i})$ in coordinate $\beta \in W$. We can choose a set $S(-i) \subseteq \{0, 1, \ldots, r-1\}$ of s values of j such that the matrix with rows $v(j, -i), j \in S(-i)$ has rank s. Define a matrix $G(A)$ with the vectors $v(j, -i)$ as its rows, where i varies over representatives of cyclotomic cosets avoiding $\tilde{A}$, and $j \in S(-i)$. Then $G(A)$ is a generator matrix of $\mathcal{C}(A)$.*

Proof. Theorem 5 shows that the number of rows of $G(A)$ equals the dimension k of $\mathcal{C}(A)$. Also $v(j, -i)$ belongs by definition to $tr(\mathcal{B}(-Z, n, q))$, which by Theorem 6 is contained in $\mathcal{C}(A)$. ∎

The only element in Theorem 9, which is not canonically determined, is the choice of the sets $S(-i)$ in the cases when $s < r$.

3 Comparison with the traditional theory

In this section we follow the traditional lines of the theory of cyclic codes until we reach the point where the equivalence with our definition from Section 2 becomes obvious.

Definition 7. *Let $\mathcal{C}$ be a linear $q-$ary code of length n, where n is coprime to q. We call $\mathcal{C}$* **cyclic** *if there is an $n-$cycle on the coordinates, which is an automorphism of $\mathcal{C}$.*

Theorem 10. *Let $gcd(n,q)=1$. A linear q-ary code of length n is cyclic in the sense of Definition 7 if and only if it is a code $\mathcal{C}(A)$ in the sense of Section 2.*

One direction is obvious: codes $\mathcal{C}(A)$ are cyclic in the sense of Definition 7. In order to see that the reverse implication holds we sketch the traditional theory of cyclic codes. If a code is cyclic then we can choose notation such that $\pi=(0,1,2,\dots,n-1)$ is a generator of a cyclic group of automorphisms. Here the coordinates have been numbered $0,1,2,\dots,n-1$. One can identify each word $(u_0,u_1,\dots,u_{n-1})\in\mathbb{F}_q^n$ with the polynomial $u_0+u_1X+u_2X^2+\cdots+u_{n-1}X^{n-1}$. An application of π is a cyclic shift of the subscripts of the coordinates of u, where the subscripts are taken mod n. This corresponds to multiplication with X, if we calculate mod X^n-1. This implies that an $\mathbb{F}_q$-subspace $\mathcal{C}\subseteq R=\mathbb{F}_q[X]/(X^n-1)$ is a cyclic code if and only if it is an ideal. This fact is what first attracted algebraists to the study of cyclic codes. Let $g(X)\in\mathcal{C}$ be a monic nonzero polynomial of least degree in $\mathcal{C}$. Observe that we represent each element of R (and of $\mathcal{C}$) as a polynomial of degree $<n$. Then $\mathcal{C}=(g(X))$. This means that the ideal $\mathcal{C}$ of R consists precisely of the multiples of $g(X)$ (mod X^n-1). Also, $g(X)$ is uniquely determined by $\mathcal{C}$. It is called the **generator polynomial** of $\mathcal{C}$. The generator polynomial is a divisor of X^n-1. It follows that we should write X^n-1 as a product of irreducible polynomials. Each product of some of the factors is the generator polynomial of a cyclic code. This describes the cyclic codes. We have $X^n-1=\prod_{i=1}^t f_i(X)$, where the $f_i(X)$ are **different** irreducible polynomials. The number of different cyclic codes is then 2^t. Let r be the smallest natural number such that $n\mid q^r-1$. Let ζ be a generator of the subgroup W of order n of $\mathbb{F}_{q^r}^*$. The roots of X^n-1 are the powers of ζ. These are partitioned into the roots of the $f_i(X)$. If ζ^a is a root of $f_i(X)$, then all the roots of $f_i(X)$ are precisely the ζ^b, where b is in the same cyclotomic coset as a. It follows that the irreducible factors $f_i(X)$ are in bijection with the cyclotomic cosets (see Definition 4), the degree of $f_i(X)$ being the length of the corresponding cyclotomic coset. Let now $\mathcal{C}$ be the cyclic code with

$g(X) = \prod_{l=1}^{s} f_l(X)$ as generator polynomial. As the codewords of $\mathcal{C}$ are precisely the products $g(X)p(X)$, where $p(X)$ is an arbitrary polynomial of degree $< n$, we see that $dim(\mathcal{C}) = n - \sum_{l=1}^{s} deg(f_l(X))$. Let A be the union of the cyclotomic cosets corresponding to the roots of $f_l(X), l = 1, 2, \ldots, s$. We claim that $\mathcal{C}$ is identical with the code $\mathcal{C}(A)$ as defined in Section 2. As the dimensions are equal it suffices to show that $\mathcal{C}$ is orthogonal to each row of the check matrix $tr(\mathcal{B}(A))$ from Definition 5.

In order to make the comparison we introduce coordinates. The elements of the cyclic group W may be written as $\zeta^i, i = 0, 1, \ldots, n-1$. The row of $tr(\mathcal{B}(A))$ corresponding to polynomial $\gamma \cdot X^a$ (where $\gamma \in F, a \in A$) has then entry $tr(\gamma\zeta^{ia})$ in coordinate i. Consider an arbitrary n-tuple $(\chi_i), i = 0, 1, \ldots, n-1$ with entries in $\mathbb{F}_q$. According to the traditional metaphorics of cyclic codes we write this as a polynomial $p(X) = \sum_i \chi_i X^i$. Orthogonality to our row of $tr(\mathcal{B}(A))$ means $0 = \sum_i \chi_i tr(\gamma\zeta^{ia}) = tr(\gamma \cdot \sum_i \chi_i \zeta^{ia}) = tr(\gamma \cdot p(\zeta^a))$. This will hold for all $\gamma \in F$ if and only if $p(\zeta^a) = 0$. As the codewords of $\mathcal{C}$ are multiples of $\prod_{l=l}^{s} f_l(X)$ our claim is equivalent with the following: for every $l, 1 \leq l \leq s$ and every element a in the cyclotomic coset corresponding to $f_l(X)$ we have $f_l(\zeta^a) = 0$. We know that this is true. This proves Theorem 10. The proof is due to Yves Edel.

Observe that we restrict attention to the case when the length of the code is coprime to the characteristic.

