Primitive idempotent tables of cyclic and constacyclic codes

van Zanten, A. J.

DOI
10.1007/s10623-018-0495-0

Publication date
2018

Document Version
Final published version

Published in
Designs, Codes, and Cryptography

Designs, Codes and Cryptography (2019) 87:1199–1225
https://doi.org/10.1007/s10623-018-0495-0

Primitive idempotent tables of cyclic and constacyclic codes

A. J. van Zanten[1,2]

Received: 24 January 2018 / Revised: 5 April 2018 / Accepted: 15 May 2018 / Published online: 9 July 2018

Abstract
For any $\lambda \in GF(q)^*$ a λ-constacyclic code $C^{n,q,\lambda} := \langle g(x) \rangle$, of length n is a set of polynomials in the ring $GF(q)[x]/x^n - \lambda$, which is generated by some polynomial divisor $g(x)$ of $x^n - \lambda$. In this paper a general expression is presented for the uniquely determined idempotent generator of such a code. In particular, if $g(x) := (x^n - \lambda)/P_t^{n,q,\lambda}(x)$, where $P_t^{n,q,\lambda}(x)$ is an irreducible factor polynomial of $x^n - \lambda$, one obtains a so-called minimal or irreducible constacyclic code. The idempotent generator of a minimal code is called a primitive idempotent generating polynomial or, shortly, a primitive idempotent. It is proven that for any triple (n, q, λ) with $(n, q) = 1$ the set of primitive idempotents gives rise to an orthogonal matrix. This matrix is closely related to a table which shows some resemblance with irreducible character tables of finite groups. The cases $\lambda = 1$ (cyclic codes) and $\lambda = -1$ (negacyclic codes), which show this resemblance most clearly, are studied in more detail. All results in this paper are extensions and generalizations of those in van Zanten (Des Codes Cryptogr 75:315–334, 2015).

Keywords Constacyclic codes · Cyclic codes · Negacyclic codes · Idempotent generating polynomials · Semisimple rings · Irreducible character tables

Mathematics Subject Classification 12E05 · 12E20 · 16S34 · 20C05 · 20C15 · 20C20 · 94B15 · 94B60

1 Introduction

A λ-*constacyclic* (shortly *constacyclic*) *code* $C^{n,q,\lambda} := \langle g(x) \rangle \bmod x^n - \lambda$ of length n is generated by some polynomial divisor $g(x)$ over $GF(q)$ of $x^n - \lambda$, with $\lambda \in GF(q)^*$. So, $C^{n,q,\lambda}$ is a set of polynomials in the ring $R^{n,q,\lambda} := GF(q)[x]/x^n - \lambda$. For $\lambda = 1$ one obtains the family of *cyclic codes* which are well known [18, 19, 24]. For $\lambda = -1$ one obtains the

Communicated by I. Landjev.

✉ A. J. van Zanten
a.j.vanzanten@ewi.tudelft.nl

[1] Faculty of Mathematics and Informatics, Delft University of Technology, Delft, The Netherlands

[2] Department of Communication and Informatics, University of Tilburg, Tilburg, The Netherlands

so-called *negacyclic codes* [2, 8, 26]. For general values of λ ($\neq 0$), constacyclic codes have first been introduced in [2]. For more general information about these codes, we refer to [1, 3–5, 20, 21] and to the lists of references in these publications.

Let the decomposition of $x^n - \lambda$ into monic irreducible polynomials over $GF(q)$ be given by

$$x^n - \lambda = \prod_{t \in T^{n,q,\lambda}} P_t^{n,q,\lambda}(x), \tag{1}$$

where $T^{n,q,\lambda}$ is an index set containing the indices of all these irreducible polynomials. If $f_t(x) := (x^n - \lambda)/P_t^{n,q,\lambda}(x)$ for some fixed $t \in T^{n,q,\lambda}$, then the code $\langle f_t(x) \rangle$ is called a *minimal* or *irreducible constacyclic code*. In algebraic terms, such a code is a minimal ideal in the ring $R^{n,q,\lambda}$. The code $\langle P_t^{n,q,\lambda}(x) \rangle$ is called a *maximal constacyclic code*. An *idempotent polynomial* in $R^{n,q,\lambda}$ is a polynomial $e^{n,q,\lambda}(x) \in R^{n,q,\lambda}$ with the property that

$$e^{n,q,\lambda}(x)^2 = e^{n,q,\lambda}(x). \tag{2}$$

It will be clear that if (2) holds, then all positive powers of $e^{n,q,\lambda}(x)$ are identical. If $e^{n,q,\lambda}(x)$ generates the code C, then it is called an *idempotent generating polynomial* of C, or shortly an *idempotent generator*. One can easily prove that each constacyclic code has a uniquely determined idempotent generator (cf. [18, 19, 24]). The idempotent generators of minimal constacyclic codes are denoted by $\theta_t(x)$ and those of the maximal constacyclic codes by $\vartheta_t(x)$, $t \in T^{n,q,\lambda}$ [16, 22, 25]. The polynomials $\theta_t(x)$ are often called *primitive idempotent polynomials*, since any idempotent generator can be written as a linear combination of these polynomials for fixed values of n, q and λ. Constacyclic codes with special parameter values or constacyclic codes constructed by special methods are discussed in [9, 11, 12, 14, 15].

In the next section we shall formulate a few simple properties of (primitive) idempotent generating polynomials which are well known for cyclic codes, and which also hold for constacyclic codes. The proofs are completely similar to those for cyclic codes, and will therefore be omitted in most of the cases. Actually, all relations mentioned in Sect. 2 can be seen as special cases of properties of idempotents in the context of semi-simple algebras (cf. [6, 23, 24]).

The notation $C^{n,q,\lambda}$ stands for a λ-constacyclic code of length n over $GF(q)$, where the positive integer n, the prime power q and the parameter λ satisfy the conditions

$$(n, q) = 1, \ \lambda \in GF(q)^*. \tag{3}$$

Under these assumptions $x^n - \lambda$ has no multiple zeros, and hence the irreducible polynomials have no common zeros. Throughout the paper we shall assume that (3) holds, without stating so every time. In Sect. 2 we also present a general formula which enables us to determine the idempotent generator for any constacyclic code $C^{n,q,\lambda}$, where the three parameters n, q and λ satisfy the conditions in (3). In Sect. 3 we discuss codes $C^{n,q,\lambda}$ for fixed values of n and q and for various values of λ as subcodes of the cyclic code $C^{kn,q,1}$, where k is the multiplicative order of λ in $GF(q)$. In Sect. 4.1 the notion of *constacyclotomic coset* is introduced as a generalization of cyclotomic coset, and in Sect. 4.2 the notion of *constacyclonomial*, generalizing cyclonomials. The vector space spanned by these constacyclonomials for fixed n, q and λ is called $A^{n,q,\lambda}$. Furthermore, this vector space is equipped with a bilinear form. In Sect. 5 it is shown that with respect to this bilinear form, both the constacyclonomials and the primitive generator polynomials constitute an orthogonal basis of $A^{n,q,\lambda}$. The orthogonal transformation matrix between these two bases can be interpreted as an orthogonal table of

primitive idempotent generators. It turns out that such tables resemble, in a way, the well-known irreducible character tables of finite groups, thus generalizing similar results in [25]. Therefore, we shall speak of *primitive idempotent tables*. The most striking examples of this resemblance are obtained by taking $\lambda = 1$ (cyclic codes) or $\lambda = -1$ (negacyclic codes). Respectively in Sects. 6 and 7 these cases are discussed in more detail. Among other things, we define the notions of *r-conjugateness* for primitive idempotent generators and *blocks* of r-conjugated idempotents. As for our notation in the remaining sections, if this will not give rise to confusion we shall drop the indices n and q from the names of variables for reasons of convenience. So, we shall write $e^{\lambda}(x)$ instead of $e^{n,q,\lambda}(x)$, $P_t^{\lambda}(x)$ for $P_t^{n,q,\lambda}(x)$, etc. Only in places where the variable n takes on various values such as in Sect. 4.2, we shall use the more extended notation. In order to keep the reader aware of the dependence on n and q, we always maintain the full notation in the names of the sets these variables are taken from, like $R^{n,q,\lambda}$, $A^{n,q,\lambda}$, $S^{n,q,\lambda}$, $T^{n,q,\lambda}$, $C^{n,q,\lambda}$ and $C_t^{n,q,\lambda}$.

2 Idempotent generators

In order to formulate the announced properties, we introduce a couple of notions and corresponding notation. Firstly, we write the n zeros of $x^n - \lambda$ as $\alpha\zeta^i$, $i \in \{0, 1, \ldots, n-1\}$, where ζ is a primitive nth root of unity in some extension field of $GF(q)$ and α a fixed element of the same extension field, say in $F := GF(q)(\alpha, \zeta)$, which satisfies $\alpha^n = \lambda$ (cf. also Theorem 4). From standard theory on polynomials in $GF(q)[x]$, we know that $\alpha\zeta^i$ and $\alpha\zeta^j := (\alpha\zeta^i)^q$ are zeros of the same irreducible polynomial, for any $i \in \{0, 1, \ldots, n-1\}$. As a consequence, when having chosen a fixed element $\alpha \in F$, one can take for the index set $T^{n,q,\lambda}$ in (1) an appropriate subset of $\{0, 1, \ldots, n-1\}$. Usually, we shall take the minimal i-value for which $\alpha\zeta^i$ is a zero of the irreducible polynomial to be indexed. In case that $\lambda = 1$ we can take $\alpha = 1$, and we obtain the usual set of indices representing the cyclotomic cosets modulo n with respect to q, called the q-cyclotomic cosets modulo n.

Theorem 1 *Let $C := \langle g(x) \rangle$ be a λ -constacyclic code in $R^{n,q,\lambda}$ and let $h(x)$, defined by $g(x)h(x) = x^n - \lambda$, be its check polynomial.*

(i) *If $e^{\lambda}(x)$ is the uniquely determined idempotent generator of C , then there exist polynomials $p(x)$ and $q(x)$ such that $e^{\lambda}(x) = p(x)g(x)$ and $g(x) = q(x)e^{\lambda}(x)$ in $R^{n,q,\lambda}$.*
(ii) *$e^{\lambda}(\alpha\zeta^i) = 0$ if $g(\alpha\zeta^i) = 0$ and $e^{\lambda}(\alpha\zeta^i) = 1$ if $h(\alpha\zeta^i) = 0$ for $i \in \{0, 1, \ldots, n-1\}$.*
(iii) *If $e^{\lambda}(x)^*$ is the idempotent generator of the code $C^* := \langle h(x) \rangle$, then $e^{\lambda}(x) + e^{\lambda}(x)^* = 1$.*
(iv) *$c(x) \in C$ if and only if $e^{\lambda}(x)c(x) = c(x)$.*
(v) *If C_1 and C_2 are λ -constacyclic codes with idempotent generators $e_1^{\lambda}(x)$ and $e_2^{\lambda}(x)$, then $C_1 \cap C_2$ and $C_1 + C_2$ are also λ -constacyclic codes with idempotent generators $e_1^{\lambda}(x)e_2^{\lambda}(x)$ and $e_1^{\lambda}(x) + e_2^{\lambda}(x) - e_1^{\lambda}(x)e_2^{\lambda}(x)$, respectively.*

The proofs are completely similar to the proofs for cyclic codes which can be found e.g. in [18, 19, 24]. The same holds for the properties listed in the next theorem.

Theorem 2 *Let $\{\theta_t(x)\ t \in T^{n,q,\lambda}\}$ be the set of primitive idempotent generators of the λ -constacyclic codes generated by divisors of $x^n - \lambda$. Then one has for all $t, u \in T^{n,q,\lambda}$ the following properties*:

(i) *$\theta_t(x)\theta_u(x) = 0$ if $t \neq u$ and $\theta_t(x)^2 = \theta_t(x)$;*
(ii) *$\theta_t(\alpha\zeta^i) = 1$ if $\alpha\zeta^i$ is a zero of $P_t^{\lambda}(x)$, while $\theta_t(\alpha\zeta^i) = 0$ if $\alpha\zeta^i$ is a zero of $P_u^{\lambda}(x)$, $u \neq t$;*

(iii) $\theta_{i_1}(x) + \theta_{i_2}(x) + \cdots + \theta_{i_r}(x)$ *is the idempotent generator of the constacyclic code* $\langle f_{i_1}(x) f_{i_2}(x) \ldots f_{i_r}(x) \rangle$;

(iv) $\vartheta_t(x) = 1 - \theta_t(x)$ and $\sum_{t \in T^{n,q,\lambda}} \theta_t(x) = 1$;

(v) *If* $e^{\lambda}(x)$ *is the idempotent generator of some* λ *-constacyclic code in* $R^{n,q,\lambda}$ *, then there exist elements* $\xi_1, \xi_2, \ldots, \xi_r \in GF(q)$ *such that* $e^{\lambda}(x) = \sum_{i=1}^{r} \xi_i \theta_i(x)$.

(vi) *Let* $P_t^{\lambda}(x)$, $t \in T^{n,q,\lambda}$ *, be a monic irreducible polynomial of degree* m_t^{λ} *, then its reciprocal* $P_t^{\lambda^*}(x) := P_t^{\lambda}(0)^{-1} x^{m_t^{\lambda}} P_t^{\lambda}(1/x)$ *is a monic irreducible polynomial* $P_{t^*}^{\lambda^{-1}}(x)$, $t^* \in T^{n,q,\lambda^{-1}}$ *, such that the zeros of* $P_{t^*}^{\lambda^{-1}}(x)$ *are the inverses of the zeros of* $P_t^{\lambda}(x)$. *The corresponding primitive idempotent generator satisfies* $\theta_{t^*}(x) := \lambda x^n \theta_t(1/x)$.

Proof The proofs for (i)–(v) are straightforward and similar to the proofs for cyclic codes, i.e. for $\lambda = 1$.

(vi) That $P_{t^*}^{\lambda}(x)$ is a monic irreducible polynomial in $R^{n,q,\lambda}$ follows immediately from its definition (cf. also [17]). We know that $x^n - \lambda = q(x) P_t^{\lambda}(x)$ for some polynomial $q(x) \in R^{n,q,\lambda}$. From this equality we derive $1 - \lambda x^n = x^{n-m_t^{\lambda}} q(1/x) x^{m_t^{\lambda}} P_t^{\lambda}(1/x) = q_0(x) P_t^{\lambda^*}(x)$, with $q_o(x) \in R^{n,q,\lambda}$. Hence, $x^n - \lambda^{-1} = -\lambda^{-1} q_o(x) P_t^{\lambda^*}(x)$ and $P_{t^*}^{\lambda^{-1}}(x) := P_t^{\lambda^*}(x)$ is a divisor of $x^n - \lambda^{-1}$. Finally, $x^n \theta_t(1/x)$has value $\lambda^{-1} \cdot 1 = \lambda^{-1}$ when we substitute for x a zero of $P_{t^*}^{\lambda^{-1}}(x)$, and it has value $\lambda \cdot 0 = 0$ when substituting one of the other zeros of $x^n - \lambda^{-1}$. So, $\lambda x^n \theta_t(1/x)$ must be identical to $\theta_{t^*}(x)$. □

We shall present a slightly different proof for part (iv), right after the next theorem which provides us with a simple expression for the uniquely determined idempotent generator of a constacyclic code.

Theorem 3 (i) *If* $g(x)$ *is a divisor of* $x^n - \lambda$ *in* $R^{n,q,\lambda}$ *, with* $(n, q) = 1$ *, then the idempotent generator of the* λ *-constacyclic code* $\langle g(x) \rangle$ *is given by the polynomial* $e^{\lambda}(x) = (n\lambda)^{-1} x h'(x) g(x)$ *in* $R^{n,q,\lambda}$ *, where* $h'(x)$ *is the formal derivative of the check-polynomial* $h(x) := (x^n - \lambda)/g(x)$.

(ii) *The idempotent generator of the dual code* $\langle g(x) \rangle^*$ *is given by* $e^{\lambda}(x)^* = (n\lambda)^{-1} x g'(x) h(x)$.

