Constacyclotomic Cosets and Constacyclonomials of Constacyclic Codes
van Zanten, A.J.

Document version:
Publisher's PDF, also known as Version of record

Publication date:
2015

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
- Users may download and print one copy of any publication from the public portal for the purpose of private study or research
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright, please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Constacyclotomic Cosets and Constacyclonomials of Constacyclic Codes

TiCC, Tilburg University

A.J. van Zanten
Abstract

This report is a continuation of a previous report which dealt with generating and cyclonomic polynomials of constacyclic codes. Now, we introduce and investigate constacyclotomic cosets, generalizing the well-known cyclotomic cosets, and also constacyclonomials which generalize cyclonomials. These notions and their properties seem to be useful for the study of idempotent generators of constacyclic codes, especially for the derivation of orthogonality relations between primitive idempotents. At the end of the report we point out how one can possibly generalize the approach we developed earlier for cyclic codes.
Contents

1. Introduction p. 4
2. Constacyclotomic cosets p. 9
3. Cyclonomials for constacyclic codes p. 17
4. Suggestions for further study of constacyclic idempotents p. 29
References p. 35
1. Introduction

This report is a continuation of [6], where we studied the idempotent generating polynomials of constacyclic codes. The \( \lambda \)-constacyclic code \( C := \langle g(x) \rangle \) modulo \( x^n - \lambda \) is generated by some divisor \( g(x) \) of the polynomial \( x^n - \lambda \), \( \lambda \in GF(q)^\times \). So, \( C \) is a set of polynomials in the ring \( R_{n,\lambda} := GF(q)[x]/x^n - \lambda \). For \( \lambda = 1 \) one obtains cyclic codes which are well-known. Let

\[
x^n - \lambda = \prod_{i \in T_{n,q,\lambda}} P_{i,\lambda}^T(x)
\]

be the decomposition of \( x^n - \lambda \) into monic irreducible polynomials over \( GF(q) \), where \( T_{n,q,\lambda} \) (or shortly \( T^\lambda \) when this will not give rise to confusion) is some index set. Throughout this report we assume that \( (n, q) = 1 \), like in most articles on (consta-)cyclic codes. Under this assumption \( x^n - \lambda \) has no multiple zeros and hence the irreducible polynomials have no common zeros. If \( f_t^{(\lambda)}(x) := (x^n - \lambda) / P_t^{(\lambda)}(x), t \in T^\lambda \), then the code \( < f_t^{(\lambda)}(x) > \) modulo \( x^n - \lambda \) is called a minimal or irreducible \( \lambda \)-constacyclic code. Moreover, the code \( < P_t^{(\lambda)}(x) > \) modulo \( x^n - \lambda \) is called a maximal \( \lambda \)-constacyclic code. An idempotent generating polynomial (shortly idempotent generator) \( e_{n,\lambda}^q(x) \in R_{n,\lambda}^q \) is a polynomial which generates some \( \lambda \)-constacyclic code of length \( n \) over \( GF(q) \), with the property that

\[
e_{n,\lambda}^q(x)^2 = e_{n,\lambda}^q(x).
\]

Every constacyclic code in \( R_{n,q}^\lambda \) has a unique idempotent generator (cf. [3,4,5]). If no confusion will arise, we shall omit one or more of the indices \( n, q \) and \( \lambda \). The idempotent generators of the minimal codes \( < f_t^{(\lambda)}(x) > \) are denoted by \( \Theta_t(x) \) and those of the maximal codes by \( \Theta_t(x), t \in T^\lambda \). The polynomials \( \Theta_t(x) \) are often called primitive idempotent polynomials. It is known from the literature (cf. [3,4,5]) that any idempotent generating polynomial of a cyclic code (for fixed values of \( n, q \) and \( \lambda \) can be written as a linear combination of the primitive idempotents. They are related to the polynomials \( \Theta_t(x) \) by the equality \( \Theta_t(x) = 1 - \Theta_t(x) \). If \( \lambda = 1 \) this relation is well known (for proofs, see e.g. [3,4,5]). Since in this report we study especially \( \lambda \)-constacyclic codes with \( \lambda \neq 1 \), we shall present an explicit proof for this relation and also for a few other relations for primitive idempotents.

Let \( \alpha_1, \alpha_2, \ldots, \alpha_n \) be the zeros of \( x^n - \lambda \), lying in some extension field of \( GF(q) \). We introduce the notion of zeros of a constacyclic code being the zeros \( \alpha_1, \alpha_2, \ldots, \alpha_r \), where \( r \) is the degree of the defining polynomial of such a code. Its nonzeros are the remaining \( \alpha_t \). As a result we have that the zeros of the primitive idempotent \( \Theta_t(x) \) are the nonzeros of the irreducible polynomial \( P_t^{(\lambda)}(x) \) and vice versa. From (2) it follows that the value of \( e(\alpha_t) \) is either zero or one, the zeros of \( \Theta_t(x) \) are equal to the zeros of \( P_t^{(\lambda)}(x) \) and its nonzeros are equal to the nonzeros of \( P_t^{(\lambda)}(x) \). If \( \alpha \) is some zero of \( P_t^{(\lambda)}(x) \) lying in some extension field of \( GF(q) \), then the zeros of \( P_t^{(\lambda)}(x) \) can be written as \( \alpha, \alpha^q, \ldots, \alpha^{q^{r-1}} \), where \( r_t \) is the degree of \( P_t^{(\lambda)}(x) \), while the other \( n-r_t \) zeros of \( x^n - \lambda \) are its
nonzeros. Before we present a few properties of the primitive idempotent generators \( \theta_i(x) \), \( t \in T^\lambda \), we shall define the index set \( T^\lambda \) more concretely. In [6, Theorem 3] it is shown that the \( n \) zeros of \( x^n - \lambda \) can be written as \( \alpha \zeta^i \), \( i \in \{0,1,\ldots,n-1\} \), where \( \zeta \) is a primitive \( n \)th root of unity and \( \alpha \) is a fixed element from the same extension field of \( GF(q) \) satisfying \( \alpha^n = \lambda \). We assume that \( \alpha \) and \( \zeta \) are lying in the same extension field of \( GF(q) \), say in \( F := GF(q)(\alpha, \zeta) \). We know that \( \alpha \zeta^i \) and \( \alpha \zeta^{i+1} := (\alpha \zeta^i)^q \) are zeros of the same irreducible polynomial contained in \( x^n - \lambda \). So, when having chosen an appropriate \( \alpha \), one can take for \( T^\lambda \) a subset of the set \( \{0,1,\ldots,n-1\} \), as we shall see later. 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 choose \( \alpha = 1 \), and hence we obtain the usual set of indices representing the cyclotomic cosets modulo \( n \) with respect to \( q \), also called the \( q \)-cyclotomic cosets modulo \( n \).

**Theorem 1**

Let \( q \) be a prime power, \( n \) an integer with \( (n, q) = 1 \) and let \( \lambda \in GF(q)^* \) have order \( k \). For the primitive idempotent generators \( \theta_i(x) \), \( t \in T^\lambda \), we have:

(i) \( \theta_i(x)\theta_u(x) = 0 \), if \( t \neq u \);

(ii) \( \theta_i(x) + \theta_2(x) + \ldots + \theta_{t} (x) \) is the idempotent generator of the constacyclic code with generator \( f^{(k)}_{n}(x)f^{(k)}_{n}(x)\ldots f^{(k)}_{n}(x) \);

(iii) \( \sum_{t \in T} \theta_i(x) = 1 \);

(iv) \( \theta_i(x) = 1 - \theta_i(x) \);

(v) \( \theta_i(\alpha \zeta^i) \) is equal to 1 if \( i \in \{t, tq + (q - 1) / k, tq^2 + (q^2 - 1) / k, \ldots, tq^{q-1} + (q^{q-1} - 1) / k \} \) and equal to 0 otherwise.

**Proof**

(i) Let \( \theta_i(x) \) generate the code \( C_i \) and \( \theta_u(x) \) the code \( C_u \) in \( R^\lambda_{n,q} \). Then \( \theta_i(x)\theta_u(x) \) generates the code \( C_i \cap C_u \). Since for \( t \neq u \) the zero polynomial is the only common element of \( C_i := < f^{(k)}_{i}(x) > \) and \( C_u := < f^{(k)}_{u}(x) > \) in \( R^\lambda_{n,q} \), it follows that \( \theta_i(x)\theta_u(x) = 0 \).

(ii) The code \( C_i + C_u \) in (i) has the idempotent generator \( \theta_i(x) + \theta_2(x) + \theta_3(x)\theta_i(x) = \theta_i(x) + \theta_u(x) \).

Applying this relation repeatedly yields (ii).

(iii) Since \( \sum_{t \in T} \theta_i(x) \) is the set of all words of length \( n \) in \( R^q_{n,\lambda} \) and 1 is the idempotent generator of this set, this relation follows from (ii).

(iv) This relation is an immediate consequence of (iii);

(v) This is a consequence of the fact that the nonzeros of \( \theta_i(x) \) are the zeros of \( P^{(k)}_{i}(x) \). Since the only values \( \theta_i(\alpha \zeta^i) \) can have are 0 and 1 because of (2), the nonzeros must be 1. So, \( \theta_i(\alpha \zeta^i) = 1 \) if and only if \( \alpha \zeta^i \) is equal to one of the zeros of \( P^{(k)}_{i}(x) : \alpha \zeta^i \), \( \alpha \zeta^{iq+(q-1)q} \), \ldots,
\( \alpha \zeta^{q^{-1}-(q^{-1}-1)/k} \), where \( r_i \) stands for the degree of \( P_i^{(x)}(x) \). Remember that \( \lambda^k = 1 \) implies that \( k \) divides \( q-1 \) and hence \( q^j - 1 \) for all integer values of \( j \).

\[ \text{Remark} \]

If \( x^e - \lambda \) has order \( e \), then \( x^n - \lambda \) is a divisor of \( x^e - 1 \) and \( e \) is the smallest positive exponent with this property (cf. [2, Theorems 4 and 8]). Let \( F \) be the splitting field of \( x^e - \lambda \), then \( F \) contains \( \alpha \) and \( \zeta \). From the identity \( \theta_j(x)^2 = \theta_j(x) \) in \( R_{e,1}^q \) it follows, for any primitive idempotent polynomial \( \theta_j(x) \), that \( \theta_j(\beta^i) \in \{0,1\} \) if \( \beta \) is a primitive \( e^{\text{th}} \) power of unity and for all integers \( i \), \( 0 \leq i \leq e-1 \).

This property holds in particular for those \( \beta^i \) which are zeros of \( x^n - \lambda \), i.e. for \( i = 1 + je/n \), \( 0 \leq j \leq n-1 \). Even more in particular, the property holds for those \( \beta \)-powers which are zeros of some irreducible factor of \( x^n - \lambda \) and which are equal to the elements \( \alpha \zeta^i \), \( i \in \{t, tq + (q-1)/k, \ldots, tq^{q-1} + (q^{-1}-1)/k\} \), mentioned in Theorem 1 (v). In Section 2 this index set will be called a constacyclicotomic coset, meant to be a generalization of the notion of cyclotomic coset.

\[ \square \]

\[ \text{Example 1} \]

We consider the case \( n = 6 \), \( q = 5 \) and \( \lambda = 2 \). We know (cf. [6, Example 2]) that \( x^6 - 2 = (x^2 + 2)(x^2 - x + 2)(x^2 + x + 2) \). We define \( \alpha \) as a zero of \( x^2 + 2 \), and for the primitive \( 6^{\text{th}} \) root of unity \( \zeta \) we take a zero of the irreducible polynomial \( x^2 - x + 1 \). In [6, Example 2] we derived that the idempotent generator of the maximal code generated by \( x^2 + 2 \) is given by the polynomial \( \mathcal{G}(x) = 2x^4 + x^2 - 1 \). Since \( \alpha^2 = -2 \), we immediately find \( \mathcal{G}(\alpha) = 2\alpha^4 + \alpha^2 - 1 = 0 \), and so \( \mathcal{G}(\alpha) = 1 - \mathcal{G}(\alpha) = 1 \). Similarly, we get \( \mathcal{G}(\alpha^5) = \mathcal{G}(\alpha^5) = 1 \). The four other values of \( \mathcal{G}(x) \) (and hence of \( \theta(x) \)) follow in the same way. E.g. we find \( \mathcal{G}(\alpha^4 \zeta^i) = 3\zeta^i - 2\zeta^2 - 2\zeta + 1 = 1 \) and so \( \mathcal{G}(\alpha^4 \zeta^i) = 0 \). Furthermore, \( \mathcal{G}(\alpha^2 \zeta^i) = 0 \), \( \mathcal{G}(\alpha^4 \zeta^i) = 0 \) and \( \mathcal{G}(\alpha^5 \zeta^i) = 0 \). These results illustrate Theorem 1 (v). Because \( \alpha \zeta^0 = \alpha \) is a zero of \( x^2 + 2 \), we should denote the corresponding idempotent generators by index 0, i.e. \( \mathcal{G}_0(x) = 2x^4 + x^2 - 1 \) and \( \mathcal{G}_0(x) = 1 - \mathcal{G}_0(x) \). Consistently, we have to write \( \mathcal{G}_1(x) = 2x^5 - x^4 + 2x^2 + x - 1 \) and \( \mathcal{G}_1(x) = 3x^5 - x^4 + 2x^2 + 3x - 1 \) for the idempotent generators of the maximal codes defined by \( x^2 - x + 2 \) and \( x^2 + x + 2 \), respectively. The subset \( T^{6,5,2} \subset \{0,1,2,3,4,5\} \) is \( T^{6,5,2} = \{0,1,4\} \). We remark that in [6] we provisionally used the indexing \( \mathcal{G}_1(x) \), \( \mathcal{G}_2(x) \) and \( \mathcal{G}_3(x) \) for the above idempotents.

\[ \square \]

In the next theorem we present a few other properties of idempotent generators which are well known for cyclic codes, and which hold as well for constacyclic codes. The proofs are completely similar.

Actually, all properties mentioned in Theorems 1 and 2 are special cases of the general theory of idempotents for semi-simple algebras (cf. [1,3]).
Theorem 2
Let \( e(x) \) be the unique idempotent generator of some \( \lambda \)-constacyclic code \( C := \langle g(x) \rangle \). Then \( e(x) \) has the following properties:
(i) \( e(\alpha \zeta^i) = 0 \) if and only if \( g(\alpha \zeta^i) = 0 \);
(ii) there exist polynomials \( p(x) \) and \( q(x) \) such that in \( R^q_{n,\lambda} \) one has \( e(x) = p(x)g(x) \) and \( g(x) = q(x)e(x) \);
(iii) \( c(x) \in C \) if and only if \( e(x)c(x) = c(x) \).

Proof
(i) and (ii) are immediate consequences of the definitions of \( g(x) \) and \( e(x) \).
(ii) Since \( e(x)c(x) = e(x)r(x) = e(x)r(x) = c(x) \).

Theorem 3
Let \( \langle g(x) \rangle \) be a \( \lambda \)-constacyclic code and \( \langle h(x) \rangle \) be the dual \( \lambda \)-constacyclic code defined by the polynomial identity \( g(x)h(x) = x^n - \lambda \) in \( GF(q)[x] \). If \( e(x) \) and \( e^\perp(x) \), respectively, are their idempotent generators, then one has \( e(x) + e^\perp(x) = 1 \).

Proof
Although this result immediately follows from Theorem 1 (ii) and (iii) (Theorem 1 (iv) is a special case), we give also an alternative proof by applying the general expression for the idempotent generator of a code \( \langle g(x) \rangle \), i.e. \( e(x) = (n\lambda)^{-1} x g'(x)h(x) \) (cf. [6, Theorem 5 (ii)]). Similarly, we have \( e^\perp(x) = (n\lambda)^{-1} x g'(x)h(x) \), and hence \( e(x) + e^\perp(x) = (n\lambda)^{-1} x (h'(x)g(x) + g'(x)h(x)) \). In \( GF(q)[x] \) it follows from \( g(x)h(x) = x^n - \lambda \), that \( h'(x)g(x) + h(x)g'(x) = nx^{n-1} \). Substituting this in the previous relation and reducing modulo \( x^n - \lambda \) yields the equality of the Theorem, which holds in \( R^q_{n,\lambda} \).