4 Constacyclic codes

Definition 8. *Let $\mathcal{C}$ be a linear q-ary code of length n. Then $\mathcal{C}$ is* **constacyclic** *if there are nonzero elements $\gamma_i \in \mathbb{F}_q$ such that for every $v = (v_{n-1}, v_{n-2}, \ldots, v_1, v_0) \in \mathcal{C}$ we also have*

$$(\gamma_{n-1} \cdot v_{n-2}, \ldots, \gamma_2 \cdot v_1, \gamma_1 \cdot v_0, \gamma_0 \cdot v_{n-1}) \in \mathcal{C}.$$

If all the $\gamma_i = 1$ we obtain the definition of a cyclic code. In order to interpret Definition 8 in a convenient way recall the operation of the monomial group $Z_{q-1} \wr S_n$ on $\mathbb{F}_q^n$. Every element of the monomial group can be written in a unique way in the form

$$diag(\lambda_{n-1}, \ldots, \lambda_0) \cdot \sigma,$$

where $diag(\lambda_{n-1}, \ldots, \lambda_0) : (v_{n-1}, v_{n-2}, \ldots, v_1, v_0) \mapsto (\lambda_{n-1}v_{n-1}, \ldots, \lambda_1 v_1, \lambda_0 v_0)$ and σ is a permutation of the coordinates. If two codes are in the same orbit under this group we call them monomially equivalent. Definition 8 says that a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is constacyclic if it is invariant under a monomial operation μ, which induces a cyclic operation of order n on the coordinates. If we replace μ, or the group generated by it, by some conjugate, we will obtain monomially equivalent codes. Conjugation under some element $diag(\lambda_{n-1}, \ldots, \lambda_0)$ shows that we can assume $\mu = diag(1, 1, \ldots, 1, \rho) \cdot (n-1, n-2, \ldots, 1, 0)$. This yields the following:

Proposition 1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a constacyclic code. Then there is a monomially equivalent code $\mathcal{C}'$, which satisfies:*
if $v = (v_{n-1}, v_{n-2}, \ldots, v_1, v_0) \in \mathcal{C}'$ then

$$(v_{n-2}, \ldots v_1, v_0, \gamma \cdot v_{n-1}) \in \mathcal{C}$$

for some nonzero $\gamma \in \mathbb{F}_q$.

If we wish to specify the constant γ in this proposition we speak of a $\gamma-$constacyclic code. This notion seems to go back to Berlekamp [1], who also speaks of a **negacyclic** code if $\gamma = -1$ (in odd characteristic). We will display a close relationship between constacyclic and cyclic codes. Although constacyclicity is more general than cyclicity we will reduce the theory of constacyclic codes to the theory of cyclic codes. Here is a first observation in this direction:

Theorem 11. *Let $\mathcal{K}$ be a constacyclic q-ary code of length n, with constant γ, such as in Proposition 1. Denote by u the multiplicative order of γ. Then the code $\mathcal{C}$ with code-words*

$$(v, \gamma v, \gamma^2 v, \ldots \gamma^{u-1} v)$$

where $v \in \mathcal{K}$ is a cyclic code.

Proof. It is clear that $\mathcal{C}$ is a linear code of length $n \cdot u$, with the same dimension as $\mathcal{K}$. It is also obvious that $\mathcal{C}$ is cyclic. ∎

Theorem 11 shows how to construct a cyclic code of larger length out of a constacyclic code. We proceed to show that this process also works in the other direction.

Theorem 12. *Let $u \mid q-1$ and $N \mid q^r - 1$ a multiple of u. Put $N = n \cdot u$. Consider the cyclic code $\mathcal{C} = \mathcal{C}(A)$ of length N with defining set A, such that all elements of $B = -\overline{\tilde{A}}$ are in the same modulus mod u. Let ω be an element of order u in $\mathbb{F}_q$.*
Then all weights of $\mathcal{C}$ are multiples of u. More precisely, there is a code $\mathcal{K}$ of length n which has the same dimension k as $\mathcal{C}$, and there is some $\gamma \in \mathbb{F}_q, \gamma^u = 1$ such that $\mathcal{C}$ is the code, whose code-words are the following:

$$(\gamma^{q-2}v, \ldots, \gamma v, v), \text{ where } v \in \mathcal{K}.$$

If $\mathcal{C}$ has parameters $[N,k,d]_q$, then $\mathcal{K}$ (a **contraction** *of $\mathcal{C}$) has parameters $[n,k,d/u]_q$.*

Proof. This follows from Theorem 9. Let ϵ be a generator of $F, \omega = \epsilon^{(q^r-1)/u}$. Put $q^r - 1 = N \cdot w, \alpha = \epsilon^w$. The elements of W are the powers $\alpha^j, j = 0,1,\ldots,N-1$. The coordinates of our code-words are parametrized by the elements $j \in \mathbb{Z}/N\mathbb{Z}$. Let $i \in B, \epsilon^k \in F$. Then $\mathcal{C}$ is generated by code-words with entry

$$tr(\epsilon^k \cdot \alpha^{ij}) = tr(\epsilon^{k+ijw})$$

in coordinate j. If we substitute $j \mapsto j+n$, we obtain entry $tr(\epsilon^{k+i(j+n)w})$. We have $\epsilon^{inw} = \omega^i \in \mathbb{F}_q$. Because of the linearity of the trace over $\mathbb{F}_q$, this becomes a factor of the entry of the code-word. As all the $i \in B$ have the same modulus mod u, this factor ω^i is the same for all choices of i. This suffices to prove the theorem. ∎

As an example consider the case $q = 3, r = 4, n = 20$. If we pick $A = [0, 10]$, then $B = \{1, 3, 7, 9\}$. It follows that $\mathcal{C}(A)$ has parameters $[20, 4, 12]_3$. The contraction $\mathcal{K}$ has parameters $[10, 4, 6]_3$. This latter code can be extended to the ternary Golay code. It is a natural question when contractions of cyclic codes are cyclic codes. Our example shows that this is not always the case. It is in fact easy to check that there is no cyclic ternary code $[10, 4, 6]_3$.

Theorem 13. *Let $\mathcal{K}$ be the contraction of a q-ary cyclic code, in the sense of Theorem 12. Then $\mathcal{K}$ is constacyclic.*

Proof. We have seen in Theorem 12 that there is a cyclic code $\mathcal{C}$ of length $u \cdot n$ whose code-words are precisely those of the form

$$(\beta^{u-1}v, \ldots, \beta v, v) \text{ for } v \in \mathcal{K}.$$

Using the cyclicity of $\mathcal{C}$ we see just as in Theorem 11 that $\mathcal{K}$ is constacyclic with constant $\gamma = 1/\beta$. ∎

We have seen the following:

Theorem 14. *The class of constacyclic codes is the same as the class of contractions of cyclic codes.*

In [7] Kschischang and S.Pasupathy considered among others ternary and quaternary constacyclic codes. It has been shown in [7] that negacyclic codes of odd length are necessarily equivalent to cyclic codes. Our next theorem generalizes this result. This is indeed a triviality.