Proof Because of the assumption $(n, q) = 1$ the polynomials $g(x)$ and $h(x)$ have no common zeros, and since both are monic we have $(g(x), h(x)) = 1$. Hence, there exist polynomials $a(x)$ and $b(x)$ such that $a(x)g(x) + b(x)h(x) = 1$. Multiplying by $a(x)g(x)$ yields $(a(x)g(x))^2 + a(x)b(x)g(x)h(x) = a(x)g(x)$, and therefore $(a(x)g(x))^2 = a(x)g(x) \bmod x^n - \lambda$. So, we can write $e^{\lambda}(x) = a(x)g(x)$. To determine $a(x)$, we take derivatives of both sides of the relation $g(x)h(x) = x^n - \lambda$, yielding $h'(x)g(x) + h(x)g'(x) = nx^{n-1}$. In $R^{n,q,\lambda}$ this is equivalent to $(n\lambda)^{-1} x(h'(x)g(x) + h(x)g'(x)) = 1$. Hence, $a(x) = (n\lambda)^{-1} x h'(x)$ and the relation in (i) now follows, as well as the relation in (ii) by interchanging $g(x)$ and $h(x)$. □

We remark that the expression for $e^{\lambda}(x)$ in Theorem 3 generalizes the expression for the idempotent generator of a cyclic code in [25] which on its turn was a generalization of the special case of binary cyclic codes (cf. [18, 19, 24]). As an application of Theorem 3 (i), we now present an alternative proof for Theorem 2 (iv).

Example 4 Consider the primitive idempotent polynomials $\theta_t(x)$, $t \in T^{n,q,\lambda}$, belonging to the polynomial in (1). So, $g(x) = \prod_{i \neq t} P_i^{\lambda}(x)$, $h(x) = P_t^{\lambda}(x)$, and hence $\theta_t(x) = (n\lambda)^{-1} x P_t^{\lambda}(x)' \prod_{i \neq t} P_i^{\lambda}(x)$, according to Theorem 3 (i). Applying the rule for determining

the derivative of a product of functions yields $\sum_{t\in T^{n,q,\lambda}} \theta_t(x) = (n\lambda)^{-1}\left(\prod_{t\in T^{n,q,\lambda}} P_t^{\lambda}(x)\right)' =$ $(n\lambda)^{-1}x(x^n-\lambda)' = (n\lambda)^{-1}xnx^{n-1} = 1 \mod x^n-\lambda$. □

3 Constacyclic codes $C^{n,q,\lambda}$ for various values of λ

In this section we study the relationship between the λ-constacyclic codes for different values of λ. To this end we shall need the notion of the *order* of a polynomial $p(x) \in GF(q)[x]$, i.e. the least positive integer e such that $p(x)$ is a divisor of x^e-1. A well known property is that the order of a product of polynomials which are pairwise relatively prime, is equal to the least common multiple (lcm) of the orders of its zeros (cf. [17, Theorem 3.9]). Another well known property is that the order of an irreducible polynomial $f(x) \in GF(q)[x]$, with $f(0) \neq 0$, of degree m is equal to the order of any of its zeros in the splitting field $GF(q^m)$ of $f(x)$ over $GF(q)$ (cf. [17, Theorem 3.3]).

Theorem 5 *Let n be a positive integer and q a prime power with $(n,q)=1$. Let F be the smallest extension field of $GF(q)$ such that it contains all zeros of $x^n-\lambda$, while $\lambda \in GF(q)^*$ has order k. Let furthermore e be the order of $x^n-\lambda$ in $GF(q)[x]$.*

(i) *If the n_0 $\left(:=\left|T^{n,q,\lambda}\right|\right)$ irreducible factor polynomials $P_t^{\lambda}(x)$ of $x^n-\lambda$ in $GF(q)[x]$ have order e_t, $1 \le t \le n_0$, then e is equal to the least common multiple $\langle e_1, e_2, \ldots, e_{n_0}\rangle$.*

(ii) *The order e of $x^n-\lambda$ is equal to kn, and if α is a zero of $x^n-\lambda$ of order e, then all its zeros can be written as $\alpha\zeta^i$, $0 \le i < n$, where $\zeta := \alpha^k$. Furthermore, one has $x^e-1 = \prod_{j=0}^{k-1}(x^n-\lambda^j)$.*

(iii) *If α is some zero of $x^n-\lambda$ and if there is no integer i, $0<i<n$, with $\alpha^i \in GF(q)$, then α has order kn in F. Conversely, if $\alpha^i=\mu \in GF(q)$, $0<i<n$, there is a minimal divisor d of n, $d<n$, such that the order of α is hd where h is the order of μ in $GF(q)$.*

(iv) *The order of α is equal to kn if and only if n is a divisor of hd. If n is not a divisor of hd, then α is a zero of $x^d-\mu$, which is a factor of $x^n-\lambda$.*

Proof

(i) The irreducible polynomial factors of $x^n-\lambda$ are pairwise prime to each other, since $(n,q)=1$, and hence $x^n-\lambda$ has no multiple zeros. So, the statement is an immediate consequence of [17, Theorem 3.9].

(ii) Let G be the multiplicative group consisting of the e zeros of x^e-1 in some extension field of F and let β be a generator of this group. Since $x^n-\lambda$ is a divisor of x^e-1, the group G contains n different elements β^b satisfying $\beta^{bn}=\lambda$. It follows that there are n different elements β^{b-b_0} all satisfying $\beta^{(b-b_0)n}=1$, for some fixed integer b_0, and so these elements form a subgroup of order n. Hence, n is a divisor of e. Furthermore, $\lambda^{e/n} = \left(\beta^{bn}\right)^{e/n} = \beta^{be} = 1$, and hence $e = akn$ for some positive integer a. However, since $\alpha^{kn} = \lambda^k = 1$ for any zero α of $x^n-\lambda$, we have that $e \le kn$. So, $a=1$ and $e=kn$. If we define $\zeta := \beta^k$, it follows that $\zeta^n = (\beta^{e/n})^n = 1$, and so ζ is a primitive nth root of unity, since n is minimal positive with respect to this property. Hence, all zeros of $x^n-\lambda$ can be written as β^{1+ik}, $0 \le i \le n-1$. Defining $\alpha := \beta$ yields the first equality in (ii). The second equality now follows easily by applying that $\alpha^n=\lambda$ implies

$(\alpha^j)^n = \lambda^j$ and from the fact that all zeros of the polynomials $x^n - \lambda^j, 0 \le j \le k-1$, are different.

(iii) Let the order of α in F be equal to f. Then we have $f \le kn$. We also have $f \ge n$, because of the condition on α. Hence, we can write $f = sn + t$, with $s \ge 1, 0 \le t < n$. It follows that $\alpha^{sn+t} = \lambda^s \alpha^t = 1$, and so $\alpha^t = \lambda^{-s} \in GF(q)$. Because of the condition on α, this can only be true for $t = 0$, and $\lambda^s = 1$. Therefore, $s \ge k$ and $f \ge kn$. We conclude that $f = kn$. Conversely, assume $\alpha^i \in GF(q)$ for some i with $0 < i < n$. Then we have for all integer values a and b that $\alpha^{an+bi} \in GF(q)$, in particular for those values a and b for which $an + bi = (n, j)$. So, for all i satisfying the above assumption, we have $\alpha^{(n,i)} \in GF(q)$. Let d be the greatest common divisor of these i-values, then $\alpha^d = \mu$ and d is minimal with respect to this property. Similarly to the proof of the first part it now follows, replacing n by d and k by h, that the order of α is equal to hd.
(iv) Since α^d generates a subgroup of order h in G and α^n a subgroup of order k, we have $k(h, n/d) = h$. So, $kn = hd$ if and only if $(h, n/d) = n/d$, or equivalently, if n/d is a divisor of h. The other results follow easily from (iii). □

We remark that the proof of Theorem 5 (iii) is based on the proof of Lemma 3.17 in [17] which deals with a similar property for the order of an arbitrary polynomial $f(x) \in GF(q)[x]$, $f(0) \neq 0$, of positive degree. We also notice that $(e, q) = (kn, q) = 1$, due to (3) and the fact that k is a divisor of $q - 1$, and so $x^e - 1$ has no multiple zeros. The following corollary is based on the fact that if α is a zero of $x^n - \lambda$, then α^j is a zero of $x^n - \lambda^j$ for $0 \le j \le k-1$. Together with Theorem 5 (ii) this yields the following result.

Corollary 6 *Let j be some integer with $0 \le j \le k-1$. If $H := \langle \zeta \rangle$, $\zeta := \alpha^k$, with α a zero of $x^n - \lambda$ of order kn, is the uniquely determined subgroup of $G := \langle \alpha \rangle$ of order n, then the cosets of H in G are $H_j = \alpha^j H$ and H_j consists of all n zeros $\alpha^j \zeta^i, 0 \le i \le n-1$, of the polynomial $x^n - \lambda^j$.*

Theorem 7 *Let $g(x)$ be a polynomial dividing the polynomial $x^n - \lambda$ of order $e(= kn)$. If $e_\lambda(x)$ is the idempotent generator of the λ-constacyclic code $\langle g(x) \rangle_\lambda$ in $R^{n,q,\lambda}$ and $e(x)$ the idempotent generator of the cyclic code $\langle g(x) \rangle$ in $R^{e,q}(:= R^{e,q,1})$, then $e_\lambda(x) = e(x)$ mod $x^n - \lambda$.*

Proof If $h_\lambda(x)$ and $h(x)$ denote the check polynomials of $g(x)$ in $R^{n,q,\lambda}$ and in $R^{e,q}$ respectively, we can write $(x^n - \lambda)h(x) = (x^e - 1)h_\lambda(x)$. Taking derivatives on both sides of this equality, applying Theorem 3 (i) and dividing by $x^n - \lambda$, yields the relation $kne(x) + nx^n t(x) = n\lambda t(x) e_\lambda(x) + knx^e \bmod x^e - 1$, with the polynomial $t(x) := x^e - 1/x^n - \lambda = \lambda^{-1} \sum_{i=0}^{k-1} \left(\frac{x^n}{\lambda}\right)^i$. Since $x^n - \lambda$ divides $x^e - 1$, the above equality also holds modulo $x^n - \lambda$. Substituting $x^n = \lambda$ and $x^e = 1$ then gives modulo $x^n - \lambda$ that $t(x) = k/\lambda$ and next $e_\lambda(x) = e(x)$. □

4 Generalization of cyclotomic cosets and cyclonomials

From standard results on cyclotomic cosets (cf. [17]) it is well known that the zeros of any irreducible factor of $x^n - 1$ can be written as $\zeta^t, \zeta^{tq}, \ldots, \zeta^{tq^{m_t - 1}}$ for some integer t, where ζ is a primitive n^{th} root of unity in some extension field of $GF(q)$, while m_t is the degree of that polynomial. So, by taking these integers t as elements of the index set $T^{n,q}(:= T^{n,q,1})$,

we establish a one-one correspondence between the irreducible polynomials $P_t^1(x)$ and the q-cyclotomic cosets mod n

$$C_t^{n,q} = (t, tq, \ldots, tq^{m_t-1}), \tag{4}$$

where m_t is the smallest positive integer which satisfies $t(q^{m_t} - 1) = 0 \bmod n$ (cf. also [25]). In the next subsection we shall generalize this correspondence for those irreducible polynomials which play a role in constacyclotomic cases, i.e. when they are divisors of $x^n - \lambda$, $\lambda \neq 1$.

4.1 Constacyclotomic cosets $C_t^{n,q,\lambda}$

We introduce the integer $l := (q-1)/k$, and we define ordered subsets of $\{0, 1, \ldots, n-1\}$ as follows.

Definition 7 For any triple of parameters n, q and λ satisfying condition (3), the set

$$C_t^{n,q,\lambda} := \left(c_0(=t), c_1, \ldots, c_{m_t^\lambda - 1}\right), \tag{5}$$

$$c_{i+1} = c_i q + l \mod n, \quad 0 \leq i < m_t^\lambda - 1, \tag{6}$$

where m_t^λ is the smallest positive integer satisfying $c_{m_t^\lambda - 1} q + l = c_0$, is called a ($q$-) constacyclotomic coset modulo n.

Next, we shall derive a number of properties of constacyclotomic cosets which we shall need in the remaining sections. In the formulation of these properties we shall use the notation $aC_t^{n,q,\lambda} + b := aC_t^{n,q,\lambda} + (b, b, \ldots, b)$, which stands for $\left(ac_0 + b, ac_1 + b, \ldots, ac_{m_t^\lambda - 1} + b\right)$, where all integers $ac_i + b$ must be computed mod n.

Theorem 8 *Let q be a prime power, n an integer with $(n, q) = 1$ and let $\lambda \in GF(q)^*$ have order k. Let furthermore α be a zero of $x^n - \lambda \in GF(q)[x]$ of order kn and let $\zeta := \alpha^k$.*

(i) *The zeros of some irreducible polynomial $P_t^\lambda(x)$ over $GF(q)$ contained in $x^n - \lambda$ can be written as $\alpha\zeta^c$ where c runs through the set $C_t^{n,q,\lambda}$, while m_t^λ is equal to the degree of that polynomial.*

(ii) *The integers c_i in (5) satisfy $c_i = tq^i + (q^i - 1)/k \bmod n$, $0 \leq i \leq m_t^\lambda - 1$.*

(iii) *The size m_t^λ of $C_t^{n,q,\lambda}$ is equal to the smallest positive integer which satisfies the relation $(kt + 1)(q^{m_t^\lambda} - 1) = 0 \bmod kn$.*

(iv) *For any integer $b \geq 0$ and for all i, $0 \leq i \leq n - 1$, one has $kc_{i+b} + 1 = q^b(kc_i + 1) \bmod kn$.*

(v) *Modulo n one has $C_0^{n,q,\lambda} = k^{-1}(0, q-1, q^2-1, \ldots)$, $C_0^{n,q,\lambda} + t(1, q, q^2, \ldots) = m_0^\lambda / m_t^\lambda \times C_t^{n,q,\lambda}$ and $kC_t^{n,q,\lambda} + 1 = m_t^\lambda / m_{kt+1} \times C_{kt+1}^{n,q}$, where the notation $a \times C^{n,q,\lambda}$ or $a \times C^{n,q}$ means that each integer of the relevant coset occurs a times in the multiset at the left hand side of the equality.*

Proof

(i) Let α be a zero of the irreducible factor $P^\lambda(x)$ of $x^n - \lambda$ of degree m_0. Then we can write $P^\lambda(x) = (x - \alpha)(x - \alpha^q) \ldots \left(x - \alpha^{q^{m_0 - 1}}\right)$. From Theorem 5 we know that for all relevant i, we can write $\alpha^{q^i} = \alpha\zeta^{c_i}$ for some integer $c_i \in \{0, 1, \ldots, n-1\}$. Hence, $\alpha^{q^{i+1}} = \alpha^q \zeta^{qc_i} = \alpha\alpha^{q-1}\zeta^{qc_i} = \alpha\zeta^{l+qc_i}$ by using $q - 1 = kl$, and we obtain

$c_{i+1} = l + qc_i$ for $0 \le i \le m_0 - 2$. Furthermore, since $\alpha^{q^{m_0}} = \alpha$, we also have $l + qc_{m_0-1} = c_0$. So, the relations (4) and (5) with $t = t_0 = 0$ define $P^{\lambda}_{t_0}(x) := P^{\lambda}(x)$. Next, let t_1 be the least integer in $\{0, 1, \ldots, n-1\} \backslash C_0^{n,q,\lambda}$ and define $P^{\lambda}_{t_1}(x)$ of degree m_{t_1} as the irreducible factor of $x^n - \lambda$ which has $\alpha\zeta^{t_1}$ as zero. Similarly as before it appears that this polynomial is defined by (4) and (5) with $t = t_1$. Proceeding in this way until all integers of $\{0, 1, \ldots, n-1\}$ have been dealt with, we end up with an index set $T^{n,q,\lambda} = \{t_0(= 0), t_1, \ldots\} \subset \{0, 1, \ldots, n-1\}$, such that any irreducible polynomial contained in $x^n - \lambda$ can be indexed by some integer in $T^{n,q,\lambda}$ and vice versa.

(ii) This relation can easily be proved by incomplete induction on i, $0 \le i \le m^{\lambda}_t - 1$.

(iii) From (ii) we have that $c_{m^{\lambda}_t} = l + tq^{m^{\lambda}_t} + l\left(q^{m^{\lambda}_t - 1} + \cdots + q\right) = tq^{m^{\lambda}_t} + \left(q^{m^{\lambda}_t} - 1\right)/k$. By requiring $c_{m^{\lambda}_t} = t$, we obtain the relation in (iii).

(iv) By iteration we get $c_{i+b} = l + lq + \cdots + lq^{b-1} + q^b c_i = (q^b - 1)/k + q^b c_i \bmod n$. Hence, $kc_{i+b} + 1 = q^b + kq^b c_i \bmod kn$.