Theorem 4
Let the order of the polynomial \( x^n - \lambda \), \( \lambda \in GF(q)^* \), be equal to \( e \) and let \( \alpha \) be a zero of this polynomial which is also of order \( e \) in some extension field \( F \) of \( GF(q) \).
(i) If \( k := \frac{e}{|n|} \), then \( \zeta := \alpha^k \) is a primitive \( n^e \) root of unity in the extension field \( GF(q)(\alpha) \).
(ii) The order of \( \lambda \) in \( GF(q) \) is equal to \( k \).
(iii) The \( n \) zeros of \( x^n - \lambda \) can be written as \( \alpha^{1+ik} \), \( 0 \leq i \leq n-1 \).
(iv) The \( n \) zeros of \( x^n - \lambda \) can be written as \( \alpha^{1+i} \zeta^k \), \( 0 \leq i \leq n-1 \).
(v) If \( l := (q-1)/k \) and if \( \alpha^{1+ik} \) is a zero of a certain irreducible polynomial contained in \( x^n - \lambda \), then \( \alpha^{1+jk} \), with \( j = l+iq \mod e \), is a zero of that same polynomial.

Proof
Firstly, we remark that for any polynomial one can find a zero the order of which equals the order of that polynomial (cf. Theorem 3 (viii)).
(i) From the definition of the notion of order it follows that \( \alpha \) is a primitive \( e^{th} \) root of unity and also that \( k \) is a divisor of \( e \). Hence, \( \zeta \) is a primitive \( n^{th} \) root of unity.

(ii) Since \( \alpha^n = \lambda \) and \( \alpha^{kn} = 1 \), one has \( \lambda^k = 1 \). Assume that the order of \( \lambda \) is less than \( k \). Then \( k \) has a proper divisor \( a \) such that \( \lambda^a = 1 \), and hence \( \alpha^{an} = 1 \) with \( an < e(=kn) \). This contradicts the minimality of \( e \) with respect to this property. So, \( \text{ord}_q(\lambda) = k \).

(iii) and (iv) Both statements now follow immediately (cf. also Theorem 3 (v) in [6]).

Example 2
Again we take the parameter values \( n = 6 \), \( q = 5 \), \( \lambda = 2 \) like in Example 1. The order \( k \) of \( \lambda \) is equal to 4. Contrary to that example however, we now define \( \alpha \) as a zero of the irreducible polynomial \( x^6 - x + 2 \). So the defining equation of \( \alpha \) is \( \alpha^2 = \alpha - 2 \). One can easily verify that this \( \alpha \) has order 24 (= \( kn \)) which is also the order of \( x^6 - 2 \) (cf. Theorem 5). Now Theorems 4 and 5 tell us that the six zeros of this polynomials are \( \alpha^{1+4i} \), \( 0 \leq i \leq 5 \). From Theorem 4 (v) we derive that \( \alpha \) and \( \alpha \zeta^i \) (\( \zeta = \alpha^4 \)) are zeros of \( x^6 - x + 2 \), \( \alpha \zeta^2 \) and \( \alpha \zeta^5 \) (\( = -\alpha \)) of \( x^2 + 2 \) and \( \alpha \zeta^3 \) and \( \alpha \zeta^4 \) of \( x^2 + x + 2 \). The primitive idempotent which corresponds to \( x^2 - x + 2 \) is \( \theta_0(x) = -2x^5 + x^4 - 2x^2 - 2x + 2 \). The index 0 now indicates that \( \alpha \zeta^0 \) is a zero of the corresponding irreducible polynomial. Substituting \( \alpha \) and \( \alpha \zeta \) yields \( \theta_0(\alpha) = \theta_0(\alpha \zeta) = 1 \), and

\( \theta_0(\alpha \zeta^2) = \theta_0(\alpha \zeta^3) = \theta_0(\alpha \zeta^4) = \theta_0(\alpha \zeta^5) = 0 \) which is in accordance with Theorem 1 (v).

Example 3
We continue Example 2 and now consider the factorization

\[ x^{24} - 1 = (x^6 - 2)(x^6 - 4)(x^6 - 3)(x^6 - 1). \]

Since \( \alpha \), as defined in Example 2, is a zero of order 24 of the polynomial \( x^6 - x + 2 \) which is a divisor of \( x^6 - 2 \), \( \alpha \) is a primitive \( 24^{th} \) root of unity in some extension field of \( GF(5) \). Hence, \( \zeta = \alpha^4 \) is a primitive \( 6^{th} \) root of unity. The six zeros of \( x^6 - 2 \) can be written as \( \alpha^{1+4i} \), with \( i \in \{0,1,\ldots,5\} \). Likewise, the zeros of \( x^6 - 4 \) can be written as \( \alpha^{2+4i} \), the zeros of \( x^6 - 3 \) as \( \alpha^{3+4i} \) and the zeros of \( x^6 - 1 \) as \( \alpha^{4i} \). More in particular one has (cf. also [6, Example 8]):

\[ x^6 - 2 = (x^2 + 2)(x^2 - x + 2)(x^2 + x + 2) = \]

\[ (x - \alpha^9)(x - \alpha^{21})(x - \alpha^1)(x - \alpha^5)(x - \alpha^{13})(x - \alpha^{17}), \]

\[ x^6 - 4 = (x + 2)(x - 2)(x^2 + 2x - 1)(x^2 - 2x - 1) = \]

\[ (x - \alpha^{18})(x - \alpha^6)(x - \alpha^{14})(x - \alpha^{22})(x - \alpha^2)(x - \alpha^{10}), \]

\[ x^6 - 3 = (x^2 - 2)(x^2 + 2x - 2)(x^2 - 2x - 2) = \]

\[ (x - \alpha^3)(x - \alpha^{15})(x - \alpha^9)(x - \alpha^{23})(x - \alpha^7)(x - \alpha^{11}), \]
\[ x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) = \\
(x - \alpha^0)(x - \alpha^{12})(x - \alpha^8)(x - \alpha^{16})(x - \alpha^4)(x - \alpha^{20}) \]

In [6] we noticed that for \( \lambda = 1 \), i.e. in the case of cyclic codes, the set \( T^{n, q, \lambda} \) (\( \equiv T^\lambda \)) can be chosen such that it consists of the indices of the \( q \)-cyclotomic cosets modulo \( n \). In order to generalize that kind of indexing, we present the next theorem.

**Theorem 5**

Let the order of \( x^n - \lambda \), \( \lambda \in GF(q)^* \), be equal to \( e \) and let the order of \( \lambda \) in \( GF(q) \) be equal to \( k \), \( 1 \leq k \leq q-1 \).

(i) \( x^e - 1 = \prod_{j=0}^{k-1} (x^n - \lambda^j) \) and \( e = kn \).

(ii) There exists a primitive \( e^{th} \) root of unity \( \alpha \) in some extension field \( F \) of \( GF(q) \) such that it is a zero of \( x^n - \lambda \).

(iii) For any \( j \), \( 0 \leq j \leq k-1 \), the \( n \) zeros of the polynomial \( x^n - \lambda^j \) can be written as \( \alpha^{j+ik} \), \( 0 \leq i \leq n-1 \).

**Proof**

(i) If the order of \( x^n - \lambda^j \) is \( e_j \), \( 0 \leq j \leq k-1 \), then \( e = [e_0, e_1, ..., e_{k-1}] \) (cf. [2, Theorem 3.9]). So, \( e_j | e \). Now, the order of \( \lambda \) is \( k \), and hence the order \( k_j \) of \( \lambda^j \) is a divisor of \( k \) for all \( j \). If \( \alpha_j \) is a zero of \( x^n - \lambda^j \), then \( \alpha_j^{k_j} = 1 \), hence \( e_j | k_j n \), and since \( k_j | q-1 \), we conclude that \( e_j | (q-1)n \).

Assume that \( (e_j, q) \neq 1 \). Since \( (q-1, q) = 1 \) and also \( (n, q) = 1 \) by assumption, we have a contradiction. So, \( (e_j, q) = 1 \) for all \( e_j \), and therefore \( (e, q) = 1 \). Thus, we may apply Theorem 7 of [6], yielding the two relations in (i).

(ii) From the proof of (i) it follows that all \( e_j \), \( 0 \leq j \leq k-1 \), are divisors of \( e = kn = e \). So, there exists at least one zero of \( x^n - \lambda \) which has order \( e \) in \( F \).

(iii) From \( \alpha^n = \lambda \), it follows that \( \alpha^{kn} = \lambda^j \). We know already from [6] that the zeros of \( x^n - \lambda \) can be written as \( \alpha^{j+ik} \), \( 0 \leq i \leq n-1 \). Replacing \( \alpha \) by \( \alpha^j \) gives the expression in (iii).

\[ \square \]

2. Constacyclotomic cosets

We now introduce \( q \)-cyclotomic cosets modulo \( e \), i.e. for any \( t \in T^{e, q, \lambda} = \{0, 1, ..., e-1\} \), we define

\[ C_t^{e, q, \lambda} := \{t, tq, ..., tq^{m_t-1}\} \mod e \] \hspace{1cm} (3)

where \( m_t \) is the minimal positive integer such that
Because of (3) and (4), we have \( C_{tq}^{n-1} = C_{tq}^{n-1} = \ldots = C_{tq}^{n-1} \). Like for cyclotomic cosets modulo \( n \), we usually shall take the least value of \( t, tq, \ldots, tq^{m-1} \) as index for a particular coset.

Let the polynomial \( x^n - \lambda \) have order \( e \). Let \( \alpha \) be a primitive \( e^{th} \) root of unity, where \( e = kn, k \equiv \text{ord}_q (\lambda) \) which is also a zero of \( x^n - \lambda \) (cf. Theorem 5). Then \( \zeta = \alpha^k \) is a primitive \( n^{th} \) root of unity and the \( n \) zeros of \( x^n - \lambda \) can be written as \( \alpha, \alpha^{1+k}, \ldots, \alpha^{1+(n-1)k} \). The \( n \) exponents can be partitioned into a number of cyclotomic cosets defined in (3). More generally, we can do the same for the polynomial \( x^n - \lambda^j \), \( j \in [0,1,\ldots,k-1] \). Since \( \lambda^j \) is a zero of \( x^n - \lambda^j \), the \( n \) zeros of this polynomial can be written as \( \alpha^j, \alpha^{j+k}, \ldots, \alpha^{j+(n-1)k} \). When doing so respectively for all \( j \)-values, we obtain all cyclotomic cosets defined in (3) precisely once.

**Example 4**

The three irreducible polynomials contained in \( x^6 - 2 \) are \( x^2 + 2 \), \( x^2 - x + 2 \) and \( x^2 + x + 2 \) (cf. Example 3). They respectively correspond to the cyclotomic cosets \( C_{9,21}^{24,5,1} = \{9, 21\} \), \( C_{1,5}^{24,5,1} = \{1, 5\} \) and \( C_{13,17}^{24,5,1} = \{13, 17\} \). Consequently, we have for \( x^6 - 2 = \prod_{t \in T_2} P_t^{(2)}(x) \), with respect to this kind of indexing, a set \( T_2 = T_{24,5,1}^{24,5,1} \subset T_{24,5,1}^{24,5,1} \) with \( T_2^{24,5,1} = \{1, 9, 13\} \).

Similarly, we have for \( x^6 - 4 = \prod_{t \in T_4} P_t^{(4)}(x) \), \( T_4 = T_{24,5,1}^{24,5,1} = \{2, 6, 14, 18\} \), where the indices stand for the cyclotomic cosets \( C_{2,10}^{24,5,1} = \{2, 10\} \), \( C_6^{24,5,1} = \{6\} \), \( C_{14,22}^{24,5,1} = \{14, 22\} \) and \( C_{18,18}^{24,5,1} = \{18\} \). These cosets correspond respectively to the irreducible polynomials \( x^2 - 2x - 1 \), \( x^2 + 2x - 1 \) and \( x^2 + x + 2 \). For \( x^6 - 3 = \prod_{t \in T_3} P_t^{(3)}(x) \), we have \( T_3 = \{3, 7, 19\} \), with \( C_{3,15}^{24,5,1} = \{3, 15\} \), \( C_{19,23}^{24,5,1} = \{19, 23\} \), \( C_{7,11}^{24,5,1} = \{7, 11\} \), corresponding respectively to \( x^2 - 2 \), \( x^2 + 2x - 2 \) and \( x^2 - 2x - 2 \). Finally, for \( x^6 - 1 = \prod_{t \in T_1} P_t^{(1)}(x) \), we have \( T_1 = \{0, 4, 8, 12\} \), and \( C_0^{24,5,1} = \{0\} \), \( C_4^{24,5,1} = \{4, 20\} \), \( C_8^{24,5,1} = \{8, 16\} \), \( C_{12}^{24,5,1} = \{12\} \) which correspond to \( x - 1 \), \( x^2 - x + 1 \), \( x^2 + x + 1 \) and \( x + 1 \) respectively.

The above method of indexing is most relevant if one is interested in all irreducible polynomials which are contained in the polynomials \( x^n - \lambda^j \), \( j \in [0,1,\ldots,k-1] \), where \( k \) is the order of \( \lambda \) in \( GF(q) \). The indices are taken from the set \( \{0, 1, \ldots, e-1\} \) (cf. also the end of Section 3). When one is focussed only on the polynomial \( x^n - \lambda \) itself, one would prefer indices from the set \( \{0, 1, \ldots, n-1\} \). We can accomplish this by applying the fact that the zeros of this polynomial can be written as \( \alpha\zeta^i \), \( i \in \{0, 1, \ldots, n-1\} \), where \( \alpha \) is some arbitrarily chosen zero of \( x^n - \lambda \) and where \( \zeta \) is a primitive \( n^{th} \) root of unity. In particular, if \( \alpha \) has order \( e = kn \), we have that \( \zeta = \alpha^k \). (cf.
Theorems 4 (v) and 5 (iii). We introduce the integer \(l := (q-1)/k\), and we define subsets of \(\{0,1,\ldots,n-1\}\) as follows

\[
C^m_{t,q,\lambda} := \{c_0(=t),c_1,\ldots,c_{m^k-1}\},
\]

\[
c_{i+1} = c_i q + l \mod n, \ 0 \leq i \leq m^k - 2,
\]

where \(m^k\) is defined as the smallest positive integer satisfying \(c_{m^k-1} q + l = c_0\).

Theorem 6

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

(i) The zeros of any irreducible polynomial over \(GF(q)\) contained in \(x^n - \lambda\) can be written as \(\alpha \zeta^c\), where \(c\) runs through the set \(C^m_{t,q,\lambda}\) of size \(m^k\) for some integer \(t \in \{0,1,\ldots,n-1\}\), while \(m^k\) is equal to the degree of that polynomial.

(ii) The integers \(c_i\) in (5) satisfy \(c_i = tq^i + (q^i - 1)/k \mod n\), \(0 \leq i \leq m^k - 1\).

(iii) The size \(m^k\) of \(C^m_{t,q,\lambda}\) is equal to the smallest positive integer satisfying the relation

\[
(kt+1)(q^{m^k} - 1) = 0 \mod kn.
\]

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

(v) Modulo \(n\) one has \(C^m_{0,q,\lambda} = k^{-1}\{0,q-1,q^2-1,\ldots\}\), \(C^m_{t,q,\lambda} = C^m_{0,q,\lambda} + t\{1,q,q^2,\ldots\}\) and \(C^m_{t,q,\lambda} = (kt+1)C^m_{0,q,\lambda} + t\).

Proof

(i) We remark that the condition on \(\alpha\), being of order \(e = kn\), can always be satisfied (cf. also Theorem 5 (ii)). Let \(\alpha\) be a zero of the irreducible factor \(P^{(\lambda)}(x)\) of \(x^n - \lambda\) of degree \(m_0\). Then \(P^{(\lambda)}(x)\) can be written as

\[
P^{(\lambda)}(x) = (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{m_0}}).
\]

From Theorem 5 (iii) (with \(j = 1\)) we know that for all relevant \(i\), we can write \(\alpha^q = \alpha \zeta^{c_i}\) for some integer \(c_i \in \{0,1,\ldots,n-1\}\).

Hence, \(\alpha^q = \alpha \zeta^{c_i}\) and we obtain \(c_{i+1} = l + qc_i\) for \(0 \leq i \leq m_0 - 2\).