Theorem 15. *Let $\mathcal{K}$ be a q-ary $\gamma-$constacyclic code of length n such that n and the multiplicative order u of γ are coprime. Then $\mathcal{K}$ is equivalent to a cyclic code.*

Proof. The fact that $\mathcal{K}$ is $\gamma-$constacyclic means that it is invariant under the element $\mu = diag(1, 1 \ldots, 1, \gamma)\sigma$ of the monomial group. Here σ is a cyclic permutation of the coordinates. We have $\mu^n = diag(\gamma, \ldots, \gamma)$, a scalar operation which leaves $\mathcal{K}$ invariant because $\mathcal{K}$ is linear. As n and u are coprime we have that μ^u is cyclic of order n and that the group generated by μ^u intersects the normal subgroup of the monomial group trivially. As $\mathcal{K}$ is invariant under μ^u, it is a cyclic code. ■

Example 2. *Let $q = 3, N = 56$. We have $56 \mid 3^6 - 1$. Two of the cyclotomic cosets are $\{7, 21\}$ and $\{1, 3, 9, 27, 25, 19\}$. Consider the cyclic code with defining set $A = [28, 0]$. Clearly it has parameters $[56, 8, 30]_3$. As our two cyclotomic cosets are disjoint from $\tilde{A}$ and all their elements are odd, Theorem 12 applies and we obtain a contraction with parameters $[28, 8, 15]_3$. This constacyclic code has optimal parameters and was first constructed in [7].*

4.1 The duals

It is clear that the dual of a constacyclic code is constacyclic. We wish to describe the dual more precisely, using the representation of Theorem 12 of constacyclic codes as contractions of cyclic codes. It is clear that the cyclic codes which occur in our context are more handily described in terms of their set B of zeroes than by their defining set A.

Theorem 16. *Let $\mathcal{K}$ be a constacyclic code described as contraction of a cyclic code $\mathcal{C}(A)$ with set of zeroes $B = -\overline{\tilde{A}}$. Then $\mathcal{K}^\perp$ is the contraction of the cyclic code with set of zeroes B', where B' is the complement of $-B$ in the set of all numbers having modulus the negative of the elements of B.*

Proof. Let us make sure that the dimension is correct. Here we use the terminology of Theorem 12. We know that $\mathcal{K}$ has dimension k, where $k = |B|$. As $\mathcal{K}^\perp$ has dimension $n - k$, the cyclic code which yields $\mathcal{K}^\perp$ by contraction

must have a set of zeroes B' of size $n-k$. As precisely n elements of $\mathbb{Z}/N\mathbb{Z}$ have a given modulus mod u our set B' has the right size.
It remains to prove that our codes are orthogonal. This is reduced in the usual way to the identity $\sum_{j=0}^{n-1}\epsilon^{(i+i')jw}=0$, whenever $i\in B, i'\in B'$. By choice of B' we have that $i+i'$ is a multiple of u, but $i+i'\neq 0$. Let $i+i'=u\cdot m$. Then $\epsilon^{(i+i')jw}$ is an n-th root of unity but not 1. The claim follows. ■

We obtain a criterion when a constacyclic code is self-dual:

Corollary 1. *Let $\mathcal{K}$ be a constacyclic code described as contraction of a cyclic code with set of zeroes B, in the terminology of Theorem 12. Let $i\in B$. Then $\mathcal{K}\subseteq\mathcal{K}^{\perp}$ if and only if i and $-i$ are in the same modulus and $B\cap(-B)=\emptyset$. If this is satisfied, then $\mathcal{K}=\mathcal{K}^{\perp}$ if and only if the set of all n numbers of the same modulus as i (mod u) is the disjoint union of B and of $-B$.*

This follows directly from the preceding theorem.

Example 3. *In Example 2 we constructed a code $\mathcal{K}_1$ with optimal parameters $[28,8,15]_3$ by contraction from the cyclic code of length 56 with set of zeroes $B_1=Z(1)\cup Z(7)$. Choose now $B_2=Z(1)\cup Z(7)\cup Z(5)$ and $B_3=B_2\cup Z(11)$ and denote by $\mathcal{K}_2,\mathcal{K}_3$ the corresponding constacyclic codes. We have a chain*

$$\mathcal{K}_1\subset\mathcal{K}_2\subset\mathcal{K}_3,$$

where $\mathcal{K}_3=\mathcal{K}_1^{\perp}$ and $\mathcal{K}_2$ is self-dual.

5 Additive cyclic codes

We generalize our theory from the category of linear codes to the category of additive codes. Here we call a code $\mathcal{C}$ **additive** if its alphabet E forms a vector space over a ground field $\mathbb{F}_q$, and $\mathcal{C}$ is linear over $\mathbb{F}_q$. The special case of linear codes is obtained when $m = 1$ and also in case $m > 1$ when E is given the structure of a field and $\mathcal{C}$ is linear over this field. Our approach to linear cyclic codes motivates the following generalization:

Let $F = \mathbb{F}_{q^r}$ and $E = \mathbb{F}_q^m$, where $m \leq r$. Let $\Phi : F \longrightarrow E$ be a surjective $\mathbb{F}_q-$linear mapping and $tr : F \longrightarrow \mathbb{F}_q$ the trace. The mapping Φ can be described as follows: there is a subset $\Gamma = \{\gamma_1, \ldots, \gamma_m\} \subset F$ such that

$$\Phi(x) = (tr(\gamma_1 x), \ldots, tr(\gamma_m x)).$$

Here Γ is linear independent over $\mathbb{F}_q$ as Φ is onto. We fix a divisor $n|(q^r - 1)$ and a subset $A \subset \mathbb{Z}/n\mathbb{Z}$. Use the terminology of Section 2.

Definition 9. *Every row of $\Phi(\mathcal{B}(A))$ can be seen as an element of $V = \mathbb{F}_q^{mn} = E^n$. Equip $E = \mathbb{F}_q^m$ and V with the standard dot product $\langle , \rangle$ and define*

$$\mathcal{C}(A) = \mathcal{C}(A, n, \Phi) = (\Phi(\mathcal{B}(A)))^{\perp}.$$

Linear cyclic codes correspond to the special case when $m = 1$ and $\Phi(x) = tr(x)$.

