Generalized Residue Codes and their Idempotent Generators

Dodunekov, S.M.; Bojilov, A.; van Zanten, A.J.

Publication date:
2011

Tilburg centre for Creative Computing
Tilburg University
http://www.uvt.nl/ticc

P.O. Box 90153
5000 LE Tilburg, The Netherlands
Email: ticc@uvt.nl

February 14, 2011

TiCC TR 2011-001

Generalized Residue Codes and their Idempotent Generators

Bulgarian Academy of Sciences, Bulgaria and

TiCC, Tilburg University

S.M. Dodunekov, A. Bojilov and A.J. van Zanten

Generalized Residue Codes and their Idempotent Generators

Bulgarian Academy of Sciences, Bulgaria and

TiCC, Tilburg University

S.M. Dodunekov, A. Bojilov and A.J. van Zanten

Abstract

Generalized Residue (*GR*-)codes $C^{i}_{n,q,t}$ are cyclic codes of length n over the field $GF(q)$, with $(n,q)=1$, while t has to be a divisor of $\varphi(n)$, where φ is the Euler function. The parameter i can have t different values for fixed values of n, q and t, and the t corresponding *GR*-codes are all equivalent. In this Report we study the idempotent generators of such codes. In particular, we shall do this for $n \in \{p, 2p, p^{\lambda}, 2p^{\lambda}\}$, $\lambda > 1$, when the codes $C^{i}_{n,q,t}$ belong to the subclass of *t*-residue codes. Explicit expressions are derived which express the idempotent generators in terms of the sizes of cyclotomic cosets mod n with respect to *q*, and of the coefficients of the one but highest power of x in the irreducible polynomials over $GF(q)$ which divide $x^{n}-1$.

Contents

1. Introduction and definitions

In [1] generalized residue codes are defined as follows. Given some positive integer n and some prime power q with $(n,q)=1$. Let $r := \mathrm{ord}_n(q)$ and let H be the multiplicative group generated by q, i.e. $H := \{1, q, ..., q^{r-1}\}$. We also introduce the group $G := U_n$, being the group of positive integers mod n, which are prime to n. Then $|U_n| = \varphi(n)$ and H is a subgroup of U_n. Furthermore, it is well known (cf. also [1,(1.2)]) that

$$x^n - 1 = (x-1)P(x)\Phi_n(x), \tag{1}$$

where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial in $GF(q)[x]$ of degree $\varphi(n)$, and where $P(x)$ is the product of all cyclotomic polynomials $\Phi_k(x)$ with $k \mid n$, $1 < k < n$. We also know that $\Phi_n(x)$ can be factorized into $\kappa := \varphi(n)/r$ irreducible polynomials $P_i(x)$, $1 \le i \le \kappa$, over $GF(q)$

$$\Phi_n(x) = \prod_{i=1}^{\kappa} P_i(x). \tag{2}$$

Next, we choose a group K, such that

$$H \subseteq K \subseteq G. \tag{3}$$

The index of K with respect to G is called t, while the index of H with respect to K is called s. The cosets of K with respect to G are denoted by $K_1 := K, K_2, ..., K_t$, and the cosets of H with respect to K by $\{H_1 := H, H_2, ..., H_s\}$. It follows that $\varphi(n) = rst$ and $\kappa = st$. So, we can write

$$G = K_1 \cup K_2 \cup ..... \cup K_t = y_1 K \cup y_2 K ..... \cup y_t K, \tag{4}$$

and

$$G = H_1 \cup H_2 \cup ..... \cup H_\kappa = x_1 H \cup x_2 H \cup ..... \cup x_\kappa H, \tag{5}$$

for suitable elements $y_1, y_2, ..., y_t$ and $x_1, x_2, ..., x_\kappa$ from G.
Let ζ be a primitive n^{th} root of unity in some extension field of $GF(q)$. Then the polynomials

$$g^{(i)}(x) = \prod_{l \in K_i} (x - \zeta^l), \quad 1 \le i \le t, \tag{6}$$

are polynomials in $GF(q)[x]$ of degree *rs*. Actually, each $g^{(i)}(x)$ is the product of *s* irreducible polynomials $P_i(x)$ over $GF(q)$ of degree *r*. We consider all these polynomials as representatives of the elements of the ring of polynomials mod $x^n - 1$ over the field $GF(q)$, which in this Report shall be denoted by R_n^q.

The polynomials $g^{(i)}(x)$ generate in R_n^q ideals

$$C_{n,q,t}^i := (g^{(i)}(x)), \quad 1 \le i \le t, \tag{7}$$

called *generalized residue codes* (*GR-codes*) with parameters *n*, *q* and *t*. These codes are all equivalent for fixed values of *n*, *q* and *t.* Furthermore, it is proven in [1, proof of Theorem 1.1] that if U_n is cyclic, its subgroup *K* of index *t* consists of the *t*-powers (*t*-residues) mod *n*. A well-known property is that U_n is cyclic if and only if $n \in \{2, 4, p^\lambda, 2p^\lambda \mid \lambda \ge 1\}$, where *p* is an odd prime and λ any integer ≥ 1. Hence, we have that for these special values of *n*, the group *K* as defined above as a subgroup of U_n with index *t*, is identical to $U_n{}^t$, the subgroup of all *t*-residues [1, Theorem 2.1].

We define a special subclass of *GR*-codes in the following way.

Definition 1
If the subgroup K of U_n with index t is identical to the subgroup $U_n{}^m$ of m-powers (*m-residues mod n*) *of the elements of U_n for some m, $m \mid \varphi(n)$, then the code $C_{n,q,t}^i$ is called an m-residue code, if m is the smallest value satisfying this identity.*

From the remarks above, it will be clear that for $n \in \{2, 4, p^\lambda, 2p^\lambda \mid \lambda \ge 1\}$ the *GR*-codes are *t*-residue codes, for all relevant values of *q*, *t* and *i.*
In general, the index $I_{n,m}$ of a subgroup $U_n{}^m$ with respect to U_n will not be equal to *m.* In stead we have the following relations. If we write for an arbitrary *n*-value

$$n = 2^{\lambda_1} p_2{}^{\lambda_2} \ldots\ldots p_l{}^{\lambda_l}, \tag{8}$$

with odd primes $p_2, \ldots\ldots, p_l$, then it follows from [1, Theorem 2.2] that

$$(m, \varphi(2^{\lambda_1}))(m, \varphi(p_2{}^{\lambda_2})) \ldots\ldots\ldots (m, \varphi(p_l{}^{\lambda_l})), \qquad \lambda_1 \le 2 \ \vee \ m \text{ odd}, \tag{9}$$

$$I_{n,m} = \Big\{$$

$$2(m, 2^{\lambda_1 - 2})(m, \varphi(p_2{}^{\lambda_2})) \ldots\ldots\ldots\ldots (m, \varphi(p_l{}^{\lambda_l})), \qquad \lambda_1 > 2 \ \wedge \ m \text{ even}. \tag{10}$$

So, we can immediately state the following theorem.

Theorem 2
If $C^i_{n,q,t}$, $1 \le i \le t$, *is an m-residue code of dimension* $n - \varphi(n)/t$, *based on some subgroup* $U_n{}^m \subset U_n$, *then* $t = I_{n,m}$.

The next example (cf. also [,Example 2.4]) shows that t is not always equal to m.

Example 3
For $n = 45$ we find $\varphi(45) = \varphi(5)\varphi(9) = 4.6 = 24$ and

$$U_{45} = \{1,2,4,7,8,11,13,14,16,17,19,22,-1,-2,-4,-7,-8,-11,-13,-14,-16,-17,-19,-22\}$$

First we take $K = U_{45}{}^2 = \{1,4,16,19,-14,-11\}$ ($m = 2$) which has index $I_{45,2} = (2,\varphi(5))(2,\varphi(9)) = (2,4)(2,6) = 4$. Since $H := < q >$ has to be a subgroup of K, we can take for instance $q = 4$ or $q = 16$. Actually, one could take any power of 4, since all 4-powers mod 45 are in K. Let $q = 4$. Then $r := \mathrm{ord}_{45}(4) = 6$, $H = K$ and $\kappa = \varphi(45)/6 = 4 = st$. So, $s = 1$ and $t = 4$ One obtains four (t=4) 2-residue codes $C^i_{45,4,4}$, $1 \le i \le 4$, over $GF(4)$ of dimension $45 - 24/4 = 39$. When taking $q = 16$ the data become $r = \mathrm{ord}_{45}(16) = 3$, $H = \{1,16,-14\}$, $\varphi(45)/3 = 8$, $s = 2$, $t = 4$. In this case one will obtain four 2-residue codes $C^i_{45,16,4}$, $1 \le i \le 4$, of length 45 over $GF(16)$ again of dimension 39.
Next we take $K = U_{45}{}^4 = \{1,16,-14\}$ ($m = 4$) with index $I_{45,4} = (4,4)(4,6) = 8$. Now one could take any power of 16 for q. Consider $q = 16$, giving $r := \mathrm{ord}_{45}(16) = 3$, $H = K$ and $\kappa = \varphi(45)/3 = 8 = st$. So, $s = 1$, $t = 8$ and one obtains eight 4-residue codes $C^i_{45,16,8}$, $1 \le i \le 8$, over $GF(16)$ of dimension $45 - 24/8 = 42$. Similarly, one obtains eight 8-residue codes $C^i_{45,16,8}$ over $GF(16)$. The latter case ($m = 8$) demonstrates that t can be equal to m when $n \notin \{2,4,p^\lambda,2p^\lambda\}$. In the first two cases one has $t > m$. □

Another non-trivial example of a group K with $H \subset K \subset U_n$, $K = U_n{}^m$, satisfying $I_{n,m} = m$, while $n \notin \{2,4,p^\lambda,2p^\lambda\}$ is presented below (cf. also [1, Example 2.5]).