Furthermore, since \(\alpha^q = \alpha\) we also have \(l + qc_{m_0-1} = c_0\). We conclude that the relations (5) and (6) with \(t = t_0 = 0\) define the irreducible polynomial \(P^{(\lambda)}_{t_0} = P^{(\lambda)}(x)\). Let \(t_1\) be the least integer in the set \(\{0,1,\ldots,n-1\}\) with \(t(t_0) = 0\) and let \(P^{(\lambda)}_{t_1}(x)\) of degree \(m_{t_1}\) be the irreducible factor of \(x^n - \lambda\) which has \(\alpha \zeta^{c_i}\) as zero. Just as before it appears that this polynomial is defined by (5) and (6) 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 a set \(T^{m,q,\lambda} = \{t_0(=0),t_1,\ldots,t_{a-1}\} \subset \{0,1,\ldots,n-1\}\), such that any irreducible polynomial contained in \(x^n - \lambda\) can uniquely be indexed by some integer in \(T^{m,q,\lambda}\) and vice versa.
(ii) Assume that the expression holds for some \( i \geq 0 \). Then
\[
c_{i+1} = l + q(tq^i + (q^i - 1)/k) = 1 + tq^{i+1} + l(q^i + q^{i-1} + \ldots + q) = tq^{i+1} + (q^{i+1} - 1)/k,
\]
by applying (5) and the equality \( kl = q - 1 \). Since (ii) is true for \( i = 0 \), it holds for all \( i \) satisfying \( 0 \leq i \leq m_1^q - 1 \) by the principle of incomplete induction.

(iii) From (ii) it follows that \( c_{m_1^q} = l + tq^{m_1^q} + l(q^{m_1^q} + q^{m_1^q-1} + \ldots + q) = tq^{m_1^q} + (q^{m_1^q} - 1)/k \). By requiring
\[
c_{m_1^q} = t,
\]
we obtain the condition in (iii).

(iv) By iteration we get
\[
c_{i+b} = l + tq + lq^{b-1} + q^b c_j = (q^b - 1)/k + q^b c_j \mod n.
\]
Hence,
\[
k_c_{i+b} + 1 = q^b + kq^b c_j \mod kn.
\]
(v) These relations follow immediately from (ii).

Because of the properties of the sets \( C_{i,n,q}^\lambda, t \in T_{n,q}^\lambda \), we call them \( q \)-constacyclotomic cosets modulo \( n \) or shortly constacyclotomic cosets. We shall show that they can be expressed in terms of the conventional \( q \)-cyclotomic cosets modulo \( n \), which we denote in this report by \( C_{i,n,q}^\lambda, t \in T_{n,q}^\lambda \).

Remark

For \( \lambda = 1 \) and hence \( k = 1 \), \( l = q - 1 \), the constacyclotomic cosets \( C_{i,n,q}^\lambda \) are not identical to the conventional cyclotomic cosets \( C_{i,n,q} \). This is due to the fact that with respect to
\[
C_{i,n,q}^\lambda = \{c_0(= t), c_1, \ldots, c_{m_1^q-1}\}
\]
the zeros of the corresponding irreducible polynomial have to be written as \( \alpha \zeta^{c_0}, \alpha \zeta^{c_1}, \ldots, \alpha \zeta^{c_{m_1^q-1}} \) with \( \alpha = \zeta \) as primitive \( n^\lambda \)th root of unity. So, by applying Theorem 6 (ii) we obtain as zeros \( \zeta^{c_0}, \zeta^{(i+1)c_1}, \ldots, \zeta^{(i+1)c_{m_1^q-1}} \), whereas \( C_{i,n,q} = \{t, tq, \ldots, tq^{m_1^q-1}\} \) yields the zeros \( \zeta^t, \zeta^{tq}, \ldots, \zeta^{tq^{m_1^q-1}} \). If we define \( bc_{i,n,q}^\lambda + a = \{bc_0 + a, bc_1 + a, \ldots, bc_{m_1^q-1} + a\} \), for any \( b \in \{0, 1, \ldots, n-1\} \), then we may conclude that the following relationship holds
\[
C_{i,n,q}^\lambda + 1 = C_{i+1,n,q}^\lambda.
\]
(7)

Since \( (n-1)q + q - 1 = -1 = n-1 \), we have \( C_{n-1,n,q}^\lambda = \{n-1\} \), and so \( C_{n-1,n,q}^\lambda + 1 = \{0\} = C_0^{n,q} \).

Example 5

For \( n = 14, q = 5, \lambda = 1 \) we have \( C_0^{14,5,1} = \{0, 4, 10, 12, 8, 2\} \), \( C_1^{14,5,1} = \{1, 9, 7, 11, 3, 5\} \), \( C_6^{14,5,1} = \{6\} \) and \( C_{13}^{14,5,1} = \{13\} \). One can immediately verify that relation (7) holds in this case.

The next theorem presents some other relations between the two types of cyclotomic cosets.

Theorem 7

(i) Let \( c_i \) be an integer of \( C_{i,n,q}^\lambda = \{c_0(= t), c_1, \ldots, c_{m_1^q-1}\} \) as defined by (5) and (6). If \( kc_i + 1 \in C_{i,n,q}^\lambda \), then \( C_{i,n,q}^\lambda \subseteq kC_{i,n,q}^\lambda + 1 \).

(ii) For all relevant triples \( (n, q, \lambda) \) one has \( kC_{i,n,q}^\lambda + 1 = C_{ki+1,n,q}^\lambda \).
(iii) If $\Delta C_i^{n,q,\lambda} := \{c_1 - c_0, c_2 - c_1, \ldots, c_0 - c_{m_i-1}\}$, then $\Delta C_i^{n,q,\lambda} = lC_{k+1}^{n,q}$.

(iv) The sizes $m_i$ and $m_{k+1}$ of the cosets $C_i^{n,q,\lambda}$ and $C_{k+1}^{n,q}$ satisfy $m_i = d_m k$, where $d_m$ is a divisor of $(k,n)$.

**Proof**

(i) Since $kc_1 + 1 \in C_u^{n,q}$, we may write $kc_1 + 1 = aq^j$ for some $j$, $0 \leq j \leq m_u - 1$. Applying Theorem 6 (iv) now yields $kc_{i+b} + 1 = aq^{i+b}$ for all relevant values of $b$, and so $kc_{i+b} + 1 \in C_u^{n,q}$.

(ii) Applying definition (5) and (6) yields $kC_i^{n,q,\lambda} + 1 = \{kt + 1, ktq + kl + 1, \ldots\} = \{kt + 1, (kt + 1)q, \ldots\} = C_{k+1}^{n,q} \text{ mod } n$.

(iii) From (6) we have $c_{i+1} - c_i = (q-1)c_i + l = l(kc_i + 1)$ for all $i$, $0 \leq i \leq m_i$. If $m_{k+1}$ is the smallest positive integer with $(kt + 1)(q^{m_{k+1}} - 1) = 0 \text{ mod } n$. Assume that $(kt + 1)(q^m - 1) = 0 \text{ mod } n$ and $m > m_{k+1}$. Then $(kt + 1)(q^m - q^{m_{k+1}} + q^{m_{k+1}} - 1) = 0 \text{ mod } n$, $(kt + 1)q^{m_{k+1}}(q^{m-m_{k+1}} - 1) = 0 \text{ mod } n$, and hence $(kt + 1)(q^{m-m_{k+1}} - 1) = 0 \text{ mod } n$, since $(q,n) = 1$. If we take $m$ such that it is minimal with respect to these properties, it follows $m - m_{k+1} = m_{k+1}$ or $m = 2m_{k+1}$. Continuing in this way yields that in general $m = dm_{k+1}$ for some positive integer $d$. A similar result holds for the relation $(kt + 1)(q^m - 1) = 0 \text{ mod } kn$, since $k \mid q - 1$ and so $(q,k) = (q,kn) = 1$.

To simplify the formalism somewhat, we restrict ourselves from now on to the case $t = 0$. Let $q^m - 1 = 0 \text{ mod } n$ with $m_1 = \text{ord}_n (q)$, so $m_1$ is the minimal positive integer satisfying this property. Since $q - 1 \equiv k\mod k$, we have that $q = 1 \mod k$ and hence $q^b = 1 \mod k$ for all $b \geq 0$. So, $q^m - 1 = 0 \mod k$ as well, and therefore $\langle k,n \rangle \mid q^m - 1$, where $\langle k,n \rangle$ denotes the least common multiple of $k$ and $n$. It follows that for any positive integer $d$ we can write $q^m - 1 = (q^m - 1)(q^{m(d-1)} + q^{m(d-2)} + \ldots + 1) = c < k,n > (d + ak) = cd < k,n > \text{ mod } kn$ for certain integers $c$ and $a$. If we take for $d$ the minimal positive integer such that $(k,n)$ divides $cd$, we have that $(k,n) < k,n > = kn$ divides $q^{m_1} - 1$ and $dm_1$ is minimal w.r.t. this property. So, $dm_1 = m_0^2$, while $d$ is a divisor of $(k,n)$. In the general case $0 \leq t \leq n - 1$ the arguments are similar since $(k,kt+1) = 1$. Because $d$ depends on $t$, we write $m_1^2 = d_m k_{k+1}$.

**Remark**

As for the notation in Theorem 7 (ii), strictly speaking $kC_i^{n,q,\lambda} + 1$ (and similarly $lC_{k+1}^{n,q}$ in (iii)) can be a multiset (e.g. $4C_5^{4,5,2} + 1 = 4\{5,12\} + 1 = \{7,7\}$). From Theorem 7 (iii) it follows that all integers in such a multiset occur the same number of times. We also remark that the relation in Theorem 7 (ii) does not define a one-to-one mapping from the set $\{C_i^{n,q,\lambda} \mid t \in T^{n,q,\lambda}\}$ to the set $\{kt + 1 \mid t \in T^{n,q}\}$. In the case $n = 14$, $q = 5$, $\lambda = 2$, e.g., we have that
We summarize the question of indexing the irreducible polynomials \( P_{l}^{(i,j)}(x) \) in (1) as follows.

**Theorem 8**

(i) The irreducible polynomial \( P_{l}^{(i,j)}(x) \) in (1) corresponds to the \( q \)-cyclotomic coset \( C_{i}^{\alpha \zeta} \) modulo \( e(=kn) \), where \( t \in T_{\lambda} \subseteq T_{\alpha \zeta}^{e,q} \), \( \bigcup_{\lambda} T_{\lambda} = T_{\alpha \zeta}^{e,q} \).

(ii) The irreducible polynomial \( P_{l}^{(i,j)}(x) \) in (1) corresponds to the \( q \)-constacyclic coset \( C_{i}^{n,q,\lambda} \)

modulo \( n \), where \( t \in T_{\lambda}^{n,q,\lambda} \)

\( kC_{i}^{n,q,\lambda} + 1 = \bigcup_{\alpha \zeta} C_{i}^{n,q,\lambda} \), \( \bigcup_{\lambda,\mu} T_{\lambda,\mu} = T_{\alpha \zeta}^{n,q} \).

Right after Theorem 6 it was already remarked that for \( \lambda = 1 \), \( \alpha \) and \( \zeta \) can be identified, both being primitive \( n^{th} \) roots of unity. Since \( k = 1 \) and \( l = q - 1 \) in this case Theorem 6 (ii) gives

\( c_{i} + 1 = (t + 1)q^{i} \). Hence, by augmenting modulo \( n \) the integers of the \( q \)-constacyclic coset \( C_{i}^{n,q,\lambda} \) with 1, we obtain the integers of the \( q \)-cyclotomic coset \( C_{i}^{\alpha \zeta} \). On the other hand, subtracting 1 modulo \( n \) from the integers of \( C_{i}^{n,q,\lambda} \) yields the constacyclic coset \( C_{i}^{n,q,\lambda} \). More generally, for \( (k,n) = 1 \) one has that the constacyclic coset \( C_{i}^{n,q,\lambda} \) is obtained by subtracting \( k' \) from the integers of the cyclotomic coset \( C_{i+k'} \), where \( k' \) is the uniquely defined integer with the property \( kk' = 1 \operatorname{mod} n \).

**Example 6**

Applying Theorem 6 to the case of Example 3, we deal as follows.

We start with the zero \( \alpha \zeta^{0} \), where \( \alpha \) is a zero of \( x^{6} - 2 \) of order 24, and we put \( c_{0} := 0 \). Since \( k = 4 \), we have \( l = 4/4 = 1 \). Next, we find \( c_{1} = 1 + 5c_{0} = 1 \), while \( 1 + 5c_{1} = 6 = 0 \operatorname{mod} 6 \). Hence, \( C_{0}^{6,5,2} = \{0,1\} \). Similarly, we obtain \( c_{2} := 2 \), \( c_{3} = 1 + 5c_{2} = 5 \), while \( 1 + 5c_{3} = 3 \), so \( C_{2}^{6,5,2} = \{2,5\} \) and \( c_{3} := 3 \), \( c_{4} = 1 + 5c_{3} = 4 \), while \( 1 + 5c_{4} = 3 \), so \( C_{3}^{6,5,2} = \{3,4\} \). The integers of these constacyclic cosets correspond respectively to the sets of zeros: \( \{\alpha \zeta^{i}, \alpha \zeta^{-i}\} \), \( \{\alpha \zeta^{2}, \alpha \zeta^{-2}\} \) and \( \{\alpha \zeta^{3}, \alpha \zeta^{-3}\} \).

Next, we express the constacyclic cosets \( C_{i}^{6,5,2}, t \in \{0,2,3\} \), in terms of the cyclotomic cosets \( C_{i}^{6,5} = \{0\}, C_{2}^{6,5} = \{1,5\}, C_{2}^{6,5} = \{2,4\} \) and \( C_{3}^{6,5} = \{3\} \), yielding \( 4C_{0}^{6,5,2} + 1 = \{1,5\} = C_{1}^{6,5} \), \( 4C_{2}^{6,5,2} + 1 = \{3,3\} = C_{3}^{6,5} \cup C_{3}^{6,5} = \{1,3\} \) and \( 4C_{3}^{6,5,2} + 1 = \{1,5\} = C_{1}^{6,5} \). Here, we identified the multiset \{3,3\} and the set \{3\}. The values of the parameter \( d \) are respectively: \( d_{0} = 1 \), \( d_{2} = 2 \) and \( d_{3} = 1 \) (cf. Theorem 7 (ii) and (iii)).

If we do the same for the polynomial \( x^{6} - 1 \), the only difference is that \( k = 1 \), and so \( l = q - 1 = 4 \). Now we find the constacyclic cosets: \( C_{0}^{6,5,1} = \{0,4\}, C_{1}^{6,5,1} = \{1,3\}, C_{2}^{6,5,1} = \{2\} \) and
$C_{6,5,1} = \{5\}$. These cosets correspond to the sets of zeros $\{\alpha \zeta^0, \alpha \zeta^4\}$, $\{\alpha \zeta^1, \alpha \zeta^3\}$, $\{\alpha \zeta^2\}$ and $\{\alpha \zeta^5\}$. When taking $\alpha = \zeta$ we get the sets $\{\zeta^1, \zeta^5\}$, $\{\zeta^2, \zeta^4\}$, $\{\zeta^3\}$ and $\{\zeta^0\}$. These are the sets delivered by applying the usual cyclotomic cosets modulo 6: $C_{6,5}^{0} = \{0\}$, $C_{6,5}^{1} = \{1, 5\}$, $C_{6,5}^{2} = \{2, 4\}$ and $C_{6,5}^{5} = \{3\}$.

Expressing the constacyclotomic cosets $C_{6,5,1}^{k}$ in terms of the cyclotomic cosets $C_{k+1}^{6,5}$ yields:

$C_{6,5,1}^{0} + 1 = \{1, 5\} = C_{6}^{1}$, $C_{6,5,1}^{1} + 1 = \{2, 4\} = C_{6}^{2}$, $C_{6,5,1}^{2} + 1 = \{3\} = C_{6}^{5}$ and $C_{6,5,1}^{5} + 1 = \{0\} = C_{6}^{0}$.

In this case the values of the parameter $d$ are; $d_0 = d_1 = d_2 = d_3 = 1$, as should be the case of course, since $(k, n) = (1, 6) = 1$.

**Example 7**

Take $n = 8$, $q = 5$, $\lambda = 2$. It follows that $k := \text{ord}_s (2) = 4$. Since $x^8 - 2$ does not divide $x^{16} - 1$, the order $e$ of $x^8 - 2$ is equal to $kn = 32$. According to Theorem 7 in [6] we have the factorization

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

The 5-cyclotomic cosets modulo 32 for $\lambda = 1$ are:

$C_{32,5,1}^{0} = \{0\}$, $C_{32,5,1}^{1} = \{1, 5, 25, 29, 17, 21, 9, 13\}$, $C_{32,5,1}^{2} = \{2, 10, 18, 26\}$, $C_{32,5,1}^{3} = \{3, 15, 11, 23, 19, 31, 27, 7\}$, $C_{32,5,1}^{4} = \{4, 20\}$, $C_{32,5,1}^{6} = \{6, 30, 22, 14\}$, $C_{32,5,1}^{8} = \{8\}$, $C_{32,5,1}^{12} = \{12, 28\}$, $C_{32,5,1}^{16} = \{16\}$, $C_{32,5,1}^{24} = \{24\}$.