5.1 The dimension of additive cyclic codes

Definition 10. *Call a polynomial $p(X) \in F[X]$* **cyclotomic** *if all the exponents of its nonzero monomials belong to the same cyclotomic coset.*

Clearly $dim(\mathcal{C}(A)) = mn - dim(\Phi(\mathcal{B}(A)))$, where $dim(\Phi(\mathcal{B}(A)))$ denotes the dimension of the row space of $\Phi(\mathcal{B}(A))$.

Let $\mathcal{B} \subset F^n$ be an F-linear code. We define

$$(\mathcal{B}, \Gamma) = \{(\gamma_1 \cdot v | \gamma_2 \cdot v | \ldots | \gamma_m \cdot v) \mid v \in \mathcal{B}\},$$

a code of length mn and the same dimension as $\mathcal{B}$. By definition of Φ we have $\Phi(\mathcal{B}(A)) = tr(\mathcal{B}(A), \Gamma)$. Let $\mathcal{D}(A)$ be the Galois closure of $(\mathcal{B}(A), \Gamma)$, that is the smallest code containing $(\mathcal{B}(A), \Gamma)$, which is Galois invariant. Theorem 4 yields the following:

Theorem 17. *$dim_{F_q}(\mathcal{C}(A)) = mn - dim_F(\mathcal{D}(A))$, where $\mathcal{D}(A)$ is the Galois closure of $(\mathcal{B}(A), \Gamma)$.*

In order to determine the dimension of the twisted code $\mathcal{C}(A)$, it suffices to determine the dimension $d(A)$ of the F-linear code $\mathcal{D}(A)$.

It will be convenient to identify the row of $\mathcal{B}(A)$ indexed by polynomial $p(X)$ with that polynomial itself. In this notation the elements of $(\mathcal{B}(A), \Gamma)$ are the m-tuples $(\gamma_1 \cdot p(X), \ldots, \gamma_m \cdot p(X))$, where $p(X) \in \mathcal{P}(A)$. The underlying space $V_F = F^{mn}$ can be viewed as a tensor product $V \otimes_{F_q} F$ obtained from V by extension of constants. We equip it with the dot product $\langle , \rangle$ again. Because of Lemma 1 the notational convention leads to the following formula:

$$\langle X^i, X^j \rangle = \begin{cases} 0 & \text{if } i + j \neq 0 \\ n(\gamma_1^2 + \cdots + \gamma_m^2) & \text{if } i + j = 0. \end{cases}$$

Here the exponents are mod n, as always.

Lemma 3. *Let Z be a cyclotomic coset. Denote by $V_F(Z)$ the set of $(p_1(X), \ldots, p_m(X))$, where all $p_i(X) \in \mathcal{P}(Z)$. Then $dim(V_F(Z)) = m|Z|$,*

$$V_F = \bigoplus_Z V_F(Z)$$

and $V_F(Z)^\perp$ is the sum of all $V_F(Z')$, where $Z' \neq -Z$.

This is trivial. If $p(X) \in \mathcal{P}(Z)$, then the Galois closure of $(\gamma_1 \cdot p(X), \ldots, \gamma_m \cdot p(X))$ is contained in $V_F(Z)$. It follows that $\mathcal{D}(A)$ is the direct sum of its subspaces $\mathcal{D}(A \cap Z) = \mathcal{D}(A) \cap V_F(Z)$, where Z varies over the cyclotomic cosets. Lemma 3 shows that the dual $\mathcal{D}(A)^\perp$ decomposes in a similar way:

$$\mathcal{D}(A)^\perp = \bigoplus_Z \mathcal{D}(A \cap Z)^\perp \cap V_F(-Z)$$

Define $\mathcal{E}(A \cap Z) = \mathcal{D}(A \cap Z)^\perp \cap V_F(-Z)$. By Delsarte's theorem we have $\mathcal{C}(A) = (\mathcal{D}(A)^\perp)_{F_q}$. As $\mathcal{D}(A \cap Z)$ is Galois-closed, the same is true of $\mathcal{E}(A \cap Z)$. It follows $\mathcal{E}(A \cap Z)_{F_q} = tr(\mathcal{E}(A \cap Z))$. We obtain a decomposition $\mathcal{C}(A) = \sum_Z tr(\mathcal{E}(A \cap Z)) = \sum_Z \mathcal{E}(A \cap Z)_{F_q}$.

Theorem 18. *Let* $\mathcal{E}(A\cap Z)=\mathcal{D}(A\cap Z)^{\perp}\cap V_F(-Z)$. *Then* $\mathcal{D}(A\cap Z)$ *and* $\mathcal{E}(A\cap Z)$ *are Galois-closed. We have* $\mathcal{D}(A)=\bigoplus_Z\mathcal{D}(A\cap Z)$ *and* $\mathcal{D}(A))^{\perp}=\bigoplus_Z\mathcal{E}(A\cap Z)$. *Furthermore we have the decomposition*

$$\mathcal{C}(A)=\bigoplus_Z tr(\mathcal{E}(A\cap Z))=\bigoplus_Z\mathcal{E}(A\cap Z)_{F_q}.$$

Let $d(A\cap Z)$ be the dimension of $\mathcal{D}(A\cap Z)$. We have seen $d(A)=\sum_Z d(A\cap Z)$ and $c(A)=dim_{F_q}\mathcal{C}(A)=mn-d(A)=\sum_Z c_Z(A)$, where $c_Z(A)=m|Z|-d(A\cap Z)=dim(\mathcal{E}(A\cap Z))$.

Let us collect some obvious information on these dimensions. Clearly $d(A\cap Z)\leq m|Z|$, equivalently $c_Z(A)\geq 0$. If $Z\cap A=\emptyset$, then clearly $d(A\cap Z)=0$ and $c_Z(A)=m|Z|$. In the other extreme case when $Z\subseteq A$ we have $d(A\cap Z)=m|Z|$ and $c_Z(A)=0$. In order to obtain a general bound observe that $(\mathcal{B}(A\cap Z),\Gamma)$ has dimension $|A\cap Z|$ and the Galois group has order r. It follows that the dimension of the Galois closure satisfies $d(A\cap Z)\leq r|A\cap Z|$. Also, as $\mathcal{D}(A\cap Z)$ is contained in a space of dimension $m|Z|$, we trivially have $d(A\cap Z)\leq m|Z|$.