(v) These relations follow immediately from (ii). □

Remark 9 We remark that putting $\lambda = 1$, and hence $k = 1$, $l = q - 1$ in (5) and (6), does not provide us with the cyclotomic cosets (4). In terms of the integers of $C^{n,q,1}_t = (c_0(= t), c_1, \ldots, c_{m_t-1})$, the zeros of the corresponding irreducible polynomial can be written as $\alpha\zeta^{c_0}$, $\alpha\zeta^{c_i}$, ..., $\alpha\zeta^{c_{m_t-1}}$, with $\alpha = \zeta$ as primitive n^{th} root of unity. We call this the α, ζ*-representation.* On the other hand, the integers of (3) give these zeros in the form ζ^t, $\zeta^{tq}, \ldots \zeta^{tq^{m_t-1}}$, the ζ*-representation.* Application of Theorem 8 (v) with $\lambda = 1$ and $k = 1$, shows that the two types of cosets are related by

$$C^{n,q,1}_{t-1} + 1 = C^{n,q}_t. \tag{7}$$

This relation implies that $m^1_{t-1} = m_t$ for all $t \in T^{n,q}$. In the next we keep calling $C^{n,q,1}_t$, $t \in T^{n,q,1}$, a constacyclotomic coset and $C^{n,q}_t$, $t \in T^{n,q}$, a cyclotomic coset. Furthermore, as was already remarked in Theorem 8 (v), the set $kC^{n,q,\lambda}_t + 1$ is, strictly speaking, an ordered multiset such that any integer it contains occurs the same number of times. This is due to the fact that all operations on the integers have to be carried out modulo n. Finally, we emphasize that the third relation in Theorem 8 (v) does not always define a one-one mapping from the set of constacyclotomic cosets to the set of cyclotomic cosets for $\lambda \ne 1$. E.g. $4C^{14,5,2}_0 + 1 = (1, 5, 11, 13, 9, 3)$ and $4C^{14,5,2}_4 + 1 = (3, 1, 5, 11, 13, 9)$.

Next, we present a theorem which shows how to determine constacyclotomic cosets $C^{n,q,\mu}_t$ for various $\mu \in GF(q)^*$ in a way, other than by the recurrence relation (6) or by the rules of Theorem 8 (ii). To this end we shall need the irreducible polynomial which has as zeros the s-powers of the zeros of $P^{\lambda}_t(x)$ (cf. Theorem 8), for $t \in T^{n,q,\lambda}$ and for $s \ge 0$. This polynomial is an irreducible factor of $x^n - \lambda^s$, denoted by $P^{\lambda^s}_{t_s}(x)$.

Theorem 10 *Under the conditions of Theorem* 8, *the following relations hold.*

(i) *In* $GF(q)[x]$ *one has the factorization* $x^{kn} - 1 = \prod_{s=1}^{k} (x^n - \lambda^s)$.

(ii) *The zeros of* $x^n - \lambda^s$, $1 \le s \le k$, *can be written as* α^{ki+s} *or, equivalently, as* $\alpha^s\zeta^i$, $0 \le i \le n - 1$.

(iii) *The integers of the constacyclotomic coset* $C^{n,q,\lambda^s}_t = (c_0(= t), c_1, \ldots, c^{m-1}_t)$, $m := m^{\lambda^s}_t$, *satisfy the recurrence relation* $kc_{i+1} + s = (kc_i + s)q \bmod kn$, $0 \le i \le m - 1$.

(iv) *For any* s, $1 \le s \le k$, *the mapping of* $\{0, 1, \ldots, n-1\}$ *into* $\{0, 1, \ldots, kn\}$ *defined by* $i \to ki + s$ *yields a one-one correspondence between the constacyclotomic cosets* C_t^{n,q,λ^s}, $t \in T^{n,q,\lambda^s}$, *and the cyclotomic cosets* $C_{kt+s}^{kn,q}$, $kt + s \in T^{kn,q}$. *For* $s = 0$ *the mapping yields a one-one correspondence between the cyclotomic cosets* $C_t^{n,q}$, $t \in T^{n,q}$, *and the cyclotomic cosets* $C_{kt}^{kn,q}$, $kt \in T^{kn,q}$.

(v) *For any* $s \ge 0$ *the* s*-powers of the zeros* $\alpha\zeta^i$, $i \in C_t^{n,q,\lambda}$, *of the irreducible polynomial* $P_t^{\lambda}(x)$, $t \in T^{n,q,\lambda}$, *are zeros of the irreducible polynomial* $P_{t_s}^{\lambda^s}(x)$, *where* $t_s = (k, s)t$ *is an index in the* α', ζ' *-representation with* $\alpha' = \alpha^s$ *and* $\zeta' = \zeta^{s/(k,s)}$. *Each zero of* $P_{t_s}^{\lambda^s}(x)$ *corresponds to* $m_t^{\lambda}/m_{t_s}^{\lambda^s}$ *zeros of* $P_t^{\lambda}(x)$.

Proof

(i) The definition of the order of a polynomial implies that $x^n - \lambda \mid x^{kn} - 1$. So all zeros of $x^n - \lambda$ lie in an extension field F of $GF(q)$. For any s, $1 \le s \le k$, we have that the order of λ^s is a divisor of k, and so the order of $x^n - \lambda^s$ divides kn as well. Hence, all kn zeros of these polynomials are in F. Now, $(n, q) = 1$, and since $k \mid q - 1$ we also have $(kn, q) = 1$, which implies that the polynomials have no zeros in common. This proves the factorization.

(ii) This follows immediately from Theorem 8 (i) and from the relation $(\alpha^s)^n = \lambda^s$.

(iii) Let $\alpha^s\zeta^{c_0}$, $\alpha^s\zeta^{c_1}$, $\ldots$, $\alpha^s\zeta^{c_{m-1}}$ be the zeros of the irreducible polynomial $P_t^{\lambda^s}(x)$ of degree m. Then we can write $(\alpha^s\zeta^{c_0})^{q^i} = \alpha^s\zeta^{c_i}$, $0 \le i \le m-1$. So, $(\alpha^s\zeta^{c_0})^{q^{i+1}} = (\alpha^s)^q\zeta^{qc_i} = \alpha^{sq}\alpha^{kqc_i} = \alpha^{(kc_i+s)q}$. On the other hand, $(\alpha^s\zeta^{c_0})^{q^{i+1}} = \alpha^s\zeta^{c_{i+1}} = \alpha^{kc_{i+1}+s}$, and so $kc_{i+1} + s = (kc_i + s)q \bmod kn$.

(iv) Let $C_a^{kn,q}$ be some cyclotomic coset. Since $0 \le a \le kn - 1$, there is precisely one way to write $a = kt + s$, for any s with $1 \le s \le k$. It follows that $0 \le t \le n - 1$, and so there is precisely one constacyclotomic coset C_t^{n,q,λ^s} which is mapped to $C_a^{kn,q}$. If $s = 0$ the zeros of $x^{kn} - 1$ are written as α^{kt}, and hence the zeros of $x^n - \lambda^0 = x^n - 1$ as α^t, $0 \le t \le n - 1$. This proves the second statement in (iv) (cf. also Remark 9).

(v) If $\alpha\zeta^i$ is a zero of $x^n - \lambda$, then $\alpha^s\zeta^{is}$ is a zero of $x^n - \lambda^s$. Let $\alpha\zeta^i$ be a zero of $P_t^{\lambda}(x)$, then $\alpha^s\zeta^{is}$ is a zero of some irreducible polynomial $P_{t_s}^{\lambda^s}(x)$, and this polynomial is the same for all $i \in C_t^{n,q,\lambda}$. We put $\alpha' := \alpha^s$ and $\zeta' := \alpha'^{k/(k,s)}$, where $k/(k, s)$ is the order of λ^s in $GF(q)$, and so $\zeta' = \alpha^{sk/(k,s)} = \zeta^{s/(k,s)}$. It follows that the zeros of $P_{t_s}^{\lambda^s}(x)$ can be written as $\alpha'\zeta'^j$, $j \in C_{t_s}^{n,q,\lambda^s}$, with $t_s = (k, s)t$. Each integer in $C_{t_s}^{n,q,\lambda^s}$ corresponds $m_t^{\lambda}/m_{t_s}^{\lambda^s}$ times to some integer in $C_t^{n,q,\lambda}$. □

Example 11 Take $n = 8$, $q = 5$ and $\lambda = 2$. It follows that $k := \mathrm{ord}_5(2) = 4$. Since $x^8 - 2$ does not divide $x^{16} - 1$, its order is $kn = 32$. We have the following factorization

$$x^{32} - 1 = \prod_{s=0}^{k-1} (x^8 - \lambda^s) = (x^8 - 2)(x^8 - 4)(x^8 - 3)(x^8 - 1).$$

The 5-cyclotomic cosets modulo 32 are $C_0^{32,5} = (0)$, $C_1^{32,5} = (1, 5, 25, 29, 17, 21, 9, 13)$, $C_2^{32,5} = (2, 10, 18, 26)$, $C_3^{32,5} = (3, 15, 11, 23, 19, 31, 27, 7)$, $C_4^{32,5} = (4, 20)$, $C_8^{32,5} = (8)$, $C_{16}^{32,5} = (16)$, $C_{12}^{32,5} = (12, 28)$ and $C_{24}^{32,5} = (24)$.

The factorization of the polynomials $x^8 - \lambda^s$, $s = 0$ and $s = 2$, into irreducible polynomials over $GF(5)$ is respectively $x^8 - 1 = (x + 1)(x - 1)(x + 2)(x - 2)(x^2 + 2)(x^2 - 2)$ and $x^8 - 4 = (x^4 + 2)(x^4 - 2)$, while $x^8 - 2$ and $x^8 - 3$ are irreducible themselves. Only $C_1^{32,5}$ contains integers equal to $1 (= s)$ modulo $4 (= k)$. So, there is only one constacyclotomic coset

in the case $s = 1$. Subtracting 1 from the integers in $C_1^{32,5}$ and next dividing the results by 4, provides us with $C_0^{8,5,2} = (0, 1, 6, 7, 4, 5, 2, 3)$ (cf. Theorem 10 (iv)). Similarly, for $s = 2$, we obtain $C_0^{8,5,4} = (0, 2, 4, 6)$ and $C_1^{8,5,4} = (1, 7, 5, 3)$ from $C_2^{32,5}$ and $C_6^{32,5}$, respectively. In the case $s = 3$, the cyclotomic coset $C_3^{32,5}$ delivers $C_0^{8,5,3} = (0, 3, 2, 5, 4, 7, 6, 1)$. For $s = 4$ we obtain from the cyclotomic cosets $C_i^{32,5}$, $i \in \{0, 4, 8, 12, 16, 24\}$, the constacyclotomic cosets $C_7^{8,5,1} = (7)$, $C_0^{8,5,1} = (0, 4)$, $C_1^{8,5,1} = (1)$, $C_2^{8,5,1} = (2, 6)$, $C_3^{8,5,1} = (3)$ and $C_5^{8,5,1} = (5)$. Finally, for $s = 0$ we find the cyclotomic cosets $C_0^{8,5} = (0)$, $C_1^{8,5} = (1, 5)$, $C_2^{8,5} = (2)$, $C_3^{8,5} = (3, 7)$, $C_4^{8,5} = (4)$ and $C_6^{8,5} = (6)$ from $C_0^{32,5}$, $C_4^{32,5}$, $C_8^{32,5}$, $C_{12}^{32,5}$, $C_{16}^{32,5}$ and $C_{24}^{32,5}$. The cosets in the cases $s = 4$ and $s = 0$ are related by (7). To illustrate Theorem 10 (v), we take the irreducible polynomial $P_0^{8,5,2}(x) = x^8 - 2$. Let α be one of its zeros of order 32. Then the complete set of zeros can be written as $\alpha\zeta^i$, $i \in C_0^{8,5,2}$, with $\zeta = \alpha^k = \alpha^4$. The 2-powers of these zeros are α^2, $\alpha^2\zeta^2$, $\alpha^2\zeta^4$ and $\alpha^2\zeta^6$, and each of them occurs twice. These 2-powers are zeros of $P_{(4,2),0}^{2^2}(x) = P_0^4(x) = x^4 - 2$, since the zeros of that polynomial are determined by $C_0^{8,5,4} = (0, 2, 4, 6)$. To see this one has to apply relation (6) with $l' = (q - 1)/k' = 4/2 = 2$. □

Theorem 12 (i) *Let r be a fixed integer with $(r, n) = 1$. Let a satisfy $0 \le a < n$ and $ka - r + 1 = 0$ mod $n/(l, n)$. Then $C_{rt+a}^{n,q,\lambda} = rC_t^{n,q,\lambda} + (a, a, \ldots)$ with $m_{rt+a} = m_t$, and the mapping $t \to rt + a$ mod n of $[0, n - 1]$ onto itself induces a permutation of order at most (l, n) on the set $\left\{ C_t^{n,q,\lambda} \,\middle|\, t \in T^{n,q,\lambda} \right\}$.*

(ii) *If $a = n/(l, n)$, then $C_{t+a}^{n,q,\lambda} = C_t^{n,q,\lambda} + (a, a, \ldots)$, and the mapping $t \to t + a$ mod n defines a permutation on $\{C_t^{n,q,\lambda} | t \in T^{n,q,\lambda}\}$ of order at most (l, n).*

(iii) *If a satisfies $ka + 2 = 0$ mod $n/(l, n)$, then $C_{-t+a}^{n,q,\lambda} = -C_t^{n,q,\lambda} + (a, a, \ldots)$, and the mapping $t \to -t + a$ mod n defines a permutation on the set $\left\{ C_t^{n,q,\lambda} \,\middle|\, t \in T^{n,q,\lambda} \right\}$ of order at most 2.*

Proof (i) We know from (6) that the elements of $C_t^{n,q,\lambda}$ satisfy $c_{i+1} = qc_i + l$ mod n for $0 \le i \le m_t^\lambda - 1$. Now, we define $d_i := rc_i + a$ mod n. If we require that the elements of $C_t^{n,q,\lambda}$ keep their mutual order under the mapping on C_{rt+a}^λ, we must have that $d_{i+1} = rc_{i+1} + a$ mod n. Consequently, $d_{i+1} - qd_i - l = rc_{i+1} + a - rqc_i - aq - l = (r - 1)l - a(q - 1) = 0$ mod n, and the condition on a follows by applying $q - 1 = kl$. Since $(r, n) = 1$, multiplying the integers c_i of $C_t^{n,q,\lambda}$ by r does not alter the size of the coset, and neither does adding the same integer a to all rc_i mod n.
(ii) and (iii) follow immediately from (i) by substituting respectively $r = 1$ and $r = -1$. □

We emphasize that the conditions on r are sufficient but not necessary for the properties mentioned in Theorem 12. As the proof in (i) shows, they are necessary as well if one requires that the mutual order of the integers in $C_t^{n,q,\lambda}$ is not to be changed by the mapping. An example is provided by the constacyclotomic cosets $C_0^{12,7,2} = (0, 2, 4, 6, 8, 10)$, $C_1^{12,7,2} = (1, 9, 5)$ and $C_3^{12,7,2} = (3, 11, 7)$, with $k = 3$ and $l = 2$. The equation $3a + 2 = 0$ mod 6 has no solutions, but the mapping $t \to -t + 2$ defines a permutation of order 2 on the set of the three constacyclotomic cosets, while it reverses the order of the integers. As preparation for Sect. 6 and 7, we notice that for $\lambda = 1$ and for $\lambda = -1$ an integer a as mentioned in Theorem 12 (iii) exists. In the cyclic case of $\lambda = 1$, we have $k = 1$ and hence $a = -2$ is a solution of the equation in (iii). So, the mapping $t \to -t - 2$ mod n yields a permutation of order 1 or 2 on the

set $\left\{ C_t^{n,q,1} \,\middle|\, t \in T^{n,q,1} \right\}$. By applying (7), one can see that this is equivalent to a permutation on the set $\left\{ C_t^{n,q} \,\middle|\, t \in T^{n,q} \right\}$ induced by $t \to n-t$. In the negacyclic case of $\lambda = -1$, we have $k = 2$ which provides us with $a = -1$ and the mapping $t \to n-t-1$ which acts similarly on $\left\{ C_t^{n,q,-1} \,\middle|\, t \in T^{n,q,-1} \right\}$. We define $C_{t^*}^{n,q,1} := C_{n-t-2}^{n,q,1}$ as the *conjugated constacyclotomic coset* of $C_t^{n,q,1}$, and equivalently $C_{t^*}^{n,q} := C_{n-t}^{n,q}$ as the *conjugated cyclotomic coset* of $C_t^{n,q}$. Similarly, $C_{t^*}^{n,q,-1} := C_{n-t-1}^{n,q,-1}$ is the *conjugated constacyclotomic coset* of $C_t^{n,q,-1}$.