Example 4
Take $n = 36$ and $q = 17$. Since $\mathrm{ord}_{36}(17) = 2$, the group $H = \{1, 17\}$.
Now, we define $K := U_{36}{}^3 = \{1, 17, -1, -17\}$. Hence, $|U_{36}{}^3| = 4 = \varphi(36)/(3,2)(3,6) = 12/3$., and the index of K is 3.

On the other hand, for $m = 6$ we find $I_{36,6} = (6,2)(6,6) = 12 \neq 6$.

We conclude that the choice $K = U_{36}{}^{3}$ delivers three equivalent 3-residue codes over $GF(17)$. These codes are generated by polynomials $g^{(i)}(x)$, $1 \le i \le 3$, of degree 4. Each such polynomial is the product of two irreducible polynomials over $GF(17)$ of degree 2. A choice $K = U_{36}{}^{6} = \{1\}$ is not possible, since H would not be contained in K.

The next case we shall explore is $K = U_{45}{}^{3} = \{1,8,17,19,-1,-8,-17,-19\}$ which has index $t = I_{45,3} = (3,\varphi(5))(3,\varphi(9)) = (3,4)(3,6) = 3$. If we take $q = 8$, the group $H = \{1,8,19,17\}$ has index 2 with respect to K, and so $s = 2$. Furthermore, $r = 4$ and $\kappa = 24/4 = 6$ in accordance with $st = 6$, $s = 2$ and $t = 3$. Hence, there are three 3-residue codes $C^{i}_{45,8,3}$, $1 \le i \le 3$, of length 45 over $GF(8)$. Each of the minimal generators is the product of 2 (=s) irreducible polynomials of degree 4 over $GF(8)$. In this case we also have $t = m(= 3)$.

Now, let $K = U_{45}{}^{6} = \{1,19\}$ with index $t = I_{45,6} = (6,4)((6,6) = 12$. The only possible non-trivial group $H \subseteq K$ is $H = K = \{1,19\}$ generated by $q = 19$. The corresponding parameter values are $r := \mathrm{ord}_{45}(19) = 2$, $\varphi = 12$, $s = 1$, $t = 12$. So, there are twelve 6-residue codes of length 45 over $GF(19)$ of dimension $n - \varphi(n)/t = 45 - 24/12 = 43$.

If one defines $K = \{1,8,17,19\}$ there is no m-value such that $K = U_{45}{}^{m}$, and therefore *GR*-codes based on this group K do not belong to the family of m-residue codes. Possible values for q are 8, 17, 19 or powers of these values. Taking $q = 8$ gives $r = 4$, $\kappa = 6$, $t = 6$, $s = 1$. So, there are six *GR*-codes $C^{i}_{45,8,6}$, $1 \le i \le 6$, of length 45 over $GF(8)$. □

For more examples of *GR*-codes and for their relationship with similar codes already present in the literatue, we refer to [1]. In this Report we shall focus on the idempotent generators for *GR*-codes, especially for a couple of families of *t*-residue codes. After a general introduction to idempotent generators for cyclic codes in Section 2, we develop a new approach to this topic in Section 3 by defining a matrix M the columns of which yield the primitive idempotent generators for cyclic codes of length n. In particular, we apply this approach to *GR*-codes in Section 4. In Sections 5, 6, 7 and 8, we study the idempotent generators for *GR*-codes of length p, $2p$, p^{λ} and $2p^{\lambda}$, respectively. All these codes belong to the subfamily of *t*-residue codes. The reason to treat the cases $n = p$ and $n = p^{\lambda}$ separately, is that the case $n = p$ and q an arbitrary prime power with $(p,q) = 1$, is dealt with in the literature as a generalization of quadratic residue codes (when q is a quadratic residue (cf. [1])), while the case $n = p^{\lambda}$ is a further generalization (cf. [1,4]). The other two families of *t*-residue codes, i.e. the cases $n = 2p$ and $n = 2p^{\lambda}$, are less known. In our next report we shall present a couple of references where these codes are introduced. Finally, in Section 9, we investigate a *GR*-code which is not covered by one the previous cases, by taking $n = 21$.

We would like to remark that in practice, the *M*-matrix approach is not a very efficient substitute for the methods which were briefly discussed in Section 3, since one needs the coefficients of the one-but highest power of x in *all* irreducible factors of $x^n - 1$.

2. Idempotent generators of cyclic codes

Let $g(x)$ be the minimal generator polynomial of a cyclic code C of length n over the field $GF(q)$, and let $h(x)$ be its check polynomial. So we have

$$x^n - 1 = g(x)h(x)\,, \tag{11}$$

and hence, in R_n^q

$$g(x)h(x) = 0\,. \qquad . \tag{12}$$

Definition 5
Let C be a cyclic code. A polynomial $e(x) \in C$, of degree less than n, which is an identity element of C is called the idempotent generator of C.

One can easily derive from this definition, that every cyclic code has an idempotent generator which is unique and which satisfies

$$e(x)^2 = e(x)\,. \tag{13}$$

As for the uniqueness of such an idempotent, we refer to the textbooks, e.g. [3,5]. It is also well-known, that $e(x)$ can be obtained from the relation

$$a(x)g(x) + b(x)h(x) = 1\,, \tag{14}$$

which holds for certain polynomials $a(x)$ and $b(x)$ in R_n^q, because $g(x)$ and $h(x)$ have no common divisors, except the constant polynomial 1. By defining

$$e(x) = a(x)g(x) \tag{15}$$

and by applying (12) and (14) we find that the polynomial $e(x)$ in (15) satisfies (13). A few well-known properties of idempotent generators are listed in the next theorem.

Theorem 6
(i) *An idempotent polynomial in C which is a unit for C, is an idempotent generator of C*;
(ii) *Relation* (13) *is equivalent to* $e(\zeta^i) = 0$ *if* $g(\zeta^i) = 0$ *and* $e(\zeta^i) = 1$ *if* $h(\zeta^i) = 0$, *where the* ζ^i, $1 \le i \le n$, *are the* n^{th} *roots of unity lying in some extension field of* $GF(q)$;
(iii) $c(x) \in C$ *if and only if* $e(x)c(x) = c(x)$.

For the proofs we again refer to [3,5].

Of course the polynomial $a(x)$, and hence $e(x)$, can be obtained by carrying out Euclid's algorithm to determine the gcd of two polynomials. Though this algorithm is rather efficient, in practice one better can use sometimes the following property, which is faster in general.

Theorem 7
The idempotent generator $e(x)$*, defined in* (15)*, can be written as element of* R_n^q *as*

$$e(x) = n^{-1} x h'(x) g(x), \tag{16}$$

where n^{-1} *is the inverse of n in the field* $GF(q)$ *and where* $h'(x)$ *stands for the formal derivative of the polynomial* $h(x)$.

Proof
First we remark that the degree of the polynomial in the rhs of (16) is less than *n,* since we interpret that polynomial as an element of R_n^q. This implies that we have to subtract a term $x^n - 1$ in case that the degree of the polynomial is not a multiple of the characteristic of the field $GF(q)$. Let ζ^i be a zero of $g(x)$. Then it follows immediately from (16) that $e(\zeta^i) = 0$. Now, assume that ζ^i is a zero of $h(x)$. From the polynomial identity (11) it follows by taking derivatives that

$$g(x)h'(x) + g'(x)h(x) = nx^{n-1},$$

where the coefficient *n* is taken modulo *q*, and hence can be considered as an element of $GF(q)$ (remember that $(n,q) = 1$). So,

$$e(\zeta^i) = n^{-1}\zeta^i g(\zeta^i) h'(\zeta^i) = n^{-1}\zeta^i . n\zeta^{i(n-1)} = \zeta^{in} = 1.$$

According to Theorem 6 (ii), and because of the uniqueness of the idempotent generator, it follows that $e(x)$ equals the expression in the rhs of (16). □

Corollary 8
The idempotent generator of a cyclic code of length n over the field $GF(2^m)$ *is equal to*

$$e(x) = g(x)h^o(x) = g(x)h^e(x), \tag{17}$$

where, $h^o(x)$ *and* $h^e(x)$ *are the polynomials obtained from* $h(x)$ *by taking only the odd respectively the even powers of x in* $h(x)$.

Since $n = 1 \mod 2$, the proof is straightforward. For the binary case, Theorem 7 and its Corollary are presented in [5, Ch. 8, Problem (17)], as an exercise.

In particular, we can apply the above expressions for $e(x)$ to generalized residue codes which were introduced in [1] (cf. Section 1). We shall give a few examples.

Example 9
Take $n = 7$ and $q = 2$. Since $\mathrm{ord}_7(2) = 3$, the splitting field of $x^7 + 1$ over $GF(2)$ is $GF(2^3)$. The generating element of the multiplicative group $GF(2^3)^*$ is α defined by $\alpha^3 + \alpha + 1 = 0$. Here, we have accidently $\alpha = \zeta$.
The factorization of $x^7 - 1$ into $x - 1$ and two irreducible polynomials of degree 3 over $GF(2)$ is

$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

If we define $g(x) := x^3 + x + 1$, then $h(x) = x^4 + x^2 + x + 1$. Corollary 8 now provides us with $e(x) = (x^3 + x + 1)x = x^4 + x^2 + x$.

