Generalized Mattson - Solomon Transformations

and

Weight Spectra of Primitive Cyclic Codes

Faculty of Mathematics and Informatics. Delft University of Technology. The Netherlands/

Department of Communication and Information. University of Tilburg. The Netherlands

A.J. van Zanten

Abstract

This paper is a continuation of ref. 4. *Firstly, a trial is made to introduce a more general type Mattson-Solomon transformation, by replacing* $-1(=n-1)$ *in* $A(x)=\sum_{j\in C_1^{n,q}} r(\zeta^j)x^{-1}$ *by an arbitrary power prime to* n. *However, it turns out readily that such a change is equivalent to choosing a different primitive* n^{th} *root* ζ *of unity in the original M.S. transformation. In the final sections a number of examples is studied how to apply the M.S. transformation to determine the weight of the code words of a minimal cyclic code. In order to apply this method to a general case more knowledge is required about the nature of the zeros of the so-called modified cyclonomials.*

Contents

1. Introduction and preliminaries

In this report we investigate properties of idempotents and cyclonomials belonging to primitive cyclic codes. For definitions, conventions and notation, we refer to the introductions of [3,4,5].

2. The Mattson – Solomon transformation

We start by giving the definition of the Mattson – Solomon transformation as formulated in [2,3].

Definition 1

Let $p(x) := a_{n-11}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ *be a polynomial over* $GF(q^m)$ *of degree at most* $n-1$.

Then the polynomial $(\Phi p)(x)$ *is defined as* $P(x) := \sum_{j=1}^{n} p(\zeta^j)x^{n=j} = \sum_{j=0}^{n-1} p(\zeta^{n-j})x^j$ *, where* ζ *is some primitive* n^{th} *root of* 1.

The polynomial $P(x)$ is called the *Mattson – Solomon polynomial (transform)* or *M.S. transform* of $p(x)$ and is again an element of $GF(q^m)[x]$ or better of the ring R^{n,q^m} . In the next we shall denote an M.S. transform of a polynomial by the capital version of its name. The next theorem presents some simple properties of M.S. polynomials.

Theorem 2

(i) *For any polynomial* $p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ *in* R^{n,q^m} *one has the inverse transformation* $p(x) = n^{-1}(\Phi P)(x^{-1})$ *and* $a_k = n^{-1}P(\zeta^{-k})$.

(ii) *Let* $a(x)$ *and* $b(x)$ *be two elements of the ring* R^{n,q^m} *, then we have for their polynomial product and their Kronecker product the equality* $\Phi(a(x)) \otimes \Phi(b(x)) = \Phi(a(x)b(x))$ *or, equivalently,* $A(x) \otimes B(x) = AB(x)$.

(iii) *The mapping* Φ *defines an isomorphism between the algebras* A^{n,q^m} *and* $A^{n,q^m,\otimes}$.

For the proofs we refer to Section 4 of [3].

Theorem 3

For any $s,t \in U^{n,q} (= S^{n,q} = T^{n,q})$ *the following Mattson – Solomon transformations hold.*

(i) *The M.S. transform of the irreducible polynomial* $p_t(x)$ *is* $P_t(x) = \underline{p}_t(x^{-1}) = x^{-m}\, \underline{p}_t^{rev}(x)$,

where $\underline{p}_t(x) := \sum_{j=0}^{n-1} p(\zeta^j) x^j$.

(ii) *The M.S. transform of the cyclonomial* $c_s(x)$ *is* $C_s(x) = n\theta_s(x)$.

(iii) *The M.S. transform of the primitive idempotent* $\theta_t(x)$ *is* $\Theta_t(x) = c_{n-t}(x)$.

We remind the reader of the definition $p^{rev}(x) := x^m p(x^{-1})$, where $p(x)$ is any irreducible polynomial of degree m. The zeros of $p^{rev}(x)$ are the inverses of the zeros of $p(x)$.

In [5] we introduced the following bilinear form for two elements $a(x), b(x) \in R^{n,q}$:

$$(a,b) := \sum_{i=0}^{n-1} a(\zeta^i) b(\zeta^i), \tag{1}$$

where ζ is a primitive n^{th} root of unity (cf. eq. (11) in [5] with $\alpha \neq \zeta^{-1}$). We now declare this definition valid for all elements of the ring R^{n,q^m} in order to apply (11) to M.S. transforms.

Theorem 4

If $a(x)$ *and* $b(x)$ *are two elements of* R^{n,q^m} *and if* $A(x)$ *and* $B(x)$ *are their M.S. transforms, then one has* $(A,B) = n(a,b^{rev})$.

Proof

Applying the definition of M.S. transforms and eq. (11), we obtain straightforwardly

$$(A,B) = \sum_{k=0}^{n-1} \sum_{i=1}^{n} a(\zeta^i) \zeta^{-ki} \sum_{j=1}^{n} b(\zeta^j) \zeta^{=kj} = \sum_{i,j=1}^{n} a(\zeta^i) b(\zeta^j) \sum_{k=0}^{n-1} \zeta^{-k(i+j)} .$$

When the index j runs from 1 until n then, for fixed values of i and k, the only nonzero contribution occurs for $j = -i$. Hence, we get

$$(A,B) = n \sum_{i=1}^{n} a(\zeta^i) b(\zeta^{-i}) = n \sum_{i=1}^{n} a(\zeta^i) b^{rev}(\zeta^i) = n(a,b^{rev}) \tag{2}$$

■

3. More Mattson – Solomon type transformations

For the definition of other M.S. type transformations we introduce the well-known multiplicative group of integers modulo n which are prime to, of size $\varphi(n)$

$$U(n) := \{r \mid (r,n) = 1,\ 0 < r < n\}. \tag{3}$$

Definition 5

Let $p(x) := a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ *be a polynomial over* $GF(q^m)$ *of degree at most* $n-1$. *Let furthermore* $\underline{p}(x) := \sum_{j=0}^{n-1} p(\zeta^j)x^j$ *be the associated polynomial of* $p(x)$ *for some primitive* n^{th} *root* ζ *of unity. Then the* r^{th} *Mattson – Solomon polynomial of* $p(x)$ *is defined as* $(\Phi_r p)(x) = P_r(x) = \underline{p}(x^r)$.