4.2 Constacyclonomials $c_s^{n,q,\lambda}(x)$

A second notion in the theory of cyclic codes that we shall generalize is that of *cyclonomic polynomial* or *cyclonomial* (cf. e.g. [25]). To each cyclotomic coset $C_s^{n,q}$ of size m_s there corresponds a cyclonomial

$$c_s^{n,q}(x) := x^s + x^{sq} + \cdots + x^{sq^{m_s-1}} \mod x^n - 1. \tag{8}$$

Clearly, such a polynomial, shortly written as $c_s(x)$, (cf. Sect. 1) has the property

$$c_s(x)^q = c_s(x) \mod x^n - 1. \tag{9}$$

In the following definition is s an integer of $\{0, 1, \ldots, n-1\}$, and λ an arbitrary element of $GF(q)^*$.

Definition 13 The polynomial $c_s^\lambda(x) := x^s + x^{sq} + \cdots + x^{sq^{m_s^\lambda - 1}} \bmod x^n - \lambda$ in $R^{n,q,\lambda}$ is called a monic constacyclonomial of size m_s^λ, if it is not the zero polynomial and if m_s^λ is the smallest positive integer such that $\left(x^{sq^{m_s^\lambda - 1}}\right)^q = x^s \bmod x^n - \lambda$.

Since $\beta^q = \beta$, for any $\beta \in GF(q)^*$, we could call any polynomial $\beta c_s^\lambda(x)$ with $c_s^\lambda(x)$ satisfying the equality in Definition 13, a constacyclonomial. However, we shall reserve this term for *monic* polynomials. For $\lambda = 1$ we obtain the usual cyclonomials. We identify these two types of cyclonomials by writing $c_s^1(x) \equiv c_s(x)$. It will be obvious that if $c_s^\lambda(x)$ contains a term βx^t, $\beta \in GF(q)^*$, then $c_t^\lambda(x) = \beta^{-1} c_s^\lambda(x)$, and so $c_t^\lambda(x)$ and $c_s^\lambda(x)$ are linearly dependent polynomials. For fixed values of n and q, we shall use the notation $S^{n,q,\lambda}$ for a maximal set of indices of independent constacyclonomials. Usually, we take the lowest exponent of the x-powers as index of a constacyclonomial, similarly as in the case of constacyclotomic cosets, but actually one can take any of its exponents because of the above mentioned dependency. Let $s \in S^{n,q,\lambda}$ and assume that $c_s^\lambda(x)$ does not contain a term βx^{n-s}. Then it follows easily from Definition 13 that $c_{n-s}^\lambda(x)$ is a different constacyclonomial of the same size. The monic constacyclonomials $c_s^\lambda(x)$ and $c_{n-s}^\lambda(x)$ are called a pair of *conjugated constacyclonomials*. If $c_s^\lambda(x)$ does contain such a term βx^{n-s}, it is called a *self conjugated constacyclonomial*. If $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$, is not self conjugated, we assume that $n - s$ is also in $S^{n,q,\lambda}$, even if it is not the lowest exponent in the relevant polynomial.

Definition 14 The conjugate $c_s^{\lambda *}(x)$ of the constacyclonomial $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$, is defined as $c_s^{\lambda *}(x) = c_{n-s}^\lambda(x)$ if $c_s^\lambda(x)$ is not self conjugated, while $c_s^{\lambda *}(x) = c_s^\lambda(x)$ otherwise.

From the condition prior to its definition, it follows that $c_s^{\lambda *}(x)$ is a (monic) constacyclonomial for all $s \in S^{n,q,\lambda}$. Next, we define the following subset of $R^{n,q,\lambda}$ spanned by the constacyclonomials with fixed values for n, q and λ

$$A^{n,q,\lambda} := \left\{ \sum_{s \in S^{n,q,\lambda}} \alpha_s c_s^{\lambda}(x) | \alpha_s \in GF(q) \right\}. \tag{10}$$

This set $A^{n,q,\lambda}$ and its elements have the following simple properties.

Theorem 15 *(i) The polynomial $c_s^{\lambda}(x)$is a constacyclonomial of size m_s^{λ} if and only if it is not the zero polynomial and if m_s^{λ} is the smallest positive integer satisfying $s(q^{m_s^{\lambda}} - 1) = 0$ mod kn.*

(ii) Any polynomial $p(x)$ of $A^{n,q,\lambda}$ satisfies $p(x)^q = p(x)$.

(iii) Let m be the smallest positive integer such that $x^{sq^m} = \beta x^s$ mod $x^n - \lambda$ for some $\beta \in GF(q)^*$. Then the polynomial $p(x) = x^s + x^{sq} + \cdots + x^{sq^{lm-1}}$, $l := ord_q(\beta)$, is the constacyclonomial $c_s^{\lambda}(x)$ of size $m_s = m$ for $\beta = 1$, whereas $p(x)$is the zeropolynomial for $\beta \neq 1$.

(iv) A constacyclonomial has no proper subpolynomial which is also a constacyclonomial.

(v) If all nonzero coefficients of $c_s^{\lambda}(x)$ are changed into 1, one obtains the cyclonomial $c_s(x)$.

(vi) By reduction modulo $x^n - \lambda$ of the cyclonomial $c_s^{e,q}(x)$, $e = kn$, one obtains either a constacyclonomial $c_{s'}^{\lambda}(x)$, $s' = s$ mod n, with $m_{s'}^{\lambda} = m_s$, or one obtains the zeropolynomial.

(vii) If a constacyclonomial $c_s^{\lambda}(x)$ is self conjugated, then either $m_s = 1$ and $s \in \{0, n/2\}$, or m_s is even and $s(q^{m_s/2} + 1) = 0$ mod n.

Proof (i) If the condition in Definition 13 holds we have that $x^{s(q^{m_s^{\lambda}} - 1)} = 1 \bmod x^n - \lambda$. When writing $s(q^{m_s^{\lambda}} - 1) = an + b$, with $a \geq 0$, $0 \leq b < n$, it follows that $x^{an+b} = \lambda^a x^b = 1$. Hence, $k \mid a$ and $b = 0$. So, $kn \mid s(q^{m_s^{\lambda}} - 1) = 0$. Conversely, if $s(q^{m_s^{\lambda}} - 1) = 0 \bmod kn$, then $x^{s(q^{m_s^{\lambda}} - 1)} = x^{ckn} = \lambda^{ck} = 1$.

(ii) This statement follows immediately from Definition 13.

(iii) From the given condition it follows that $x^{sq^{jm}} = \beta^j x^s$, for $0 \leq j \leq l - 1$. If $\beta = 1$, it follows from Definition 13 that $p(x) = c_s^{\lambda}(x)$ and that $m_s = m$. If $\beta \neq 1$ the resulting coefficient of x^s is equal to $1 + \beta + \beta^2 + \cdots + \beta^{l-1} = 1 - \beta^l / 1 - \beta = 0$. Thus $p(x)$ is the zeropolynomial.

(iv) If we define a subpolynomial of a polynomial $p(x)$ as a polynomial not equal to the zero polynomial or to $p(x)$ itself and such that all its terms are also terms of $p(x)$, then the statement is an immediate consequence of Definition 13.

(v) The first term of both polynomials $c_s^{\lambda}(x)$ and $c_s(x)$ is x^s. Each term of $c_s^{n,q,\lambda}(x)$ is obtained from the previous one $a_i x^{c_i}$ by changing it into $a_i \lambda^{d_i} x^{c_{i+1}}$ where $d_i = [qc_i/n]$, while $x^{c_{i+1}}$ is the next term in $c_s^{n,q}(x)$. The statement now follows immediately.

(vi) It is clear that $x^s \bmod x^n - \lambda$ is equal to $\alpha x^{s'}$, with $s' = s \bmod n$, for some $\alpha \in GF(q)$. Furthermore, it follows from the definition of $c_s^{e,q}(x)$ that every term in $c_s^{e,q}(x) \bmod x^n - \lambda$ is equal to the q^{th} power of its predecessor and that $\alpha x^{s'} = x^{sq^{m_s}} \bmod x^n - \lambda$, though m_s need not be the smallest integer with this property. The result now follows

from Definition 13 and part (iii). (vii) If $c_s^\lambda(x) = c_{n-s}^\lambda(x)$, then also $c_s(x) = c_{n-s}(x)$ by (v), and so the cyclotomic cosets $C_s^{n,q}$ and $C_{n-s}^{n,q}$ are identical. Hence, sq^i and $(n-s)q^i$ are both in $C_s^{n,q}$ for all relevant values of i. So, the elements of $C_s^{n,q}$ occur in pairs unless $s = n - s \bmod n$. It follows that either $s = 0$ or $s = n/2$ and so $m_s = 1$, or $sq^j = n - s \bmod n$ for some minimal integer $j > 0$. Hence, $s(q^j + 1) = 0 \bmod n$, and $m_s = 2j$. The only-if-part of the statement is obvious. □

We remark that as a consequence of Theorem 15 (v) the number of constacyclonomials is at most equal to the number of cyclonomials $c_s(x)$, for fixed values of $c_s^\lambda(x)n$, q and λ. It appears that for $\lambda \neq 1$ the first number is the smaller one in many cases.

4.3 A bilinear form in $R^{n,q,\lambda}$

In this subsection we present a number of properties of constacyclonomials which they share with cyclonomials. To this end we introduce a bilinear form $(,)_\lambda$ in $R^{n,q,\lambda}$, while a polynomial $p(x)$ occasionally will be denoted by p in this context.

Definition 16 For every pair of elements $p(x)$ and $q(x)$ of $R^{n,q,\lambda}$ a bilinear form

$$(p, q)_\lambda := \sum_{i=0}^{n-1} p(\alpha\zeta^i)q(\alpha\zeta^i), \tag{11}$$

is defined, where α is a zero of $x^n - \lambda$ of order kn and ζ a primitive nth root of unity.

One can easily verify that this definition really yields a bilinear form in $R^{n,q,\lambda}$ with values which do not depend on the choice of α and ζ. In the next theorem the irreducible polynomials $P_t^\lambda(x)$ introduced in Eq. (1) will play a role. We know that the degree of $P_t^\lambda(x)$, $t \in T^{n,q,\lambda}$, is equal to m_t^λ being the size of the constacyclotomic coset $C_t^{n,q,\lambda}$. The coefficient of its one but highest power $x^{m_t^\lambda - 1}$ is denoted by $p_t^{n,q,\lambda}$ or shortly by p_t^λ (remember the conventions mentioned in Sect. 1). Furthermore, we remind the reader of the fact that the size of the constacyclonomial $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$, and also of the cyclotomic coset $C_s^{n,q}$ is equal to m_s. In the next theorem and its proof we shall show that the set $A^{n,q,\lambda}$ of polynomials (10) is an algebra and that the constacyclonomials $c_s^\lambda(x)$ constitute an orthogonal basis of $A^{n,q,\lambda}$ for fixed values of n, q and λ.

Theorem 17 (Orthogonal basis of constacyclonomials) *Let α be a zero of $x^n - \lambda$ of order kn, where k is the order of λ in $GF(q)$, and let $\zeta := \alpha^k$.*

(i) *The set $A^{n,q,\lambda}$ is an algebra over $GF(q)$ with basis $\left\{ c_s^\lambda(x) \,\middle|\, s \in S^{n,q,\lambda} \right\}$, and it consists of all polynomials $p(x) \in R^{n,q,\lambda}$ which satisfy the relation $p(x)^q = p(x)$.*

(ii) *For any $s \in S^{n,q,\lambda} \backslash \{0\}$, and for any j one has $\sum_{i=0}^{n-1} c_s^\lambda(\alpha^j\zeta^i) = 0$, while $\sum_{i=0}^{n-1} c_0^\lambda(\alpha^j\zeta^i) = n$.*

(iii) *With respect to the bilinear form (11), the constacyclonomials $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$, form an orthogonal basis of $A^{n,q,\lambda}$, such that for any pair $j, k \in S^{n,q,\lambda}$ one has $(c_j^{\lambda^*}, c_k^\lambda)_\lambda = nm_j\lambda^{a_j}\delta_{j,k}$, with $a_j = j(q^{\lceil m_j/2 \rceil} + 1)/n$ if $c_j^\lambda(x)$ is self conjugated, while $a_j = 1$ if $c_j^\lambda(x)$ is not self conjugated.*

Proof (i) By definition $A^{n,q,\lambda}$ is spanned by the constacyclonomials $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$. All polynomials $p(x) \in A^{n,q,\lambda}$ satisfy $p(x)^q = p(x)$ and $A^{n,q,\lambda}$ is a vector space. To see this in detail one should apply the property $(\beta p_1(x) + \gamma p_2(x))^q = \beta p_1(x)^q + \gamma p_2(x)^q$

for all $\beta, \gamma \in GF(q)$. An exhaustive construction of constacyclonomials by applying Definition 13 for fixed values of n, q and λ, shows that together these polynomials contain any power x^i, $0 \le i \le n-1$, at most once. So, they are independent and they constitute a basis of $A^{n,q,\lambda}$. On the other hand, let $p(x) \in R^{n,q,\lambda}$ be a polynomial such that $p(x)^q = p(x)$, and let βx^s be one of its terms. It follows from the exhaustive construction that there is precisely one constacyclonomial which contains the x-power x^s. By multiplying with an appropriate factor and adjusting its label, we may denote this polynomial by $c_s^\lambda(x)$. Now, $p_1(x) := p(x) - \beta c_s^{n,q,\lambda}(x)$ also satisfies $p_1(x)^q = p_1(x)$, and so we can continue this process, leading to $p_2(x) := p(x) - \beta c_s^{n,q,\lambda}(x) - \gamma c_u^{n,q,\lambda}(x)$. Proceeding in this way, we finally get the zeropolynomial. We conclude that $p(x) = \beta c_s^{n,q,\lambda}(x) + \gamma c_u^{n,q,\lambda}(x) + \cdots \in A^{n,q,\lambda}$. That $A^{n,q,\lambda}$ is closed under multiplication is a consequence of the relation $(p_1(x)p_2(x))^q = p_1(x)p_2(x)$.

(ii) If $s \neq 0$, the polynomial $c_s^\lambda(x)$ is a sum of terms $\alpha_l x^l$, $\alpha_l \in GF(q)^*$, where l runs through a subset U of $\{1, 2, \ldots, n-1\}$. So, any term $\alpha_l x^l$ occurring in $c_s^\lambda(x)$ contributes to the sum $\sum_{i=0}^{n-1} c_s^\lambda(\alpha^j \zeta^i)$ an amount of $\alpha_l \alpha^{jl}(1 + \zeta^l + \cdots + \zeta^{(n-1)l})$, which is equal to zero for all $l \in U$. If $s = 0$, one obtains $\sum_{i=0}^{n-1} c_0^\lambda(\alpha^j \zeta^i) = 1 + 1 + \cdots + 1 = n$.