The factorization of the polynomials $x^8 - \lambda^j$ into irreducible polynomials over $GF(5)$ is as follows:

$$x^8 - 1 = (x + 1)(x - 1)(x + 2)(x - 2)(x^2 + 2)(x^2 - 2),$$
$$x^8 - 4 = (x^4 + 2)(x^4 - 2),$$
while $x^8 - 2$ and $x^8 + 2$ are irreducible themselves.

As primitive 32nd root of unity we choose a zero of the irreducible polynomial $x^8 - 2$, which enhances $\alpha^{16} = -1$, $\alpha^8 = 2$ and $\alpha^{24} = -2$. Hence, the eight zeros of $x^8 - 2$ are $\alpha, \alpha^5, \alpha^9, \alpha^{13}, \alpha^{17}, \alpha^{21}, \alpha^{25}$ and $\alpha^{29}$. Moreover, it follows that $\alpha^4$ and $\alpha^{20}$ are zeros of $x^2 - 2$, $\alpha^{12}$ and $\alpha^{28}$ are zeros of $x^2 + 2$, $\alpha^2, \alpha^{10}, \alpha^{18}, \alpha^{26}$ of $x^4 - 2$ (since $\alpha^{2+10+18+26} = \alpha^{24} = -2$) and that $\alpha^6, \alpha^{30}, \alpha^{22}, \alpha^{14}$ are the zeros of $x^4 + 2$. Finally, we conclude that $\alpha^3, \alpha^{15}, \alpha^{11}, \alpha^{23}, \alpha^{19}, \alpha^{31}, \alpha^{27}, \alpha^7$ are the zeros of $x^8 + 2$.

So, we can take for the index set $T_{32,5,1}^{2} = \{0, 1, 2, 3, 4, 6, 8, 12, 16, 24\}$, and for the index sets $T_{8,5,2}^{5,1}$, $\lambda \in \{0, 1, 2, 3\}$, we have respectively: $T_{8,5,1}^{8,5,1} = \{0, 8, 16, 24, 4, 12\}$, $T_{8,5,2}^{8,5,2} = \{1\}$, $T_{8,5,4}^{8,5,4} = \{2, 6\}$ and $T_{8,5,3}^{8,5,3} = \{3\}$.
As we can verify, we have the following relation:

$$T^{32,5,1} = \bigcup_{j=0}^{3} T^{8,5,2j},$$

while the zeros of $x^8 - \lambda^j$, $0 \leq j \leq 3$, can be written, respectively as $\alpha^{0+ik}$, $\alpha^{1+ik}$, $\alpha^{2+ik}$, $\alpha^{3+ik}$, with $k = 4$ and $0 \leq i \leq 7$.

Suppose we are only interested in the zeros of $x^8 - 4$. Then $\lambda = 4$, $k = 2$, $l = 2$, and the eight zeros can be written as $\alpha^{i\zeta^l}$, $i \in \{0,1,\ldots,7\}$, where $\alpha$ is a zero of this polynomial of order 32. Then $\zeta := \alpha^4$ is a primitive 8th root of unity. Applying relations (5) and (6) provides us with the following constacyclotomic cosets modulo 8: $C_{0}^{8,5,4} = \{0, 2, 4, 6\}$ and $C_{1}^{8,5,4} = \{1, 7, 5, 3\}$. These cosets correspond to the sets of zeros \{ $\alpha\zeta^{0}, \alpha\zeta^{-2}, \alpha\zeta^{-4}, \alpha\zeta^{-6}$ \} and \{ $\alpha\zeta^{4}, \alpha\zeta^{-3}, \alpha\zeta^{-5}, \alpha\zeta^{-7}$ \}, respectively. The first set contains the zeros of $(x - \alpha)(x - \alpha\zeta^{2})(x - \alpha\zeta^{4})(x - \alpha\zeta^{-6}) = x^4 - 2$, and so the second set contains the zeros of $x^4 + 2$. We express the above constacyclotomic cosets $C_{t}^{8,5,2}$, $t \in \{0,1\}$ in terms of the cyclotomic cosets $C_{t}^{8,5}$: $2C_{0}^{8,5,2} + 1 = \{1, 3, 5, 7\} = C_{1}^{8,5} \cup C_{3}^{8,5}$ and $2C_{1}^{8,5,2} + 1 = \{0, 2, 4, 6\} = C_{0}^{8,5} \cup C_{2}^{8,5} \cup C_{4}^{8,5} \cup C_{6}^{8,5}$. 

□

**Example 8**

Like in the previous example we take again $n = 8$, $q = 5$, but we now consider the case $\lambda = 1$. The constacyclotomic cosets as defined by (5) and (6) are:

$C_{0}^{8,5,1} = \{0\}$, $C_{1}^{8,5,1} = \{1\}$, $C_{2}^{8,5,1} = \{2, 6\}$, $C_{3}^{8,5,1} = \{3\}$, $C_{4}^{8,5,1} = \{5\}$, $C_{7}^{8,5,1} = \{7\}$.

The conventional 5-cyclotomic cosets modulo 8 are:

$C_{0}^{8,5} = \{0\}$, $C_{1}^{8,5} = \{1, 5\}$, $C_{2}^{8,5} = \{2\}$, $C_{3}^{8,5} = \{3, 7\}$, $C_{4}^{8,5} = \{4\}$, $C_{6}^{8,5} = \{6\}$.

As one can verify, one can obtain the constacyclotomic cosets $C_{t}^{8,5,1}$ from the conventional cyclotomic cosets $C_{r+1}$ by subtracting 1 mod 8 from all integers in these conventional cosets. 

□

In the next we shall try to answer the question whether there is a natural (or canonical) one-to-one mapping between the irreducible polynomials in the right hand side of (1) and the so-called cyclonomials, for any value of $\lambda \in GF(q)$ (cf. [6]). Since to each of such irreducible polynomials there corresponds a constacyclotomic coset and vice versa, we can equally well try to find a one-one correspondence between constacyclotomic cosets and cyclonomials for fixed values of $n$, $q$ and $\lambda$.

The example of $n = 6$, $q = 5$, $\lambda = 2$ in [6] showed that at least we have to redefine the notion of cyclonomial. For more details and for other examples we also refer to [6]. We emphasize that also in the next of this report the parameters $n$ and $q$ are assumed to be prime to each other, i.e. $(n,q) = 1$, and furthermore that $\lambda \in GF(q)^*$. 

16
3. Cyclonomials for constacyclic codes

First we present a definition of constacyclonomial which narrows down the notion of cyclonomial as introduced in [6] for $\lambda \geq 1$. Let

$$c_s^{n,q,\lambda}(x) := x^l + x^{lq} + \ldots + x^{lq^{m_s-1}} \mod x^n - \lambda$$

be a polynomial in $R_{n,\lambda}^q$.

**Definition 9**

The polynomial $c_s^{n,q,\lambda}(x)$ is called a constacyclonomial of size $m_s$, if and only if it is not the zero-polynomial and if $m_s$ is the smallest positive integer such that $c_s^{n,q,\lambda}(x)^s = c_s^{n,q,\lambda}(x) \mod x^n - \lambda$.

As for this definition we also refer to [6, Section 7]. For $\lambda = 1$ we obtain the usual cyclonomials. We identify these two types of cyclonomials by writing $c_s^{n,q,\lambda}(x) = c_s^{n,q}(x)$. It will be obvious that if $c_s^{n,q,\lambda}(x)$ contains a term $\beta x^l$, $\beta \in GF(q)^*$, then $\beta c_s^{n,q,\lambda}(x) = c_s^{n,q,\lambda}(x)$, and so $c_s^{n,q,\lambda}$ and $c_s^{n,q,\lambda}$ are dependent polynomials. For fixed values of $n$ and $q$, we shall use the notation $S^{n,q,\lambda}$ (or shortly $S^{\lambda}$) for a maximal set of indices $s$ of independent constacyclonomials. If $s \in S^{n,q,\lambda}$ and $c_s^{n,q,\lambda}(x)$ does not contain a term $\beta x^{l-s}$, $\beta \in GF(q)^*$, then the monic constacyclonomials $c_s^{n,q,\lambda}(x)$ and $c_s^{n,q,\lambda}(x)$ are called adjoint constacyclonomials. If $x^{l-s}$ does occur in $c_s^{n,q,\lambda}(x)$, we call this polynomial a self-adjoint constacyclonomial. Usually we take the lowest exponent of the $x$-powers in a constacyclonomial as its index, but actually one can use any of its exponents, just as in the case of constacyclotomic cosets with respect to its integers.

The constacyclonomials $c_s^{n,q,\lambda}(x)$ have the following simple properties.

**Theorem 10**

(i) $c_s^{n,q,\lambda}(x) \neq 0$ is a constacyclonomial if and only if $m_s$ is the smallest positive integer with

$$(x^{q^{m_s-1}})^s = x^l \mod x^n - \lambda.$$  

(ii) The conditions in Definition 9 and in (i) are equivalent to the condition that $m_s$ is the smallest positive integer satisfying $s(q^{m_s} - 1) = 0 \mod kn$, where $k$ is the order of $\lambda$ in $GF(q)^*$.

(iii) If $c_s^{n,q,\lambda}(x)$ is a constacyclonomial, then it has no proper subpolynomial which is also a constacyclonomial.

(iv) If $c_s^{n,q,\lambda}(x)$ is a constacyclonomial, and if all its coefficients $\neq 0$ are changed into $1$, then one obtains the cyclonomial $c_s^{n,q}(x) \equiv c_s^{n,q,\lambda}(x)$.

(v) The size $m_s$ of the constacyclonomial $c_s^{n,q,\lambda}(x)$ is equal to the size of the cyclotomic coset $C_s^{n,q}$, and also to the degree of the irreducible polynomial $P_s^{(1)}(x)$, $s \in T^{n,q}$.

(vi) By reduction modulo $x^n - \lambda$ of the cyclonomial $c_s^{n,q}(x) \equiv c_s^{n,q,\lambda}(x)$, $e = kn$, one obtains either a constacyclonomial $c_s^{n,q,\lambda}(x)$ with multiplicity $\neq 0$, where $s' \in \{0,1,\ldots, n-1\}$, $s' = s \mod n$. 

17
or the zero polynomial.

(vii) If \( q^m - 1 = 0 \mod N \) and \( q^n - 1 = 0 \mod N \), then \( q^d - 1 = 0 \mod N \), with \( d = (m, n) \).

**Proof**

(i) The if-part of the statement is obvious. To prove the only-if-part we assume that \( i \) is the smallest positive integer such that \( x^{iq} = \alpha x^i \mod x^n - \lambda \) for some \( \alpha \in GF(q) \). Assume \( \alpha \neq 1 \). Then \( x^{iq} = \alpha^j x^i \), for \( 0 \leq j \leq k - 1 \), where \( k := \text{ord}_q(\alpha) \). So, \( x^{iq} = x^i \) and the resulting coefficient of \( x^i \) in (8) for \( m = ki \) is equal to \( 1 + \alpha + \ldots + \alpha^{k-1} = 0 \). It follows that all coefficients in (8) are zero for \( m = ki \), and hence, by definition, this polynomial is not a constacyclonomial.

(ii) If the condition is satisfied we have \( x^{iq} = x^i \mod x^n - \lambda \) which is equivalent to \( x^{i(q^n-1)} = 1 \).

When writing \( s(q^m - 1) = an + b \) with \( a \geq 0 \) and \( 0 \leq b < n \), it follows that \( x^{i(q^n-1)} = x^{am+b} = \lambda^a x^b = 1 \), and so \( k | a \) and \( b = 0 \). Therefore, \( kn \mid s(q^m - 1) \). Conversely, if \( s(q^m - 1) = 0 \mod kn \), then \( x^{i(q^n-1)} = x^{kn} = \lambda^{dk} = 1 \).

(iii) This statement follow immediately from (i).

(iv) When constructing \( c_s'^{n,q,\lambda}(x) \) each term is obtained from its predecessor \( a_i x^{i-1} \) by changing this into \( a_i \lambda^d x^{i-1} \), where \( d_i \) is determined by \( q \) and where \( x^{i-1} \) is the next term in \( c_s'^{n,q}(x) \).

(v) We know from the theory developed in [7] that there is a uniquely defined irreducible polynomial \( P^{(1)}(x) \) which corresponds to \( c_s'^{n,q}(x) \) and hence to \( c_s'^{n,q,\lambda}(x) \), by (iv).

(vi) It is clear that \( x^i \mod x^n - \lambda \) is equal to \( \alpha x^i \), with \( s' = s \mod n \), for some \( \alpha \in GF(q) \).

Furthermore, it follows from the definition of \( c_s'^{n,q,\lambda}(x) \) that every term is the \( q \)-power of its predecessor \( x^n - \lambda \). The statement now follows immediately.

(vii) It follows from Theorem 10 (ii) that \( q^m - 1 = aN \), \( q^m - 1 = bN \). If \( d := (m, n) \), then \( q^d - 1 \) is a divisor of \( q^m - 1 \) as well as of \( q^n - 1 \), and so \( q^d - 1 | (q^m - 1, q^n - 1) \). We can even replace \( | \) by the equality sign, as we shall show now. Assume wlg that \( m_s \geq m_i \). For \( m_s = m_i \) the statement is true. Assume \( m_s > m_i \). From the equality \( q^m - 1 = q^m (q^m - 1) + q^n - 1 \) it follows that \( (q^m - 1, q^n - 1) = (q^m - 1, q^n - 1) \). Continuing this process with \( m_r := m_s - m_i \) and \( m_s \), we finally end up with \( (q^m - 1, q^n - 1) = (0, q^d - 1) = q^d - 1 \) (actually this process is similar to Euclid’s Algorithm). Hence, there exist integers \( a \) and \( b \) such that \( q^d - 1 = a(q^m - 1) + b(q^n - 1) \). Since both terms in the rhs are equal to \( 0 \mod N \), we also have \( q^d - 1 = 0 \mod N \).

\[ \square \]

**Remark**

A proper subpolynomial of a polynomial \( p(x) \) is a polynomial not equal to the zero polynomial or to \( p(x) \) itself, such that all its terms are also terms of \( p(x) \).

**Remark**

As for Theorem 10 (ii), one should be aware of the possibility that by reducing polynomials \( c_s'^{n,q,\lambda}(x) \)
modulo $x^n - \lambda$, one obtains the zero polynomial. So, generally the number of constacyclonomials $c_{\bar{\lambda}}^{n,q}(x)$ is less than or equal to the number of cyclonomials $c_{\lambda}^{n,q}(x)$. (A similar remark holds for constacyclonomials $c_{\bar{\lambda}}^{n,q}(x)$ with $\lambda \neq 1$.) According to Theorem 10 (iv), to each such constacyclonomial there corresponds a cyclonomial $c_{\lambda}^{n,q}(x)$, but this statement cannot be reversed.

In the following theorem we present a number of properties of constacyclonomials which they share with the “old” cyclonomials. Prior to that theorem we introduce a bilinear form $(\cdot, \cdot)_\lambda$ in $R_{n,\lambda}^q$.

**Definition 11**

For every pair of elements $p$ and $q$ in $R_{n,\lambda}^q$ we define the bilinear form

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

(9)

where $\alpha$ is a zero of $x^n - \lambda$ of order $kn$ ($= e$) and $\zeta$ is some primitive $n^{th}$ root of unity.

One can easily verify that the above definition really yields a bilinear form in $R_{n,\lambda}^q$, the value of which does not depend on the choice of $\alpha$ and $\zeta$. In the next theorem the irreducible polynomials $P_i^{(\lambda)}(x)$ will play a role. In order to distinguish between various values of $\lambda$, we shall replace $\lambda$ by $\lambda^j$ where $\lambda$ is a fixed element of $GF(q)^*$ of order $k$, and $j \in \{0,1,\ldots,k-1\}$. The degree of $P_i^{(\lambda)}(x)$ will be denoted by $m_i^j$ and the coefficient of its one but highest power $x^{m_i^j-1}$ by $p_i^{(j)}$. We remark that the size of the constacyclonomial $c_{\bar{\lambda}}^{n,q}(x)$ is equal to $m_i$ and is equal to the size of the cyclotomic coset $C_{\bar{\lambda}}^{n,q} = \{t, tq,\ldots\}$ for all $\lambda$, whereas $m_i$ is equal, by definition, to the size of the constacyclonomial coset $C_{\bar{\lambda}}^{n,q} = \{t, tq + l,\ldots\}$, which is equal to the degree of the irreducible polynomial $P_i^{(\lambda)}(x)$. In the case of cyclic codes we have $m_i^1 = m_i$.