Theorem 19. *Let* $d(A)$ *be the dimension of the Galois closure* $\mathcal{D}(A)$ *of* $(\mathcal{B}(A),\Gamma)$ *and* $c(A)=dim_{F_q}(\mathcal{C}(A))$. *Then* $d(A)+c(A)=mn$. *Let* $c_Z(A)=dim(\mathcal{E}(A\cap Z))$. *Then* $d(A\cap Z)+c_Z(A)=m|Z|$. *We have* $d(A)=\sum_z d(A\cap Z)$ *and* $c(A)=\sum_z c_Z(A)$. *The dimensions* $c_Z(A)$ *satisfy the following:*

- *In general* $0\leq c_Z(A)\leq m|Z|$ *and*
- $c_Z(A)\geq m|Z|-r|A\cap Z|$.
- *If* $Z\cap A=\emptyset$, *then* $c_Z(A)=m|Z|$.
- *If* $Z\subseteq A$, *then* $c_Z(A)=0$.

Theorem 20. *In the situation of Theorem 19, let* r' *be a divisor of* r, Z *a cyclotomic coset of length* $s\mid r'$ *and* Γ *contained in* $F_0=\mathbb{F}_{q^{r'}}$. *Then*

$$c_Z(A)\geq m|Z|-r'|A\cap Z|.$$

Proof. Let $g(x) = x^{q^{r'}}$. Then g is an element of order r/r' of the Galois group. A basis of $(\mathcal{B}(A \cap Z), \Gamma)$ is given by the $v_z = (\gamma_1 X^z | \dots | \gamma_m X^z)$, where we have used our earlier convention and z varies over $A \cap Z$. As $\gamma_i \in F_0$ and because of our assumption on the length of Z we have that g stabilizes v_z. This implies that the subgroup of order r/r' of the Galois group G leaves $(\mathcal{B}(A \cap Z), \Gamma)$ invariant. The dimension $d(A \cap Z)$ of the Galois closure can therefore not exceed $r'|A \cap Z|$. ∎

Let us study the dimensions in more detail. We have that a basis of $(\mathcal{B}(A \cap Z), \Gamma)$ consists of the vectors $v_z = (\gamma_1 X^z | \dots | \gamma_m X^z)$, where z varies over $A \cap Z$. The Galois closure $\mathcal{D}(A \cap Z)$ is therefore generated by the $v_z^{q^j}$, where $j = 0, 1, \dots, r-1$. These are $r|A \cap Z|$ elements. Fix now some $y \in Z$. Let $G(z, y) = \{j \mid zq^j = y\}$, the set of elements of the Galois group mapping $z \mapsto y$, where $z \in Z$. Clearly $|G(z, y)| = r/s$, where $s = |Z|$. Define

$$\mathcal{D}(A \cap Z, y) = \langle v_z^{q^j} \mid z \in A \cap Z, j \in G(z, y) \rangle.$$

We have $\mathcal{D}(A \cap Z, y) \subseteq V_F(y)$ with obvious terminology. Observe that $V_F(Z) = \bigoplus_{y \in Z} V_F(y)$. As the elements of G permute the spaces $\mathcal{D}(A \cap Z, y)$, they all have the same dimension. Let $d(A \cap Z, y) = dim(\mathcal{D}(A \cap Z, y))$. We have seen

$$d(A \cap Z) = s \cdot d(A \cap Z, y) \text{ for all } y \in Z.$$

We are reduced to describe $d(A \cap Z, y)$ for some fixed but arbitrary $y \in Z$.

Consider $v_z^{q^j}$, where $z \in A \cap Z$ and $j \in G(z, y)$. These $\frac{r}{s}|A \cap Z|$ elements form a set of generators of $\mathcal{D}(A \cap Z, y)$. Let $a(z, j)$ be coefficients of a linear dependence, hence $\sum_{z,j} a(z, j) v_z^{q^j} = 0$. Here (z, j) vary over all pairs such that $z \in A \cap Z, zq^j = y$. The definition of v_z shows that this is equivalent with $\sum_{z,j} a(z, j)\gamma^{q^j} = 0$, for all $\gamma \in \Gamma$. The dimension of the space of solutions is the codimension in $\frac{r}{s}|A \cap Z|$ of $d(A \cap Z, y)$. It is also the codimension of the rank of the corresponding coefficient matrix. We arrive at the following description:

Theorem 21. *Let A and a cyclotomic coset Z of length s be given. Fix some $y \in Z$. Define a matrix M with m rows and $\frac{r}{s}|A \cap Z|$ columns as follows:*

- *the rows are parametrized by* $\gamma \in \Gamma$,
- *the columns by the pairs* (z, j), *where* $zq^j = y$,
- *the corresponding entry is* γ^{q^j}.

Dimension $d(A \cap Z, y)$ *is the rank of* M *and we have*

$$d(A \cap Z) = s \cdot d(A \cap Z, y),\ c_Z(A) = s(m - d(A \cap Z, y)).$$

Observe that in case $m = 1$, the case of linear cyclic codes, we obtain the usual expression for the dimension. In fact, if $A \cap Z = \emptyset$, then $c_Z(A) = s$ as remarked earlier. If $A \cap Z \neq \emptyset$, we obtain a matrix M with just one row, which is not the 0-matrix. It follows $d(A \cap Z, y) = 1$, hence $c_Z(A) = 0$. It follows that $c(A)$ is the sum of the lengths of the cyclotomic cosets, which intersect A trivially, as expected.

Consider next case $m = 2$. Recall that $dim(V_F(Z)) = 2s \geq c_Z(A)$, and $c_Z(A)$ is a multiple of s. We have $c_Z(A) = 2s$ if and only if $A \cap Z = \emptyset$. It remains to decide when $c_Z(A) = s$. Choose without restriction $\Gamma = \{1, \gamma\}$, where $\gamma = \gamma_2$ and let $\kappa = [\mathbb{F}_q(\gamma) : \mathbb{F}_q]$. Further let $H < G$ be the subgroup of order r/κ, that is H consists all elements of the Galois group, which fix γ. Choose $y \in A \cap Z$. Theorem 21 shows that $c_Z(A) = s$ is equivalent to $d(A \cap Z, y) = 1$, which means that matrix M must have rank 1. As the first row of M is constant 1 we must have that all columns of M are identical. This means that each element of G mapping some element of $A \cap Z$ to some element of $A \cap Z$ must be in H. Let us say that H affords **complete action** on $A \cap Z$ in this case.