Example 10
Take $n = 5$ and $q = 19$. We write $x^5 - 1 = (x-1)\Phi_5(x)$. Since $\mathrm{ord}_5(19) = 2$, the factorization of $\Phi_5(x)$ in $GF(19)[x]$ contains $4/2 = 2$ irreducible polynomials of degree 2. Explicitly, we find

$$x^5 - 1 = (x-1)(x^2 - 4x + 1)(x^2 + 5x + 1).$$

Let $g(x) = (x-1)(x^2 + 5x + 1)$, then $h(x) = x^2 - 4x + 1$. Actually, this generating polynomial defines an extended *GR*-code. Theorem 7 gives the idempotent

$$e(x) = 5^{-1} x g(x)(2x - 4) = 4(4x^4 - 5x^3 - 5x^2 + 4x + 2).$$

Indeed, one can verify that in R_5^{19} one has $e(x)^2 = e(x)$, if the coefficients are considered to be elements of $GF(19)$. □

Example 11
Take $n = 6$ and $q = 7$. We write

$$\begin{aligned} x^6 - 1 &= (x-1)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2 + x + 1)(x^2 - x + 1) \\ &= (x-1)(x+1)(x-2)(x-4)(x+2)(x+4). \end{aligned}$$

We define $g(x) = (x+1)(x^2 + x + 1) = x^3 + 2x^2 + 2x + 1)$, giving rise to

$h(x) = (x-1)(x^2 - x + 1) = x^3 - 2x^2 + 2x - 1$. Strictly speaking, this polynomial $g(x)$ does not generate a *GR*-code. Theorem 7 gives for the idempotent corresponding to $g(x)$ the expression

$$e(x) = 6^{-1} x g(x) h'(x) = 6^{-1} x(x^3 + 2x^2 + 2x + 1)(3x^2 - 4x + 2) = 5x^5 + x^3 + 5x + 4 .$$

Again, one can easily verify the idempotency relation $e(x)^2 = e(x)$ in R_6^7. □

Example 12
Take $n = 11$ and $q = 4$. Since $\text{ord}_{11}(4) = 5$, the polynomial $\Phi_{11}(x)$ can be factorized into two irreducible polynomials over $GF(4)$ of degree 5. In explicit form we can write

$$x^{11} + 1 = (x+1)(x^5 + \alpha x^4 + x^3 + x^2 + \alpha^2 x + 1)(x^5 + \alpha^2 x^4 + x^3 + x^2 + \alpha x + 1),$$

where α satisfies $\alpha^2 + \alpha + 1 = 0$. Actually, a primitive 11^{th} root of unity is defined as a zero of one of these two 5^{th} degree polynomials. If we define
$g(x) = x^5 + \alpha x^4 + x^3 + x^2 + \alpha^2 x + 1$, then $h(x) = x^6 + \alpha x^5 + \alpha x^4 + \alpha^2 x^2 + \alpha^2 x + 1$, and so $h^o(x) = \alpha x^5 + \alpha^2 x$.
Consequently, using Corollary 8, we find

$$e(x) = h^o(x) g(x) = \alpha x^{10} + \alpha^2 x^9 + \alpha x^8 + \alpha x^7 + \alpha x^6 + \alpha^2 x^5 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha x^2 + \alpha^2 x .$$

By a straightforward computation we verified that this expression satisfies the idempotency relation in R_{11}^4. □

Remark 13
Because of the uniqueness of the idempotent generator, we have as a consequence of the relations (15) and (16) the equalities $a(x) = n^{-1} x h'(x)$ and $b(x) = n^{-1} x g'(x)$. Therefore, in stead of (14) we have in R_n^q the identity

$$n^{-1} x(g(x)h'(x) + g'(x)h(x)) = 1 , \tag{18}$$

or equivalently,

$$n^{-1} x(g(x)h'(x) + g'(x)h(x)) = 1 \ \text{mod}\ x^n - 1 , \tag{19}$$

which of course is obviously true.

There is still another tool to compute idempotent generators of cyclic codes. This tool is based on the so-called *inversion rule* (cf. e.g. [5, Ch. 7]).

Theorem 14
Let $c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_0$ *be a polynomial in* R_n^q. *Then the coefficients* c_i, $0 \le i \le n-1$, *can be obtained by* $c_i = n^{-1}\sum_{j=0}^{n-1} c(\zeta^j)\zeta^{-ij}$, *where* ζ *is a primitive* n^{th} *root of unity in some extension field of* $GF(q)$.

Applying this property to the idempotent generator $e(x)$ of a cyclic code yields the following theorem.

Theorem 15
Let $e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + ... + e_0$ *be the idempotent generator of a cyclic code C, generated by the minimal polynomial* $g(x)$. *Then the coefficients* e_i, $1 \le i \le n-1$, *can be obtained by* $e_i = n^{-1}\sum_{j\in N} \zeta^{-ij}$, *where N is the set of exponents of the nonzeros* ζ^j *of* $g(x)$.

Example 16
We shall apply Theorem 15 to the *GR*-code with parameters $n = 13$, $q = 3$ and $t = 4$, generated by the polynomial $g^{(1)}(x) = x^3 - x - 1$. This code $C^1_{13,3,4}$, is also studied in [1, Examples 2.2, 3.1 and 4.3]. The zeros of $g^{(1)}(x)$ are ζ, ζ^3 and ζ^9. Hence, it follows from Theorem 15 that

$$e_i = 13^{-1}\sum_{j=0}^{12} e(\zeta^j)\zeta^{-ij} = 1 + \zeta^{-2i} + \zeta^{-4i} + \zeta^{-5i} + \zeta^{-6i} + \zeta^{-7i} + \zeta^{8i} + \zeta^{-10i} + \zeta^{-11i} + \zeta^{-12i}.$$

The primitive 13^{th} root of unity ζ is defined by $g^{(1)}(\zeta) = 0$, which provides us with the identities: $\zeta^3 = \zeta + 1$, $\zeta^4 = \zeta^2 + \zeta$, $\zeta^5 = \zeta^2 + \zeta + 1$, $\zeta^6 = \zeta^2 - \zeta + 1$, $\zeta^7 = -\zeta^2 - \zeta + 1$, $\zeta^8 = -\zeta^2 - 1$, $\zeta^9 = \zeta - 1$, $\zeta^{10} = \zeta^2 - \zeta$, $\zeta^{11} = -\zeta^2 + \zeta + 1$ and $\zeta^{12} = \zeta^2 - 1$. By also making use of the identity $\sum_{j=0}^{12}\zeta^j = 0$, it is easy to derive $e_1 = e_3 = e_9 = 1$, $e_2 = e_6 = e_5 = -1$, $e_7 = e_8 = e_{11} = 1$ and $e_4 = e_{12} = e_{10} = 0$.
Hence, the idempotent generator of the code defined by $g^{(1)}(x)$ is equal to

$$e^{(1)}(x) = x^{11} + x^9 + x^8 + x^7 - x^6 - x^5 + x^3 - x^2 + x + 1.$$

To apply Theorem 7, we first determine the polynomial $h(x) := x^{13} - 1/g(x)$. We find

$$h(x) = x^{10} + x^8 + x^7 + x^6 - x^5 - x^4 + x^2 - x + 1$$

and next

$$h'(x) = x^9 - x^7 + x^6 + x^4 - x^3 - x - 1 .$$

When evaluating $e^{(1)}(x) := g(x)h'(x)$, we end up with the same expression which was derived before.

Similarly, we can determine the idempotent generator of the code $C^3_{13,3,4}$ defined by its minimal polynomial $g^{(3)}(x) = x^3 + x^2 - 1$, with zeros ζ^4, ζ^{12} and ζ^{10}. The result is

$$e^{(3)}(x) = x^{12} - x^{11} + x^{10} - x^8 - x^7 + x^6 + x^5 + x^4 + x^2 . \qquad \square$$

Example 17

For $n = 15$, we have $U_{15} = \{1,2,4,7,8,11,13,14\}$ and $\varphi(15) = 8$. The cyclotomic polynomial $\Phi_{15}(x)$ can be obtained from

$$x^{15} - 1 = (x-1)\Phi_3(x)\Phi_5(x)\Phi_{15}(x),$$

giving

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 .$$

We consider $\Phi_{15}(x)$ as a polynomial over $GF(2)$ and write

$$\Phi_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 .$$

Since $\text{ord}_{15}(2) = 4$, we can factorize $\Phi_{15}(x)$ in R_{15}^2 into two irreducible polynomials of degree 4 (cf. [1,Section1])

$$\Phi_{15}(x) = (x^4 + x + 1)(x^4 + x^3 + 1) .$$

The complete factorization of $x^{15} - 1$ in R_{15}^2 is

$$x^{15} - 1 = (x+1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1) .$$

Let ζ be a primitive 15^{th} root of unity, defined as a zero of $x^4 + x + 1$. Then it can easily be derived that among the irreducible polynomials in the above factorization one has the following distribution of zeros:

$$\begin{array}{ll} x^4 + x + 1 & \text{with zeros} \quad \zeta^1, \zeta^2, \zeta^4, \zeta^8, \\ x^4 + x^3 + 1 & \text{with zeros} \quad \zeta^3, \zeta^6, \zeta^{12}, \zeta^9, \end{array}$$

$$x^4 + x^3 + x^2 + x + 1 \quad \text{with zeros} \quad \zeta^7, \zeta^{14}, \zeta^{13}, \zeta^{11},$$
$$x^2 + x + 1 \quad \text{with zeros} \quad \zeta^5, \zeta^{10},$$
$$x + 1 \quad \text{with zero} \quad \zeta^0.$$

For $q = 2$, the only m-values less than 8 and such that $2 \in U_{15}{}^m$ are 1, 3, 5 and 7, while $U_{15}{}^1 = U_{15}{}^3 = U_{15}{}^5 = U_{15}{}^7 = U_{15}$. So, the only binary m-residue code is the trivial code $C^1_{15,2,1}$ which is a 1-residue code and which is obtained by choosing $K := U_{15} \supset H =< 2 >$. When we choose $K := H = \{1,2,4,8\}$, it follows that $t = 8/4 = 2$, and we obtain two binary equivalent *GR*-codes $C^i_{15,2,2}$, $1 \le i \le 2$, which are not m-residue codes for any m.