(iii) Since $A^{n,q,\lambda}$ is a $GF(q)$-algebra, we may write $c_j^{n,q,\lambda *}(x) c_k^{n,q,\lambda}(x) = \sum_{s \in S^{n,q,\lambda}} \alpha_s c_s^{n,q,\lambda}(x) \mod x^n - \lambda$, $\alpha_s \in GF(q)$. So, the bilinear form (11) yields $(c_j^{\lambda *}, c_k^\lambda)_\lambda = (c_{n-j}^\lambda, c_k^\lambda)_\lambda = \sum_{s \in S^{n,q,\lambda}} \sum_{i=0}^{n-1} \alpha_s c_s^\lambda(\alpha \zeta^i)$. Assume that $c_j^\lambda(x)$ is not self conjugated. If $k \neq j$ it is obvious that $\alpha_0 = 0$, and hence by (ii) we have $(c_j^{\lambda *}, c_k^\lambda)_\lambda = 0$. If $k = j$, we have $c_j^{\lambda *}(x) c_k^\lambda(x) = (x^{n-j} + x^{(n-j)q} + \cdots + x^{(n-j)q^{m_j - 1}})(x^j + x^{jq} + \cdots + x^{jq^{m_j - 1}}) \mod x^n - \lambda$. Here we used $m_{n-j} = m_j$. So, the coefficient of x^0 in the rhs is equal to $\lambda + \lambda^q + \cdots + \lambda^{q^{m_j - 1}} = m_j \lambda$. Hence, the result in this case is $(c_j^{\lambda *}, c_j^\lambda)_\lambda = n m_j \lambda$, since $\sum_{i=0}^{n-1} c_0^\lambda(\alpha \zeta^i) = n$ because of part (ii) of this theorem.
Next, we assume that $c_j^\lambda(x)$ is self conjugated, and so $(c_j^{\lambda *}, c_k^\lambda)_\lambda = (c_j^\lambda, c_k^\lambda)_\lambda$. Like before we may conclude that for $k \neq j$ the rhs is equal to 0, since the inverses of the x-powers in $c_j^\lambda(x)$ are in $c_j^\lambda(x)$ itself and not in $c_k^\lambda(x)$. Let $k = j$. Since $c_j^\lambda(x)$ is assumed to be self conjugated, it contains pairs of terms x^{jq^i} and $x^{(n-j)q^i}$. Hence, m_j is even and $j(q^{m_j/2} + 1) = 0 \mod n$, or $m_j = 1$ and $j \in \{0, n/2\}$. Consequently, if m_j is even, the polynomial $c_j^\lambda(x)$ contains the term $\lambda^{a-1} x^{n-j} = \lambda^a x^{-j}$ with $a_j := j(q^{m_j/2} + 1)/n$. So, in the product $(x^j + x^{jq} + \cdots + \lambda^a x^{-j} + \lambda^{aq} x^{-jq} + \cdots)(x^j + x^{jq} + \cdots + \lambda^a x^{-j} + \lambda^{aq} x^{-jq} + \cdots)$, the coefficient of x^0 is equal to $\lambda^a + \lambda^{aq} + \cdots + \lambda^{aq^{m_j - 1}} = m_j \lambda^a$, and the result follows in the same way as before. The case $j = 0$, $m_0 = 1$ is covered by the general result with $a_0 = 0$, while for $j = n/2$, $m_{n/2} = 1$ we have $a_{n/2} = \frac{n}{2}(q^{[1/2]} + 1)/n = 1$ which yields also the correct answer. □

5 An orthogonal transformation matrix

In this section we shall show that the primitive idempotents $\theta_t(x)$, $t \in T^{n,q,\lambda}$, form an alternative orthogonal basis for $A^{n,q,\lambda}$. It then follows that the transformation matrix between this basis and the orthogonal basis of constacyclonomials is an orthogonal matrix.

5.1 An orthogonal basis of primitive idempotent polynomials

Theorem 18 (Orthogonal basis of primitive idempotents)

(i) *With respect to the bilinear form* (11) *the primitive idempotents* $\theta_t(x)$, $t \in T^{n,q,\lambda}$, *form an orthogonal* $GF(q)$*-basis of the vector space* $A^{n,q,\lambda}$, *satisfying* $(\theta_t, \theta_u)_\lambda = m_t^\lambda \delta_{t,u}$ *for all* $t \in T^{n,q,\lambda}$.

(ii) *The number* n_0 *of irreducible polynomials* $P_t^\lambda(x)$ *and the number of primitive idempotents* $\theta_t(x)$, $t \in T^{n,q,\lambda}$, *are both equal to the number of constacyclonomials* $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$.

Proof (i) From their definition we know $\theta_t(x)^2 = \theta(x)$, and hence $\theta_t(x)^q = \theta_t(x)$ for all $t \in T^{n,q,\lambda}$. So, all $\theta_t(x)$ belong to $A^{n,q,\lambda}$ by Theorem 15 (ii). From Theorem 2 (ii) and Theorem 8 (i) it follows that $\theta_t(\alpha\zeta^i)$ is equal to 1 if $i \in C_t^{n,q,\lambda}$ and equal to 0 otherwise. Hence, $(\theta_t, \theta_u)_\lambda = \sum_{i=0}^{n-1} \theta_t(\alpha\zeta^i)\theta_u(\alpha\zeta^i)$ is equal to 0 for $t \neq u$ and equal to m_t^λ for $t = u$. To show that $A^{n,q,\lambda}$ is spanned by the idempotent polynomials $\theta_t(x)$, $t \in T^{n,q,\lambda}$, we assume that $p(x) \in A^{n,q,\lambda}$ is orthogonal to all $\theta_t(x)$. So, $\sum_{i=0}^{n-1} \theta_t(\alpha\zeta^i)p(\alpha\zeta^i) = 0$ for all $t \in T^{n,q,\lambda}$. Applying Theorem 2 (ii) then yields $\sum_{i \in C_t^{n,q,\lambda}} p(\alpha\zeta^i) = 0, t \in T^{n,q,\lambda}$. From Theorem 15 (ii) we have that $p(x)^q = p(x)$, or equivalently $p(x^q) = p(x)$. Since for any pair $i, j \in C_t^{n,q,\lambda}$ there is a positive integer a such that $\alpha\zeta^i = (\alpha\zeta^j)^{q^a}$, we can write $\sum_{i \in C_t^{n,q,\lambda}} p(\alpha\zeta^i) = m_t^\lambda p(\alpha\zeta^j)$ for some $j \in C_t^{n,q,\lambda}$ and for all $t \in T^{n,q,\lambda}$. It follows that $p(\alpha\zeta^i) = 0$ for $0 \leq i \leq n-1$, and since the degree of $p(x)$ is less than n, we conclude that $p(x) = 0$. Hence, the polynomials $\theta_t(x)$ form an orthogonal basis of $A^{n,q,\lambda}$.

(ii) Since the basis of primitive idempotents $\theta_t(x)$, $t \in T^{n,q,\lambda}$, and the basis of constacyclonomials $c_s^\lambda(x)$, $s \in S^{n,q,\lambda}$, must have the same number of elements, it follows that $n_0 := \left|T^{n,q,\lambda}\right| = \left|S^{n,q,\lambda}\right|$ (cf. also Theorem 5 (i)). Furthermore, there is a one-one correspondence between the primitive idempotent $\theta_t(x)$ and the irreducible polynomial $P_t^\lambda(x)$ with zeros $\alpha\zeta^t$ for $t \in T^{n,q,\lambda}$. □

Since the constacyclonomials constitute an orthogonal basis for $A^{n,q,\lambda}$, each element $p \in A^{n,q,\lambda}$ can be developed as (cf. Theorem 17 (iii))

$$p(x) = \sum_{s \in S^{n,q,\lambda}} \xi_s c_s^\lambda(x), \ \xi_s = (c_s^{\lambda *}, p)_\lambda / n m_s \lambda^{a_s}. \tag{12}$$

In particular we can write for the primitive idempotent $\theta_t(x)$, $t \in T^\lambda$, the expression

$$\theta_t(x) = \sum_{s \in S^{n,q,\lambda}} \xi_s^t c_s^\lambda(x), \ \xi_s^t = (c_s^{\lambda *}, \theta_t)_\lambda / n m_s \lambda^{a_s}. \tag{13}$$

Theorem 19 (Orthogonality relations for primitive idempotents)

(i) *Let* $\mu_{s,t}$ *stand for the sum of the* s*-powers of the zeros of* $P_t^\lambda(x)$, *for* $s \in S^{n,q,\lambda}$ *and* $t \in T^{n,q,\lambda}$. *Then the coefficients of the idempotent* $\theta_t(x)$ *can be written as* $\xi_s^t = \mu_{s,t}/n\lambda^{a_s}$ *when* $c_s^\lambda(x)$ *is self conjugated, and as* $\xi_s^t = \mu_{n-s,t}/n\lambda^{a_s}$ *when* $c_s^\lambda(x)$*is not self conjugated.*

(ii) *The sum* $\mu_{s,t}$ *can be written in terms of irreducible polynomials as* $\mu_{s,t} = -m_t^\lambda p_{(k,s)t}^{\lambda^s}/m_{(k,s)t}^{\lambda^s}$.

(iii) *If* $w_s := m_s \lambda^{a_s}$, *then* $n \sum_{s \in S^{n,q,\lambda}} \frac{w_s}{m_t^\lambda} \xi_s^t \xi_{n-s}^u = \delta_{t,u}$ *and* $n \sum_{t \in T^{n,q,\lambda}} \frac{w_s}{m_t^\lambda} \xi_s^t \xi_{n-r}^t = \delta_{s,r}$ *for* $t, u \in T^{n,q,\lambda}$ *and* $s, r \in S^{n,q,\lambda}$.

Proof (i) We know that $\theta_t^\lambda(\alpha\zeta^i)$ is equal to 1 if $\alpha\zeta^i$ is a zero of the irreducible polynomial $P_t^\lambda(x)$, while it is equal to 0 otherwise. Let $c_s^\lambda(x)$ be self conjugated. Then $c_s^{\lambda *}(\alpha\zeta^i) = c_s^\lambda(\alpha\zeta^i) = (\alpha\zeta^i)^s + (\alpha\zeta^i)^{sq} + (\alpha\zeta^i)^{sq^2} \cdots$, and hence $(c_s^{\lambda *}, \theta_t^\lambda)_\lambda = \sum_{i=0}^{n-1} c_s^\lambda(\alpha\zeta^i)\theta_t^\lambda(\alpha\zeta^i) = \sum_i (\alpha\zeta^i)^s + \sum_i (\alpha\zeta^i)^{sq} + \sum_i (\alpha\zeta^i)^{sq^2} + \cdots$, where the summation indices i in the m_s terms of the rhs run through the set $C_t^{n,q,\lambda}$. Since $\alpha\zeta^i$ is a zero of $P_t^\lambda(x)$, we have that $(\alpha\zeta^i)^{q^j}$ is also a zero of $P_t^\lambda(x)$ and we can write $(\alpha\zeta^i)^{q^j} = \alpha\zeta^{i'}$, $i' \in C_t^{n,q,\lambda}$.The mapping $i \to i'$ is one-to-one, and so the m_s summations are all equal to $\sum_{i \in C_t^{n,q,\lambda}} (\alpha\zeta^i)^s$. The individual terms in this summation are the s -powers of the zeros of $P_t^\lambda(x)$, and they are zeros themselves of some irreducible polynomial $P_{t_s}^{\lambda_s}(x)$. So, $\xi_s^t = m_s\mu_{s,t}/nm_s\lambda^{a_s} = \mu_{s,t}/n\lambda^{a_s}$. If $c_s^\lambda(x)$ is not self conjugated, we have $c_s^{\lambda *}(x) = c_{n-s}^\lambda(x)$. The result then follows in a similar way and by using $a_{n-s} = a_s = 1$ in this case.

(ii) This follows immediately from Theorem 10 (v).

(iii) Substituting the given expressions yields $(\theta_t, \theta_u)_\lambda = \sum_{s,s'} \xi_s^t \xi_{s'}^u (c_s^\lambda, c_{s'}^\lambda)_\lambda = \sum_{s \in S^{n,q,\lambda}} \xi_s^t \xi_{n-s}^u (c_s^\lambda, c_{n-s}^\lambda)_\lambda = n \sum_{s \in S^{n,q,\lambda}} m_s \lambda^{a_s} \xi_s^t \xi_{n-s}^u$, by applying Theorem 17 (iii). By putting $w_s = m_s\lambda^{a_s}$ the first relation follows. Combining the expression for ξ_s^t in (i) with the expression in Theorem 17 (iii) provides us with $nw_s\xi_s^t = m_t^\lambda c_{n-s}^\lambda(\alpha\zeta^t)$. Hence, $n^2 w_s w_r \sum_{t \in T^{n,q,\lambda}} \frac{1}{m_t^\lambda} \xi_s^t \xi_r^t = \sum_{i=0}^{n-1} c_{n-s}^\lambda(\alpha\zeta^i) c_{n-r}^\lambda(\alpha\zeta^i) = nw_s\delta_{s,n-r}$, again by applying Theorem 17 (iii). The second relation follows by replacing r by $n - r$. □

We remind the reader that all integers which occur in Theorem 19 are to be taken in $GF(q)$. In case that a denominator m_i or m_t^λ is equal to zero modulo q, one must consider this variable in connection with the numerator of the fraction to which it belongs to get an equality which makes sense. E.g. the fraction $\frac{w_s\xi_s^t}{m_t^\lambda} = \frac{m_s\mu_{s,t}}{nm_t^\lambda}$ in (iii) appears to be a well defined integer by applying (ii). Another remark is that for $q = 2$ and odd n, Theorem 19 (i) delivers the well-known result for primitive idempotents in the binary case [18, Ch. 8, Theorem 6].

5.2 Idempotent tables $\Xi^{n,q,\lambda}$ and $\mathrm{M}^{n,q,\lambda}$

We shall reformulate now the orthogonality relations of Theorem 19 (iii) in terms of matrices.

Definition 20 (*Definition of primitive idempotent table for constacyclic codes*) The $n_0 \times n_0$-matrix $\Xi^{n,q,\lambda}$over $GF(q)$ has elements $\Xi_{s,t}^{n,q,\lambda} := \xi_s^t$, $s \in S^{n,q,\lambda}$, $t \in T^{n,q,\lambda}$. The adjoint matrix $\Xi^{n,q,\lambda *}$ is the matrix with elements $\Xi_{s,t}^{n,q,\lambda *} := \frac{w_s}{m_t^\lambda} \xi_{n-s}^t$.

Theorem 21

(i) $\Xi^{n,q,\lambda}\Xi^{n,q,\lambda *} = \Xi^{n,q,\lambda *}\Xi^{n,q,\lambda} = nI$.

(ii) *Let* $e(x) = \sum_{t \in T^{n,q,\lambda}} \eta_t\theta_t(x)$, *be the idempotent generator of some constacyclic code* $C^{n,q,\lambda}$, *and let* $\eta = (\eta_0, \eta_1, \ldots, \eta_{n_0-1})^T \in GF(q)^{n_0}$. *Then* $e(x) = \sum_{s \in S^{n,q,\lambda}} \xi_s c_s^\lambda(x)$, $\xi = (\xi_0, \xi_1, \ldots, \xi_{n_0-1})^T = n^{-1}\Xi^{n,q,\lambda *}\eta$.

The next simple example will enable the reader to verify all properties stated in Theorems 18 and 19.

Example 22 Let $n = 12$, $q = 7$ and $\lambda = 2$. Hence, $k = 3$ and $l = 2$.