Lemma 4. *Let* $m = 2, \Gamma = \{1, \gamma\}$ *and* $H < G$ *the stabilizer of* γ *in* G. *Then the following holds:*

$$c_Z(A) = \begin{cases} 2s & \text{if } A \cap Z = \emptyset \\ s & \text{if } A \cap Z \neq \emptyset \text{ and } H \text{ affords complete action on } A \cap Z \\ 0 & \text{otherwise} \end{cases}$$

Consider the special case when $m = 2$ and $\mathbb{F}_q(\gamma) = F$. This means that H is the identity subgroup. The second case of Lemma 4 will happen only if $|A \cap Z| = 1$ and $|Z| = s = r$.

Lemma 5. *Let $m = 2, \Gamma = \{1, \gamma\}$ and $\mathbb{F}_q(\gamma) = F$. Then the following holds:*

$$c_Z(A) = \begin{cases} 2s & \text{if } A \cap Z = \emptyset \\ s & \text{if } |A \cap Z| = 1 \text{ and } s = r \\ 0 & \text{otherwise} \end{cases}$$

It is important to have criteria when $c_Z(A) = 0$. Here is one such sufficient condition.

Theorem 22. *Assume there is some $y \in A \cap Z$ and an interval J of m numbers such that $yq^{-j} \in A \cap Z$ for all $j \in J$. Then $c_Z(A) = 0$. Observe that this is satisfied in particular if $\{y, y^q, \ldots, y^{q^{m-1}}\} \subseteq A \cap Z$.*

Proof. Let $\Gamma = (\gamma_1, \ldots, \gamma_m)^T$ and $J = \{j, j+1, \ldots, j+m-1\}$. Matrix M contains columns $\Gamma^{q^j}, \ldots, \Gamma^{q^{j+m-1}}$. Assume the corresponding quadratic submatrix of M is not regular. Let $c_0, \ldots, c_{m-1} \in F$ be coefficients of a linear combination of the columns. Consider the polynomial $p(X) = c_0 X^{q^j} + \cdots + c_{m-1} X^{q^{j+m-1}}$. We have $p(\gamma_1) = \cdots = p(\gamma_m) = 0$. It follows that $p(X)$ vanishes at the subspace $\langle \gamma_1, \ldots, \gamma_m \rangle$. Let $p(X) = q(X)^{q^j}$, where $q(X)$ has degree q^{m-1}. As it has too many roots we see that $q(X)$ is the 0-polynomial, hence $c_0 = \cdots = c_{m-1} = 0$, contradiction. ∎

5.2 The minimum distance of additive cyclic codes

Theorem 23 (*BCH* **bound).** *If A contains an interval of size t (mod n), then $\Phi(\mathcal{B}(A))$ is an orthogonal array of strength t. The minimum distance of $\mathcal{C}(A)$ is $\geq t + 1$.*

Proof. We follow the lines of the proof of the BCH-bound for cyclic codes. Clearly we can assume $A = [l, l+t-1]$. The fact that $\Phi(\mathcal{B}(A))$ has strength t follows from Lagrange interpolation. It follows from $\mathbb{F}_q$-linearity that the minimum distance of $\mathcal{C}(A)$ agrees with its minimum nonzero weight, just as in the case of linear codes. Let $x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}(A)$ such that $x_i = 0, i > t$. We have to show $x = 0$. Let $i \leq t, e \in E$. As $\Phi(\mathcal{B}(A))$ has strength t we can find some $y = (y_1, y_2, \ldots, y_n) \in \Phi(\mathcal{B}(A))$ such that $y_j = 0$ for all $j \leq t, j \neq i$ and $y_i = e$. Orthogonality shows $\langle x_i, e \rangle = 0$. As this is true for all $i \leq t$ and $e \in E$ we conclude from the non-degeneracy of $\langle , \rangle$ that $x = 0$. ■

6 A class of low-dimensional cyclic additive codes

Let $r = 2r'$ and consider the subfield $F_0 = \mathbb{F}_{q^{r'}}$. Let $m \leq r'$ and choose $\Gamma \subset F_0$. We consider the primitive case $n = q^r - 1$. In this situation we consider the lowest-dimensional twisted codes $\mathcal{C}(A)$. These arise for the following choices of the defining interval:

$$A_1 = [0, q^r - q^{r-m} - 2], \; A_2 = [0, q^r - q^{r-m} - q^{r'-m} - 2].$$

Consider the corresponding codes $\mathcal{C}_i = \mathcal{C}(A_i)$. Clearly

$$\mathcal{C}_1 \subset \mathcal{C}_2.$$

We start by showing that intervals larger than A_1 give no contribution.

Theorem 24. *Let $A = [0, q^r - q^{r-m} - 1]$. Then $c(A) = 0$.*

Proof. We have to show that for every z the corresponding cyclotomic coset $Z(z)$ satisfies the conditions of Theorem 22. Let $\pi(i) = (\alpha_{r-1}(i), \ldots, \alpha_0(i))$ be the coefficients of the q-ary representation of number i, in descending order. Observe that $Z(i)$ consists of the numbers whose representation is obtained by cyclic permutation from $\pi(i)$. We remark that this interpretation of the permutation representation of the Galois group has been exploited by Rédei in [6] as well. We have

$$\pi(q^r - q^{r-m} - 1) = (q-1, \dots, q-1, q-2, q-1, \dots),$$

where $\alpha_{r-m} = q-2$, all other $\alpha_j = q-1$. Let now μ denote the minimum of the $\alpha_j(z)$. The claim is obvious if $\mu < q-2$. Consider the remaining case $\mu = q-2$. Choose z as a representative of its cyclotomic coset such that $\alpha_{r-1}(z) = q-2$. Shifting $m-1$ times to the right we clearly obtain elements $< q^r - q^{r-m} - 1$. The same remains true if we shift once more. Theorem 22 applies. ■

Consider $\mathcal{C}_1$. Its minimum weight is $\geq q^r - q^{r-m}$ by the $BCH-$bound. The cyclotomic coset $Z(-1)$ of length r meets A_1 in precisely $m-1$ elements:

$$Z(-1) \cap A_1 = \{q^r - q^{r-m+1} - 1, q^r - q^{r-m+2} - 1, \dots, q^r - q^{r-1} - 1\}$$

Let $z_0 = -q^{r-1}, z_1 = z_0/q, \dots, z_{m-2} = -q^{r-m+1} = z_0/q^{m-2}$. Then $Z(-1) \cap A_1 = \{z_0, z_1, \dots, z_{m-2}\}$. It follows from Theorem 19 that $c_{Z(-1)}(A_1) \geq r$, hence $dim(\mathcal{C}_1) \geq r$. We want to be as explicit as possible.