Next, we consider $\Phi_{15}(x)$ in the polynomial ring $GF(4)[x]$. Since $\text{ord}_{15}(4) = 2$, we now have a factorization into four polynomials of degree 2 which are irreducible in $GF(4)[x]$

$$\Phi_{15}(x) = (x^2 + x + \alpha)(x^2 + x + \alpha^2)(x^2 + \alpha x + \alpha)(x^2 + \alpha^2 x + \alpha^2),$$

where α satisfies $\alpha^2 + \alpha + 1 = 0$.
We conclude that when taking $q = 4 \in K = \{1,4\}$, there are $\left| U_{15} / K \right| = \varphi(15)/2 = 4$ quaternary equivalent *GR*-codes $C^i_{15,4,4}$, $1 \le i \le 4$. Since $K = U_{15}{}^2$, these codes are even 2-residue codes (over $GF(4)$). We define, $g^{(1)}(x) := x^3 + x + \alpha$, $g^{(3)}(x) := x^2 + x + \alpha^2$, $g^{(2)}(x) := x^2 + \alpha x + \alpha$ and $g^{(4)}(x) := x^2 + \alpha^2 x + \alpha^2$. In order to obtain the idempotent generator of the code $C^1_{15,4,4} := (g^{(1)}(x))$, we first determine the corresponding check polynomial

$$h^{(1)}(x) = x^{13} + x^{12} + \alpha^2 x^{11} + x^{10} + \alpha x^8 + \alpha x^7 + x^6 + \alpha x^5 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha x + \alpha^2.$$

Applying Theorem 7 or Corrollary 8 gives the idempotent generator

$$e^{(1)}(x) = x^{14} + x^{13} + \alpha^2 x^{12} + x^{11} + \alpha x^9 + \alpha x^8 + x^7 + \alpha x^6 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha x^2 + \alpha^2 x + 1.$$

Similarly, we obtain the idempotent generator of $(g^{(2)}(x))$ by successively computing

$$h^{(2)}(x) = x^{13} + \alpha x^{12} + x^{11} + x^{10} + \alpha x^8 + \alpha^2 x^7 + \alpha x^6 + \alpha x^5 + \alpha^2 x^3 + x^2 + \alpha^2 x + \alpha^2,$$

$$e^{(2)}(x) = \alpha x^{14} + \alpha^2 x^{13} + \alpha x^{12} + \alpha x^{11} + \alpha^2 x^9 + x^8 + \alpha^2 x^7 + \alpha^2 x^6 + x^4 + \alpha x^3 + x^2 + x.$$

The idempotent generators $e^{(3)}(x)$ and $e^{(4)}(x)$ follow from $e^{(1)}(x)$ and $e^{(2)}(x)$ by replacing α with α^2, respectively. □

Example 18

Let $n=10$ and take first $q=3$. Then $\Phi_{10}(x)=x^4-x^3+x^2-x+1$. Since $\mathrm{ord}_{10}(3)=4$, $\kappa=\varphi(10)/4=1$, and so the polynomial $\Phi_{10}(x)$ is irreducible in $GF(3)[x]$. Taking $g(x):=\Phi_{10}(x)$ as generator polynomial of the *GR*- code $C^1_{10,3,1}$, gives a check polynomial $h(x)=x^6+x^5-x-1$. Hence, the idempotent generator of this code is

$$e(x)=10^{-1}\ xh'(x)g(x)=-x^9+x^8-x^7+x^6+x^5+x^4-x^3+x^2-x\,.$$

Next we take $q=9$. Since $r:=\mathrm{ord}_{10}(9)=2$ and $\varphi(10)=4$, we know that $\Phi_{10}(x)$ can be written as the product of two irreducible polynomials over $GF(9)$ of degree 2. From the equality $x^{10}-1=(x-1)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)$, we derive

$$\Phi_{10}(x)=(x^2+\alpha x+1)(x^2-(\alpha+1)x+1)\,,$$

where α is defined as one the roots of the equation $x^2+x-1=0$ (cf. [1, Example 7.1]), while the other root is α^3.

We define $K:=H=<9>$. So, $K=\{1,9\}$ and $t=\varphi(10)/2=2$. Hence, there are two equivalent 9-ary codes $C^i_{10,9,2}, 1\le i\le 2$, generated by $g^{(1)}(x)=x^2+\alpha x+1$ and $g^{(2)}(x)=x^2-(\alpha+1)x+1$, respectively. We shall determine the idempotent generator of the code $(g^{(1)}(x))$. First, we find for the check polynomial

$$h^{(1)}(x)=x^8-\alpha x^7-\alpha x^6+x^5-x^3+\alpha x^2+\alpha x-1\,.$$

Next, applying Theorem 7, we get the idempotent

$$\begin{aligned}e^{(1)}(x)\ &=\ \alpha x^9+(\alpha+1)x^8-(\alpha+1)x^7-\alpha x^6-x^5-\alpha x^4-(\alpha+1)x^3+(\alpha+1)x^2+\alpha x-1\\ &=\alpha x^9-\alpha^3x^8+\alpha^3x^7-\alpha x^6-x^5-\alpha x^4+\alpha^3x^3-\alpha^3x^2+\alpha x-1\,.\end{aligned}$$

By a straightforward calculation we verified that $e^{(1)}(x)^2=e^{(1)}(x)$.

Since $\alpha^3=-\alpha-1$, we can obtain the expression for $h^{(2)}(x)$ by replacing α in $h^{(1)}(x)$ with α^3, and similarly, by the same substitution, we can get $e^{(2)}(x)$ from $e^{(1)}(x)$. The result is

$$e^{(2)}(x)=\alpha^3x^9-\alpha x^8+\alpha x^7-\alpha^3x^6-x^5-\alpha^3x^4+\alpha x^3-\alpha x^2+\alpha^3x-1\,.$$

We remark that a primitive 10^{th} root ζ of unity can be defined by as a zero of $g^{(1)}(x)$ in $GF(9^2)$ [x]. This implies $\zeta^2 = -\alpha\zeta - 1$, or equivalently $\alpha = -(\zeta + \zeta^{-1})$. □

It is well known that in the binary case, i.e. for $q = 2^\lambda$, the idempotent generator of some cyclic code C of length n is the sum of polynomials $c_s(x)$. Such a polynomial $c_s(x)$ corresponds to a cyclotomic coset C_s mod n, with respect to 2, in the following way

$$c_s(x) = \sum_{i \in C_s} x^i . \tag{20}$$

It can easily be proven (cf. also [3,5]) that this property holds more generally for cyclic codes over a finite field $GF(q)$, if C_s stands for a coset mod n with respect to q, i.e.

$$C_s = \{s, qs, ..., q^{m_s - 1}\} . \tag{21}$$

Theorem 19
Let C be a cyclic code of length n over the field $GF(q)$, with $(n,q) = 1$, and let $e(x)$ be its idempotent generator. Then one can write $e(x) = \sum_s \xi_s c_s(x)$, where s runs through the set of indices of cyclotomic cosets mod n, and with $\xi_s \in GF(q)$.

Proof
If $e(x)$ is an idempotent generator of C, then by definition $e(x)^2 = e(x)$, and hence $e(x)^k = e(x)$ for all positive integers k. We write $e(x) = \sum_i \xi_i x^i$, $\xi_i \in GF(q)$, and we take $k := q$, yielding $e(x)^q = \sum_i \xi_i{}^q x^{qi} = \sum_i \xi_i x^{qi} = \sum_j \xi_j x^j$. If $i \in C_s$ for some s, then also $qi \in C_s$. Putting $j = qi$ in the right hand side of the above equation, gives $\xi_{qi} = \xi_i$. This implies the statement. □

The above theorem is clearly illustrated by the idempotent generators derived in the previous examples.