In order to deal with the “inner product” (11) in case that $p$ and $q$ are constacyclonomials we first present a lemma for cyclotomic cosets.

**Lemma 12**

Let the cyclotomic cosets $C_{\lambda}^{n,q}$ and $C_{\bar{\lambda}}^{n,q}$ be identical. Then we have the following possibilities for $m_i$:

(i) $m_i = 1$ and $s = 0$ or $s = n/2$;

(ii) $m_i$ is even and $s(q^{m_i/2} + 1) = 0 \mod n$.

**Proof**

Since $s$ and $n-s$ are both elements of $C_{\lambda}^{n,q}$, we also have that $sq^i$ and $(n-s)q^i$ are both in $C_{\lambda}^{n,q}$ for all relevant values of $i$. So, the elements of $C_{\lambda}^{n,q}$ occur in pairs, unless $s = n-s \mod n$. This proves

(i) If $m_i > 1$, then $m_i$ must be even and there is an integer $j > 0$ such that $sq^i = n-s \mod n$. It
follows that $s^{q^{2j}} = n - (n - s) = s \mod n$, and hence $s(q^{2j} - 1) = 0 \mod n$. Since $m_s$ is the minimal positive integer satisfying $s(q^{m_s} - 1) = 0 \mod n$, we may conclude that $2j = m_s \mod n$ and $s^{m_s/2} = n - s \mod n$, which proves (ii).

**Theorem 13**

Let $C_{n,q}^\lambda$ be the set of constacyclicomials as defined in Definition 9 and let $S_{n,q}^\lambda$ be a set of indices as discussed right after that definition. Let $\alpha$ be a zero of $x^n - \lambda$, of order $kn$, $k = \text{ord}_q(\lambda)$, and let $\zeta$ be a primitive $n^{th}$ root of unity.

(i) The set $A := \{ \sum_{\nu \in S} \alpha^\nu c_{\nu}^{n,q,\lambda}(x) | c_{\nu}^{n,q,\lambda} \in C_{n,q}^\lambda, \alpha^\nu \in GF(q) \} \subseteq R_{n,\lambda}^q$, consists of all elements $p(x) \in R_{n,\lambda}^q$ which satisfy the relation $p(x)^q = p(x)$.

(ii) The set $A$ is a vector space over $GF(q)$ with basis $\{c_{\nu}^{n,q,\lambda}(x) | s \in S_{n,q}^\lambda \}$.

(iii) $A$ is an algebra.

(iv) For any $s \neq 0$ and for any $j$, $0 \leq j \leq k - 1$, one has that $\sum_{i=0}^{n-1} c_{\nu}^{n,q,\lambda}(\alpha^i \zeta^j) = 0$, while $\sum_{i=0}^{n-1} c_{0}^{n,q,\lambda}(\alpha^i \zeta^j) = n$.

(v) For any pair of non-negative integers $i$ and $j$ and for any $s \in S_{n,q}^\lambda$ one has $c_{s}^{n,q,\lambda}(\alpha^i \zeta^j) = -\frac{m_s}{m^{\nu_s}} p_{s}^{\nu_s}$, with $s \in \Omega^{n,q,\lambda}$.

(vi) With respect to the bilinear form (9), the constacyclicomials $c_{s}^{n,q,\lambda}(x), s \in S_{n,q}^\lambda$, form an orthogonal basis of the vector space $A$, such that for any pair $j, k \in S_{n,q}^\lambda$ one has $(c_{j}^{n,q,\lambda}, c_{k}^{n,q,\lambda}) = mn, \lambda \delta_{j-k} = mn, \lambda \delta_{j-k}$, if $c_{j}^{n,q,\lambda}$ is not self-adjoint, while in case that $c_{j}^{n,q,\lambda}$ is self adjoint $(c_{j}^{n,q,\lambda}, c_{k}^{n,q,\lambda}) = mn, \lambda \delta_{j,k}$, with $a = j(q^{m/2} + 1)/n$.

**Proof**

(i) It will be clear that constructing all constacyclicomials $c_{s}^{n,q,\lambda}(x)$ and taking all linear combinations provides us with polynomials $p(x)$ which satisfy $p(x)^q = p(x)$. Here, we use the fact that if $p_1(x)^q = p_1(x)$ and $p_2(x)^q = p_2(x)$, then $(p_1(x) + p_2(x))^q = p_1(x)^q + p_2(x)^q = p_1(x) + p_2(x)$, and also that if $p(x)^q = p(x)$, then $(\beta p(x))^q = \beta^q p(x)^q = \beta p(x)$ for all $\beta \in GF(q)$. Conversely, if $p(x) \in R_{n,\lambda}^q$ satisfies $p(x)^q = p(x)$, then one can show by determining successively the various coefficients of $p(x)$ written as a linear combination of constacyclicomials, that $p(x) \in A$.

(ii) By definition $A$ is spanned by the constacyclicomials $c_{s}^{n,q,\lambda}(x)$. It is obvious that all requirements for a vector space are satisfied. Moreover, the polynomials $c_{s}^{n,q,\lambda}(x), s \in S$, are independent and therefore they constitute a basis of $A$, by (i).
(iii) To show that \( A \) is also closed under multiplication, we only have to apply repeatedly that 
\[
(p_1(x)p_2(x))^q = p_1(x)^q p_2(x)^q = p_1(x)p_2(x)
\]
for all \( p_1(x) \) and \( p_2(x) \) in \( A \).
(iv) If \( s \neq 0 \), the polynomial \( c_s^{n,q,\alpha}(x) \) is a sum of terms \( \alpha_i x^{l_i} \), \( \alpha_i \in GF(q)^* \), where \( l \) runs through a subset \( U \) of \( \{1, 2, \ldots, n-1\} \). So, any term \( \alpha_i x^{l_i} \) occurring in \( c_s^{n,q,\alpha}(x) \) contributes to the sum
\[
\sum_{i=0}^{n-1} c_s^{n,q,\alpha}(\alpha_i/\zeta^i) \text{ an amount of } \alpha_i \alpha_i'/(1 + \zeta^i + \zeta^{2i} + \ldots + \zeta^{(n-1)i}) \text{, which is equal to 0 for any } \alpha_i \in GF(q)^*.
\]
Hence, for \( s = 0 \) we get
\[
\sum_{i=0}^{n-1} c_s^{n,q,\alpha}(\alpha_i/\zeta^i) = 1 + 1 + \ldots + 1 = n.
\]
Take the polynomial \( c_s^{n,q,\alpha}(x) \) and substitute \( x' = x \) for \( x \).
From \( c_s^{n,q,\alpha}(\alpha_i/\zeta^i) = \alpha_i^{\alpha_i'} \zeta^i + \alpha_i^{\alpha_i'} \zeta^{2i} + \ldots \) we infer that the rhs contains all zeros of \( P_{is}^{x}(\alpha_i^{\alpha_i'}) \) the same number of times. This number is equal to \( \frac{m_j}{m_j^\alpha} \), where \( m_j \) is the size of \( c_s^{n,q,\alpha}(x) \), which is equal to the size of the cyclotomic coset \( C_s^{\alpha} \). Since \( \alpha \) is a zero of \( x^\alpha - \lambda^\alpha \) with \( \text{ord}(\alpha) = kn \), \( \alpha^{\alpha'} \) is a zero of \( x^\alpha - \lambda^\alpha \) with \( \text{ord}(\alpha^{\alpha'}) = km \). Hence, \( m_j^\alpha \) is the degree of the irreducible polynomial \( P_{is}^{x}(\alpha^{\alpha'}) = (x - \alpha^{\alpha'} \zeta^{js})(x - \alpha^{\alpha'} \zeta^{js})(x - \alpha^{\alpha'} \zeta^{js}) \ldots (x - \alpha^{\alpha'} \zeta^{js}) \), \( m_j^\alpha = m_j^{\alpha'} \), which is equal to the size of the constacyclomorphic coset \( C_s^{n,q,\alpha} \). So, we obtain \( m_j / m_j^{\alpha'} \) times the sum of the zeros of the polynomial \( P_{is}^{x}(\alpha^{\alpha'}) \). On the other hand, the sum of the zeros of \( P_{is}^{x}(\alpha^{\alpha'}) \) is equal to \( -p^{x}_0 \). This proves equality (v). Notice that we have to take \( is \) modulo \( n \) and \( js \) modulo \( k \).
(vi) From (iii) we know that \( c_s^{n,q,\alpha}(x)c_{n,q,\alpha}(x) = \sum \alpha_i c_s^{n,q,\alpha}(\alpha_i^{\alpha_i'} x^{\alpha_i'}) \). Hence,
\[
(c_s^{n,q,\alpha}, c_{n,q,\alpha})_\lambda = \sum_{i=0}^{n-1} c_s^{n,q,\alpha}(\alpha_i^{\alpha_i'}) c_{n,q,\alpha}(\alpha_i^{\alpha_i'}) = \sum_{i=0}^{n-1} \sum_{i=0}^{n-1} c_s^{n,q,\alpha}(\alpha_i^{\alpha_i'}) c_{n,q,\alpha}(\alpha_i^{\alpha_i'})
\]
not both be self adjoint. For \( k \neq j \) it is obvious that \( \alpha_0 = 0 \) and therefore
\[
(c_s^{n,q,\alpha}, c_{n,q,\alpha})_\lambda = 0 \text{ by applying (iv). For } k = j \text{ we have}
\]
\[
c_j^{n,q,\alpha}(x)c_{n,q,\alpha}(x) = (x^{j' + jq} + \ldots + x^{(n-j)^{jq}}) (x^{j' + jq} + \ldots + x^{(n-j)^{jq}}) \text{, where we used that}
\]
\( m_j = m_j \) is the size of the cyclotomic cosets \( C_j^{n,q} \) and \( C_{n,q} \). So, the coefficient of \( x^0 \) in the rhs of this equality modulo \( x^\alpha - \lambda \) is equal to \( \lambda + \lambda^q + \ldots + \lambda^{q^\alpha} \) \( = m_j \lambda \). Hence, since \( \sum_{i=0}^{n} m_j \lambda = m_j \lambda \),
\[
(c_j^{n,q,\alpha}, c_{n,q,\alpha})_\lambda = (c_j^{n,q,\alpha}, c_{n,q,\alpha})_\lambda = nm_j \lambda.
\]
Next, suppose that \( e_j^{n,q,\alpha} \) is self adjoint. Like before, we may conclude that \( (c_j^{n,q,\alpha}, c_{n,q,\alpha})_\lambda = 0 \) for \( k \neq j \). For \( k = j \) and \( m_j \) even, the term \( \lambda^{q^\alpha} x^{(n-j)^{jq}} \) occurs in the polynomial \( c_j^{n,q,\alpha}(x) \) with \( a = j(q^{m_j/2} + 1)/n \), by applying Lemma 12. So in the product
\[
(x^j + x^{jq} + \ldots + x^{\lambda^q x^{jq}} + \ldots)(x^j + x^{jq} + \ldots + x^{\lambda^q x^{jq}} + \ldots),
\]
the coefficient of \( x^0 \) is equal to \( \lambda^a + \lambda^{aq} + \ldots + \lambda^{aq^{m_j/2}} = \lambda^a + \lambda^{aq} + \ldots + \lambda^a = m_j \lambda^a \), and the result follows in the same way as before. If \( m_j \) is odd we know from Lemma 12 that \( m_j = 1 \) and \( j = 0 \) or \( j = n/2 \). The case \( j = 0 \) is
covered by the general result with \( a = 0 \), while for \( j = n / 2 \) we have \( m_j = 1 \), and hence
\[
a = \frac{n}{2} (q^{[1/2]} + 1) = \frac{1}{2} (q^{0} + 1) = 1.
\]

**Remarks**
The multiplication is in Theorem 13 (v), where \( s \in S = S^{n,q,\lambda} \subset \{0,1,\ldots,n-1\} \) and where \( i \) is some integer, firstly has to be carried out in the ring \( \mathbb{Z}_n \), whereupon next one has to determine \( t \in T^{n,q,\lambda} \) such that \( t = is^l \) for some integer \( l \). The multiplication \( js \) takes place in the ring \( \mathbb{Z}_k \).

We also remark that for \( \lambda = 1 \) Theorem 13 (vi) yields the same result as derived in the proof of [7, Theorem 7 and eq. (19)], i.e. 
\[
c_i (\zeta^s) = \frac{-m_s}{m_t}, \quad \text{where} \quad m_s \quad \text{and} \quad m_t \quad (= m_t^1) \quad \text{stand for the size of the cyclotomic cosets} \quad C_{i, s}^{n,q} \quad \text{and} \quad C_{i, t}^{n,q}, \quad \text{respectively.}
\]
Of course, putting \( j = 0 \) yields the same.

A final remark concerns the constacyclotomic coset \( C_{i, s}^{n,q,\lambda^j} \) mentioned in the proof of Theorem 13 (v). When writing its integers explicitly in the form as described in Theorem 6, one should take care that the variables \( \alpha \) and \( \zeta \) which occur throughout Theorem 13 and its proof, are related by \( \zeta = \alpha^k \), as defined in Theorem 6 which dealt with the zeros of \( x^n - \lambda \). So, when applying Theorem 6 to \( x^n - \lambda^j \), we should use \( \lambda' := \lambda^j \), \( \alpha' := \alpha^j \) and \( \zeta' := \alpha^k \) with \( k' := k / (k, js) \). Actually, it seems more convenient in this context to express the zeros of \( x^n - \lambda \) and the zeros of \( x^n - \lambda^j \) for all \( j \) on the same footing, i.e. as powers of \( \alpha \). We shall do so in our next report.

**Example 9**
Take \( n = 6 \) and \( q = 5 \). We have the cyclotomic cosets \( C_0 = \{0\} \), \( C_1 = \{1,5\} \), \( C_2 = \{2,4\} \) and \( C_3 = \{3\} \). For \( \lambda = 2 \) expression (8) gives us the constacyclonomials \( c_0^{6,5,2} (x) = 1 \), \( c_1^{6,5,2} (x) = x + x^5 \) and \( c_2^{6,5,2} (x) = x^2 + 2x^4 \). Notice that that there is no constacyclonomial containing \( x^3 \), since 
\[
(x^3)^5 = 4x^3 \neq x^3.
\]
This is also the case for \( \lambda = 3 \), while for \( \lambda = 1 \) and for \( \lambda = -1 \) we have 
\[
c_3^{6,5,1} (x) = c_3^{6,5,-1} (x) = x^3.
\]
We compute in \( R_{6,2}^5 \): 
\[
c_1^{6,5,2} (x) c_2^{6,5,2} (x) = (x + x^5)(x^2 + 2x^4) = 2(x + x^5).
\]
Applying this result yields 
\[
(c_1^{6,5,2}, c_2^{6,5,2}) = 2 \sum_{i=0}^5 (\alpha^{\zeta^i} + \alpha^5 \zeta^{5i}) = 2(\alpha + \alpha^5)(1 + \zeta + \ldots + \zeta^5) = 0,
\]
since \( \zeta \) and \( \zeta^5 \) are primitive 6th roots of unity.

Similarly we obtain 
\[
c_1^{6,5,2} (x) c_1^{6,5,2} (x) = 4 + x^2 + 2x^4 \]
and hence 
\[
(c_1^{6,5,2}, c_1^{6,5,2}) = 4 + 2 \sum_{i=0}^5 (4 + \alpha^2 \zeta^{2i} + 2\alpha^4 \zeta^{4i}) = 4 \sum_{i=0}^5 4 = 24.
\]
Theorem 13 (vi) yields the same result, since \( n = 6 \), \( q = 5 \), \( \lambda = 2 \), \( s = 1 \), \( m_i = 2 \) and so \( a = (5^1 + 1) / 6 = 1 \), giving \( 6.2.2^1 = 24 = 4 \) in \( GF(5) \). Similarly, we find 
\[
(c_2^{6.5.2}, c_2^{6.5.2}) = 6.2.2^2 = 48 = 3 \quad \text{in} \quad GF(5)
\]
by Theorem 13 (vi), while the coefficient of \( x^5 \) in the product \((x^2 + 2x^3(x^2 + 2x^4)\) equals 8, which also yields the answer \( 6.8 = 48 = 3 \). □

**Example 10**

We also shall present an example which demonstrates Theorem 13 (v). Again we take \( n = 6, q = 5 \), but now with \( \lambda = -1 \). So, \( c_0^{6.5.1}(x) = 1 \), \( c_1^{6.5.1}(x) = x^4 + x^5 \), \( c_2^{6.5.1}(x) = x^2 - x^4 \) and \( c_3^{6.5.1} = x^3 \).