Recall $\mathcal{E}(A_1 \cap Z(-1)) = \mathcal{D}(A_1 \cap Z(-1))^{\perp} \cap V_F(Z(1))$. We have $s = |Z(-1)| = r$ and choose $y = z_0 = -q^{r-1}$. A basic relation says $d(A_1 \cap Z(-1)) = r \cdot d(A_1 \cap Z(-1), z_0)$. In order to determine the latter dimension we observe that $\mathcal{D}(A_1 \cap Z(-1))$ is generated by the vectors $v_z^{q^j}$, where $z \in A_1 \cap Z(-1))$ and $j \in G(z, z_0)$. Here $v_z = (\gamma_1 X^z | \dots | \gamma_m X^z)$ in our short notation, hence

$$\mathcal{D}(A_1 \cap Z(-1), z_0) = \langle v_{z_j}^{q^j} | j = 0, 1, \dots, m-2 \rangle.$$

We have

$$\mathcal{E}(A_1 \cap Z(-1), z_0) = \langle v_{z_j}^{q^j} | j = 0, 1, \dots, m-2 \rangle^{\perp} \cap V_F(-z_0).$$

The definition of the scalar product shows that $(\eta_1 X^z|\ldots|\eta_m X^z) \in \mathcal{E}(A_1 \cap Z(-1), z_0)$ if and only, with respect to the ordinary dot product we have

$$(\eta_1,\ldots,\eta_m)\cdot(\gamma_1,\ldots,\gamma_m)^{q^j}=0,\ j=0,\ldots,m-2.$$

Lemma 6. *Let $\mathbb{F}_q \subset F = \mathbb{F}_{q^r}$ and $\gamma_1,\ldots,\gamma_m \in F$ be elements, which are linearly independent over $\mathbb{F}_q$. Let $v=(\gamma_1,\ldots,\gamma_m) \in F^m$. Consider the $(m-1,m)-$matrix M with rows $v^{q^i}, i=0,1,\ldots,m-2$.*

Then M has rank $m-1$. Let W be the space generated by the rows of M and $(\eta_1,\ldots,\eta_m)$ a generator of the 1-dimensional space $W^\perp$. Then $\eta_1,\ldots,\eta_m$ are linearly independent over $\mathbb{F}_q$.

Proof. Consider the square matrix with rows $v^{q^i}, i=0,1,\ldots,m-1$. A familiar argument shows that M is regular. It follows $rank(M)=m-1$. Assume there are elements $c_1,\ldots,c_m \in \mathbb{F}_q$ such that $\sum_j c_j\eta_j=0$. The vector $c=(c_1,\ldots,c_m)\in \mathbb{F}_q^m$ is then in W. There must be coefficients $a_i \in F$ such that

$$c=\sum_{i=0}^{m-2} a_i v^{q^i}.$$

Raising to the $q-$th power we obtain

$$c=c^q=\sum_{i=0}^{m-2} a_i^q v^{q^{i+1}}$$

By comparison of coefficients we obtain $a_0=0, a_1=a_0^q=0,\ldots,a_{m-2}=a_{m-3}^q=0$, hence $c=0$. ∎

As $-z_0=q^{r-1}$ we have in the terminology of Lemma 6 that the 1-dimensional $F-$vector space $\mathcal{E}(A_1\cap Z(-1),z_0)$ is generated by $(\eta_1 X^{r-1}|\ldots|\eta_m X^{r-1})$. Application of the trace yields $\mathcal{E}(A_1\cap Z(-1))_{F_q}$. These are all the vectors

$$(tr(a\eta_1 u^{q^{r-1}}),\ldots,tr(a\eta_m u^{q^{r-1}})), u\in F^*,$$

where a varies over F. Consider a vector given by some fixed $a \neq 0$. Remember that we consider m-tupels as entries. Such an entry (parametrized by u) vanishes if and only if $tr(a\eta_1 u^{q^{r-1}}) = \cdots = tr(a\eta_m u^{q^{r-1}}) = 0$. By Lemma 6 this describes an $(r-m)$-dimensional subspace. It follows that $q^{r-m}-1$ entries vanish. The same type of argument shows that every nonzero m-tuple appears with frequency q^{r-m}. It follows from Theorem 24 that this describes all of $\mathcal{C}_1$. Here is a different argument, which leads to the same conclusion: We have seen that every nonzero element of $\mathcal{C}_1$ has weight $q^r - q^{r-m}$. Concatenation with the Simplex code $[q^m-1, m, q^{m-1}]_q$ yields a q-ary linear code $[(q^m-1)(q^r-1), k, q^{m-1}(q^r-q^{r-m})]_q$, where $k = dim(\mathcal{C}_1) \geq r$. The Griesmer bound shows that $k = r$ (and the concatenated code meets the Griesmer bound with equality).

Lemma 7. *Let $\mathcal{C}_1 = \mathcal{C}(A_1)$, where $A_1 = [0, q^r - q^{r-m} - 2]$. Then $\mathcal{C}_1 = \mathcal{E}(A_1 \cap Z(-1))$, $dim(\mathcal{C}_1) = r$ and every nonzero word of $\mathcal{C}_1$ has weight $q^r - q^{r-m}$.*

Let $t = q^r - q^{r-m} - q^{r'-m} - 1 = -(q^{r-m} + q^{r'-m})$. We want to show that $\mathcal{C}([0,t]) = \mathcal{C}_1$. As $Z(-1) \cap [0,t] = Z(-1) \cap A_1$ it suffices to show that for all cyclotomic cosets $Z \neq Z(-1)$ we have $c_Z([0,t]) = 0$. As before we choose $z \in Z, \mu$ the minimum of the $\alpha_j(z)$ and use Theorem 22. We can assume $\mu = q-2$ and $\alpha_{r-1}(z) = q-2$. Compare with

$$\pi(t) = (q-1, \dots, q-2, q-1, \dots, q-2, q-1, \dots),$$

the only numbers $\alpha_j(z) \neq q-1$ being $\alpha_{r-m}(z) = \alpha_{r'-m} = q-2$ (a first segment of m ends with a $q-2$, the next segment of length r' ends with $q-2$ again, follows by a string of $r'-m$ entries $q-1$). Only $zq^{-(m-1)}$ is critical. Assume this is $> t$. The first segment (length m) must be identical to the first segment of t, the second segment (length r') must have all entries $q-1$. Let ω be the last segment. If all entries of ω are $q-1$, we have $Z(z) = Z(-1)$, contradiction. Start from an entry $q-2$ in ω. Clearly Theorem 22 applies.