So, we obtain in explicit form the following expression for the r^{th} M.S. polynomial of $p(x)$

$$P_r(x) = \sum_{j=0}^{n-1} p(\zeta^j)x^{rj}. \tag{4}$$

As stated in its definition, the polynomial $P_r(x) = (\Phi_r p)(x)$ will be called the r^{th} Mattson-Solomon transform or r^{th} M.S. transform of $p(x)$, while the mapping Φ_r is called the r^{th} M.S. transformation. For $r = -1$ we get the conventional M.S. polynomial and for $r = 1$ the associated polynomial of $p(x)$.

Theorem 6

(i) *For any polynomial* $p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ *in* R^{n,q^m} *one has the inverse transformation* $n^{-1}(\Phi_{r^{-1}}P_r)(x^{r^{-1}}) = p(x)\ mod\ x^n - 1$.

(ii) $a_{-kr} = n^{-1}P_r(\zeta^k)$.

Proof

(i) It follows from Definition 5 and eq. (4) that

$$\underline{P}_r(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p(\zeta^j)\zeta^{rij}x^i \,, \tag{5}$$

and hence

$$(\Phi_s P_r)(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p(\zeta^j)\zeta^{rij}x^{si} = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} p(\zeta^i)\zeta^{rij}x^{sj} \,. \tag{6}$$

Taking $s=-r$ and $j=rk$ yields na_k as coefficient of x^k in (6), due to the relation $\sum_{j=0}^{n-1}\zeta^{bj} = \delta_{b,0}$.

Since this holds for any k, $0 \le k \le n-1$, the equality in (i) now follows.
(ii) From (4) we immediately obtain

$$P_r(\zeta^k) = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i\zeta^{ji}\zeta^{krj} = \sum_{i,j=0}^{n-1} a_i\zeta^{j(i+kr)}\sum_{j=0}^{n-1} a_{-kr} = na_{-kr} \,. \qquad \blacksquare$$

From Definition 5 it is already clear that the "normal" M.S. polynomial $P(x)(=P_{-1}(x))$ depends on the choice one makes for the primitive n^{th} root of unity ζ. So, we better could denote such a polynomial by $P(x,\zeta) \equiv P_{-1}(x)$ and more generally $P_r(x,\zeta) \equiv P_r(x)$. The next theorem shows that choosing a different primitive root, i.e. taking an appropriate power of ζ yields the r^{th} M.S. polynomial for any $r \in U(n)$.

Theorem 7

For any $r \in U(n)$ one has $P(x,\zeta^{-r^{-1}}) = P_r(x)$.

Proof

Since $r \in U(n)$ implies $r^{-1} \in U(n)$ and hence $-r^{-1} \in U(n)$, we have that $\zeta' = \zeta^{-r^{-1}}$ is another primitive n^{th} root of unity. So we may write $P(x,\zeta^{-r^{-1}}) = \sum_{j=0}^{n-1} p(\zeta^{-r^{-1}j})x^{-j}$. Replacing the summation index j by $j' = -r^{-1}j$ yields finally $P(x,\zeta') = \sum_{j'=0}^{n-1} p(\zeta'^{j'})x^{rj'}$. $\blacksquare$

Actually, Theorem 6 (i) can be seen as an immediate consequence of the above theorem and proving it separately is not really necessary. The same remark can be made for Theorems 2 and 4, which results in the following reformulation of their contents.

Theorem 8

If $a(x)$ *and* $b(x)$ *are two elements of* R^{n,q^m} *and if* $A_r(x)$ *and* $B_r(x)$ *are their* r^{th} *M.S. transforms, then the following relations hold for any* $r \in U(n)$.

(i) $\Phi_r(a(x)) \otimes \Phi_r(b(x)) = \Phi_r(a(x)b(x))$ *and the mapping* Φ_r *defines an isomorphism between the algebras* $A^{n.q^m}$ *and* $A^{n,q^m,\otimes}$.

(ii) $(A_r, B_r) = n(a, b^{rev})$.

The next theorem presents the r^{th} M.S. transforms of some special polynomials, generalizing similar results in [3].

Theorem 9

(i) *For any primitive idempotent* $\theta_t(x)$ *and for all* $r \in U(n)$ *one has* $(\Theta_t)_r(x) = c_{rt}(x)$;

(ii) *For any cyclonomial* $c_s(x)$ *and for all* $r \in U(n)$ *one has* $(C_s)_r(x) = n\theta_{-s/r}(x)$.

Proof

(i) From the definition of the r^{th} M.S. transform of a polynomial in R^{n,q^m} we have for all $t \in T^{n,q}$

$$(\Theta_t)_r(x) = \sum_{j=0}^{n-1} \theta_t(\zeta^j) x^{tj} = x^{rt} + x^{rtq} + ... + x^{rtq^{m_t-1}} = c_{rt}(x),$$

Since $\theta_t(\zeta^j)$ is equal to 1 if $j \in C_t = (t, tq, ..., tq^{m_t-1})$, whereas it equals 0 otherwise.

(ii) Similarly, we have for all $s \in S^{n,q}$

$$(C_s)_r(x) = \sum_{j=0}^{n-1} c_s(\zeta^j) x^{rj} = \sum_{j=0}^{n-1} (x^{js} + x^{jsq} + ... + x^{jsq^{m_s-1}}) x^{rj} = \sum_{j=0}^{n-1} \mu_{j,s} x^{rj},$$

where $\mu_{j,s}$ stands for the sum of the j - powers of the zeros of the irreducible polynomial $p_s(x)$. From [alg, theorem 4 (i)] we know that $\mu_{-s,t} = n\xi_s^t$, where ξ_s^t is the general coefficient in the expression for a primitive idempotent w.r.t. the basis of cyclonomials in $A^{n,q}$, i.e. $\theta_t(x) = \sum_s \xi_s^t c_s(x)$ (cf. [3,4,5]. Applying these relations provides us with

$$C_s(x) = \sum_{j=0}^{n-1} \xi_{-j}^s x^{rj} = \sum_{j=0}^{n-1} \xi_j^s x^{-rj} = n \sum_{u \in S^{n,q}} \xi_u^s c_u(x^{-r}) = n\theta_s(x^{-r}).$$