The binomial $x^{12}-2$ can be factorized into three irreducible polynomials over $GF(7)$ as $x^{12}-2=(x^6-3)(x^3+2)(x^3-2)$. Let α be a zero of x^6-3 of order 36. The zeros of $x^{12}-2$ can be written as $\alpha\zeta^i$, $0\le i<12$, with $\zeta=\alpha^3$. The three constacyclonomials in this case are $C_0^{12,7,2}=(0,2,4,6,8,10)$, $C_1^{12,7,2}=(1,9,5)$ and $C_3^{12,7,2}=(3,11,7)$. Since $\alpha^{12}=2$, we have $(\alpha\zeta^1)^3=\alpha^{12}=2$ and $(\alpha\zeta^3)^3=\alpha^{30}=5$, and so we can index the irreducible factors as $P_0^2(x)=x^6-3$, $P_1^2(x)=x^3-2$ and $P_3^2(x)=x^3+2$. Though there are nine cyclotomic cosets $C_s^{12,7}$ in this case, only three of them, i.e. $C_0^{12,7}=(0)$, $C_3^{12,7}=(3,9)$ and $C_6^{12,7}=(6)$, give rise to a constacyclonomial $c_s^2(x):=c_s^{12,7,2}(x)$, according to Theorem 18 (ii). These three constacyclonomials are $c_0^2(x)=1$, $c_3^2(x)=x^3+2x^9$ and $c_6^{12}(x)=x^6$, and we define $S^{12,7,2}:=\{0,3,6\}$. There are also three primitive idempotents $\theta_t(x)$, $t\in T^{12,7,2}$, with $T^{12,7,2}=\{0,1,3\}$. By applying the general expression of Theorem 3 (ii), we find $\theta_0(x)=-x^6+4$, $\theta_1(x)=2x^9+4x^6+x^3+2$ and $\theta_3(x)=-2x^9+4x^6-x^3+2$. These expressions, together with (13), yield the transformation matrix

$$\Xi^{12,7,2}=\begin{bmatrix}4&2&2\\0&1&6\\6&4&4\end{bmatrix}.$$

The rows are indexed by respectively 0, 3, 6, the integers of $S^{12,7,2}$, and the columns by 0, 1, 3, the integers of $T^{12,7,2}$. We collect the weights $w_s(=m_s\lambda^{a_s})$, $s\in S^{12,7,2}$, in the weight vector $\sigma=(1,1,2)\in GF(7)^3$, and similarly the weights $1/m_t$, $t\in T^{12,7,2}$, in the weight vector $\tau=(6,5,5)\in GF(7)^3$. With the help of these vectors, one can easily verify in this case the orthogonality relations of Theorem 19 (iii). We also present the closely related matrix $\mathrm{M}^{12,7,2}$, the elements $\mu_{s,t}$ of which are the sums of the s-powers of the zeros of the irreducible polynomials $P_t^2(x)$. Since the three constacyclonomials are self conjugated, $\mathrm{M}^{12,7,2}$ is obtained by multiplying the rows of $\Xi^{12,7,2}$ by $n\lambda^{a_s}$ for s equal to 0, 3 and 6. With $a_0=0$, $a_3=2$ and $a_6=1$, we get

$$\mathrm{M}^{12,7,2}=\begin{bmatrix}6&3&3\\0&6&1\\4&5&5\end{bmatrix}.$$

One can also produce this result by applying Theorems 19 (ii) and 10 (v), or by determining the sums $\mu_{s,t}$ straightforwardly. Apart from the polynomials $P_t^2(x)$, the relevant irreducible polynomials to carry this out are $P_0^{2^0}(x)=x-1$, $P_0^{2^3}(x)=x^2+4$, $P_0^{2^6}(x)=x-3$, $P_3^{2^0}=x+1$, $P_3^{2^3}(x)=x-2$, $P_3^{2^6}(x)=x+3$, $P_9^{2^0}(x)=x+1$, $P_9^{2^3}(x)=x+2$ and $P_9^{2^6}(x)=x+3$. Notice that e.g. $P_0^{2^0}(x)$ and $P_0^{2^3}(x)$, though $2^0=2^3=1$ in $GF(7)$, are different polynomials, due to the representation of their zeros as defined in Theorem 10 (v). □

We introduced $\Xi^{n,q,\lambda}$ as the transformation matrix from one orthogonal basis to another. However, because of its orthogonality over $GF(q)$, we could equally well consider $\Xi^{n,q,\lambda}$, for any relevant triple (n,q,λ), as a *primitive idempotent table*, (shortly *idempotent table*) resembling the *irreducible character tables* for finite groups (cf. e.g. [7, 13]). In this picture the columns of the table $\Xi^{n,q,\lambda}$, which represent the primitive idempotents with labels $t\in T^{n,q,\lambda}$, being the indices of the constacyclotomic cosets $C_t^{n,q,\lambda}$, correspond to irreducible characters. The labels $s\in S^{n,q,\lambda}$ of the rows are the indices of those cyclotomic cosets $C_s^{n,q}$ which afford a constacyclonomial. These constacyclonomials or these cosets can be seen as the counterparts of the classes of conjugated elements in a finite group. Instead of $\Xi^{n,q,\lambda}$, we shall mostly consider the matrix $\mathrm{M}^{n,q,\lambda}$ (e.g. in Example 22) with elements

$$\mu_{s,t}=n\lambda^{a_s}\Xi^{n,q,\lambda}_{s*,t}, \tag{14}$$

where $s^* = s$ when $c_s^\lambda(x)$ is self conjugated, and $s^* = n - s$ otherwise (cf. Theorem 19 (i)).

6 The case of cyclic codes

The analogy between the two types of tables, mentioned in the previous section, is even stronger for $\lambda = 1$, i.e. in the case of cyclic codes. In this section we shall take a closer look at this case.

6.1 Primitive idempotent tables $M^{n,q}$

For the sake of simplicity, we choose the ζ-representation for the zeros of $x^n - 1$ and omit the parameter value $\lambda = 1$ (cf. Remark 9). So, instead of the sets $S^{n,q,1}$ and $T^{n,q,1}$ we take the index sets $S^{n,q}$ and $T^{n,q}$. These two sets can be chosen identical. In order to establish more similarities with character tables, we defined in Sect. 4 $C_{t^*}^{n,q} := C_{-t}^{n,q}$ as the *conjugated cyclotomic coset* of $C_t^{n,q}$, $t \in T^{n,q}$, where $t^* := n - t$ is an integer in $[0, n-1]$. It will be obvious that $m_{t^*} = m_t$. Correspondingly, we define $P_{t^*}(x)$ of degree m_t as the *conjugated irreducible polynomial* of $P_t(x)$ and $\theta_{t^*}(x)$ as the *conjugated primitive idempotent of* $\theta_t(x)$. Actually, the polynomial $P_{t^*}(x)$ is the *monic reciprocal of* $P_t(x)$, formally expressed by

$$P_{t^*}(x) = P_t(0)^{-1} x^{m_t} P_t(1/x), \tag{15}$$

which was introduced in Theorem 2 (vi) for any $P_t^\lambda(x)$, $t \in T^{n,q,\lambda}$. We say that $P_t(x)$ is *self conjugated* if $P_{t^*}(x) = P_t(x)$, and similarly that $\theta_t(x)$ is *self conjugated* if $\theta_{t^*}(x) = \theta_t(x)$. We also introduced in Definition 14 the constacyclonomial $c_s^{\lambda *}(x)$ as the conjugate of $c_s^\lambda(x)$. We now write this polynomial as $c_{s*}^\lambda(x)$, so $s* = s$ if $C_s^\lambda(x)$ is self conjugated and $s* = n - s$ otherwise. Because of these decisions and definitions, and because the s-powers of the zeros of any irreducible polynomial contained in $x^n - 1$ are the zeros of some other (or the same) irreducible factor of $x^n - 1$, we can simplify and extend the relations of Theorem 19 as follows.

Theorem 23

(i) *The coefficients of the idempotent $\theta_t(x)$ for a cyclic code can be written as $\xi_s^t = \mu_{s,t}/n$, where $\mu_{s,t}$ stands for the sum of the s-powers of the zeros of $P_t(x)$, for all $s \in S^{n,q}$ and $t \in T^{n,q}$.*

(ii) *The sum $\mu_{s,t}$ can be expressed in terms of irreducible polynomials as $\mu_{s,t} = -m_t\, p_{st}/m_{st}$.*

(iii) *For all $s, r \in S^{n,q}$ and for all $t, u, \in T^{n,q}$, one has $\xi_{s*}^t = \xi_s^{t*}$.*

(iv) $n \sum_{s \in S^{n,q}} \frac{m_s}{m_t} \xi_s^t \xi_{s*}^u = \delta_{t,u}$ *and* $n \sum_{t \in T^{n,q}} \frac{m_s}{m_t} \xi_s^t \xi_{r*}^t = \delta_{s,r}$.

(v) *The number of self conjugated primitive idempotent generators is equal to the number of self conjugated cyclonomials.*

The expression in (ii) is immediately clear if one realizes that the s-powers of the zeros of $P_t(x)$ are zeros of $P_{st}(x)$. This expression was already derived in [25] in a slightly different way. The equality in (iii) follows from (i) and (ii) and by applying $m_{n-s} = m_s$ and $m_{n-t} = m_t$. The statement in (v) is also obvious, since for all $s \in S^{n,q} (= T^{n,q})$ both polynomials $c_s(x)$ and $\theta_s(x)$ are self conjugated if and only if the corresponding cyclotomic coset $C_s^{n,q}$ is self conjugated.

Theorem 24 (Primitive idempotent table for cyclic codes) *The entries $\mu_{s,t}$ of the table* $\mathrm{M}^{n,q}$, *$s \in S^{n,q}$, $t \in T^{n,q} (= S^{n,q})$, satisfy the following properties.*

(i) $\sum_{s\in S^{n,q}} \frac{m_s}{m_t}\mu_{s,t}\mu_{s*,u} = n\delta_{t,u}$, $\sum_{t\in T^{n,q}} \frac{m_s}{m_t}\mu_{s,t}\mu_{r*,t} = n\delta_{s,r}$,
(ii) $\mu_{s*,t} = \mu_{s,t*}$, $m_s\mu_{s,t} = m_t\mu_{t,s}$.
(iii) $\mu_{s,0} = 1$ *for all* $s \in S^{n,q}$ *and* $\mu_{0,t} = m_t$ *for all* $t \in T^{n,q}$.
(iv) *If* n *is even* $\mu_{s,n/2} = (-1)^s$ *for all* $s \in S^{n,q}$ *and* $\mu_{n/2,t} = (-1)^t m_t$ *for all* $t \in T^{n,q}$.

Proof (i) and (ii) These relations follow immediately from the orthogonality relations in Theorem 19 (iii) and from the equality for $\mu_{s,t}$ in Theorem 19 (ii).

(iii) and (iv) follow from Theorem 19 (ii) by substituting respectively $p_0 = -1$ and $p_{n/2} = 1$. These values are yielded by the irreducible polynomials $P_0(x) = x - 1$ and $P_{n/2}(x) = x + 1$. □

The statements in Theorem 23 provide us with a link to the theory of idempotents of cyclic codes as developed in [25]. The column of $\mathrm{M}^{n,q}$ with index 0 (its 'first' column) is the all-one column, and so θ_0 corresponds to the trivial character χ_1 of a finite group G. Furthermore, the row of $\mathrm{M}^{n,q}$ with index 0 (its 'first' row) contains all values m_t, i.e. the sizes of the cyclonomials. One could consider these values as counterparts of the dimensions (degrees) χ_1^j of the irreducible representations of a finite group . Now, the second orthogonality relation of Theorem 23 (i) gives for $s = r = 0$ that $\sum_{t\in T^{n,q},1} m_t = n$. It is tentative to see this elementary equality as the counterpart of the well known Burnside relation $\sum_j (\chi_1^j)^2 = n$, which results from a similar orthogonality relation for character tables. All these similarities with irreducible character tables, strengthen the introduction of the name of primitive idempotent table for the matrix $\mathrm{M}^{n,q}$, and more in general for $\mathrm{M}^{n,q,\lambda}$ (cf. Sect. 5). We remark that the similarities between the orthogonality relations and their consequences for idempotent generators on the one hand and irreducible characters on the other, will not come as a surprise if one realizes that both topics can be embedded in the general theory of idempotents for semi-simple algebras (cf. [6, 23, 24]).

6.2 Blocks of conjugated cyclonomials and idempotents

Inspired by the previous remarks we introduce the following notions. Let r be an element of the multiplicative group U_n consisting of the positive integers modulo n which are prime to n. It will be obvious that the set $rC_s^{n,q}$ is identical to the cyclotomic coset $C_{rs}^{n,q}$. We shall call it the *r-conjugate* of $C_s^{n,q}$. Similarly, the cyclonomial $c_{rs}(x)$ is the *r-conjugate of* $c_s(x)$, and the irreducible polynomial $P_{rt}(x)$ the *r-conjugate* of $P_t(x)$. Since $(n, r) = 1$, one easily proves that $m_{rs} = m_s$, that $c_{rs}(x)$ and $c_s(x)$ have the same size, and that $P_{rt}(x)$ and $P_t(x)$ have the same degree. For $r = n - 1$ $(= -1 \bmod n)$ we obtain the notions of conjugated irreducible polynomial and conjugated cyclonomial which were introduced already earlier in this text, and which correspond to the notion of conjugated cyclotomic coset at the end of Sect. 4. We say that $c_s(x)$ is *r-self conjugated* if $c_{rs}(x) = c_s(x)$, and that $P_t(x)$ is *r-self conjugated* if $P_{rt}(x) = P_t(x)$. If $\theta_{rt}(x)$ is the primitive idempotent generated by $P_{rt}(x)$, then $\theta_{rt}(x)$ and $\theta_t(x)$ are also said to be *r-conjugated,* and if they are equal $\theta_t(x)$ is said to be *r-self conjugated*. There exists a simple relationship between the primitive idempotent $\theta_t(x)$ and its r-conjugate $\theta_{rt}(x)$. Let $1/r$ be the inverse of r in U_n. From Theorem 2 (ii) it follows that $\theta_t(x^{1/r}) = 1$ for $x = \beta^r$ and β is a zero of $P_t(x)$, and that $\theta_t(x^{1/r}) = 0$ for $x = \beta^r$ and β is a zero of $P_u(x)$, $u \neq t$. We conclude that for all $t \in T^{n,q}$

$$\theta_{rt}(x) = \theta_t(x^{1/r}), r \in U_n. \tag{16}$$

Furthermore, the set of all cyclonomials is denoted by

$$Cy^{n,q} := \{c_s(x) \,|s \in S^{n,q}\}, \tag{17}$$

and the set of all primitive idempotent generators by

$$Id^{n,q} := \{\theta_t(x) \,|t \in T^{n,q}\}. \tag{18}$$

Let H be the subgroup of U_n generated by q. Remember that $(n, q) = 1$, so $q^i \in U_n$ for all i. It will be clear that the elements of H are the same as those of the cyclotomic coset $C_1^{n,q}$, and so $|H| = \mathrm{m}_1$. Since $|U_n| = \varphi(n)$, the quotient group U_n/H has $a := \varphi(n)/m_1$ elements and we write

$$U_n = H_{r_1} \cup H_{r_2} \cup \cdots \cup H_{r_a}, \tag{19}$$

with $H_{r_i} := r_i H$, for $1 \leq i \leq a$, and $H_{r_1} := H$. The elements r_i are determined up to powers of q. Since the same holds for the integers in $S^{n,q}$, we can chose $r_1(= 1), r_2, \ldots, r_d$ such that they are the integers of the set $S_1^{n,q} S^{n,q} \cap U_n$. More generally, we define for each divisor $d \leq n$ of n

$$S_d^{n,q} := \left\{s \middle| s \in S^{n,q}, \middle|(n, s) = d\right\}. \tag{20}$$

We remark that for any $s \in S_d^{n,q}$, any integer $i \in C_s^{n,q}$ satisfies $(n, i) = d$, since $(n, q) = 1$. Hence, the cyclotomic cosets defined by (20) together contain all integers $i \in [0, n-1]$ with $(n, i) = d$, and so

$$S^{n,q} = \bigcup_d S_d^{n,q}. \tag{21}$$

We also remind the reader that the elements of any cyclotomic coset $C_i^{n,q}$ can be obtained from the subgroup $C_1^{n,q}$ by applying

$$iC_1^{n,q} = \frac{m_1}{m_i} \times C_i^{n,q}. \tag{22}$$

The expression in the rhs of (22) stands for the multiset where each integer of $C_i^{n,q}$ occurs m_1/m_i times (cf. also Theorem 8 (v)). The above lines show that U_n induces a group G of permutations on the set of cyclotomic cosets by means of the transformation $C_s^{n,q} \to C_{rs}^{n,q}$, and hence, that U_n also induces permutation groups G' and G'' acting on the sets $Cy^{n,q}$ and $Id^{n,q}$. These groups are isomorphic and the orbits of G' and G'' are called *blocks of cyclonomials* and *blocks of idempotents*. The subgroup H of U_n contains precisely those elements which induce the identity permutation on these sets. Because $T^{n,q}$ is identical to $S^{n,q}$, we define $T_d^{n,q} := S_d^{n,q}$ for all $d| \ n$. For even n, there exists another permutation group acting on the set of cyclotomic cosets, and hence on $Cy^{n,q}$ and $Id^{n,q}$, induced by $i \to i + n/2 \bmod n$ for all integers $i \in \{0, 1, \ldots, n-1\}$. One can easily verify that this operation transforms $C_s^{n,q}$ into $C_{s+n/2}^{n,q}$. The orbits of this group have size 2 or 1. In the first case we shall speak of pairs of *associated cyclotomic cosets*, *associated cyclonomials* and *associated idempotents*. In the second case all these objects are called *self associated*.

Theorem 25 *The primitive idempotents for cyclic codes $C^{n,q}$, $(n, q) = 1$, have the following properties.*

(i) *The blocks of cyclonomials can be identified as $B_d^{Cy} = \{c_s(x) \,|s \in S_d^{n,q}\}$ and the blocks of idempotents as $B_d^{Id} = \{\theta_t(x) \,|t \in T_d^{n,q}\}$ for all $d| \ n$.*

(ii) *The blocks B_d^{Cy} and B_d^{Id} both contain $\varphi(n/d)/m_d$ elements, and the group $U_{n/d}$ acts transitively on these blocks.*

(iii) *The components of the columns μ_j and μ_l of the idempotent table $\mathrm{M}^{n,q}$, $j, l \in T_d^{n,q}$, form a permutation of each other, such that the components of μ_l with index in $S_{d'}^{n,q}$ are a permutation of the similar components of μ_j, for all d'. The same holds for the idempotent table $\Xi^{n,q}$.*

(iv) *The number of r-self conjugated primitive idempotents is equal to the number of r-self conjugated cyclonomials for any $r \in U_n$. The same holds for the number of self associated idempotents and the number of self associated cyclonomials.*

Proof (i) For all $r \in U_n$ we have that $(n, s) = d$ implies $(n, rs) = d$. Hence, $c_s(x)$ implies $c_{rs}(x) \in B_d^{Cy}$, and similarly $\theta_t(x) \in B_d^{Id}$ implies $\theta_{rt}(x) \in B_d^{Id}$. Moreover, if s and s' are both in $S_d^{n,q}$ then certainly there is an integer $r \in U_n$ such that $s' = rs$. So, $c_s(x)$and $c_{s'}(x)$ belong to the same orbit of G. This proves that the set B_d^{Cy} really is an orbit under the action of G. The proof for B_d^{Id} is completely similar.