Consider $\mathcal{C}_2$ next. By the $BCH-$bound its minimum distance is $\geq q^r - q^{r-m} - q^{r'-m}$. Let t as before. We see that $Z(t)$ intersects A_2 precisely in $tq, \dots, tq^{m-1}$. The length of our cyclotomic coset is $|Z(t)| = r'$. It follows from Theorem 20 that $c_{Z(t)}(A_2) \geq mr' - r'(m-1) = r'$, hence $dim(\mathcal{C}_2) \geq r + r' = 3r'$.

Let us be explicit again. Choose $z_0 = -(q^{r-1} + q^{r'-1})$. Then $z_0 = -q^{r-1}, z_1 = z_0/q, \dots, z_{m-2} = -q^{r-m+1} = z_0/q^{m-2}$. We have $Z(t) \cap A_2 =$

$\{z_0, z_1, \ldots, z_{m-2}\}$, where $z_1 = z_0/q, \ldots, z_{m-2} = z_0/q^{m-2}$. Space $\mathcal{D}(A_2 \cap Z(t))$ is generated by the vectors $v_{z_i}^{q^i}$ and $v_{z_i}^{q^{r'+i}}$, where $i = 0, 1, \ldots, m-2$. As the second set of generators coincides with the first set in our situation we see that $\mathcal{D}(A_2 \cap Z(t), z_0)$ is generated by the $v_{z_i}^{q^i}$. It follows from Lemma 7 that we have equality in our general bound: $d(A_2 \cap Z(t), z_0) = m-1$, $d(A_2 \cap Z(t)) = r'(m-1)$ and $c_{Z(t)}(A_2) = r'$. The 1-dimensional $F-$vector space $\mathcal{E}(A_2 \cap Z(t), z_0)$ is generated by vector $(\eta_1 X^{-z_0}| \ldots |\eta_m X^{-z_0})$, where the tuple $(\eta_1, \ldots, \eta_m)$ is the same as in the former case of $\mathcal{C}_1$. We will make use of the fact that we can choose $\eta_j \in F_0$. The $r'-$dimensional space $\mathcal{E}(A_2 \cap Z(t))_{F_q}$ consists of the words with entry

$$(tr(b'\eta_1 u^{-z_0}), \ldots, tr(b'\eta_m u^{-z_0})),$$

in coordinate u. As the trace factors we can describe this equivalently as

$$(Tr(b\eta_1 u^{-z_0}), \ldots, Tr(b'\eta_m u^{-z_0})), u \in F^*,$$

where b varies in F_0. For dimensional reasons this is the precise description of $\mathcal{E}(A_2 \cap Z(t))_{F_q}$.

Lemma 8. *Code $\mathcal{C}_2 = \mathcal{C}(A_2)$ is the direct sum of $\mathcal{C}_1$ and the $r'-$dimensional subcode $\mathcal{E}(A_2 \cap Z(t))_{F_q}$, whose elements are parametrized by $b \in F_0$, with the following entry in coordinate section $u \in F^*$:*

$$(Tr(b\eta_j u^{q^{r-1}+q^{r'-1}}))_j, \; j = 1, 2, \ldots m.$$

Here $Tr : F_0 \longrightarrow \mathbb{F}_q$.

The elements of the $3r'-$dimensional code $\mathcal{C}_2$ will be denoted by $v(a, b)$, where $a \in F, b \in F_0$. The entry of $v(a, b)$ in coordinate section u is

$$(tr(a\eta_j u^{q^{r-1}}) + Tr(b\eta_j u^{q^{r-1}+q^{r'-1}}))_j$$

Let $x = u^{q^{r-1}}$. Denote by T and N the trace and norm of the quadratic field extension $F_0 \subset F$. The entry of $v(a, b)$ in section u is

$$(tr(a\eta_j x) + Tr(b\eta_j N(x)))_j$$

This is beginning to look nice. As $u \mapsto x$ is a field automorphism we can see this as entry in coordinate section x. We want to determine the weight of $v(a,b)$ or more generally the frequency of entries. As tr factors we can write the first expression as $Tr(\eta_j T(ax))$ and the whole expression becomes

$$(Tr(\eta_j \cdot (T(ax) + bN(x)))_j$$

Let $W_0 = \langle \eta_1 \dots . \eta_m \rangle^\perp \cap F_0$, where the dual is with respect to Tr. Then $dim(W_0) = r' - m$ and $v(a,b)$ vanishes at x if and only if $T(ax) + bN(x) \in W_0$. Cases $a = 0$ and $b = 0$ have been dealt with already, so assume $ab \neq 0$. The substitution $x \mapsto \alpha x$ corresponds to $v(a\alpha, bN(\alpha)$. We can therefore assume $a = 1$ and have to consider the simple expression $T(x) + bN(x) = c$, that is for given values $b, c \neq 0$ we want to count the solutions $x \in F^*$. This makes things easy and in fact no theory is needed. This direct approach is pursued in [2].

7 Conclusion

We have given a new approach to cyclic codes. This simplified theory enabled us to describe constacyclic codes as contractions of cyclic codes. A natural generalization leads to a theory of cyclic additive codes. While the basic idea to study such generalizations of linear codes certainly is not new (see for example [3, 5]) our theory appears to be new. An important point is that we can find generator matrices in an essentially canonical way. The efficiency of the theory was exemplified by studying a large family of low-dimensional codes.

References

[1] E R Berlekamp: *Algebraic Coding Theory*, McGraw-Hill, New York 1968.

[2] J.Bierbrauer: *Direct constructions of additive codes,* manuscript.

[3] J.M.Jensen: *Subgroup Subcodes, IEEE Transactions on Information Theory* **41** (1995),781-785.

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

[5] M.Hattori, R.J.McEliece and G.Solomon: *Subspace subcodes of Reed-Solomon codes, IEEE Transaction on Information Theory* **44**(1998),1861-1880.

[6] L.Rédei: *Lückenhafte Polynome,* Birkhäuser Verlag, Basel, Stuttgart 1970.

[7] F.R.Kschischang and S.Pasupathy: *Some ternary and quaternary codes and associated sphere packings, IEEE Transactions on Information Theory* 38(1992),227-246.