Eq. (16) in [5] we pointed out that $\theta_{rt}(x) = \theta_t(x^{1/r})$ for all $r \in U(n)$ and $t \in T^{n,q}$. Replacing r by $-1/r$ which is also an element of $U(n)$ gives the result in (ii). ■

We remark that idempotents like $\theta_t(x)$ and $\theta_{rt}(x)$, with $r \in U(n)$ were called r- conjugated idempotents [4,5]. Another remark we should make is that the relationship between the weight of a polynomial and the number of zeros of its normal M.S. transform (cf. [3, Theorem 18]) is also valid for its r^{th} M.S. transform. Again, it is not necessary to prove this explicitly, since this relationship in the normal case already holds for any primitive ζ. Applying Theorem 7 then gives the "general result" immediately.

We shall now apply this to the primitive idempotents and cyclonomials belonging to the primitive cyclic code $\mathbf{C}_1^{n,q} := < f_1(x)) > := < (x^n - 1)/P_1(x) >$ where the irreducible polynomial $P_1(x) = (x - \zeta^1)(x - \zeta^q)....(x - \zeta^{q^{m-1}})$ divides $x^n - 1$. The other irreducible dividing polynomials of $x^n - 1$ are labeled by the index $s \in S^{n,q}$, as well as the corresponding cyclonomials , while the corresponding idempotents are labeled by an index $t \in T^{n,q}$. We always choose $S^{n,q} = T^{n,q} =: U^{n,q}$. So, we can write $x^n - 1 = \prod_{s \in S^{n,q}} P_s(x) = \prod_{s \in U^{n,q}} P_s(x)$.

Theorem 10

Let $P_1(x)$ be an irreducible polynomial over $GF(q)$ of order n, and let ζ be one of its zeros. Let furthermore $\{c_s(x) \mid s \in S^{n,q}\}$, be the set of cyclonomials and $\{\theta_t(x) \mid t \in T^{n,q}\}$ be the set of primitive idempotents in the algebra $A^{n,q}$. Then the following relations hold for any $r \in U(n)$.

(i) *$c_{rt}(x)$ has d zeros of type ζ^j, if and only if $\theta_t(x)$ has weight $n - d$;*

(ii) *$c_s(x)$ has weight w, if and only if $\theta_{-s/r}(x)$ has $m - w$ zeros of type ζ^j ;*

(iii) *If $c_t(x)$ has zeros ζ^{i_1}, ζ^{i_2},...., ζ^{i_l}, then $\theta_{r^{-1}t}(x)$ has zero coefficients at positions i_1, i_2,...., i_l and vice versa.*

(iv) *If $\theta_s(x)$ has zeros $\zeta^{i_1}, \zeta^{i_2}, ..., \zeta^{i_l}$, then $c_{-rs}(x)$ has zero coefficients at positions $i_1, i_2, ..., i_l$.*

All these statements are consequences of Theorems 9 and 6 (ii).

As preparation for the study of the weight spectra of minimal (primitive) cyclic codes, we now present a few properties of the cyclonomials $Cy := \{c_s(x) \mid s \in S^{n,q}\}$ and the primitive idempotents $Id := \{\theta_t(x) \mid t \in T^{n,q}\}$. All these polynomials are elements of $A^{n,q}$, which is equipped with the bilinear form

$$(p,q) := \sum_{i=1}^{n} p(\zeta^i)q(\zeta^i). \tag{7}$$

Theorem 11

(i) *Both sets* Cy *and* Id *form an orthogonal basis of the algebra* $A^{n,q}$ *considered as vector space.*

(ii) *For any pair* $j,k \in S^{n,q}$ *one has* $(c_{j^*}, c_k) = nm_j\delta_{j,k}$.

(iii) *For any pair* $l,m \in T^{n,q}$ *one has* $(\theta_l, \theta_m) = m_l\delta_{l,m}$.

(iv) *The transition between these bases is given by the following relation* $\theta_t(x) = \sum_{s\in S^{n,q}} \xi_s^t c_s(x)$,

$\xi_s^t = \mu_{s^*,t}/n$ *and by* $c_s(x) = \sum_{t\in T^{n,q}} \eta_t^s \theta_t(x)$, $\eta_t^s = n\frac{m_s}{m_t}\xi_{s^*}^t$, *for any* $s,t \in S^{n,q} (= T^{n,q})$, *and where* $\mu_{s,t}$ *stands for the sum of the* s *- powers of the sum of the* m_t *zeros of* $P_t(x)$.

For the proofs we refer to [3, Theorems 3 and 4]. We remark that an index $j^* \in S^{n,q}$ is equivalent to the index $-j \in S^{n,q}$. Furthermore, we have $\mu_{s,t} = -m_t p_{st}/m_{st}$,where p_{st} is the coefficient of the one but highest power of x in the irreducible polynomial $P_{st}(x)$.

4. The weight spectrum of a minimal cyclic code

Firstly, we present a compilation of properties of the codewords of a minimal cyclic code $\boldsymbol{C}_t^{n,q}$ which is defined by an irreducible polynomial $P_t(x)$, $t \in T^{n,q}$, which is of order n. We always assume that ζ is one of its zeros. So, ζ is a primitive n^{th} root of 1.

Theorem 12

(i) *The codewords of* $\boldsymbol{C}_t^{n,q}$ *can be written as* $a(x) = s(x)g(x) \mod x^n - 1$, *where* $g(x) = \prod_{i\notin C_t^{n,q}} (x - \zeta^i)$ *and* $s(x)$ *is an arbitrary polynomial over* $GF(q)$ *of degree less than* m_t.

(ii) *The codewords of* $\boldsymbol{C}_t^{n,q}$ *can be written as* $a(x) = r(x)\theta_t(x) \mod x^n - 1$, *where* $r(x)$ *is an arbitrary polynomial over* $GF(q)$ *of degree less than* m_t.