3. A matrix determining all primitive idempotent generators

We now shall develop a fourth method to derive the idempotent generator of a cyclic code of length *n.* We consider the complete factorization of $x^n - 1$ into irreducible polynomials over $GF(q)$, $(n,q) = 1$, which is written as

$$x^n - 1 = \prod_{i=0}^{l} P_i(x), \quad P_0(x) = 1. \tag{22}$$

Let ζ be again a primitive n^{th} root of unity in some extension field of $GF(q)$, defined as a zero of one of the polynomials in the rhs of (22) which we shall assume to be $P_1(x)$. Then $\zeta, \zeta^q, ..., \zeta^{q^{m_1-1}}$ are the m_1 zeros of $P_1(x)$, where m_1 is the degree of $P_1(x)$ In general, the irreducible polynomial $P_s(x)$ has zeros $\zeta^s, \zeta^{sq}, ..., \zeta^{sq^{m_s-1}}$, where m_s is the degree of $P_s(x)$ So, there is a one-to-one correspondence between the cyclotomic cosets

$$C_s = \{s, sq, ..., sq^{m_s-1}\} \tag{23}$$

and the polynomials $P_s(x)$ which we write explicitly as

$$P_s(x) = x^{m_s} + p_{s,1}x^{m_s-1} + ... + p_{s.m_s}. \tag{24}$$

We adopt the convention that the index *s* stands for the least integer of the relevant coset. Together these indices constitute an index set *S.*
On the other hand, there is also a one-to-one correspondence between the cyclotomic cosets C_s and the polynomials (*cyclonomials*) $c_s(x) \in R_n^q$, $s \in S$, which are defined as

$$c_s(x) = x^s + x^{sq} + ... + x^{sq^{m_s-1}}. \tag{25}$$

For any $i \in \{1, 2, ..., n\}$ and for any $s \in S$, we define the (multi)set

$$C_s^{(i)} = \{is, isq, ..., isq^{m_s-1}\}, \tag{26}$$

containing all products ia, with $a \in C_s$. It will be clear that all elements in $C_s^{(i)}$ belong to the same cyclotomic coset, be it that these elements may occur more than once. We shall denote this cyclotomic coset by the index is, though this is not necessarily the least integer in the coset. If the multiset $C_s^{(i)}$ contains each element of C_{is} *a* times, we shall write $C_s^{(i)} = aC_{is}$. More precisely, we have the following lemma.

Lemma 20
For all $i \in \{1,2,....,n\}$ *and all* $s \in S$ *one has*
(i) $C_s^{(i)} = n_s^i C_{is}$ *for some positive integer* n_s^i *which divides* m_s*;*
(ii) $c_s(\zeta^i) = -n_s^i p_{is,1}$.

Proof
(i) Each element of $C_s^{(i)}$ can be obtained from is by a multiplication with some power of q, and each element occurs $n_s^i := \mid C_s \mid / \mid C_{is} \mid = m_s / m_{is}$ times.
(ii) By definition $P_{is}(\zeta^{is}) = 0$, and hence $P_{is}(\zeta^{isq}) = ... = P_{is}(\zeta^{isq^{m_{is}-1}}) = 0$. Moreover, $c_s(\zeta^i) = \zeta^{is} + \zeta^{isq} + ... + \zeta^{isq^{m_s-1}} = n_s^i c_{is}(\zeta)$. So, $c_s(\zeta^i) = -n_s^i p_{is,1}$. □

In the next, we consider n_s^i as an element of $GF(q)$, and we introduce an $\mid S \mid \times \mid S \mid$-matrix M with elements

$$\mu_{i,s} := -n_s^i p_{is,1}, \quad i,s \in S. \tag{27}$$

In particular, we have

$$\mu_{0,s} = m_s \quad \text{and} \quad \mu_{i,0} = 1. \tag{28}$$

We also introduce two more operations on the family of cyclotomic cosets for certain fixed values of *n* and *q*. In the first place we define the sum of two cosets

$$C_i + C_j = \{a + b \mid a \in C_i, b \in C_j\}, \tag{29}$$

and secondly, the product

$$C_i C_j = \{ab \mid a \in C_i, b \in C_j\}, \tag{30}$$

where the sums and products of the integers *a* and *b* are taken mod *n*.
It will be obvious that the multiset in the rhs of (29) is a union of cyclotomic cosets, where a coset may occur more than once. Hence, one can write in general

$$C_i + C_j = \bigcup_l a_l C_l, \tag{31}$$

for certain integers a_l which depend on *i* and *j*. The same can be said about the product (30), so

$$C_i C_j = \bigcup_l b_l C_l \tag{32}$$

for certain integers b_l. All indices in (31) and (32) are elements of *S*.
The following simple properties hold.

Lemma 21
Let A be the family of unions of cyclotomic cosets for fixed values of n and q. Then
(i) *A is closed under the operations as defined in* (31) *and* (32);
(ii) *the integer* a_0 *in* (31) *is equal to* m_i *if* $j = -i$, *and to* 0 *if* $j \neq -i$
(iii) *the set of polynomials* $c_s(x)$, $s \in S$, *is closed in* R_n^q *under multiplication*;
(iv) $c_s(x^i) = n_s^i c_{is}(x)$;
(v) $c_i(x)c_j(x) = \sum_l a_l c_l(x)$ *with the integers* a_l *from* (31), *and* $a_0 = m_i$ *if* $j = -i$ *and* $a_0 = 0$ *otherwise*;
(vi) *if* ζ *is a primitive* n^{th} *root of unity, then* $\sum_k c_k(\zeta^i)$ *is equal to 0 for* $i \neq 0$, *and to n for i=0.*

We are now ready to formulate a theorem which provides us with another method to determine the idempotent generator of the cyclic code generated by an irreducible polynomial $P_i(x)$ from (22). In the formulation of this theorem we introduce vectors ε_i, $i \in S$, over $GF(q)$ and of length $|S|$, which have a one on position *i* and zeros on all positions of $S\backslash\{i\}$.

Theorem 22
Let the indices of the irreducible polynomials in (22) *be such that the primitive* n^{th} *root of unity* ζ, *which lies in some extension field of* $GF(q)$, $(n,q) = 1$, *is defined as a zero of the irreducible polynomial* $P_1(x)$. *Let furthermore* $C_{n,q,t}^u$ *be the cyclic code of length n generated by the irreducible polynomial* $P_u(x)$, $u \in S$, *also from* (22), *and let* $e_u(x) = \sum_{s \in S} \xi_s c_s(x)$, $\xi_s \in GF(q)$, *be its idempotent generator. Then the coefficients* ξ_s *are uniquely determined by the set of linear equations* $\sum_{s \in S} \mu_{i,s} \xi_s = e_u(\zeta^i)$, $i \in S$, *with* $e_u(\zeta^i) = 0$ *for* $i = u$ *and* $e_u(\zeta^i) = 1$ *for* $i \neq u$, *or equivalently in matrix form, by* $M\xi = \delta_u$ *with column vectors* ξ *and* $\delta_u = 1 - \varepsilon_u$ *of length* $|S|$.

Proof
From Theorem 6 we know that the set of equations $e_u(\zeta^i) = 0$ for $i = u$ and $e_u(\zeta^i) = 1$ for $i \neq u$, has a solution and such a solution must be unique. Substituting the relation of Lemma 20 (ii) and using (27) gives the linear set of equations as stated in the Theorem. □

Example 23
Take $n=15$ and $q=2$ (cf. also Example 17).
The cyclotomic cosets are

$C_0=\{0\}$, $C_1=\{1,2,4,8\}$, $C_3=\{3,6,12,9\}$, $C_5=\{5,10\}$, $C_7=\{7,14,13,11\}$.

The index set $S=\{0,1,3,5,7\}$.
The only n_s^i having a value $\neq 1$ are $n_1^0=n_3^0=n_7^0=4$ and $n_5^0=n_5^3=2$.
Corresponding to the above cyclotomic cosets we have the polynomials

$c_0(x)=1$, $c_1(x)=x+x^2+x^4+x^8$, $c_3(x)=x^3+x^6+x^{12}+x^9$, $c_5(x)=x^5+x^{10}$,
$c_7(x)=x^7+x^{14}+x^{13}+x^{11}$.

The factorization in (22) is given by $x^{15}-1=\prod_{s\in S}P_s(x)$ with
$P_0(x)=x+1$, $P_1(x)=x^4+x+1$, $P_3(x)=x^4+x^3+1$, $P_5(x)=x^2+x+1$,
$P_7(x)=x^4+x^3+x^2+x+1$.

We define a primitive 15^{th} root of unity ζ by requiring $P_1(\zeta)=0$.
The idempotent generator of the code C^1 can be written as $e_1(x)=\sum_{s\in S}\xi_s c_s(x)$.
According to Theorem 22, we have the following set of equations for the ξ_s

$$
\begin{aligned}
1\xi_0+0\xi_1+0\xi_3+0\xi_5+0\xi_7&=e_1(\zeta^0)=1,\\
1\xi_0+0\xi_1+1\xi_3+1\xi_5+1\xi_7&=e_1(\zeta^1)=0,\\
1\xi_0+1\xi_1+1\xi_3+0\xi_5+1\xi_7&=e_1(\zeta^3)=1,\\
1\xi_0+0\xi_1+0\xi_3+1\xi_5+0\xi_7&=e_1(\zeta^5)=1,\\
1\xi_0+1\xi_1+1\xi_3+1\xi_5+0\xi_7&=e_1(\zeta^7)=1.
\end{aligned}
$$

In matrix form we write this linear set of equations as

$$M\xi=\delta_1.$$

with the column vectors $\xi=(\xi_0,\xi_1,\xi_3,\xi_5,\xi_7)^T$ and $\delta_1=(1,0,1,1,1)^T$ and the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Since the idempotent generator is unique, this system has precisely one solution which turns out to be $\xi = (1,1,1,0,0)^{\,t}$. If we take for the rhs of the matrix equation the vector $\delta_3 = (1,1,0,1,1)^t$, which corresponds to the polynomial $P_3(x)$, we find $\xi = (1,0,1,0,1)^T$ as solution. Hence, for the idempotent generators of the two *GR*-codes, we find

$$e_1(x) = 1 + x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12},$$

$$e_3(x) = 1 + x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}.$$

We verified that the same expressions are delivered by eq. (16), using the check polynomials

$$h_1(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1,$$

$$h_3(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1. \qquad \square$$

Example 24

Again we study the case $n = 10$ and $q = 3$ (cf. Example 18). The cyclotomic cosets are $C_0 = \{0\}$, $C_1 = \{1,3,9,7\}$, $C_2 = \{2,6,8,4\}$, $C_5 = \{5\}$, and the corresponding irreducible polynomials $P_0(x) = x - 1$, $P_1(x) = x^4 - x^3 + x^2 - x + 1$, $P_2(x) = x^4 + x^3 + x^2 + x + 1$, $P_5(x) = x + 1$. We know that $\Phi_{10}(x) = P_1(x)$ is irreducible and that $P_1(x)$ generates $C^1_{10,3,1}$. The coefficients ξ_i, $i \in S = \{0,1,2,5\}$, can be determined by the matrix equation

$$M\xi = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} \xi_0 \\ \xi_1 \\ \xi_2 \\ \xi_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

We find $\xi = (0,-1,1,1)^T$, and so the idempotent generator of the *GR*-code C_1 is

$$e_1(x) = -x + x^2 - x^3 + x^4 + x^5 + x^6 - x^7 + x^8 - x^9.$$

We obtained the same expression by applying (16) with $h_1(x) = x^6 + x^5 - x - 1$.