We have the following factorization into irreducible polynomials:
\[
x^6 + 1 = (x^2 + 2x - 1)(x^2 + 2x - 1)(x + 2)
\]

Let \( \alpha \) be a zero of \( x^2 + 2x - 1 \). Since \( \text{ord}(\alpha) = 12 (= kn = 2.6) \), \( \zeta = \alpha^2 \) is a primitive 6th root of unity and the zeros of \( x^6 + 1 \) can be written as \( \alpha \zeta^i \), \( 0 \leq i < 6 \).

More precisely, we have that \( \alpha \zeta^0 \) and \( \alpha \zeta^2 \) are the zeros of \( P_0^{(-1)}(x) = P_2^{(-1)}(x) \), \( \alpha \zeta^3 \) and \( \alpha \zeta^5 \) are the zeros of \( P_1^{(-1)}(x) = P_3^{(-1)}(x) \), \( \alpha \zeta^4 \) is the zero of \( P_2^{(-1)}(x) \) and \( \alpha \zeta^5 \) is the zero of \( P_4^{(-1)}(x) \).

We obtain \( c_1^{6.5.1}(\alpha \zeta^i) = \alpha \zeta^i + \alpha \zeta^{5+i} \), \( s = 1 \), yielding:

for \( i = 1 \), \( 2 \alpha \zeta \) which is twice the sum of the zeros of \( P_1^{(-1)}(x) = x - 2 \), \( s = 1 \), \( m_i / m_i^{-1} = 2 / 1 = 2 \);
for \( i = 2 \), \( \alpha \zeta^3 + \alpha \zeta^0 \) which is the sum of the zeros of \( P_2^{(-1)}(x) = x^2 - 2x - 1 \), \( m_i / m_i^{-1} = 2 / 2 = 1 \);
for \( i = 3 \), \( \alpha \zeta^3 + \alpha \zeta^5 \) which is the sum of the zeros of \( P_3^{(-1)}(x) = x^2 + 2x - 1 \), \( m_i / m_i^{-1} = 2 / 2 = 1 \);
for \( i = 4 \), \( 2 \alpha \zeta^4 \) which is twice the sum of the zeros of \( P_4^{(-1)}(x) = x + 2 \), \( m_i / m_i^{-1} = 2 / 1 = 2 \);
for \( i = 5 \), \( \alpha \zeta^5 + \alpha \zeta^3 \) which is the sum of the zeros of \( P_5^{(-1)}(x) = x^2 + 2x - 1 \), \( m_i / m_i^{-1} = 2 / 2 = 1 \);
for \( i = 0 \), \( \alpha \zeta^0 + \alpha \zeta^2 \) which is the sum of the zeros of \( P_0^{(-1)}(x) = x^2 - 2x - 1 \), \( m_i / m_i^{-1} = 2 / 2 = 1 \).

For a similar computation of \( c_2^{6.5.1}(\alpha \zeta^i) \) we need also the factorization
\[
x^6 - 1 = (x - 1)(x^2 - x + 1)(x^2 + x + 1)(x + 1).
\]

From the definition of \( \alpha \) it follows that \( \alpha^2 \) is a zero of \( x^6 - (-1)^2 = x^6 - 1 \) and that the zeros of \( x^6 - 1 \) can be written as \( \alpha \zeta^i \), \( 0 \leq i < 6 \), since \( \text{ord}(\alpha^2) = 6 \).

More precisely, \( \alpha^2 \zeta^0 \) and \( \alpha^2 \zeta^4 \) are the zeros of \( P_0^{(1)}(x) = P_4^{(1)}(x) \), \( \alpha^2 \zeta^3 \) and \( \alpha^2 \zeta^1 \) are the zeros of \( P_1^{(1)}(x) = P_3^{(1)}(x) \), \( \alpha^2 \zeta^2 \) is the zero of \( P_2^{(1)}(x) \) and \( \alpha^2 \zeta^5 \) is the zero of \( P_5^{(1)}(x) \).

Now, we obtain: \( c_2^{6.5.1}(\alpha \zeta^i) = \alpha \zeta^{2i} - \alpha^4 \zeta^{4i} \), \( s = 2 \), yielding:

for \( i = 1 \), \( \alpha^2 \zeta^2 + \alpha^2 \zeta^2 = -2 \) which is twice the sum of the zeros of \( P_2^{(1)}(x) = x + 1 \), \( m_2 / m_2^{-1} = 2 \);
for \( i = 2 \), \( \alpha^2 \zeta^4 + \alpha^2 \zeta^4 \) which is the sum of the zeros of \( P_4^{(1)}(x) = x^2 - x + 1 \), \( m_2 / m_2^{-1} = 1 \);
for \( i = 3 \), \( \alpha^2 \zeta^0 + \alpha^2 \zeta^0 \) which is the sum of the zeros of \( P_0^{(1)}(x) = x^2 - x + 1 \), \( m_2 / m_2^{-1} = 1 \);
for \( i = 4 \), \( \alpha^2 \zeta^2 + \alpha^2 \zeta^2 \) which is twice the sum of the zeros of \( P_2^{(1)}(x) = x + 1 \), \( m_2 / m_2^{-1} = 2 \);
for \( i = 5 \), \( \alpha^2 \zeta^4 + \alpha^2 \zeta^4 \) which is the sum of the zeros of \( P_4^{(1)}(x) = x^2 - x + 1 \), \( m_2 / m_2^{-1} = 1 \)
for \( i = 0, \alpha^2 \zeta^0 + \alpha^2 \zeta^4 \) which is the sum of the zeros of \( P_0^{(1)}(x) = x^2 - x + 1, \ m_2 / m_0^1 = 1 \).

Notice that the zeros are written as \( \alpha^2 \zeta^i \), and not as \( \alpha \zeta^i \). This is because \( \alpha \) is a zero of \( x^6 + 1 \) and so \( \alpha^2 \) is a zero of \( x^6 - 1 \). Compare this with Theorem 4 (iv) with \( \alpha \) replaced by \( \alpha^2 \).

We also consider the trivial case of \( c_0^{6,5,-1}(x) = x^0 \). Substitution of \( \alpha \zeta \) for \( x \) yields \( c_0^{6,5,-1}(\alpha \zeta^i) = (\alpha^0) = 1 \). Since \( \alpha^6 = -1 \), we have \( (\alpha^i)^6 = (\alpha^0)^6 = 1 \) which is indeed the only zero of \( P_0^{(1)}(x) = x - 1 \). The same holds for \( \alpha \zeta^2 \), i.e. for \( i = 2 \). Notice that in both cases \( \lambda^j = (-1)^{1,0} = 1 \).

Next, we derive from \( c_3^{6,5,-1}(x) = x^3 \), that \( c_3^{6,5,-1}(\alpha \zeta^i) = \alpha^3 \zeta^j \). Hence, \( c_3^{6,5,-1}(\alpha \zeta^2) = \alpha^3 \zeta^3 \) which is the zero of \( P_3^{(1)}(x) = x + 2, \ c_3^{6,5,-1}(\alpha \zeta^2) = \alpha^3 = 2 \), which is the zero of \( P_3^{(1)}(x) = x - 2 \), \( c_3^{6,5,-1}(\alpha \zeta^2) = \alpha^3 \zeta^3 \), which is the zero of \( P_3^{(1)}(x) = x + 2 \), etc.

Notice that if we introduce \( \alpha' = \alpha^2 \) and \( \zeta' = \alpha^d = \alpha^6 \), Theorem 6, with \( k' = 1, l' = 4 \), would provide us with \( C_0^{6,5,1} = \{0,4\}, C_1^{6,5,1} = \{1,3\}, C_2^{6,5,1} = \{2\}, C_3^{6,5,1} = \{5\} \). With respect to this kind of indexing we get \( P_0^{(1)}(x) = P_4^{(1)}(x) = (x-\alpha')(x-\alpha' \zeta^{-4}) = (x-\alpha')(x-\alpha^5) \), \( P_2^{(1)}(x) = x-\alpha' \zeta = x-\alpha^3 = x-1 \), \( P_3^{(1)}(x) = x-\alpha' \zeta^5 = x-\alpha^6 = x-1 \), etc. \( \square \)

**Example 11**

Take \( n = 14 \) and \( q = 5 \).

The cyclotomic cosets and negacyclotomic cosets are:

\( C_0^{14,5} = \{0\}, C_1^{14,5} = \{1,5,11,13,9,3\}, C_2^{14,5} = \{2,10,8,12,4,6\}, C_7^{14,5} = \{7\} \) and \( C_0^{14,5,-1} = \{0,2,12,6,4,8\}, C_1^{14,5,-1} = \{1,7,9,5,13,11\}, C_3^{14,5,-1} = \{3\}, C_{10}^{14,5,-1} = \{10\} \).

Since there are 4 negacyclotomic cosets there are also 4 negacyclonomials:

\( c_0^{14,5,-1}(x) = 1, c_1^{14,5,-1}(x) = x^1 + x^5 - x^{11} + x^{13} + x^9 - x^3, c_2^{14,5,-1} = x^2 + x^{10} - x^8 - x^{12} - x^4 + x^6, \)
\( c_7^{14,5,-1}(x) = x^7 \).

Let \( \alpha \) be a zero of \( x^{14} + 1 \) of order 28, and let \( \zeta = \alpha^2 \). Then it follows that \( \alpha \zeta^3 = \alpha^7 = 2 \).

In order to verify Theorem 13 (v), we carried out the following calculations:

\( \lambda = -1, s = 1, i = 1, j = 1 \)
\( c_1^{14,5,-1}(\alpha \zeta^i) = \alpha^1 \zeta^1 + \alpha^1 \zeta^7 + \alpha^1 \zeta^9 + \alpha^1 \zeta^5 + \alpha^1 \zeta^{13} + \alpha^1 \zeta^{11}, \)
which equals the sum of the zeros of \( P_1^{(1)}(x), m_i / m_i^{-1} = 6 / 6 = 1; \)
\[ \lambda = -1, \ s = 1, \ i = 2, \ j = 1 \]
\[ c_{1}^{4,5,-1}(\alpha^i\zeta^j) = \alpha^1\zeta^2 + \alpha^1\zeta^{12} + \alpha^1\zeta^6 + \alpha^1\zeta^4 + \alpha^1\zeta^8 + \alpha^1\zeta^0 \]
which equals the sum of the zeros of \( P_{2}^{(-1)}(x) \), \( m_1/m_2 = 6/6 = 1 \);
\[ \lambda = -1, \ s = 1, \ i = 3, \ j = 1 \]
\[ c_{1}^{4,5,-1}(\alpha^i\zeta^j) = \alpha^3\zeta^3 + \alpha\zeta^3 + \alpha^2\zeta^3 + \alpha^3\zeta^3 + \alpha^3\zeta^3 \]
which equals six times the sum of the zeros of \( P_{3}^{(-1)}(x) = x - \alpha^3\zeta^3 = x - 2 \), \( m_1/m_3 = 6/1 = 6 \);
\[ \lambda = -1, \ s = 2, \ i = 2, \ j = 1 \]
\[ c_{2}^{4,5,-1}(x) = \alpha^2\zeta^4 + \alpha^2\zeta^{10} + \alpha^2\zeta^{12} + \alpha^2\zeta^8 + \alpha^2\zeta^2 + \alpha^2\zeta^0 \]
which equals the sum of the zeros of \( P_{4}^{(-1)}(x) \).

Notice that the exponents of \( \zeta \) are not the integers of \( C_{1}^{4,5,-1} = \{4, 8, 0, 2, 12, 6, \} \). This is because the identity \( \zeta^j = \zeta^2 \) does not hold for \( \lambda^j = (-1)^j = 1 \). However, this does not affect the sum of the zeros of \( P_{4}^{(-1)}(x) \) (cf. also Example 10).

Example 12
Take \( n = 28 \) and \( q = 5 \). We have the following cyclotomic cosets:
\[ C_0^{28,5} = \{0\}, \ C_7^{28,5} = \{7\}, \ C_{14}^{28,5} = \{14\}, \ C_{21}^{28,5} = \{21\}, \ C_1^{28,5} = \{1, 5, 25, 13, 9, 17\}, \]
\[ C_{2}^{28,5} = \{2, 10, 22, 26, 18, 6\}, \ C_3^{28,5} = \{3, 15, 19, 11, 27, 23\} \text{ and } C_4^{28,5} = \{4, 20, 16, 24, 8, 12\}, \]
which yield the polynomials \( c_{0}^{28,5,\lambda}, c_{7}^{28,5,\lambda}, c_{14}^{28,5,\lambda}, c_{21}^{28,5,\lambda}, c_{1}^{28,5,\lambda}, c_{2}^{28,5,\lambda}, c_{3}^{28,5,\lambda} \text{ and } c_{4}^{28,5,\lambda} \).

For \( \lambda = 1 \) all these polynomials are (consta)cyclonomials (cf. Definition 10).

For \( \lambda = -1 \) the polynomials \( c_{0}^{28,5,\lambda}, c_{14}^{28,5,\lambda}, c_{1}^{28,5,\lambda}, c_{2}^{28,5,\lambda}, c_{3}^{28,5,\lambda} \text{ and } c_{4}^{28,5,\lambda} \) are constacyclonomials.

For \( \lambda = 2 \) and \( \lambda = 3 \) only the polynomials \( c_{0}^{28,5,\lambda}, c_{2}^{28,5,\lambda} \text{ and } c_{4}^{28,5,\lambda} \) are constacyclonomials.

As one can see immediately, the constacyclonomials \( c_{1}^{28,5,\lambda} \text{ and } c_{3}^{28,5,\lambda} \) are the only ones which are not self adjoint. So, we can define e.g. that \( S_{28,5,-1} := \{0, 14, 2, 4, 1, 27\} \text{ and } S_{28,5,2} := \{0, 2, 4\}. \)

As for the mutual inner products, we find e.g. for the polynomials (notice that \( \lambda \in GF(q) \), so \( \lambda^4 = 1 \))
\[ c_{1}^{28,5,\lambda}(x) = x^1 + x^2 + x^{25} + x^{11} + \lambda^2 x^9 + \lambda^3 x^{17}, \]
\[ c_{27}^{28,5,\lambda}(x) = x^{27} + x^{23} + x^3 + x^{15} + \lambda^2 x^{19} + \lambda x^{11}, \]
\[ c_{4}^{28,5,\lambda}(x) = x^4 + x^{20} + \lambda^3 x^{16} + \lambda x^{24} + \lambda^2 x^8 + \lambda^2 x^{12}, \]
that \( (c_{1}^{28,5,\lambda}, c_{2}^{28,5,\lambda}) = 0, (c_{1}^{28,5,\lambda}, c_{1}^{28,5,\lambda}) = \frac{28.6}{6} \lambda = 3 \lambda \text{ and } (c_{2}^{28,5,\lambda}, c_{2}^{28,5,\lambda}) = \frac{28.6.3 \lambda}{28} = 3 \lambda \). All these results agree with Theorem 13 (vi), where we have to take \( a = 2(5^3 + 1)/28 = 9 \) and \( \lambda^9 = \lambda \).
Theorem 14
(i) With respect to the bilinear form (8), the primitive idempotents \(\theta_t(x), t \in T^\lambda\), form an orthogonal \(GF(q)\)-basis of the vector space \(A\).

(ii) The number of irreducible polynomials \(P_t(x)\) contained in \(x^n - \lambda\), the number of primitive idempotents \(\theta_t(x), t \in T_\lambda\), and the number of constacyclics \(c_{s,q}^{n,q}(.), s \in S\), are all equal to the number of \(q\)-constacyclic cosets \(C_{s,q}^{n,q}\), \(t \in T_\lambda\).