(iii) *The polynomials* $r(x)$ *and* $s(x)$ *are related by the equality* $s(x) = n^{-1}xh'(x)r(x) \mod P_t(x)$

(iv) *The minimal cyclic code* $\boldsymbol{C}_t^{n,q}$ *is isomorphic to the field* $GF(q^{m_t})$.

(v) *An isomorphism* φ *between* $\boldsymbol{C}_t^{n,q}$ *and* $GF(q^{m_t})$ *is given by* $\varphi(a(x)) = a(\zeta)$, *where*

$a(x) \in \boldsymbol{C}_t^{n,q}$ *and* ζ *is a zero of* $P_t(x)$.

(vi) *The set of polynomials* $r(x)$ *is a field isomorphic to* $GF(q^{m_t})$ *under addition and multiplication modulo* $P_t(x)$.

(vii) *If one defines* $\boldsymbol{F}^{n,q,t}$ *as the field of the polynomials* $r(x)$, *then the mapping* $\boldsymbol{C}_t^{n,q} \to \boldsymbol{F}^{n,q,t}$ *induced by* $a(x) \to r(x)$ *is an isomorphism.*

For the proofs we refer to [3, Theorems 21 and 22]. We also copy the results of [3, Theorem 25 and 32].

Theorem 13

(i) *Let* $a(x) = r(x)\theta_t(x)$ *mod* $x^n - 1$ *be a codeword of the code* $\boldsymbol{C}_t^{n,q}$, *where* $r(x)$ *is some polynomial over* $GF(q)$ *of degree less than* m_t. *If* $R(x)$ *is the Mattson – Solomon transform of* $r(x)$ *and* $\Theta_t(x)$ *of* $\theta_t(x)$, *then* $A(x) = R(x) \otimes \Theta_t(x)$ *is the Mattson – Solomon transform of* $a(x)$ *and one can write* $A(x) = \sum_{j \in C_{t^*}^{n,q}} r(\zeta^{-j})x^j$ *or equivalently*

$$A(x) = \sum_{j \in C_{t^*}^{n,q}} r(\zeta^j)x^{n-j} = \sum_{j \in C_t^{n,q}} r(\zeta^{-j})x^j .$$

(ii) *If* $r(x)$ *is not the zero polynomial, then the zeros of* $A(x)$ *satisfy the equation* $\sum_{j \in C_t^{n,q}} r(\zeta^j)x^{n-j} = 0$, *where* ζ *is a zero of* $P_t(x)$ *and hence a primitive* n^{th} *root of* 1.

We can simply generalize this result for the r^{th} M.S. transform of a codeword.

Theorem 14

(i) *Let* $a(x) = r(x)\theta_t(x)$ *be a codeword of* $\boldsymbol{C}_t^{n,q}$, *where* $r(x)$ *is some polynomial over* $GF(q)$ *of degree less than* m_t. *Then its* r^{th} *Mattson – Solomon transform is equal to*

$$A_r(x) = r(\zeta^t)x^{rt} + (r(\zeta^t)x^{rt})^q + ... + (r(\zeta^t)x^{rt})^{q^{m_t-1}} .$$

(ii) *The* r^{th} *M.S. transform of a code word* $a(x) = r(x)\theta_1(x) \in C_1^{n,q}$ *can be written as* the modified cyclonomial $c_1(r(\zeta)x^{rt})$.

Proof

(i) According to Theorem 8, we get the r^{th} M.S.-transform of $A(x)$ by replacing $R(x)$ by $R_r(x)$ and $\Theta_t(x)$ by $(\Theta_t)_r(x) = c_{rt}(x)$. Hence, $A_r(x) = \sum_{j=1}^{n} r(\zeta^j)x^{rj} \otimes (x^{rt} + x^{rtq} + ... + x^{rtq^{m_t-1}})$ which is equal to $A_r(x) = r(\zeta^t)x^{rt} + r(\zeta^{tq})x^{rtq} + ... + r(\zeta^{tq^{m_t-1}})x^{rtq^{m_t-1}}$. By applying $r(\zeta^{tq^i}) = r(\zeta^{rt})^{q^i}$, we get $A_r(x) = r(\zeta^t)x^{rt} + (r(\zeta^t)x^{rt})^q + ... + (r(\zeta^t)x^{rt})^{q^{m_t-1}}$.

(ii) This follows immediately from (i) by substituting $t = 1$ and by the definition of $c_1(x)$.

■

Theorem 14 is a generalization of Theorem 32 and Corollary 33 in [3].

Corollary 15

Let $a(x) = r(x)\theta_1(x)$ be some codeword of the code $\boldsymbol{C}_1^{n,q}$ which is defined by the irreducible polynomial $P_1(x)$ over $GF(q)$ of degree m_1 and of order n. Then the conventional Mattson-Solomon-transform is $A_r(x) = c_1(r(\zeta)x^{-1}) = c_1(r(\zeta^{-1})x)$.

We now investigate the possible zeros of a cyclonomial $c_1(x)$ in order to derive information about the weight spectrum of the codewords of $\boldsymbol{C}_1^{n,q}$. From Theorem 11 (iv) we know that the cyclonomials can be expressed in terms of idempotents by

$$c_s(x) = \sum_{t \in T^{n,q}} \eta_t^s \theta_t(x), \quad \eta_t^s = \frac{m_s}{m_t} \mu_{s,t}. \tag{8}$$

The next theorem is a slight generalization of Theorem 31 in [3].

Theorem 16

(i) *If $\eta_t^s = 0$ for some $t \in T^{n,q}$, then $P_t(x)$ is a divisor of $c_s(x)$.*

(ii) *$P_t(x)$ is a divisor of $c_s(x)$ if and only if $Tr(P_{st}(x)) = 0$ or if m_s / m_{st} is a multiple of the characteristic of $GF(q^m)$.*

Proof

(i) This follows from (8) and from the fact that $P_t(x)$ is a divisor of all $\theta_u(x)$ for $u \neq t$.