(ii) There are $\varphi(n/d)$ integers s, satisfying $(n, s) = d$ and $0 < s \leq n$. This follows immediately from the property that $(n, s) = d$ if and only if $(n/d, s/d) = 1$. Hence, there are $\varphi(n/d)/m_d$ different cyclotomic cosets $C_{dr_i}^{n,q}$, and they all have size m_d (cf. Eqs. (19) and (22)). Because of the one-one correspondence between cyclotomic cosets on the one hand and cyclonomials and idempotents on the other, the statement now follows. Let $i, j \in S_d^{n,q}$. Then $(n, i) = (n, j) = d$, and hence $(n/d, i/d) = (n/d, j/d) = 1$. Since $U_{n/d}$ is a group, there exists an integer $r \in U_{n/d}$ such that $ri/d = j/d \bmod n/d$, and so $ri = j \bmod n$.

(iii) Take an index $i \in S_{d'}^{n,q}$, and so $(n, i) = d'$. Since j and l are in $S_d^{n,q}$, the integer j/l is in U_n, and therefore $(n, j/l) = 1$ and $(n, ij/l) = d'$. Hence, there is an index $k \in S_{d'}^{n,q}$ such that $ij = kl$. Now $m_j = m_l$ and so $\mu_{i,j} = -m_j p_{ij} m_{ij} = -m_l p_{kl} m_{kl} = \mu_{k,l}$. The equivalent relation for $\Xi^{n,q}$ follows by applying Theorem 19 (i).

(iv) Both statements follow immediately from the fact that $c_s(x)$ as well as $\theta_s(x)$ is r-self conjugated (self associated) if and only if $C_s^{n,q}$ is r-self conjugated (self associated). □

We give an alternative proof for Theorem 25 (iii) which seems more suitable for generalizations for values of $\lambda > 1$. If $j, l \in T_d^{n,q}$, there exists an integer $r \in U_n$ such that $rj = l$. From (16) it follows that $\theta_{rj}(x) = \theta_j(x^{1/r}) = \sum_s \xi_s^j c_s(x^{1/r}) = \sum_s \xi_{rs}^j c_s(x)$. On the other hand, we have $\theta_{rj}(x) = \theta_l(x) = \sum_s \xi_s^l c_s(x)$, and hence $\xi_s^j = \xi_{rs}^j$. Since s and rs are both integers of $S_{d'}^{n,q}$ for some d', the statement for $\Xi^{n,q}$ now follows. Theorem 25 (iii) and (iv) and Eq. (16) show that the explicit expression for just one primitive idempotent of some block B_d^{Id} is sufficient to derive the expressions for all other idempotents which belong to the same block. We remark that the corresponding polynomials $P_t(x)$, $t \in T_d^{n,q}$, are the irreducible factors of the *cyclotomic polynomial* $\Phi_{n/d}(x)$ (cf. [17]). Finally, we present an example by which one can verify this property and also all other properties mentioned in Theorems 24 and 25.

Example 26 We consider the case $n = 16$ and $q = 5$. The cyclotomic cosets are $C_0^{16,5} = (0)$, $C_1^{16,5} = (1, 5, 9, 13)$, $C_2^{16,5} = (2, 10)$, $C_3^{16,5} = (3, 15, 11, 7)$, $C_4^{16,5} = (4)$, $C_6^{16,5} = (6, 14)$, $C_8^{16,5} = (8)$ and $C_{12}^{16,5} = (12)$. Thus we have the index subsets $S_{16}^{16,5} = \{0\}$, $S_1^{16,5} = \{1, 3\}$, $S_2^{16,5} = \{2, 6\}$, $S_4^{16,5} = \{4, 12\}$, $S_8^{16,5} = \{8\}$. The relevant irreducible polynomials are $P_0(x) = x - 1$, $P_1(x) = x^4 + 2$, $P_3(x) = x^4 + 3$, $P_2(x) = x^2 + 2$, $P_6(x) = x^2 + 3$, $P_4(x) = x + 2$, $P_{12}(x) = x + 3$ and $P_8(x) = x + 1$.

By using the expression $\mu_{s,t} = -m_t\, p_{st}/m_{st}$ we are able to construct the idempotent table $\mathrm{M}^{16,5}$. Its rows and column are labelled by the integers from the index set $S^{16,5} = T^{16,5} = \{0, 1, 3, 2, 6, 4, 12, 8\}$:

$$\mathrm{M}^{16,5} = \begin{bmatrix} 1 & 4 & 4 & 2 & 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 3 & 2 & 4 \\ 1 & 0 & 0 & 0 & 0 & 2 & 3 & 4 \\ 1 & 0 & 0 & 1 & 4 & 4 & 4 & 1 \\ 1 & 0 & 0 & 4 & 1 & 4 & 4 & 1 \\ 1 & 2 & 3 & 3 & 3 & 1 & 1 & 1 \\ 1 & 3 & 2 & 3 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 1 & 1 & 1 \end{bmatrix}.$$

It will be clear that there are five index subsets (20): $S_1^{16,5} = \{1, 3\}$, $S_2^{16,5} = \{2, 6\}$, $S_4^{16,5} = \{4, 12\}$, $S_8^{16,5} = \{8\}$, $S_{16}^{16,5} = \{0\}$, and so there are five blocks B_i^{Cy} and five blocks B_i^{Id}, $i \in \{1, 2, 4, 8, 16\}$. Since $\varphi(16)/m_1 = \varphi(8)/m_2 = \varphi(4)/m_4 = 2$, the blocks with index 1, 2 and 4 have size 2, and since $\varphi(2)/m_8 = \varphi(1)/m_{16}\ (= \varphi(1)/m_0) = 1$, the blocks with index 8 and 16 have size 1. □

7 The case of negacyclic codes

In this final section we focus on the class of negacyclic codes, so we take $\lambda = -1$ and $k = 2$.

7.1 Primitive idempotent tables $\mathrm{M}^{n,q,-1}$

The zeros of the irreducible polynomial $P_t^{-1}(x)$ are written in the α, ζ-representation, i.e. as $\alpha\zeta^i$, with $\zeta = \alpha^2$ and $i \in C_t^{n,q,-1}$. Since for binary codes there is no distinction between cyclic and negacyclic codes, we assume that q is odd. At the end of Sect. 4 we defined $C_{t*}^{n,q,-1} = C_{n-t-1}^{n,q,-1}$ as the conjugated negacyclotomic coset of $C_t^{n,q,-1}$, $t \in T^{n,q,-1}$. The integer $t* = n - t - 1$ is an integer in $[0, n-1]$, and we assume that it is an element of $T^{n,q,-1}$. As a consequence of Theorem 12 (i) we have $m_{t^*}^{-1} = m_t^{-1}$. Similarly as in the case $\lambda = 1$, we define $P_{t^*}^{-1}(x)$ as the conjugated irreducible polynomial of $P_t^{-1}(x)$ and $\theta_{t^*}(x)$ as the conjugated primitive idempotent of $\theta_t(x)$. Just as in the case $\lambda = 1$ in Sect. 6, $P_{t^*}^{-1}(x)$ is the monic reciprocal of $P_t^{-1}(x)$ (cf. Theorem 2 (vi)). We now present a number of properties of the matrix elements $\mu_{s,t}$ of $\mathrm{M}^{n,q,-1}$. According to Theorem 19 (i) these are equal to the sums of the s-powers of the zeros of $P_t^{-1}(x)$. Similar properties for the matrix elements of $\Xi^{n,q,-1}$ can be obtained by $\xi_s^t = (-1)^{a_s}\mu_{s,t}/n$.

Theorem 27 (Primitive idempotent table for negacyclic codes) *The entries $\mu_{s,t}$ of the table $\mathrm{M}^{n,q,-1}$, $s \in S^{n,q,-1}$, $t \in T^{n,q,-1}$, satisfy the following properties.*

(i) $\frac{1}{n}\sum_{s\in S^{n,q,-1}} (-1)^{a_s}\frac{m_s}{m_t^{-1}}\mu_{s,t}\mu_{s*,u} = \delta_{t,u}$, $\frac{1}{n}\sum_{t\in T^{n,q,-1}} (-1)^{a_s}\frac{m_s}{m_t^{-1}}\mu_{s*,t}\mu_{r,t} = \delta_{s,r}$.

(ii) *If s is odd, the sum $\mu_{s,t}$ can be written as $\mu_{s,t} = -m_t^{-1}p_{t_s}^{-1}/m_{t_s}^{-1}$, where $t_s = st + (s-1)/2$ refers to the α, ζ-representation with $\zeta = \alpha^2$. If s is even, one can write $\mu_{s,t} = -m_t^{-1}p_{t_s}^{1}/m_{t_s}^{1}$, where $t_s = 2t$ refers to the α', ζ'-representation with $\alpha' = \alpha^s$, $\zeta' = \alpha'$.*

(iii) *For all $t \in T^{n,q,-1}$ one has $\mu_{0,t} = m_t^{-1}$, and if n is odd $\mu_{s,(n-1)/2} = (-1)^s$.*

(iv) *For $s^* = n - s$ and $t^* = n - t - 1$, one has $\mu_{s^*,t} = \mu_{s,t^*}$ and $\mu_{s^*,t^*} = \mu_{s,t}$.*

Proof (i) and (ii) follow immediately from Theorem 19.

(iii) The sum of the 0th powers of the zeros of $P_t^{-1}(x)$ equals $1+1+\cdots+1 = m_t^{-1}$. If n is odd, the polynomial $x+1$ is a divisor of x^n+1, and we write $P_{(n-1)/2}^{-1}(x) = x+1$, since $\alpha\zeta^{(n-1)/2} = \alpha^n = -1$.

(iv) If $\alpha\zeta^t$ is a zero of $P_t^{-1}(x)$, then $\alpha\zeta^{n-t-1}$ is a zero of $P_{t^*}^{-1}(x)$. Since $\zeta = \alpha^2$, $\alpha^n = -1$ and $\zeta^n = 1$, we have that $(\alpha\zeta^t)^{s*} = (\alpha\zeta^t)^{n-s} = -\alpha^{-s-2st}$ and $(\alpha\zeta^{t*})^s = (\alpha\zeta^{n-t-1})^s = \alpha^{-s-2st}$. Summing over all zeros of $P_t^{-1}(x)$ yields $\mu_{s*,t} = \mu_{s,t*}$. The second equality follows by replacing t by $t*$. □

In [25] it was shown, by a few examples, that in the case of cyclic codes the idempotent table or parts of it can sometimes be determined without explicit knowledge of the irreducible polynomials contained in x^n-1. Here, we shall show that the same is possible sometimes for negacyclic codes.

Example 28 We take $n = 9$ and $q = 5$. For these values we have the following cyclic and negacyclic cosets $C_0^{9,5} = (0)$, $C_1^{9,5} = (1,5,7,8,4,2)$, $C_3^{9,5} = (3,6)$, $C_0^{9,5,-1} = (0,2,3,8,6,5)$, $C_1^{9,5,-1} = (1,7)$, $C_4^{9,5,-1} = (4)$. We take $S^{9,5,-1} = \{0,1,3\}$, $T^{9,5,-1} = \{0,1,4\}$, while $m_0 = 1$, $m_1 = 6$, $m_3 = 2$, $m_0^{-1} = 6$, $m_1^{-1} = 2$, $m_4^{-1} = 1$. We label the rows of the tables $\Xi^{9,5,-1}$ and $\mathrm{M}^{9,5,-1}$ by 0, 1, 3 and their columns by 4, 1, 0. By applying Theorem 27 (iii) we find for $\mathrm{M}^{9,5,-1}$ as first row vector $r_0 = (1,2,1)$ and as third column vector $t_4 = (1,0,3)^t$. Furthermore, we represent the second row by the vector $r_1 = (a,b,0)$ and the third one by $r_3 = (c,d,3)$, with $a,b,c,d \in GF(5)$. The weights $1/m_t^{-1}$, $t \in T^{9,5,-1}$, are collected in the weight vector $\tau = (1,3,1)$ and the weights w_s, $s \in S^{9,5,-1}$, in $\sigma = (1,1,2)$. The orthonormality relations in Theorem 27 (i) now yield the set of equations $a+b = 0$, $a^2+3b^2 = 4$, $c+d = 0$ and $c^2+3d^2 = 3$. This set has two solutions, i.e. $c = 4$, $d = 3$ and $a = -b = \pm 1$. To settle the remaining question of the right sign of a and b, one needs one extra piece of information, e.g. the coefficient of the one but highest power of x in the irreducible polynomial $P_1^{-1}(x) = x^2 - x + 1$. From its value one easily derives that $a = -b = -1$. So, the complete idempotent table now reads.

$$\mathrm{M}^{9,5,-1} = \begin{bmatrix} 1 & 2 & 1 \\ 4 & 1 & 0 \\ 4 & 3 & 3 \end{bmatrix}.$$

Together with the negacyclonomials $c_0^{-1}(x) = 1$, $c_1^{-1}(x) = x^1 + x^5 + x^7 - x^8 - x^4 - x^3$, $c_3^{-1}(x) = x^3 - x^6$, and by using the relation $\Xi^{9,5,-1} = -\mathrm{M}^{9,5,-1}$, one can obtain the explicit expressions for the primitive idempotent generators.

7.2 Blocks of conjugated negacyclonomials and idempotents

In order to define r-conjugated negacyclonomials, negacyclotomic cosets and idempotent generators, we first prove the following theorem.

Theorem 29

(i) *Let r be some element of U_n and let $a \in \{1,2,\ldots,n-1\}$ satisfy $2a = r-1$ mod n. Then $C_{rt+a}^{n,q,-1} = rC_t^{n,q,-1} + a$ and $m_{rt+a}^{-1} = m_t^{-1}$ for every $t \in T^{n,q,-1}$.*

(ii) *The transformations $C_t^{n,q,-1} \to C_{rt+a}^{n,q,-1}$, $r \in U_n$, constitute a permutation group G on the set of negacyclotomic cosets, while the subgroup $H := \langle q \rangle$ of U_n contains all elements of U_n which induce the identity permutation on that set.*

Proof The equation $2x = r - 1 \bmod n$ has a unique solution $(r-1)/2$ if n is odd. If n is even, there are two solutions which differ by $n/2$. We choose one of these as the integer a. Both (i) and (ii) now follow immediately from Theorem 12, by taking $k = 2$, and by applying Definition 7 with $l = (q-1)/2$. □

We call $C_{rt+q}^{n,q,-1}$ the *r-conjugate* of $C_t^{n,q,-1}$ for any $r \in U_n$. Consistently, the irreducible polynomial $P_{rt+a}^{-1}(x)$ is called the *r-conjugate* of $P_t^{-1}(x)$ and the corresponding primitive idempotent $\theta_{rt+a}(x)$ the *r-conjugate* of $\theta_t(x)$. For $r = -1$ one gets the normal conjugated objects as defined earlier in this section. The definitions of *r-self conjugateness* are completely similar to those in the case $\lambda = 1$. Analogously to Eq. (16), there exits a simple relationship between $\theta_t(x)$ and its r-conjugate.