Now, we take $q = 9$. The cyclotomic cosets C_1 and C_3 split and we have new cosets $C_0 = \{0\}$, $C_1 = \{1,9\}$, $C_2 = \{2,8\}$, $C_3 = \{3,7\}$, $C_4 = \{4,6\}$, $C_5 = \{5\}$ and $S = \{0,1,2,3,4,5\}$. Using the same indices, we have the following irreducible polynomials $P_0(x) = x - 1$ with zero ζ^0, $P_1(x) = x^2 + \alpha x + 1$ with zeros ζ, ζ^9, $P_2(x) = x^2 + (\alpha+1)x + 1$ with zeros ζ^2, ζ^8, $P_3(x) = x^2 - (\alpha+1)x + 1$ with zeros ζ^3, ζ^7, $P_4(x) = x^2 - \alpha x + 1$ with zeros ζ^4, ζ^6 and $P_5(x) = x + 1$ with zero ζ^5. Here, the element $\alpha \in GF(9)$ satisfies $\alpha^2 + \alpha - 1 = 0$.
The matrix M in this case can readily be determined and is equal to

$$M = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -\alpha & -\alpha-1 & \alpha+1 & \alpha & -1 \\ 1 & -\alpha-1 & \alpha & \alpha & -\alpha-1 & 1 \\ 1 & \alpha+1 & \alpha & -\alpha & -\alpha-1 & -1 \\ 1 & \alpha & -\alpha-1 & -\alpha-1 & \alpha & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}.$$

The equation $M\xi = \delta_1$ with $\xi = (\xi_0, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5)^T$ and $\delta_1 = (1,0,1,1,1,1)^T$ yields the solution $\xi = (-1, \alpha, \alpha+1, -\alpha-1, -\alpha, -1)^T$, which indeed corresponds to the idempotent generator $e^{(1)}(x)$ as computed in Example 18. □

Due to the previous examples the following theorem presents itself.

Theorem 25
Let $P_{i_1}(x), P_{i_2}(x), ..., P_{i_l}(x)$, with $i_1, i_2, ..., i_l \in S$, be l irreducible polynomials introduced in (2), and let C be the cyclic code generated by the product $P(x)$ of these polynomials. Then the idempotent generator $e(x) = \sum_{s \in S} \xi_s c_s(x)$ of C is determined by the set of linear equations $M\xi = \delta$, where δ is the column vector of length $|S|$ with zeros on the positions $i_1, i_2, ..., i_l$, and ones elsewhere.

In particular, one obtains the *primitive idempotent generators*, i.e. the idempotent generators of the so-called *minimal* or *irreducible codes* (cf. e.g. [5]), by taking for δ a vector with just one one and zeros on all other positions, whereas the idempotent generators for the *maximal codes* are obtained by taking for δ a vector with just one zero and ones on all other positions.

It turns out that the inverse of the matrix M can easily be determined.

Theorem 26
Let M be the matrix the elements of which are defined in (27) *and let* M^P *be the matrix obtained from M by interchanging the columns indexed by s and* $-s$, *for all* $s \in S$. *Then* $M^{-1} = n^{-1}M^P$, *where the inverse of n is to be taken in* $GF(q)$.

Proof
We consider the inner product of row i and column s of the matrix M. Using (27) and Lemma 20 (ii), we get

$$\sum_{k\in S} \mu_{i,k}\mu_{k,s} = \sum_{k\in S} c_k(\zeta^i)c_s(\zeta^k) =$$
$$\sum_{k\in S} (\zeta^{ik} + \zeta^{ikq} + ... + \zeta^{ikq^{m_k-1}})(\zeta^{sk} + \zeta^{skq} + ... + \zeta^{skq^{m_s-1}}) =$$
$$\sum_{k\in S}\sum_{a=0}^{m_s-1}(\sum_{b=0}^{m_k-1}\zeta^{(iq^b+sq^a)k}) = \sum_{k\in S}\sum_{a=0}^{m_s-1}(\sum_{b=0}^{m_k-1}\zeta^{(i+sq^{a-b})kq^b}).$$

In order to evaluate the rhs of the last equality, we shall make use of the fact that for every fixed value of b, the set $\{sq^{a-b} \mid 0 \le a \le m_s - 1\}$ is equal to the cyclotomic coset $C_s = \{sq^c \mid 0 \le c \le m_s - 1\}$. Hence, we obtain

$$\sum_{k\in S}\sum_{c=0}^{m_s-1}(\sum_{b=0}^{m_k-1}\zeta^{(i+sq^c)kq^b}) =$$
$$\sum_{c=0}^{m_s-1}[\sum_{k\in S}(\zeta'^k + \zeta'^{kq} + ... + \zeta'^{kq^{m_k-1}})] = \sum_{c=0}^{m_s-1}[\sum_{l=0}^{n-1}\zeta'^l],$$

where $\zeta' = \zeta^{i+sq^c}$ is some (not necessarily primitive) n^{th} root of unity. For $s \neq -i$ one has that $\zeta' \neq 1$, and hence the expression between brackets is equal to 0 for each value of c. For $s = -i$ this expression is also 0, except for $c = 0$, giving $\zeta'^0 + \zeta'^0 + ... + \zeta'^0 = n$. Hence, we may conclude that $\sum_{k\in S} \mu_{i,k}\mu_{k,s} = 0$, for $s \neq -i$ and $\sum_{k\in S} \mu_{i,k}\mu_{k,-i} = n$ for $s = -i$. □

Corollary 27
The primitive idempotent generators $\theta_u(x) = \sum_{s\in S} \xi_{u,s}c_s(x)$, $u \in S$, *of the minimal cyclic codes for certain values of n and q, are determined by the vector* $\xi_u = n^{-1}M^P\varepsilon_u$, *where* ε_u *is the vector over* $GF(q)$ *of length* $|S|$ *with a one on position u and zeros elsewhere. The idempotent generators* $\vartheta_u(x) = \sum_{s\in S} \xi'_{u,s}\, c_s(x)$ *which generate the maximal cyclic codes, are determined by* $\xi'_u = n^{-1}M^P\delta_u$, *with* $\delta_u = 1 - \varepsilon_u$, *and where* 1 *stands for the all-one vector of length* $|S|$.

This corollary implies that the primitive idempotent generator of the cyclic code generated by $\prod_{i \neq u} P_i(x)$, $u \in S$, corresponds to the column of M with index $-u$, occasionally called μ_{-u}. For practical reasons, we denote this idempotent generator by $\theta_u^*(x)$, and so we have for all $u \in S$

$$\theta_u^*(x) = \theta_{-u}(x) = n^{-1} \sum_{s \in S} \mu_{s,-u} c_s(x) = n^{-1} \sum_{s \in S} (\mu_{-u})_s c_s(x) \tag{33}$$

and similarly,

$$\vartheta_u^*(x) = 1 - \theta_u^*(x) = 1 - \theta_{-u}(x). \tag{34}$$

In the next theorem we state some simple symmetry properties of the matrix *M.* To do this in a concise way, we shall make use of the Kronecker symbol $\delta_{a,b}$ which stands for 1 if $a = b$, and for 0 if $a \neq b$.

Theorem 28
If we denote the elements of the matrix M by $\mu_{i,j}$, $i, j \in S$, *then the following relations hold in* $GF(q)$:

(i) $m_i \mu_{i,j} = m_j \mu_{j,i}$;

(ii) $\sum_k \mu_{i,k} \mu_{k.j} = n \delta_{i,-j}$;

(iii) $\sum_k m_k \mu_{k,i} \mu_{k,j} = n m_i \delta_{i,-j}$;

(iv) $\sum_k m_k^{-1} \mu_{i,k} \mu_{j,k} = n m_i^{-1} \delta_{i,-j}$.

Proof
Equality (i) follows immediately from the definition (37) of the elements of *M.*
The other relations are immediate consequences of (i) and Theorem 26 . □

Remark 29
The inverses in Theorem 28 (iv), are only defined as long as m_k and m_i are unequal to zero in $GF(q)$. Multiplying both sides of relation (iv) by m_i $(= m_j)$ gives the factor $m_j \mu_{j,k} / m_k$ in the lhs which always exists.
Notice that in the above theorem, all summations are over *S*, and that all integers m_l and *n* are to be taken in $GF(q)$.