(ii) Let ζ^s, ζ^{sq}, …., $\zeta^{sq^{m_s-1}}$ be the m_s zeros of $P_s(x)$. The cyclonomial $c_s(x)$ is defined as $c_s(x) = x^s + x^{sq} + ... + x^{q^{m_s-1}} \mod x^n - 1$. Since $\zeta^n = 1$, it follows that $c_s(\zeta) = \zeta^s + \zeta^{sq} + ... + \zeta^{sq^{m_s-1}} = Tr(P_s(x))$. Hence, ζ is a zero of $c_s(x)$ if and only if $Tr(P_s(x)) = 0$. The same holds for all the other zeros of $P_s(x)$. More generally, when we substitute the zero ζ^t of $P_t(x)$ in $c_s(x)$, we get $c_s(\zeta^t) = \zeta^{st} + \zeta^{stq} + ... + \zeta^{stq^{m_s-1}} = \mu_{t,s}$. We conclude that ζ^t is also a zero of $c_s(x) - \mu_{t,s}$. The same holds for all other zeros of $P_t(x)$ and so $P_t(x)$ divides $c_s(x) - \mu_{t,s} = c_s(x) - Tr(P_{st}(x))$. Furthermore, since $\mu_{t,s}$ is the sum of the m_s t-

powers of the zeros of $P_s(x)$, we can write $\mu_{t,s} = -\frac{m_s}{m_{st}} p = \frac{m_s}{m_{st}} Tr(P_{st}(x))$, where p is the coefficient of the one but highest x- power in $P_{st}(x)$. This proves the statement in (ii). ■

From now on we shall refrain from talking about the r^{th} M.S. transform of some polynomial and just focus on the "normal" M.S. transform, since we learned from Theorem 14 that an r^{th} transform can be seen as the M.S. transform with a different ($\zeta^{1/r}$ instead of ζ) primitive n^{th} root of unity.

We continue by revisiting our running example of the primitive cyclic code $\boldsymbol{C}^{10,3}$.

Example 17

This code was defined in e.g. [3, Ex.34] and [4, Ex.15] as the cyclic code corresponding to the irreducible polynomial $P_1(x) = x^4 - x^3 + x^2 - x + 1$ (which is of order 10) and to the cyclotomic coset $C_1^{10,3} = (1,3,9,7)$. So, w.r.t. the M.S. transformation we have to deal with the zeros of the cyclonomial $c_1(x) = x^1 + x^3 + x^9 + x^7 = x^1 + x^3 + x^9 + x^{27} \mod x^{10} - 1$. (For reasons of convenience we leave out the upper indices 10 and 3).
We know (cf. [4, Ex. 15]) that we have the following factorization

$$\sum_{j=0}^{3} x^{3^j} = x(x^2+1)(x^4+x^2-1)(x^4-x^2-1)(x^4+x^2-x+1)\ (x^4+x^2+x+1)(x^4+x-1))(x^4-x-1).$$

By straightforward computation we obtain $c_1(x) = x(x^2+1)^4$. Hence, the zeros of $c_1(x)$ are 0, ω^{20} (multiplicity 4) and ω^{60} (multiplicity 4), where ω is a *primitive* 80^{th} root of unity. We define (cf. [M.S. Ex. 36]) ω as a zero of $P(x) = x^4 - x^3 - 1$ (order 80). It turns out, by using the table for $\omega(\equiv \alpha)$-powers in [4. Example 36], that ω^8 is a zero of $P_1(x)$ and so we can take $\zeta := \omega^8$. Now, the M.S. transforms of the 80 non-zero code words can be written as $c_1(\omega^{-j}x)$, $0 \le j \le 79$. Applying the general expression $\theta_1(x) = n^{-1} x h'(x) g(x)$ with $g(x) = (x^{10}-1)/P_1(x)$ and $h(x) = P_1(x)$, we find that the idempotent generator of $\boldsymbol{C}^{10,3}$ is equal to $\theta_1(x) = x^9 - x^8 + x^7 - x^6 - x^5 - x^4 + x^3 - x^2 + x + 1$ which has weight 10. By straightforward computation, we next derive that e.g. the codeword $(x^3+1)\theta_1(x)$ is equal to $x^8 + x^5 - x^3 - 1$ and so has weight 4. (Notice that we can write $(x^3+1)\theta_1(x) = (x^3+1)(x^5-1)$, but that the conclusion $\theta_1(x) = x^5 - 1$ is wrong of course, since x^3+1 is not an element of the field $\boldsymbol{C}_1^{10,3}$).
Now, the M.S. transform of $a(x) = (x^3+1)\theta_1(x)$ is equal to the modified cyclonomial $A(x) :=$

$c_1((\zeta^3+1)x^{-1}) = (\zeta^3+1)x^9 + (\zeta^3+1)^3 x^7 + (\zeta^3+1)^9 x^1 + (\zeta^3+1)^7 x^3$. Substituting for x the values ζ^k with $k \in \{1, 2, 4, 6, 7, 9\}$, we obtain $c_1((\zeta^3+1)x^{-1}) = 0$, while $k \in \{0, 3, 5, 8\}$ gives a result $\neq 0$. So, $a(x)$ has vanishing x - powers on positions 1, 2, 4, 6. 7, 9 and its weight is 4, which is correct. To be more precise, $c_1((\zeta^3+1)x^{-1})$ equals $-1,-1,1,1$ for the x - values $\zeta^0, \zeta^3, \zeta^5, \zeta^8$ respectively. Hence, according to Theorem 16 (ii) in [3] the coefficients of $a(x) = (x^3+1)\theta_1(x)$ are $a_0 = a_3 = -1$ and $a_5 = a_8 = 1$. As one can verify, this is correct. One can also verify that not all conjugates of a zero are zeros as well. The reason is that the coefficients of $A(x)$ are not all elements of the ground field $GF(3)$, contrary to the M.S. transform $\Theta(x)$ of $\theta(x)$ (cf. [3, Theorem 20]. Furthermore, we remark that the value $A(\zeta^k)$ is the trace of $(\zeta^3+1)\zeta^{-k}$ which is an example of the general relation $A(\zeta^k) = Tr(r(\zeta)\zeta^{-k})$.