Theorem 30 *Let $1/r$ be the inverse of r in U_n and let the integer a be as defined in Theorem 29. Then for all $t \in T^{n,q,-1}$ one has $\theta_{rt+a}(x) = \theta_t(x^{1/r})$ if and only if $rv = 1$ mod $2n$, whereas $\theta_{rt+a}(x) = \theta_t(-x^{1/r})$ if and only if $rv = 1$ mod $2n$, where $v = 1/r$ mod n.*

Proof If $\theta_{rt+a}(\beta) = 1$, then β is a zero of $P_{rt+a}^{-1}(x)$, say $\beta = \alpha\zeta^{rt+a} = \alpha^{r(2t+1)}$, where we used $\zeta = \alpha^2$. Let e be such that $\beta^e = \alpha\zeta^t = \alpha^{2t+1}$, which implies that β^e is a zero of $P_t^{-1}(x)$ and $\theta_t(\beta^e) = 1$. The condition on the integer e is true if and only if $\alpha^{er(2t+1)} = \alpha^{2t+1}$ or, equivalently, if and only if $(er-1)(2t+1) = 0 \bmod 2n$. If we require this to hold for all $t \in T^{n,q,-1}$, we must have $e = 1/r \bmod n$ and $er - 1 = 0 \bmod 2n$. So, $\theta_{rt+(r-1)/2}(\beta) = \theta_t(\beta^{1/r}) = 1$. If $\theta_{rt+(r-1)/2}(\beta) = 0$, then β is a zero of $P_u^{-1}(x)$, $u \neq rt + (r-1)/2$, which along similar lines leads to $\theta_{rt+(r-1)/2}(\beta) = \theta_t(\beta^{1/r}) = 0$. It follows from Theorem 2 (ii) that the first equality of the Theorem has been proven now. Putting $\beta = -\alpha\zeta^t = \alpha^{n+2t+1}$ leads to $(er-1)(2t+1) = 0 \bmod n$ for all $t \in T^{n,q,-1}$, yielding the second equality. □

Next, we introduce the notation (cf. (17) and (18))

$$Cy^{n,q,-1} := \{c_s^{-1}(x) | s \in S^{n,q,-1}\} \tag{23}$$

for the set of all negacyclonomials and

$$Id^{n,q,-1} := \{\theta_t(x) | t \in T^{n,q,-1}\}. \tag{24}$$

for the set of all primitive idempotent generators. Just like in Sect. 6, the group U_n induces a permutation group G' on the set (23), while the subgroup $H := \langle q \rangle$ of U_n contains all elements which induce the identity permutation. Because of the one-one correspondence between negacyclotomic cosets and irreducible polynomials, it follows from Theorem 29 (ii) that U_n also induces a permutation group G'' on the set $Id^{n,q,-1}$ of (24).

We next define, as the negacyclic counterpart of (20), for each positive divisor of $d \leq n$ of n

$$T_d^{n,q,-1} := \{t \in T^{n,q,-1} | (n, 2t+1) = d\}. \tag{25}$$

Underlying this definition, is that $(n, 2t+1) = d$ implies $\left(n, 2t'+1\right) = d$ for $t' := tq + (q-1)/2$, making the particular choice of t, as index of some negacyclotomic coset, irrelevant (cf. Eq. (6) with $l = (q-1)/2$. It also makes clear that the union of negacyclotomic cosets whose indices are in (25) contains all integers $i \in [0, n-1]$ with $(n, 2i+1) = d$, and also that

$$T^{n,q,-1} = \bigcup_d T_d^{n,q,-1}. \tag{26}$$

Just as in Sect. 6, the orbits of G'' in the set (24) are called *blocks of idempotents*. In Sect. 6 we defined the transformations $C_s^{n,q} \to C_{rs}^{n,q}$ and correspondingly $c_s(x) \to c_{rs}(x)$ for $r \in U_n$. In

the next we shall restrict the first transformation to those cyclotomic cosets which correspond to a negacyclonomial $c_s^{-1}(x)$. For odd n this concerns all $C_s^{n,q}$ (cf. Theorem 13 (i) with $k = 2$), but for even n this is not always true. Suppose $c_s^{-1}(x)$ is a negacyclonomial and let n be even. Then $r \in U_n$ is odd, and by applying Theorem 13 (i) again, it appears that $c_{rs}^{-1}(x)$ is also a negacyclonomial. So, for all n the transformation $s \to rs$ defines a permutation on the set (23). The orbits are called *blocks of negacyclonomials*. We are ready now to formulate and to prove the analogue of Theorem 25 for primitive idempotents of negacyclic codes.

Theorem 31 *The primitive idempotents of the negacyclic code $C^{n,q,-1}$, with q odd and $(n, q) = 1$, have the following properties.*

(i) The blocks of negacyclonomials can be identified as $B_d^{Cy} = \{c_s^{-1}(x) | s \in S_d^{n,q,-1}\}$, and the blocks of primitive idempotents as $B_d^{Id} = \{\theta_t(x) | 2t + 1 \in T_d^{n,q,-1}\}$ for all $d|n$.

(ii) The blocks B_d^{Cy} contain $\varphi(n/d)/m_d$ elements, while the blocks B_d^{Id} contain $\varphi(n/d)/m_{(d-1)/2}^{-1}$ elements for n odd, and $2\varphi(n/d)/m_{(d-1)/2}^{-1}$ for n even. The group $U_{n/d}$ acts transitively on both types of blocks.

Proof (i) Take some integer $s \in S^{n,q,-1}$. Then we have for any $r \in U_n$ that $rs \in U_n$, according to the arguments preceding this theorem. Since $(n, r) = 1$, the condition $(n, s) = d$ implies $(n, rs) = d$. This proves the first statement. The second statement follows from the lines preceding Eq. (26).

(ii) The size of the blocks B_d^{Cy} is derived in a similar way as Theorem 25 (ii). The negacyclotomic cosets with an index in $T_d^{n,q,-1}$ contain all integers $i \in [0, n-1]$ satisfying $(n, 2i + 1) = d$. Now, the equation $2x + 1 = u$ has a unique solutions in U_n for odd n, while it has two solutions, differing by $n/2$, for even n. So, the total number of such integers is equal to $\varphi(n/d)$ if n is odd, and to $2\varphi(n/d)$ if n is even. Since all these integers are contained in negacyclotomic cosets of size $m_{(d-1)/2}^{-1}$ the results follow. □

Example 32 Let $n = 20$, $q = 3$ and $\lambda = -1$.

There are six negacyclotomic cosets, $C_0^{20,3,-1} = (0, 1, 4, 13)$, $C_2^{20,3,-1} = (2, 7)$, $C_3^{20,3,-1} = (3, 10, 11, 14)$, $C_5^{20,3,-1} = (5, 16, 9, 8)$, $C_6^{20,3,-1} = (6, 19, 18, 15)$ and $C_{12}^{20,3,-1} = (12, 17)$.

Now, $P_0^{-1}(x) = x^4 + x^2 + x + 1$ is an irreducible divisor of $x^{20} + 1$. Let α be a zero of this polynomial of order 40. The other five irreducible factors are $P_2^{-1}(x) = x^2 - x - 1$, $P_3^{-1}(x) = x^4 + x^2 - x + 1$, $P_5^{-1}(x) = x^4 - x^3 + x^2 + 1$, $P_6^{-1}(x) = x^4 + x^3 + x^2 + 1$ and $P_{12}^{-1}(x) = x^2 - x - 1$, which have respectively α^5, α^7, α^{11}, α^{13} and α^{25} as zeros. Furthermore, the six negacyclonomials are $c_0^{-1}(x) = 1$, $c_1^{-1}(x) = x^1 + x^3 + x^9 - x^7$, $c_5^{-1}(x) = x^5 + x^{15}$, $c_2^{-1}(x) = x^2 + x^6 + x^{18} + x^{14}$, $c_4^{-1}(x) = x^4 + x^{12} - x^{16} - x^8$ and $c_{11}^{-1}(x) = x^{11} - x^{13} + x^{19} + x^{17}$. It follows that we can define the index sets $S^{20,3,-1} = \{0, 1, 2, 4, 5, 11\}$ and $T^{20,3,-1} = \{0, 2, 3, 5, 6, 12\}$. It will be obvious that $c_1^{-1}(x)$ and $c_{11}^{-1}(x)$ are each other's conjugate, while all other negacyclonomials are self conjugated. In order to determine the elements of the table $\mathrm{M}^{20,3,-1}$, we also need the irreducible polynomials contained in $x^{20} - 1$. These are $P_0(x) = x - 1$, $P_1(x) = x^4 - x^2 + x + 1$, $P_{10}(x) = x + 1$, $P_5(x) = x^2 + 1$, $P_4(x) = x^4 + x^3 + x^2 + x + 1$, $P_2(x) = x^4 - x^3 + x^2 - x + 1$ and $P_{11}(x) = x^4 + x^3 - x + 1$. The indices refer to the ζ-representation of the zeros, based on the zero $\zeta (= \alpha^2)$ of $P_1(x)$, which has order 20. By applying the rule that $\mu_{s,t}$ is equal to the sum of the s-powers of the zeros of $P_t^{-1}(x)$ we find for the idempotent table $\mathrm{M}^{20,3,-1}$, the rows of which are indexed respectively by 0, 1, 2, 4, 11, 5 and the columns by 0, 2, 3, 6, 12, 5.

$$\mathrm{M}^{20,3,-1} = \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 0 & 2 & 0 \\ 2 & 2 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

Next, by using relation (14), we derive the related table

$$\Xi^{20,3,-1} = \begin{bmatrix} 2 & 1 & 2 & 2 & 1 & 2 \\ 1 & 1 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 2 & 2 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

We collect the weights w_s, $s \in S^{20,3,-1}$, in a weight vector $\sigma = (1, 2, 2, 1, 2, 1) \in GF(3)^6$, and similarly the weights $1/m_t^{-1}$, $t \in T^{20,3,-1}$, in a weight vector $\tau = (1, 2, 1, 1, 2, 1) \in GF(3)^6$. With the help of these vectors one easily can verify the orthogonality relations in this case. The columns of $\Xi^{20,3,-1}$ provide us with the coefficients ξ_s^t in the expressions $\theta_t(x) = \sum_{s \in S^{20,3,-1}} \xi_s^t c_s^{-1}(x)$ for the primitive idempotents. These results are confirmed by the general method of Theorem 3, with $h(x) := P_t^{-1}(x)$ and $g(x) = (x^{20} + 1)/h(x)$. There are five non-empty index subsets $S_1^{20,3,-1} = \{1, 11\}$, $S_2^{20,3,-1} = \{2\}$, $S_4^{20,3,-1} = \{4\}$, $S_5^{20,3,-1} = \{3\}$ and $S_{20}^{20,3,-1} = \{0\}$, and so there are that many blocks of negacyclonomials. On the other hand, there are two non-empty index subsets $T_1^{20,3,-1} = \{0, 3, 5, 6\}$ and $T_5^{20,3,-1} = \{2, 12\}$. Hence, there are only two blocks of idempotents, i.e. B_1^{Id} containing $2\varphi(20/1)/m_0^{-1} = 16/4 = 4$ elements, and B_5^{Id} with $2\varphi(20/5)/m_2^{-1} = 4/2 = 2$ elements. Finally, we remark that there are four self conjugated negacyclonomials, whereas there are no self conjugated negacyclotomic cosets and therefore no self conjugated idempotent generators. This observation shows that Theorem 25 (iv) is not always true in the negacyclic case. Finally, we illustrate Theorem 30 by two small examples. For $r = 11$ the transformation $t \to rt + (r - 1)/2$ yields the following permutation of primitive idempotents $\theta_0(x) \to \theta_5(x)$, $\theta_2(x) \to \theta_2(x)$, $\theta_3(x) \to \theta_6(x)$, $\theta_6(x) \to \theta_3(x)$, $\theta_{12}(x) \to \theta_{12}(x)$, $\theta_5(x) \to \theta_0(x)$. One can easily verify that the transformation $\theta_t(x) \to \theta_t(x^{11})$ gives the same permutation. One can accomplish this by applying the relations $c_s^{-1}(x^{11}) = c_s^{-1}(x)$, $s \in \{0, 4, 5\}$, $c_2^{-1}(x^{11}) = -c_2^{-1}(x)$, $c_1^{-1}(x^{11}) = c_{11}^{-1}(x)$and $c_{11}^{-1}(x^{11}) = c_1^{-1}(x)$ to the expression for $\theta_t(x)$ as follows from the table $\Xi^{20,3,-1}$. In a similar way one can verify that $\theta_{3t+1}(x) = \theta_t(-x^7)$ for all $t \in T^{20,3,-1}$, by using $c_s^{-1}(-x^3) = c_s^{-1}(x)$, $s \in \{0, 2, 4\}$, and $c_s^{-1}(-x^3) = -c_s^{-1}(x)$, $s \in \{1, 5, 11\}$. Since $11.11 = 1 \bmod 40$ and $7.3 = 1 \bmod 20$, these results are in agreement with Theorem 30. □

For more examples of primitive idempotents of constacyclic and negacyclic codes we refer to [10, 16, 22, 26–28].

Acknowledgements I am greatly indepted to the unknown referees for their careful reading of the manuscript and for their useful suggestions.

References

1. Bakshi G.K., Raka M.: A class of constacyclic codes over a Finite Field. Finite Fields Appl. **18**, 362–377 (2012).
2. Berlekamp E.: Algebraic Coding Theory. Mc Graw-Hill book Company, New York (1968).
3. Berman S.D.: Semisimple cyclic and abelian codes. Kibernetika **3**, 21–30 (1967).
4. Bierbrauer J.: Algebraic Coding Theory. Chapman and Hall, Boca Raton (2005).
5. Chen B., Fan Y., Lin L., Liu H.: Constacyclic codes over finite fields. Finite Fields Appl. **18**, 1217–1231 (2012).
6. Curtis C.W.: Reiner I: Representation Theory of Finite Groups and Associative Algebras. Interscience, New York (1962).
7. Dornhoff L.: Group Representation Theory.Part A and B. Marcel Dekking Inc., New York (1972).
8. Dougherty S.T.: Cyclic and constacyclic codes. In: Dougherty S.T. (ed.) Algebraic Coding Theory over Finite Commutative Rings, pp. 83–100. SpringerBriefs in MathematicsSpringer, Cham (2017).
9. Fan Y., Zhang L.: Galois self dual codes. Des. Codes Cryptogr. **84**, 473–493 (2017).
10. Ferraz R.A., Milies C.P.: Idempotents in group algebras and minimal abelian codes. Finite Fields Appl. **13**, 382–393 (2007).
11. Hughes G.: Constacyclic codes, cocycles and $u + v|u - v$ construction. IEEE Trans. Inf. Theory **46**, 674–680 (2000).
12. Hughes G.: A Vandermonde code construction. IEEE Trans. Inf. Theory **47**, 2995–2998 (2001).
13. Isaacs I.M.: Character Theory of Finite Groups. Acadamic Press Inc., New York (1976).
14. Jensen J.: A class of constacyclic codes. IEEE Trans. Inf. Theory **40**, 951–954 (1994).
15. Lang S., Blackford T.: $Z_{p^{k+1}}$-Linear codes. IEEE Trans. Inf. Theory **48**, 2592–2605 (2002).
16. Li F., Yue Q.: The primitive idempotents and weight distributions of irreducible constacyclic codes. Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0356-2.
17. Lidl R.L., Niederreiter H.: Introduction to Finite Fields and their Applications, rev edn. Cambridge University Press, Cambridge (1997).
18. Mac Williams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. North Holland, Amsterdam (1977).
19. Pless V.: Introduction to the Theory of Error-Correcting Codes, 2nd edn. Wiley, New York (1990).
20. Radkova D.: Constacyclic Codes as Invariant Subspaces, Dissertation. Delft University of Technology, Delft. ISBN 978-90-9023852-4 (2009).
21. Radkova D., van Zanten A.J.: Constacyclic codes as invariant subspaces. Linear Algebra Appl. **430**, 855–864 (2009).
22. Sharma A., Bakshi G.K., Dumir V.C., Raka M.: Cyclotomic numbers and primitive idempotents in the ring $GF(q)[x\}/\left(x^{p^n}-1\right)$. Finite Fields Appl. **10**, 653–673 (2004).
23. van Gelder I., Olteanu G.: Finite group algebras of nilpotent groups: a complete set of orthogonal primitive idempotents. Finite Fields Appl. **17**, 157–165 (2011).
24. van Lint J.H.: Coding Theory. Springer, New York (1971).
25. van Zanten A.J., Bojilov A., Dodunekov S.M.: Generalized residue and t-residue codes and their idempotent generators. Des. Codes Crypt. **75**, 315–334 (2015).
26. van Zanten A.J.: Negacyclotomic cosets and negacyclonomials of negacyclic codes, TR 2015, TiCC, Tilburg University. http://www.tilburguniversity.edu/research/institutes-and-research-programs/cc/technical-reports.
27. van Zanten A.J.: Orthogonality and conjugation for the idempotents of constacyclic codes, TR 2016, TiCC, Tilburg University. http://www.tilburguniversity.edu/research/institutes-and-research-programs/cc/technical-reports.
28. Wu Y., Li F.: Primitive idempotents of irreducible cyclic codes and self-dual cyclic codes over Galois rings. Discret. Math. (in press).