Lemma 30
Let $(n, q) = 1$ *and let r be the order of q modulo n.*

(i) *The size* m_i *of the cyclotomic coset* C_i *is a divisor of r, for all* $i \in S$.

(ii) *If* -1 *is a q-power modulo n, then* $C_s = C_{-s}$ *for all* $s \in S$.

Proof

(i) The elements of C_1 are precisely the elements of the group $H := < q >$ of order *r*, and so $m_1 = r$. The cyclotomic coset C_s consists of the elements $\{s, sq, ..., sq^{m_s - 1}\}$, and hence m_s must be a divisor of $m_1 = r$.

(ii) If $-1 = q^l$, then $-s = q^l s$, so all elements of C_{-s} can be written as a *q*-power. Since $\mid C_s \mid = \mid C_{-s} \mid$, the relation in (ii) follows immediately. □

The following – at least in the binary case – well-known properties can easily be derived in the usual way (cf. [3,5]).

Theorem 31

For any n and prime power q with $(n,q) = 1$*, one has that the primitive idempotent generators* $\theta_s(x)$*,* $s \in S$*, of cyclic codes of length n over q satisfy*:

(i) $\sum_{s \in S} \theta_s(x) = 1$;

(ii) $\theta_s(x)\theta_u(x) = 0$ *for all* $s, u \in S$ *with* $s \neq u$;

(iii) $\vartheta_u(x) = 1 - \theta_u(x)$;

(iv) *if* $e(x)$ *is the idempotent generator of some cyclic code, then* $e(x) = \sum_{s \in T} \theta_s(x)$ *for some subset* $T \subseteq S$;

(v) *the code with generator polynomial* $P_{i_1}(x)P_{i_2}(x).....P_{i_l}(x)$ *has idempotent generator* $1 - \theta^*_{i_1}(x) - \theta^*_{i_2}(x)..... - \theta^*_{i_l}(x)$.

4. Idempotent generators of *GR*-codes

Let again n be some positive integer and q some prime power satisfying $(n,q)=1$. We consider the *GR*-codes $C^i_{n,q,t}$, $1 \le i \le t$, as defined in Section 1. It will be clear that the elements of the group $H:=<q>$ (cf. Section 1) are the same as the elements of the cyclotomic coset $C_1 = \{1, q, ..., q^{r-1}\}$. Similarly, the elements of the coset $H_i := x_i H$ (cf. (5)), are the same as the elements of the cyclotomic coset C_i if $x_i \in C_i$, for $1 \le i \le \kappa$. Therefore, we can identify x_i with the least element i of C_i. As a consequence, the index i of H_i now runs through the set $S \cap U_n$, i.e. the set of indices of the cyclotomic cosets mod n which are coprime with n, and we write from now on instead of (2)

$$\Phi_n(x) = \prod_{s \in S \cap U_n} P_s(x), \tag{35}$$

where the irreducible polynomial $P_s(x)$, $s \in S$, is defined by

$$P_s(x) = \prod_{j \in C_s} (x - \zeta^j). \tag{36}$$

If we take $K := H$ when constructing the code $C^i_{n,q,t}$, we have $\kappa = t$ and so $\varphi(n) = rt$. With this choice for K, the *GR*-codes are 'maximal' codes, defined by the generators $g^{(i)}(x) := P_i(x)$, $i \in S \cap U_n$. The idempotent generator of $C^i_{n,q,t}$, as follows from Corollary 27, can be written as $e^{(i)}(x) = \sum_{j \in S} \xi_{i,j} c_j(x)$, where $\xi_{i,j}$ is the j^{th} component of the column vector $\xi_i = \varepsilon_0 - \mu_{-i}$ and μ_{-i} is the column with index $-i$ of the matrix M, and hence, $\xi_{i,j} = \delta_{0,j} - \mu_{j,-i}$.

Now we know that for any $i \in S \cap U_n$, the value of m_i is equal to $r := \mathrm{ord}_n(q)$, and hence, we have for such matrix elements $\mu_{j,i}$

$$\mu_{j,i} = -\frac{r}{m_{ij}} p_{ij,1}, \quad i \in S \cap U_n. \tag{37}$$

We remark, that m_{ij} is the degree of the polynomial $P_{ij}(x)$, while $p_{ij,1}$ is the coefficient of $x^{m_{ij}-1}$ in that same polynomial. In the present case of *GR*-codes with $P_i(x)$, $i \in S \cap U_n$, as generator, we also know that

$$\left| S \cap U_n \right| = \varphi(n)/r = t. \tag{38}$$

In particular, it follows from (37) that the column vector μ_1 has as j^{th} component

$$\mu_{j,1} = -\frac{r}{m_j} p_{j,1}. \tag{39}$$

From Corollary 27 and from the fact that $m_{-i} = m_i$ for all $i \in S$, we may conclude the following result.

Theorem 32

The idempotent generator of the GR-code $C^i_{n,q,t}$, $i \in S \cap U_n$, *is given by* $\vartheta_i^*(x) = 1 - \theta_i^*(x)$, *with* $\theta_i^*(x) = n^{-1} \sum_{j \in S} -\frac{r}{m_{ij}} p_{-ij,1} c_j(x)$.

In order to determine all idempotent generators of the t equivalent *GR*-codes $C^i_{n,q,t}$, $i \in S \cap U_n$, it is sufficient to compute $\vartheta_1(x)$, or equivalently the column vector μ_1. The components of any other column vector μ_i of *M*, with $i \in S \cap U_n$, constitute a permutation of the components of μ_1.

Theorem 33

Let $\mu_{i,j}$, $i, j \in S$, *be the elements of the matrix M.*

(i) *If j and k are elements of* $S \cap U_n$, *and if* $l \in U_n$ *is such that* $lk = j \mod n$, *then* $\mu_{l,k} = \mu_{j,1}$;

(ii) *The components of the column vector* μ_k, $k \in S \cap U_n$, *form a permutation of the components of* μ_1;

(iii) *The group* U_n / H *acts transitively on the set of column vectors* $\{\mu_{i_1}, \mu_{i_2}, ..., \mu_{i_t}\}$, *where* $i_1, i_2, ..., i_t$ *are the t elements of* $S \cap U_n$.

Proof

(i) From (27) we infer that $\mu_{l,k} = -\frac{r}{m_{lk}} p_{lk,1} = -\frac{r}{m_j} p_{j,1} = \mu_{j,1}$.

(ii) If *j* and *k* are considered as elements of the group U_n, there is precisely one element $l \in U_n$ with $lk = j \mod n$, for any fixed pair *j* and *k*. If j and k are elements of $S \cap U_n$ considered as group, this unique element l is also in $S \cap U_n$. So, for a fixed index $k \in S \cap U_n$, the components of μ_k which correspond to elements of $S \cap U_n$, form a permutation of the same kind of components of μ_1. Next, take the subset $S_a \subset S$ with the property that $s \in S_a$ if and only if $(n, s) = a$. Divide all elements of S_a by a and consider the quotients as elements of $U_{n/a}$. By similar arguments as before, we can prove

now that the components of μ_k which correspond to elements of S_a, are a permutation of the same kind of components of μ_1. Continue this process until there are no components of μ_k left. Notice that $S_1 = S \cap U_n$ in this context.
(iii) This follows immediately from (ii), when applying the fact that $S \cap U_n$ considered as a group, is isomorphic to the quotient group U_n / H. □

Remark 34
In order to compute the idempotent generator $\vartheta_1(x)$, we must know the coefficients $p_{j,1}$ of all irreducible polynomials $P_j(x)$. In practice, the second method for computing idempotent generators, discussed in the previous section, seems to be less demanding, since one only has to compute $h^{(1)}(x) = x^n - 1 / g^{(1)}(x)$ for a given $g^{(1)}(x) := P_1(x)$.

In the next sections we shall derive construction rules for the idempotent generators of generalized residue codes in the cases $n=p$, $n = 2p$, $n = p^m$ and $n = 2p^m$. We remind the reader that these codes all belong to the subfamily of *t*-residue codes (cf. [1] and Section 1 of this Report).

5. The *case* $n = p$

In the special case $n = p$ where p is an odd prime, one has

$$x^p - 1 = (x-1)\Phi_p(x), \tag{40}$$

with deg $\Phi_p(x) = p-1$. Furthermore, q is some prime power with $(p,q) = 1$. All cyclotomic cosets C_i mod p, with respect to q, $i \neq 0$, have the same size $r := \text{ord}_p(q)$. Hence, all irreducible polynomials $P_i(x)$, $i \neq 0$, are of the same degree r and $\kappa := \varphi(n)/r = p-1/r$. Consequently, all matrix elements $\mu_{0,i}$, $i \neq 0$, are equal to r. Moreover, for the other elements of M one has

$$\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1}, \quad i, j \in S/\{0\}, \tag{41}$$

while $\mu_{j,0} = 1$ for all j, as always.