In order to investigate other code words and their M.S. transforms, we need a generator polynomial of the group $\boldsymbol{F}^{10,3,1\,*}$. By determining several powers of $x+1$ modulo $P_1(x)$ it turns out that this polynomial is a generator.
Actually, there exists a one-one correspondence between the powers of $x+1$ and the powers of some zero of the irreducible polynomial $x^4 + x^3 + x^2 - x - 1$ which is of order 80. One can also say $\zeta + 1 = \omega^l$ for some l which is prime to 80. By applying $\zeta = \omega^8$ and using the table for $\alpha(\equiv \omega)$ - powers in [4, Example 36], we find $\zeta + 1 = \omega^{29}$.
In order to prove that $x+1$ really generates $\boldsymbol{F}^{10,3,1*}$, one can rather easily verify that $(x+1)^4 = -x^3 - x^2 - x$, $(x+1)^8 = -x^4 = x^9 = x^{-1}$, $(x+1)^{16} = -x^3$, $(x+1)^{20} = x^3 - x^2 + 1$ and hence $(x+1)^{40} = -x^5 + 1 = -1$. Now, if $a_j(x) = (x+1)^j \theta_1(x)$ is a non-zero code word of $\boldsymbol{C}^{10,3,1}$, then $A_j(x) = c_1((\zeta+1)^j x^{-1})$ is its M.S. transform, for $0 \le j < 80$. We saw above that $A_3(x)$ has zeros $\zeta^1, \zeta^2, \zeta^4, \zeta^6, \zeta^7, \zeta^9$ (notice that for $j = 3$ we may write $(\zeta+1)^3 = (\zeta^3+1)$.
Next, we take $j = 1$ yielding the polynomial equation
$(\zeta+1)x^9 + (\zeta+1)^3 x^7 + (\zeta+1)^9 x^1 + (\zeta+1)^7 x^3 = 0$. which has the following ζ - powers as solutions: $\zeta^2, \zeta^3, \zeta^4, \zeta^7, \zeta^8, \zeta^9$. For other j - values we find e.g. that the polynomial $A_0(x) = x^9 + x^7 + x^3 + x^1 = x(x^2+1)^4$ has no zeros of type ζ^k and that
$A_{22}(x) = c_1((\zeta+1)^{22} x^{-1}) = c_1((-\zeta^2 - 1)x^{-1})$. The ζ - zeros of this polynomial are $\zeta^0, \zeta^2, \zeta^5$ and ζ^7 which corresponds to the zero-coefficients of $a_{22}(x) = x^9 + x^8 + x^6 + x^4 - x^3 - x$.

■

Remark 18

We found by straightforward computation that in the above example $c_1(x) = x(x^2+1)^4$. We would like to point out that the following approach also delivers the factor x^2+1.

Firstly, we write for $\sum_{j=0}^{3} x^{3^j}$ the expression

$$x^1 + x^3 + x^9 + x^{27} = x^1 + x^3 + x^9 + x^7 + x^{27} - x^7 = c_1(x) + x^7(x^{20}-1) = c_1(x) + x^7(x^{10}+1)(x^{10}-1).$$

So, we have $c_1(x) = \sum_{j=0}^{3} x^{3^j} - x^7(x^{10}+1)(x^{10}-1)$. Actually, this is eq. (7) for $n=10$, $q=3$, with the polynomial $q(x)$ explicitly written in terms of these parameters.

We know already from Example 14 that $c_1(x)$ does not contain factors which divide $x^{10}-1$. Hence, other common factors ($\neq x$) of $c_1(x)$ and $\sum_{j=0}^{3} x^{3^j}$ must be irreducible polynomials contained in $x^{10}+1$. Irreducible factors of $c_1(x)$ which do not divide $x^{80}-1$ (cf. Example 16 in [4]) are not relevant, since, even when combined with some power of ω, they never will give rise to a zero of type ζ^k. So, we can restrict ourselves to factors of $c_1(x)$ which divide $x^{80}-1$ or, equivalently, to zeros of $c_1(x)$ of type $\omega^j\zeta^k$ or just to type ω^j which is equivalent.

As for $x^{10}+1$ and $x^{10}-1$ one has the factorizations (cf. also [4, Example 15]):

$x^{10}+1 = (x^2+1)(x^4+x^3-x+1)(x^4-x^3+x+1)$ and

$x^{10}-1 = (x-1)(x^4-x^3+x^2-x+1)(x^4+x^3+x^2+x+1)(x+1)$.

The real problem is whether we can determine the zeros ζ^j of $c_1(x)$ (and of $c_1(r(x)x^{-1})$) without help of the explicit factorization of this polynomial in terms of irreducible polynomials (like in Example 17), since such a factorization will not be available in more general cases.

Assume that $c_1(x)$ has a dividing irreducible polynomial $p(x)$ with trace 0. Then $p(x)$ is contained in $\sum_{j=0}^{3} x^{3^j}$ ([3, Theorem 31] and because m is not a multiple of 3), it must also be a factor of $x^{20}-1$. From the factorization of $x^{10}+1$ it follows that $p(x) = x^2+1$.

Next, assume that $p(x)$ has trace ± 1. Then $p(x)$ is contained in $\sum_{j=0}^{3} x^{3^j} \mp 1$, and so $p(x)$ divides $x^7(x^{20}-1)\pm 1$. The easiest way to investigate this possibility seems to try out powers of ζ (in general n^{th} roots of unity) as candidates for being a zero. We shall follow this approach in the next section when dealing with a number of relatively simple cases, i.e. with small values for the parameters n and m. ■

Remark 19

The multiplicative structure of the field $\boldsymbol{F}^{10,3,1}$ is determined by the irreducible polynomial $P_1(x) = x^4 - x^3 + x^2 - x + 1$ which defines $\zeta \in GF(3^4)$ and is of order 10. The generating element ω of $GF(3^4)^*$ with the property $\omega^8 = \zeta$ is defined by the irreducible polynomial $P(x) = x^4 - x^3 - 1$ of order 80. In this sense $P(x)$ and $P_1(x)$ form a "natural" couple of polynomials. Therefore it seems also natural to derive a generating polynomial of $\boldsymbol{F}^{10,3,1}$ from this $P(x)$ in stead of the generating polynomial $x+1$ of Example 17 which stems from the irreducible polynomial $x^4 + x^3 + x^2 - x - 1$.