Proof
(i) By definition \(\theta_t(x)^2 = \theta_t(x)\), and therefore \(\theta_t(x)^t = \theta_t(x)\) for all \(t \in T\). So, all \(\theta_t(x)\) belong to \(A\). From Theorem 1 (v) and expressions (5) and (7) we know that \(\theta_t(\alpha\zeta^i)\) is equal to 1 if \(i \in C_{n,q}^{n,q}\), and equal to 0 otherwise. Hence, \(\theta_t, \theta_u\) = \(\sum_{i=0}^{n-1} \theta_t(\alpha\zeta^i)\theta_u(\alpha\zeta^i) = 0\), for \(t \neq u\), while

\(\theta_t, \theta_t\) = \(\sum_{i=0}^{n-1} \theta_t(\alpha\zeta^i)\theta_t(\alpha\zeta^i) = n\). So, these idempotents are independent. To show that they span \(A\), we assume that there is a \(p(x) \in A\) such that \(\theta_t(p) = 0\) for all \(t \in T^\lambda\). It follows that

\[\sum_{i \in C_{n,q}^{n,q}} p(\alpha\zeta^i) = 0\] for all \(t \in T^\lambda\). Since \(p(x)^q = p(x)\), we also have \(p(x^q) = p(x)\) and hence

\[p(x^q) = p(x)\] for any nonnegative integer \(a\). We know that for any pair \(i, j \in C_{n,q}^{n,q}\) there is an \(a\) such that \(\alpha\zeta^i = (\alpha\zeta^i)^a\). So, \(\sum_{i \in C_{n,q}^{n,q}} p(\alpha\zeta^i) = m^a p(\alpha\zeta^i) = 0\) for any \(j \in C_{n,q}^{n,q}\) and for all \(t \in T^\lambda\).

Since the degree of \(p(x)\) is less than \(n\), we conclude that \(p(x)\) is the zeropolynomial.

(ii) We know that there is a one-one correspondence between the constacyclic cosets \(C_{s,q}^{n,q}\) and the irreducible polynomials \(P_t(x), t \in T^\lambda\) (cf. Theorem 8 (ii)). We also know that there is a one-one correspondence between the irreducible polynomials \(P_t(x)\) and the primitive idempotents \(\theta_t(x)\) (cf. Theorem 1 (v)). Since the idempotents \(\theta_t(x), t \in T_\lambda\), and the cyclonomials \(c_{s,q}^{n,q}(.), s \in S\), both form a basis for the vector space \(A\), their numbers must be equal, so \(|T^\lambda| = |S^\lambda|\). This proves (ii).

Though \(T^\lambda (= T_{n,q}^{n,q})\) and \(S^\lambda (= S_{n,q}^{n,q})\) are both subsets of the set \(\{0,1,\ldots,n-1\}\) and are of the same size, it is still the question whether the integers in these sets can be chosen such that they are pairwise equal.

Example 13
Next, we take \(n = 7, q = 5\) and \(\lambda = 2\). It follows that \(k := \text{ord}_S(\lambda) = 4\) and so \(e = 28\).

We have the following factorization: \(x^7 - 2 = (x - 3)(x^6 - 2x^5 - x^4 + 2x^3 + x^2 - 2x - 1)\). There appear to be two 5-constacyclic cosets: \(C_{7,5,2}^0 = \{0, 1, 6, 3, 2, 4\}\) and \(C_{7,5,2}^5 = \{5\}\). This proves,
according to Theorem 14 (ii), that the second factor in the above factorization is irreducible. There are also two constacyclicomials, since Definition 9 gives \( c_{9}^{7.5.2}(x) = 1 \) and 
\[ c_{i}^{7.5.2}(x) = x^3 + x^5 - 2x^4 + 2x^6 + 2x^2 - x^3. \]
One can also apply Theorem 10 (ii), by first determining 
\[ c_{i}^{28.5.1}(x) = x^3 + x^5 + x^{25} + x^{13} + x^9 + x^{17}. \]
Reducing this expression modulo \( x^7 - 2 \) gives the same result as before.

By applying the general expression for idempotent generators [6, Theorem 5], we find the primitive idempotents 
\[ \theta_{1}(x) = -2x^6 - x^6 + 2x^4 + x^3 - 2x^2 - x - 2, \]
\[ \theta_{0}(x) = 2x^6 + x^5 - 2x^4 - x^3 + 2x^2 + x - 2. \]
Both idempotents are clearly linear combinations of the two constacyclicomials.

In [6, Ch. 2] we showed that the idempotent generator of the \( \lambda \)-constacyclic code \( < P_{t}^{(k)}(x) > \) (cf. (1)) in \( R_{\nu,\lambda}^{q} \) can be obtained from the idempotent generator of the cyclic code \( < P_{t}^{(k)}(x) > \) in \( R_{\nu,1}^{q} \) just by reducing the latter modulo \( x^n - \lambda \), where \( e \) is the order of the polynomial \( x^n - \lambda \). In [6, Example 11] we illustrated this procedure for the case \( n = 6, q = 5, \lambda = 2 \) and \( e = 24 \). We now shall expand that example further and investigate if and how the various constacyclicomials in \( R_{\nu,\lambda}^{5} \) and the cyclominals in \( R_{24,1}^{5} \) are related.

**Example 14**

In [6, Examples 8, 11] we derived the following relations for \( n = 6, q = 5 \) and \( \lambda \in \{1, 2, 3, 4\} \):

\[ x^{24} - 1 = \prod_{i=0}^{3} (x^6 - 2^i) = (x^6 - 1)(x^6 - 2)(x^6 - 4)(x^6 - 3), \]

\[ x^6 - 1 = \prod_{i \in T_1} P_{t}^{(1)}(x) = (x - 1)(x^2 - x + 1)(x^2 + x + 1)(x + 1), \]

\[ x^6 - 2 = \prod_{i \in T_2} P_{t}^{(2)}(x) = (x^2 - x + 2)(x^2 + 2)(x^2 + x + 2), \]

\[ x^6 - 4 = \prod_{i \in T_3} P_{t}^{(4)}(x) = (x^2 - 2x - 1)(x - 2)(x^2 + 2x - 1)(x + 2), \]

\[ x^6 - 3 = \prod_{i \in T_3} P_{t}^{(5)}(x) = (x^2 - 2)(x^2 - 2x - 2)(x^2 + 2x - 2). \]

The index sets in the above relations are \( T^1 = \{0, 4, 8, 12\}, T^2 = \{1, 9, 13\}, T^3 = \{2, 6, 14, 18\} \) and \( T^3 = \{3, 7, 19\} \). Together these index sets contain the indices of all irreducible polynomials in \( x^{24} - 1 \) or equivalently, the indices of all cyclotomic cosets modulo 24. As primitive \( 24^{th} \) root of unity \( \alpha \) we take a zero of \( x^2 - x + 2 \). With this choice we get the following correspondence between the cyclotomic cosets modulo 24 and the irreducible polynomials over \( GF(5) \) contained in \( x^{24} - 1 \):
\( C_0 = \{0\} \), \( P_0^{(1)}(x) = x - \alpha^0 = x - 1 \),
\( C_4 = \{4, 20\} \), \( P_4^{(1)}(x) = (x - \alpha^4)(x - \alpha^{20}) = x^2 - x + 1 \),
\( C_8 = \{8, 16\} \), \( P_8^{(1)}(x) = (x - \alpha^8)(x - \alpha^{16}) = x^2 + x + 1 \),
\( C_{12} = \{12\} \), \( P_{12}^{(1)}(x) = x - \alpha^{12} = x + 1 \),
\( C_1 = \{1, 5\} \), \( P_1^{(2)}(x) = (x - \alpha^1)(x - \alpha^5) = x^2 - x + 2 \),
\( C_9 = \{9, 21\} \), \( P_9^{(2)}(x) = (x - \alpha^9)(x - \alpha^{21}) = x^2 + 2 \),
\( C_{13} = \{13, 17\} \), \( P_{13}^{(2)}(x) = (x - \alpha^{13})(x - \alpha^{17}) = x^2 + x + 2 \),
\( C_2 = \{2, 10\} \), \( P_2^{(4)}(x) = (x - \alpha^2)(x - \alpha^{10}) = x^2 - 2x - 1 \),
\( C_6 = \{6\} \), \( P_6^{(4)}(x) = x - \alpha^6 = x - 2 \),
\( C_{14} = \{14, 22\} \), \( P_{14}^{(4)}(x) = (x - \alpha^{14})(x - \alpha^{22}) = x^2 + 2x - 1 \),
\( C_{18} = \{18\} \), \( P_{18}^{(4)}(x) = x - \alpha^{18} = x + 2 \),
\( C_3 = \{3, 15\} \), \( P_3^{(3)}(x) = (x - \alpha^3)(x - \alpha^{15}) = x^2 - 2 \),
\( C_7 = \{7, 11\} \), \( P_7^{(3)}(x) = (x - \alpha^7)(x - \alpha^{11}) = x^2 - 2x - 2 \),
\( C_{19} = \{19, 23\} \), \( P_{19}^{(3)}(x) = (x - \alpha^{19})(x - \alpha^{23}) = x^2 + 2x - 2 \).

For the indices \( t \in T^1 \) we have \( t = 0 \mod 4 \), since for such \( t \) -values \( \alpha^t \) is a 6th root of unity, or \((\alpha')^6 = 1\). Notice that all indices \( i \in C_{t}^{24,5} = \{t, tq, \ldots, tq^{m-1}\} \), \( s = 0 \mod 4 \), satisfy \((\alpha')^s = 1\) because \((q, 4) = 1\). (Remember that \( k(= 4) \) is always a divisor of \( q - 1\).) Now, by choice \( \alpha \) itself is a zero of \( x^6 - 2 \), and so \((\alpha')^6 = 2 \) for \( i = 1 \mod 4 \). It follows that \((\alpha')^6 = 4 \) for \( i = 2 \mod 4 \), and \((\alpha')^6 = 3 \) for \( i = 3 \mod 4 \). Furthermore, the cyclotomic cosets modulo 24 are associated with the constacyclotomic cosets modulo 6 in the following way:

\[
\begin{align*}
C_0^{24,5} &= \{0\} \iff C_0^{6,5,1} = \{0\} , \quad C_4^{24,5} = \{4, 20\} \iff C_4^{6,5,1} = \{1, 5\} , \quad C_8^{24,5} = \{8, 16\} \iff C_2^{6,5,1} = \{2, 4\} , \\
C_{12}^{24,5} &= \{12\} \iff C_3^{6,5,1} = \{3\} , \\
C_1^{24,5} &= \{1, 5\} \iff C_0^{6,5,2} = \{0, 1\} , \quad C_9^{24,5} = \{9, 21\} \iff C_2^{6,5,2} = \{2, 5\} , \quad C_{13}^{24,5} = \{13, 17\} \iff C_3^{6,5,2} = \{3, 4\} , \\
C_2^{24,5} &= \{2, 10\} \iff C_0^{6,5,4} = \{0, 2\} , \quad C_6^{24,5} = \{6\} \iff C_1^{6,5,4} = \{1\} , \quad C_{14}^{24,5} = \{14, 22\} \iff C_3^{6,5,4} = \{3, 5\} , \\
C_{18}^{24,5} &= \{18\} \iff C_4^{6,5,4} = \{4\} .
\end{align*}
\]
This correspondence is brought about by the mapping \( C_i^{6,5,j} \mapsto C_{4i+j}^{24,5} \), with \( \lambda = 2, \ j \in \{0,1,2,3\} \). In Theorem 15 we shall prove and specify this kind of relationship in more detail.

Next, we apply Definition 9 which yields the following constacyclonomials for \( n = 6 \) and \( \lambda \in GF(5)^* \):

\[
\begin{align*}
\lambda = 1 & \quad x^0, \ x^1 + x^5, \ x^2 + x^4, \ x^3 \\
\lambda = 2 & \quad x^0, \ x^1 + x^5, \ x^2 + 2x^4 \\
\lambda = 3 & \quad x^0, \ x^1 + x^5, \ x^2 + 3x^4 \\
\lambda = 4(-1) & \quad x^0, \ x^1 + x^5, \ x^2 - x^4, \ x^3
\end{align*}
\]

As one can see, the number of constacyclonomials is always equal to the number of irreducible polynomials for each value of \( \lambda \in GF(q)^* \). The constacyclonomials can also be obtained from the cyclonomials \( c_i^{24,5}(x) = x^1 + x^5, \ c_i^{24,5}(x) = x^2 + x^{10}, \ c_i^{24,5}(x) = x^3 + x^{15} \), by reducing modulo \( x^6 - 2 \) (cf. Theorem 10 (v)). Notice that \( x^3 + x^{15} = x^3 + 4x^3 = 0 \). □

As preparation for the next theorem, we extend the number of parameters. Let \( P^{(\lambda,j)}(x) \) be an irreducible polynomial contained in \( x^n - \lambda^j \) (cf. (1)) of degree \( m \). If \( \alpha \) is a zero of \( x^n - \lambda \), then \( \alpha^j \) is a zero of \( x^n - \lambda^j \) and the \( m \) zeros of \( P^{(\lambda,j)}(x) \) can be written as \( \alpha^j, \alpha \zeta^{c_1}, \zeta^{c_2}, ..., \alpha \zeta^{c_{m-1}} \) with \( \alpha \zeta^{c_i} = (\alpha \zeta^{c_0})^i, \ 0 \leq i \leq m-2 \) (cf. also Theorem 13 (vi) and its proof). Since this is true for any \( j \) with \( 0 \leq j \leq k-1, \ k = \text{ord}_q(\lambda) \), we define constacyclotomic cosets where both \( \lambda \) and \( j \) are to be considered as parameters:

\[
C_{i,j}^{m,q,\lambda,j} = \{c_0(=t), c_1, ..., c_{m-1}\}, \quad (10)
\]

where \( t \in T^{n,j,q,\lambda} \) and \( c_0, c_1, ..., c_{m-1} \in \{0,1, ..., n-1\} \). For \( j = 0 \) the cosets (10) are related to the cyclotomic cosets \( C_{i+1}^n \) by (7), while for \( j = 1 \) they are identical to the constacyclotomic cosets (5).

Of course one can also use (5) to obtain the zeros of the irreducible polynomial \( P_i^{(\lambda,j)}(x) \), by putting \( \mu := \lambda^j \) and next applying (5) and (6) with \( \lambda \) replaced by \( \mu \). The difference is when doing so, that the integers in (5) and hence the zeros of \( P_i^{(\lambda,j)}(x) \) are expressed in terms of a zero of \( x^n - \mu \), while (10) is based on the zero \( \alpha \) of \( x^n - \lambda \) for all values of \( j \).
4. Suggestions for further study of constacyclic idempotents

Finally, we collect the main results of this report in the next theorem. They may serve as a basis for the study of the orthogonality relations between the primitive idempotent generators of constacyclotomic codes in a possible follow-up report. Roughly speaking, there seem to be two promising approaches. When one only is interested in the constacyclic codes modulo \(x^n - \lambda^j\) for a fixed value of \(\lambda\), one should focus on the constacyclotomic cosets modulo \(n\) as defined in (5) and (6), whereas one should apply the cyclotomic cosets modulo \(kn\) and the cosets defined in (10) when the interrelationship of all constacyclic codes modulo \(x^n - \lambda^j\) is to be studied.

**Theorem 15**

Let \(q\) be a prime power, \(n\) an integer with \((n, q) = 1\), and let \(\lambda \in GF(q)^*\) have order \(k\). Let \(x^n - \lambda \in GF(q)[x]\) be a polynomial of order \(e\) and let \(\alpha\) be a zero of \(x^n - \lambda\) of order \(e\).

(i) The zeros of \(x^n - \lambda^j\), \(0 \leq j \leq k - 1\), can be written as \(\alpha^{kj}\), \(0 \leq i \leq n - 1\).

(ii) The zeros of \(x^n - \lambda^j\), \(0 \leq j \leq k - 1\), can be written as \(\alpha^j\zeta^i\), \(0 \leq i \leq n - 1\), with \(\zeta := \alpha^k\).

(iii) The integers in (10) satisfy the recurrence relation \(kc_{i+1} + j = (kc_i + j)q \mod kn\), \(0 \leq i \leq m - 1\).

(iv) The mapping of \(\{0, 1, \ldots, n - 1\}\) into \(\{0, 1, \ldots, kn - 1\}\) defined by \(i \to ki + j\) defines a one-one correspondence between the constacyclotomic cosets \(C_{t}^{n,q,\lambda^j}\), \(t \in T_\lambda\), and the cyclotomic cosets \(C_{t}^{kn,q,\lambda^j}\) for any \(j\), \(0 \leq j \leq k - 1\).