5. An approach to determine the zeros of type ζ^j of the modified cyclonomials

We shall try out the approach of Example 17 by investigating a few more special examples.

Example 20

Take $n = 8$, $q = 5$ and hence $m = 2$.

The cyclotomic cosets modulo 5 are $C_1 = (1,5)$, $C_2 = (2)$, $C_3 = (3,7)$, $C_4 = (4)$, $C_6 = (6)$.

Furthermore, we have $x^8 - 1 = (x+1)(x-1)(x+2)(x-2)(x^2+2)(x^2-2)$ and $c_1(x) = x^1 + x^5 = x(x^2+2)(x^2-2)$. We choose $P_1(x) = x^2 + 2$ which defines by definition ζ^1 and ζ^5.

By applying the general expression $\theta_1(x) = n^{-1} x h'(x) g(x)$ and using $g(x) = (x+1)(x-1)(x+2)(x-2)(x^2-2)$ and $h(x) = x^2 + 2$, we get $\theta_1(x) = -x^2(x^6 - 2x^4 - x^2 + 2)$ $= 2x^6 + x^4 - 2x^2 - 1$ and $\theta_{-1}(x) = \theta_1(x^{-1}) = -x^8 + 2x^6 + x^4 - 2x^2$. Since the M.S. transform of $\theta_{-1}(x)$ is $c_1(x)$ (cf. [3, Theorem 19]), Theorem 16 in [3] now yields that $\theta_{-1}(x)$ has zero coefficients on positions 1, 3, 5, 7 and nonzero coefficients on positions 0, 2, 4, 6. In this case we have $\theta_1(x) = \theta_{-1}(x)$ and thus the same is true for $\theta_1(x)$ and hence the code word $a(x) = \theta_1(x)$ has weight 4. The expression for $\theta_1(x)$ shows that this is indeed the case. Next, we take the code word $a(x) = (x+1)\theta_1(x)$. Its M.S. transform is $A(x) = \sum_{j \in C_1^{8,3}} r(\zeta^j) x^{-j} = c_1((\zeta+1)x^{-1})$. By applying the equalities $\zeta^2 = -2$, $\zeta^4 = -1$ and $\zeta^8 = 1$ we derive that $A(\zeta^k)$ equals $2, 0, -1, 0, -2, 0, 1, 7$ for k respectively equal to $0, 1, 2, 3, 4, 5, 6, 7$. By means of the relation $a_k = n^{-1} A(\zeta^k)$ we find indeed the code word $a(x)$. ■

Example 21

We take $n=10$, $q=3$ and hence $m=4$, i.e. our running example throughout the text in this report (cf. Example 17) as well as in [3, 4]. As primitive polynomial of order 10 we take $P_1(x)=x^4-x^3+x^2-x+1$ which defines a primitive 10^{th} root of unity ζ. More precisely, this polynomial has the zeros ζ^1, ζ^3, ζ^9, ζ^{27} and therefore corresponds to the cyclotomic coset $C_1^{10,3}=(1,3,9,27)$ and to the cyclonomial $c_1(x)=x^1+x^3+x^9+x^7$. Furthermore, we define the polynomial $q(x)$ by $\sum_{i=0}^{3} x^{3^i}=c_1(x)+q(x)(x^{10}-1)$, where $q(x)$ is a polynomial over $GF(3)$ of degree less than 10. We find immediately $q(x)=(x^7-x^{27})/(x^{10}-1)=-x^7(x^{10}+1)$. We know already that $c_1(x)$ has no irreducible divisors of type $P_t(x)$, $t\in U^{10,3}$, by applying [alg, Theorem 30 (ii)] and because of the traces of the irreducible polynomials contained in $x^{10}-1$ (cf. [3, Example 34]).

There is a slightly different way to find the zeros of $c_1(x)$, based on the fact that the cyclotomic cosets $C_1^{10,3}$ and $C_1^{20,3}$ are equal, and so $c_1^{10,3}(x)=c_1^{20,3}(x)=x^1+x^3+x^9+x^7$. As a consequence the irreducible divisors of $x^{20}-1$ with trace value 0 are also divisors of $c_1(x)(\equiv c_1^{10,3}(x))$. These divisors are firstly the same divisors of $x^{10}-1$ (which do not really exist), and secondly of the polynomial x^2+1. ■

Remark 22

One should be aware that if ξ is a zero of $c_1(x)$, one cannot conclude $Tr(\xi)=0$. Though $c_1(\xi)=0$ does imply $c_1(\xi^q)=0$ like the zeros of *irreducible* polynomials, it does not mean that $Tr(\xi)=\xi^1+\xi^q+....+\xi^{q^{m-1}}=0$. Actually, one has that if ζ is defined as a zero of a primitive polynomial $P_1(x)$ (with respect to n), $Tr(\zeta)=Tr(P_1(x))=\tau$ and $P_1(x)$ is a divisor of $c_1(x)$ if and only if $\tau=0$. So, this is a special case of Theorem 30 (ii) in [3].

A related remark is that $Tr(r(\zeta)\zeta^{-1})=0$ does not imply $Tr(c_1(r(\zeta)x^{-1}))=0$ (cf. Example 17), since, contrary to irreducible polynomials, not all zeros of this polynomial have necessarily a trace value zero. ■

Example 23

Take $n=16, q=5$, and so it follows that $m=4$.

A primitive irreducible polynomial of order 16 is $P_1(x):=x^4+2$. This polynomial defines the

primitive 16^{th} roots of unity $\zeta^1, \zeta^5, \zeta^9, \zeta^{13}$, and it corresponds to the cyclic coset $C_1 = (1,5,9,13)$ and the cyclonomial $c_1(x) = x^1 + x^5 + x^9 + x^{13}$ (we leave out the upper indices 16 and 5). In [3, Ex. 37] we found $x^{16} - 1 = (x^4 + 3)(x^4 + 2)(x^2 + 3)(x^2 + 2)(x + 2)(x + 3)(x + 1)(x + 4)$. By applying Theorem 31 in [3] we may conclude that $c_1(x) = xP_1(x)P_2(x)P_3(x)P_6(x)$, with $P_2(x) = x^2 + 3$, $P_3(x) = x^4 + 3$, $P_6(x) = x^2 + 2$. We were able to produce this result, because we had explicit knowledge of the irreducible factors of $x^{16} - 1$ by the tables in [1]. In case we have no access to such tables, we could argue as follows. Determine, e.g. by trial and error, which powers ω^j are zeros of $q(x) = (x^{25} - x^9 + x^{125} - x^{13}) / (x^{16} - 1) = x^9 + x^{13}(x^{112} - 1) / (x^{16} - 1)$ or, straightforwardly, by substituting ω^j in $c_1(x)$ where ω is a primitive 624^{th} root of unity. Doing so, one can make use of the equalities $\omega^{156} = 2$, $\omega^{312} = -1$ and $\omega^{468} = 3$. It shows that e.g. ω^{78} and $\omega^{390} = -\omega^{78}$ (both square roots of 2) are zeros of $c_1(x)$. Apparently, we will find in this way all zeros of $c_1(x)$ which all happen to be of type $\zeta^k = \omega^{39k}$, and hence it is not necessary to investigate $q(x)$ any further. So, we can restrict ourselves to investigate those ω^j with $j -$ values $39(195,351,507)$, $78(390)$, 117(585,429,273), 156, 234(546), 312, 468. Much easier of course is to verify which of the ζ - powers ζ^k, $0 \le k < 16$, $\zeta = \omega^{39}$, satisfy $c_1(x) = 0$, or even better, just try ζ^t with $t \in \{0,1,2,3,4,6,8,12\}$, which are the elements of the index set $S^{16,5}$. In this way we will find all 12 t-values that give rise to zeros of $c_1(x)$.

We conclude that, apart from 0, $c_1(x)$ has the following zeros: $\omega^{117}, \omega^{273}, \omega^{429}, \omega^{585}$ (zeros of $x^4 + 2$), $\omega^{39}, \omega^{195}, \omega^{315}.\omega^{507}$ (zeros of $x^4 + 3$), $\omega^{234}, \omega^{546}$ (zeros of $x^2 + 2$), $\omega^{78}, \omega^{390}$ (zeros of $x^2 + 3$). We write the M.S. transform of the non-zero code word $a_{-j}(x)$ as the modified cyclonomial $c_1(\omega^j x)$, $0 \le j < 624$. Such a cyclonomial has zeros ω^{-j+s}, where s is equal to one of the above exponents. We assume that the primitive 624^{th} root ω of unity is such that $\zeta = \omega^{39}$ and so ζ is a primitive 16^{th} root of unity. The zeros ω^{-j+s} of $c_1(\omega^j x)$ are powers of ζ if and only if $-j + s = 0 \mod 39$, where s equals one of the values

39, 195, 351, 507, 117, 273, 429, 585, 78, 390, 234, 546.

Firstly, we may restrict ourselves to $s \in \{39.117, 78, 234\}$, i.e. the indices of the corresponding cyclotomic cosets modulo 624. All other s-values follow by multiplying by 5 mod 624. A second remark is that all the above s-values themselves are multiples of 39. This is by accident, and is a consequence of the fact that $P_1(x) = x^4 + 2$ divides $c_1(x)$ and so $\omega^{39} (= \zeta^1)$ is a zero of $c_1(x)$ and consequently ζ^5, ζ^9 and ζ^{13} are also zeros. Finally, we shall determine the weight of the code word $a(x) = (x^2 + 1)\theta_1(x)$ by the "substitution method" demonstrated in the previous

examples. Straightforward calculation shows that $\theta_1(x) = 2x^{12} + x^8 - 2x^4 - 1 = (x^8 - 1)(2x^4 + 1)$ and $a(x) = 2x^{14} + 2x^{12} + x^{10} + x^8 - 2x^6 - 2x^4 - x^2 - 1$. The M.S. transform of this polynomial is $A(x) = c_1((\zeta^2 + 1)x^{-1}) = (\zeta^2 + 1)x^{15} + (\zeta^2 + 1)^5 x^{11} + (\zeta^2 + 1)^9 x^7 + (\zeta^2 + 1)^{13} x^3$. It appears by substitution that ζ^j is a zero of this polynomial for all odd values of j, as it should be.

We now introduce the notation (j,k) for the pairs of j - and k - values which satisfy the relation $j = s \mod 39$, expressing that the modified cyclonomial $c_1(\omega^j x)$ has a zero ζ^k, or equivalently that the coefficient of x^k in code word $a_{-j}(x)$ equals zero. Thus we have the following pairs (j,k), with $-j + s = 39k$, $0 \le k < 16$, and
$j \in \{0,39,78,117,156,195,234,273,312,351,390,429,468,507,546,585\}$,
$s \in \{39,195,351,507,117,273,429,585,78,390,234,546\}$.

Using $j' = j/39$ and $s' = s/39$ yields $-j' + s' = k$, and so we find the following pairs

$j = 0$, $k \in \{1,5,9,13,3,7,11,15,2,10,6,14\}$;
$j = 39$, $k \in \{0,4,8,12,2,6,10,14,1,9,5,13\}$;
$j = 78$, $k \in \{15,3,7,11,1,5,9,13,0,8,4,12\}$;
……
$j = 585$, $k \in \{2,6,10,14,4,8,12,16,3,11,7,15\}$.

We conclude that the corresponding words of the primitive cyclic code $\boldsymbol{C}^{16,5}$ have weight 4 $(= 16 - 12)$. ■

References

1. Lidl R.L., Niederreiter H.: Introduction to Finite Fields and their Applications, rev edn., Cambridge University Press, Cambridge (1997).

2. van Lint J.H.: Coding Theory. Springer, New York (1971).

3. van Zanten A.J.: Algebras of Primitive Idempotent Generators and Zeros of Cyclonomials, TR 2018, TiCC, Tilburg University.

4. van Zanten A.J.: The Mattson-Solomon Transformation and Modified Cyclonomials, TR 2021, TiCC, Tilburg University.

5. van Zanten A.J.: Primitive Idempotent Tables of Cyclic and Constacyclic Codes. Des. Codes Crypt. **87**, 1199-1225
(2019).