(v) There exists a one-one correspondence between the irreducible polynomials \(P_{t}^{(\lambda^j)}(x)\), the cyclotomic cosets \(C_{t}^{kn,q,\lambda^j}\) and the constacyclotomic cosets \(C_{t}^{n,q,\lambda^j}\).

(vi) The number of constacyclonomials \(c_{t}^{n,q,\lambda^j}(x)\) is equal to the number of irreducible polynomials \(P_{t}^{(\lambda^j)}(x)\), for all \(\lambda \in GF(q)^*\) and for \(0 \leq j \leq k - 1\).

**Proof**

(i) The polynomial \(x^n - \lambda\) has always a zero \(\alpha\) of order \(e = kn\) (cf. Theorem 5 (ii) and Theorem 6). Hence, \(\zeta := \alpha^k\) is a primitive \(n\)th root of unity and therefore the elements \(\alpha^{ki}\), \(0 \leq i \leq n - 1\), are the \(n\) zeros of \(x^n - 1\). Furthermore, \(\alpha\) is a zero of \(x^n - \lambda\) by definition, and so \(\alpha^{ki+1}\), \(0 \leq i \leq n - 1\), are the \(n\) zeros of \(x^n - \lambda\). More generally, since \((\alpha^j)^i = \lambda^j\) it follows that \(\alpha^{ki+j}\), \(0 \leq i \leq n - 1\), are the \(n\) zeros of the polynomial \(x^n - \lambda^j\) for \(0 \leq j \leq k - 1\) (cf. also Theorem 4 in [6]).

(ii) This follows immediately from (i).

(iii) The \(n\) zeros of \(x^n - \lambda^j\) can be written as \(\alpha^j\zeta^i\), \(0 \leq i \leq n - 1\). Let the zeros \(\alpha^j\zeta^{i_0}, \alpha^j\zeta^{i_1}, \ldots, \alpha^j\zeta^{i_{m-1}}\), with \(\alpha^j\zeta^{i_0} = (\alpha^j\zeta^{i_{m-1}})^q\), \(0 \leq i \leq m - 1\), be the zeros of the irreducible polynomial \(P_{t}^{(\lambda^j)}(x)\) of degree \(m\). We can write \((\alpha^j\zeta^{i_0})^q = \alpha^j\zeta^{i_0}\), \(0 \leq i \leq m - 1\). So, \((\alpha^j\zeta^{i_0})^q = (\alpha^j)^q\zeta^{0i_0}\) = \(\alpha^q\zeta^{0i_0} = \alpha^{q(ki_0 + j)}\). On the other hand, we have \((\alpha^j\zeta^{i_0})^q = \alpha^j\zeta^{i_0} = \alpha^{ki_0 + j}\). It follows that \(kc_{i+1} + j = (kc_i + j)q \mod kn\).

(iv) This is an immediate consequence of (iii).
(v) This is an immediate consequence of (iv).
(vi) This follows from Theorem 13 (ii).

Remark
Though there are as many constacyclonomials as there are irreducible polynomials, and hence as there are constacyclotomic cosets, for fixed values of $n$, $q$, $\lambda$, and $j$, we are not able (yet) to establish a kind of canonical one-to-one correspondence between constacyclotomic cosets and constacyclonomials like there exists in the cyclic case (i.e. in case $\lambda = 1$). A simple correspondence $C_{n,q,\lambda}^i \leftrightarrow c_{n,q,\lambda}^i(x)$ does not work out, as Example 16 will show.

Neither is there a relationship $c_{kn,p}^{j}(x) \equiv c_{n,q,\lambda}^{j}(x) \mod x^n - \lambda^j$ (cf. also Theorem 10 (ii) and Example 11). Furthermore, the second equality in Theorem 6 (v) suggests the relation $C_{n,q,\bar{\lambda}}^i = k^{-1}[0,q-1,q^2-1,\ldots] + C_{i}^{n,q,\lambda} = C_{i}^{n,q,\lambda} + C_{i}^{n,q,\bar{\lambda}}$. This is true if we consider the coset $C_{i}^{n,q}$ as a multiset containing all its elements $|C_{i}^{n,q,\lambda}|/|C_{i}^{n,q}|$ times, or similarly, if we consider $C_{i}^{n,q,\lambda}$ as a multiset in case that $|C_{i}^{n,q}| > |C_{i}^{n,q,\lambda}|$. However, it does not yield in general a one-to-one correspondence between the family of constacyclotomic cosets and the family of constacyclonomials. This is due to the fact that actually, the cyclotomic cosets $C_{iq}^{n,q} := \{iq, i(q^2)^{1}, i(q^2)^{2}, \ldots\}$, and hence the corresponding constacyclonomials $c_{n,q,\lambda}^i(x)$, are equal for all relevant values of $i$. A similar observation can be made for $C_{i}^{n,q,\lambda}$. So, if $t \in C_{i}^{n,q,\lambda}$, then both $C_{i}^{n,q}$ as well as $C_{t}^{n,q}$ can be seen as corresponding to $C_{i}^{n,q,\lambda}$. It can also happen that there is no cyclotomic coset to be found such that it contains any of the integers of $C_{i}^{n,q,\lambda}$. We shall illustrate this in Examples 16 and 17.

Example 15
We have $C_{0,5,2} = \{0,1\}$, $C_{2,5,2} = \{2,5\}$, $C_{3,5,2} = \{3,4\}$, while $c_{0,5,2}^{6,5,2}(x) = 1$, $c_{2,5,2}^{5,5,2}(x) = x^2 + 2x^4$ and $c_{3,5,2}^{6,5,2}(x) = x^3 + x^5$. Notice that $x^3 + x^{15} = x^3 + 4x^3 = 0$ and therefore, according to Definition 9, there is no constacyclonomial $c_{3,5,2}^{6,5,2}(x)$.

Furthermore, $c_{0,5,2}^{24,5,1}(x) = x^9 + x^{21} = 2x^3 + 3x^3 = 0 \mod x^6 - 2$, while $c_{2,5,2}^{5,5,2}(x) = x^2 + 2x^4$.

Example 16
In this example we determine the constacyclotomic cosets for $n = 14$, $q = 5$ and for all values of $\lambda \in GF(5)^*$ and the constacyclonomials in the various subcases. The latter polynomials will be represented by their sets of exponents which we tentatively could call (consta)cyclonomics.

\[ \lambda = 1, k = 1, l = 4 \]

\[
\begin{align*}
\{0,4,10,12,8,2\} & \quad \leftrightarrow \quad \{0\} \\
\{1,9,7,11,3,5\} & \quad \leftrightarrow \quad \{1,5,11,13,9,3\} \\
\{2,0,4,10,12,8\} & \quad \leftrightarrow \quad \{2,10,8,12,4,6\} \\
\{7,11,3,5,1,9\} & \quad \leftrightarrow \quad \{7\}
\end{align*}
\]
\[\lambda = -1, k = 2, l = 2\]

\[
\begin{align*}
\{0,2,12,6,4,8\} & \Leftrightarrow \{0\} \\
\{7,9,5,13,11,1\} & \Leftrightarrow \{7\} \\
\{3\} & \Leftrightarrow \{3,1,5,11,13,9\} \\
\{10\} & \Leftrightarrow \{10,8,12,4,6,2\}
\end{align*}
\]

\[\lambda = 2, k = 4, l = 1\] and \[\lambda = 3, k = 4, l = 1\]

\[
\begin{align*}
\{0,1,6,3,2,11\} & \Leftrightarrow \{0\} \\
\{4,7,8,13,10,9\} & \Leftrightarrow \{4,6,2,10,8,12\} \\
\{5,12\} & \Leftrightarrow \{5,11,13,9,3,1\}
\end{align*}
\]

We can see that the rule \[C_0^{n,q,\lambda} = C_0^{n,q,\lambda} + C_0^{n,q,\lambda} \mod n\] is valid if we interpret the respective (consta)cyclotomic cosets as multisets. We give a few examples:

\[
\begin{align*}
C_0^{14,5,1} + C_2^{14,5} &= \{0,4,10,12,8,2\} + \{2,10,8,12,4,6\} = \{2,0,4,10,12,8\} = C_2^{14,5,-1}, \\
C_0^{14,5,-1} + C_5^{14,5,-1} &= \{0,2,12,6,4,8\} + \{5,11,13,9,3,1\} = \{5,13,11,1,7,9\} = C_3^{14,5,-1} (= C_7^{14,5,-1}), \\
C_0^{14,5,-1} + C_3^{14,5} &= \{0,2,12,6,4,8\} + \{3,1,5,11,13,9\} = \{3,3,3,3,3,3\} = C_3^{14,5,-1}, \\
C_0^{14,5,-1} + C_7^{14,5} &= \{0,2,12,6,4,8\} + \{7,7,7,7,7,7\} = \{7,9,5,13,11,1\} = C_7^{14,5,-1}, \\
C_0^{14,5,2} + C_5^{14,5} &= \{0,1,6,3,2,11\} + \{5,11,13,9,3,1\} = \{5,12,5,12,5,12\} = C_5^{14,5,2}.
\end{align*}
\]

In all four subcases of the above example we have a one-to-one correspondence between the constacyclotomic cosets and the cyclonomics, if we consider these cyclonomics as different cyclically ordered sets whenever their first integers differ. These first integers can be taken as subindex for the cyclonomics as well as for the corresponding constacyclotomic coset. The next example will show that this cannot always be accomplished.

**Example 17**
Take \(n = 16\) and \(q = 3\) and all possible values for \(\lambda \in GF(3)^*\).

\[\lambda = 1, k = 1, l = 2\]

\[
\begin{align*}
\{0,2,8,10\} & \Leftrightarrow \{0\} \\
\{1,5\} & \Leftrightarrow \{1,3,9,11\} \\
\{3,11\} & \Leftrightarrow \{2,6\}
\end{align*}
\]
It will be clear that in both subcases it is not possible to index the constacyclotomic cosets and the cyclonomic cosets by the same indices.

We may conclude from the previous examples that though it is not clear yet whether there exists a canonical one-to-one correspondence between the set of constacyclonomials \( \{ c^{n,q}_{s} \} \) and the set of constacyclotomic cosets \( \{ C^{n,q}_{s} \} \) like in the case of \( \lambda = 1 \), there definitely is no mapping in general from the first set onto the second set such that corresponding objects can be labelled by the same common index. The following scheme recapitulates the correspondences obtained thus far between the various sets:

\[
C^{n,q}_{s} \leftrightarrow P^{(\lambda)}_{s}(x) \leftrightarrow G^{(\lambda)}_{s}(x)
\]

\[
c^{n,q}_{s}(x) \leftrightarrow c^{n,q}_{s}(x) \leftrightarrow C^{n,q}_{s} \leftrightarrow P^{(1)}_{s}(x) \leftrightarrow G^{(1)}_{s}(x)
\]

Example 18

In the case \( n = 6 \), \( q = 5 \) and \( \lambda = 2 \) we index the constacyclonomial \( x^2 + 2x^4 \) by the index 2, so \( c^{6,5}_{2}(x) = x^2 + 2x^4 \). Consequently, we have \( C^{6,5}_{2} = \{ 2, 5 \} \) and \( P^{(2)}_{2}(x) = (x - \alpha_2^{0})(x - \alpha_2^{5}) = x^2 + 2 \). By changing the coefficients of \( c^{6,5}_{2}(x) \) into 1, we get \( c^{6,5}_{1}(x) = x^2 + x^4 \), \( C_{1}^{6,5} = \{ 2, 4 \} \) and \( P^{(1)}_{2}(x) = (x - \zeta_2^3)(x - \zeta_2^{4}) = x^2 + x + 1 \). Similarly, we write \( c^{6,5}_{0}(x) = x^5 = 1 \), \( C_{0}^{6,5} = \{ 0, 1 \} \), \( P^{(2)}_{0}(x) = (x - \alpha_0^{0})(x - \alpha_0^{5}) = x^2 - x + 2 \) and \( c^{6,5}_{1}(x) = x^1 + x^5 \), \( C_{1}^{6,5} = \{ 1, 0 \} \). However, this yields a conflict in the procedure of indexing, since the coset \( \{ 0, 1 \} \) now has two different indices. Therefore, we try \( c^{6,5}_{2}(x) = x^1 + x^5 \), \( c^{6,5}_{3} = \{ 5, 1 \} \), \( P^{(2)}_{3}(x) = (x - \alpha_2^{0})(x - \alpha_2^{5}) = x^2 - x + 2 \), and finally \( c^{6,5}_{2}(x) = x^2 + 2x^4 \), \( C_{2}^{6,5} = \{ 2, 5 \} \), \( P^{(2)}_{2}(x) = (x - \alpha_2^{0})(x - \alpha_2^{5}) = x^2 + 2 \).
We can also take 4 as index for the above constacyclonomial, i.e. \( c_4^{6,5,2}(x) = x^2 + 2x^4 \), which enhances \( C_4^{6,5,2} = \{4, 3\} \). Continuing in this way we find the following consistent correspondence:

\[
c_4^{6,5,2}(x) = x^2 + 2x^4 \iff C_4^{6,5,2} = \{4, 3\}, \quad c_0^{6,5,2}(x) = x^0 \iff C_0^{6,5,2} = \{0, 1\},
\]

\[
c_5^{6,5,2}(x) = x^1 + x^5 \iff C_5^{6,5,2} = \{5, 2\}.
\]

\[\square\]

Example 19

In Example 14 we have e.g. \( C_3^{6,5,2} = \{3, 5\} \). So, \( \lambda = 2, \ k = 4 \) and \( j = 2 \), and therefore \( 4.3 + 2 = 14 \) and \( 4.5 + 2 = 22 \) are the integers of \( C_{14}^{24,5} \). Similarly, we have \( C_1^{6,5,2} = \{1, 2\} \). So, \( \lambda = 2, \ k = 4 \) and \( j = 3 \), and therefore \( 4.1 + 3 = 7 \) and \( 4.2 + 3 = 11 \) are the integers of \( C_7^{24,5} \), illustrating Theorem 14. \( \square \)

Example 20

We take \( n = 8, \ q = 3, \ \lambda = 2 \), and hence \( k = 2 \).

The polynomial \( x^8 - 2 \) can be factorized as \( (x^4 + x^3 - 1)(x^4 - x^2 - 1) \). It can easily be verified that the two polynomials in the right hand side are irreducible in \( GF(3)[x] \). For the 3-constacyclotomic cosets we find \( C_0^{8,3,2} = \{0, 1, 4, 5\} \) and \( C_2^{8,3,2} = \{2, 7, 6, 3\} \). Furthermore we find, by applying Definition 7, two constacyclonomials i.e. \( c_0^{8,3,2}(x) = 1 \) and \( c_2^{8,3,2}(x) = x^2 + x^6 \), in accordance with Theorem 13 (ii) or Theorem 14 (vi). One can also find these from \( c_0^{16,3}(x) = 1 \) and \( c_2^{16,3}(x) = x^2 + x^6 \) by reducing modulo \( x^8 - 2 \), which illustrates Theorem 10 (v). Notice that

\[
c_1^{16,3,1}(x) = x^1 + x^3 + x^9 + x^{11} = x^1 + x^3 + x^1 + x^3 = 2(x^1 + x^3) \mod x^8 - 2
\]

and that

\[
c_2^{16,3,1}(x) = x^5 + x^{15} + x^{13} + x^7
\]

gives rise to the zero polynomial when reduced modulo \( x^8 - 2 \). This shows that, in general, there is no relation \( c_{\lambda n,j}^{q}(x) = C_{\lambda}^{q,n,j}(x) \mod x^n - \lambda j \) (cf. the remarks right after Theorem 15). Finally, the two primitive idempotents are \( -x^6 - x^2 - 1 \) and \( x^6 + x^2 - 1 \), which correspond respectively to \( x^4 + x^2 - 1 \) and \( x^4 - x^2 - 1 \).

Next, we consider the same polynomial \( x^8 - 2 \), but now over \( GF(5) \). We only find one constacyclonomial: \( c_0^{8,5,2}(x) = x^0 = 1 \). So, there must be only one irreducible factor, \( x^8 - 2 \) itself. Indeed, by applying eq. (6) with \( l = 2 \), we find the constacyclic coset \( C_0^{8,5,2} = \{0, 1, 6, 7, 4, 5, 2, 3\} \) containing all integers of \( \{0, 1, ..., 7\} \). This implies that the polynomial with zeros \( \alpha \zeta^0, \alpha \zeta^1, ..., \alpha \zeta^7 \) is irreducible. \( \square \)
References