Example 35
Take $n = 13$ and $q = 3$. It follows that $r := \text{ord}_{13}(3) = 3$, and that the cyclotomic cosets mod 13 are

$$C_0 = \{0\},\ C_1 = \{1,3,9\},\ C_2 = \{2,6,5\},\ C_4 = \{4,10,12\},\ C_7 = \{7,8,11\}.$$

Furthermore, we write $x^{13}-1 = P_0(x)P_1(x)P_2(x)P_4(x)P_7(x)$ with the irreducible polynomials

$$P_0(x) = x-1,\ P_1(x) = x^3 - x - 1,\ P_2(x) = x^3 + x^2 + x - 1,\ P_4(x) = x^3 + x^2 - 1,$$

$$P_7(x) = x^3 - x^2 - x - 1.$$

By applying eq. (37) we find the following matrix

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 4 & 7 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 0 \\ 1 & -1 & 1 & 0 & -1 \\ 1 & 1 & 0 & -1 & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 2 \\ 4 \\ 7 \end{matrix}.$$

So, when using that $n^{-1} = 1 \mod 3$, the primitive idempotent generator which corresponds to C_1 is equal to

$$\begin{aligned} \theta_1^*(x) &= \sum_{s\in S} \mu_{s,-1} c_s(x) = \sum_{s\in S} \mu_{s,4} c_s(x) = -c_1(x) + c_2(x) - c_7(x) \\ &= -x - x^3 - x^9 + x^2 + x^6 + x^5 - x^7 - x^8 - x^{11}. \end{aligned}$$

Finally, we obtain

$$\vartheta_1^*(x) = 1 - \theta_1^*(x) = x^{11} + x^9 + x^8 + x^7 - x^6 - x^5 + x^3 - x^2 + x + 1,$$

which is indeed the same polynomial as we found in Example 16. □

Example 36

We take $n = 31$ and $q = 2$.

Since 31 is a prime, we have that U_{31} with elements $\{1,2,.....,30\}$ is a cyclic group.

We find that $r := \mathrm{ord}_{31}(2) = 5$, and hence $\kappa = \varphi(31)/r = 6$. The group H generated by 2 consists of the elements $\{1,2,4,8,16\}$. In this case 2 is a 3- residue, since $4^3 = 2 \mod 31$. It follows that all elements of H are 3-residues. First, we enumerate all six cosets of H :

$$H_1 = \{1,2,4,8,16\}, \quad H_2 = \{3,6,12,17,24\}, \quad H_3 = \{5,9,10,18,20\},$$
$$H_4 = \{7,14,19,25,28\}, \quad H_5 = \{11,13,21,22,26\}, \quad H_6 = \{15,23,27,29,30\}.$$

We remark that if we denote a cyclotomic coset by the least integer it contains, the correspondence with the various cosets of H is as follows

$$H_1 = C_1,\ \ H_2 = C_3,\ \ H_3 = C_5,\ \ H_4 = C_7,\ \ H_5 = C_{11},\ \ H_6 = C_{15}.$$

We extend H by adding the element $-1(=30)$, yielding the group

$$K = \{1,2,4,8,15,16,23,27,29,30\},$$

which is the full group of 3-residues. Alternatively, we can write $K = H_1 \cup H_6$.

The factorization of $x^{31}+1$ into irreducible polynomials over $GF(2)$ is

$$x^{31}+1 = (x+1)(x^5+x^2+1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)\ (x^5+x^4+x^3+x^2+1)$$
$$(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1).$$

Let the primitive 31^{th} root ζ of unity be defined as a zero of x^5+x^2+1. So,

$$\zeta^5+\zeta^2+1=0.$$

The conjugate roots of ζ are ζ^2, ζ^4, ζ^8 and ζ^{16}, and hence

$$P_1(x) := \prod_{l\in H_1}(x-\zeta^l) = x^5+x^2+1.$$

From the defining polynomial of ζ, it follows that $\zeta^{-1}=\zeta^{30}$ is a zero of the reciprocal polynomial x^5+x^3+1. Therefore, we have similarly as above that

$$P_6(x) := \prod_{l\in H_6}(x-\zeta^l) = x^5+x^3+1,$$

with zeros $\zeta^{30},\zeta^{29},\zeta^{27},\zeta^{23}$ and ζ^{15}.

Cubing the relation $\zeta^5+\zeta^2=1$ provides us with $\zeta^{15}+\zeta^{12}+\zeta^9+\zeta^6=1$, from which we infer that ζ^3 is a zero of the polynomial $x^5+x^4+x^3+x^2+1$. So, we conclude

$$P_2(x) := \prod_{l\in H_2}(x-\zeta^l) = x^5+x^4+x^3+x^2+1,$$

has zeros $\zeta^3,\zeta^6,\zeta^{12},\zeta^{24}$ and ζ^{17}.

and next, since $-3(=28) \in H_4$, that

$$P_4(x) := \prod_{l \in H_4} (x - \zeta^l) = x^5 + x^3 + x^2 + x + 1,$$

has zeros $\zeta^7, \zeta^{14}, \zeta^{28}, \zeta^{25}$ and ζ^{19}. □

6. The case $n = 2p$.

First we prove the following lemma.

Lemma 36

If p is an odd prime and q an odd prime power with $(2p, q) = 1$, *and if* $r := ord_{p^\lambda}(q)$, *then* $ord_{2p^\lambda}(q) = r$, *for any integer* $\lambda > 0$.

Proof

We have that $q^r = 1 + kp^\lambda$ for some integer $k > 0$, and r is minimal with respect to this property. Since p and q are odd, k is even, i.e. $k = 2l$. Hence, $q^r = 1 \mod 2p^\lambda$. Let $r' := \mathrm{ord}_{2p^\lambda}(q)$, then $q^{r'} = 1 + 2l' p^\lambda$, and $r' \mid r$. Now, $r' < r$ would imply $\mathrm{ord}_{p^\lambda}(q) \le r' < r$. This is a contradiction, so $r' = r$. □

In the case of $n = 2p$ we shall apply the lemma for $\lambda = 1$.

In this case, the factorization of $x^n - 1$ into cyclotomic polynomials has the form

$$x^{2p} - 1 = (x-1)\Phi_2(x)\Phi_p(x)\Phi_{2p}(x) = (x-1)(x+1)\Phi_p(x)\Phi_p(-x), \qquad (42)$$

with $\deg \Phi_p(x) = \deg \Phi_{2p}(x) = p - 1$. For q we take a prime power such that $(2p, q) = 1$. The cyclotomic coset mod $2p$ with respect to q which corresponds to $\Phi_2(x)$ is $C_p = \{p\}$. If $P_i(x)$ is a monic irreducible polynomial contained in $\Phi_p(x)$, then $(-1)^r P_i(-x)$ is a monic irreducible polynomial contained in $\Phi_{2p}(x) = \Phi_p(-x)$. Hence, all irreducible polynomials $P_i(x)$, $i \in S/\{0, p\}$, are of degree $r := \mathrm{ord}_{2p}(q) = \mathrm{ord}_p(q)$, and there are $2\kappa = 2\varphi(2p)/r = 2\varphi(p)/r$ of such polynomials. In general notation, we shall label the columns (and rows) of the matrix M by the labels

$$0, i_1, i_2, ..., i_\kappa, i_{\kappa+1}, i_{\kappa+2}, ..., i_{2\kappa}, p \ . \qquad (43)$$

The labels $i_1, i_2, ..., i_\kappa \in S$ indicate the κ monic irreducible polynomials contained in $\Phi_{2p}(x) = \Phi_p(-x)$, while $i_{\kappa+1}, i_{\kappa+2}, ..., i_{2\kappa} \in S$ indicate the monic irreducible polynomials contained in $\Phi_p(x)$.More precisely, we shall choose the indices such that $P_{i_j}(x) = (-1)^r P_{i_{\kappa+j}}(-x)$. Furthermore, since we shall choose a zero of $P_{i_1}(x)$ as primitive $2p^{th}$ root of unity, we have $i_1 := 1$. The irreducible polynomials $P_i(x)$, with $i \in \{i_1, i_2, ..., i_\kappa\}$, are minimal generators of the *GR*-codes $C^i_{2p,q,t}$, $t = \kappa$. The irreducible polynomials $P_i(x)$ with $i \in \{i_{\kappa+1}, i_{\kappa+2}, ..., i_{2\kappa}\}$ are minimal generators of codes of length $2p$ which are equivalent to *GR*-codes $C^i_{p,q,t}$.

As for the matrix elements of M, the elements $\mu_{0,i}$, $i \notin \{0, p\}$, are equal to r and $\mu_{0,0} = \mu_{0,p} = 1$. For the other elements of M one has

$$\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1} = -p_{ij,1}, \quad i, j \in S / \{0, p\},$$

(44)

while $\mu_{j,0} = 1$ and $\mu_{j,p} = \mu_{p,j} = 1$ for j even and $\mu_{j,p} = \mu_{p,j} = -1$ for j odd. In particular, we have for the column indexed by 1 (which determines the idempotent generator of the *GR*-code $C^{-1}_{2p,q,t}$), the elements $\mu_{0,1} = r$, $\mu_{j,1} = -p_{j,1}$ for $j \notin \{0, p\}$ and $\mu_{p,1} = -1$. For the column indexed by -1 (which determines the idempotent generator of the *GR*-code $C^1_{2p,q,t}$), we have similarly $\mu_{0,-1} = r$, $\mu_{j,-1} = -p_{-j,1}$ for $j \notin \{0, p\}$ and $\mu_{p,-1} = -1$. □

The following two lemmas give the precise relationship between the cyclotomic cosets mod p and those mod $2p$,with respect to q, and also with the corresponding irreducible polynomials in $GF[q](x)$. The notation S' stands for the set of indices of cyclotomic cosets mod p, while S denotes the set of indices of cyclotomic cosets mod $2p$. Similarly, the notation C'_i stands for a cyclotomic coset mod p, and C_j for a cyclotomic coset mod $2p$. Like always in this section, p is an odd prime and q is an odd prime power with $(p, q) = 1$, $r := \text{ord}_p(q)$ and $\kappa := (p-1)/r$. Let $C'_i = \{i, iq, ..., iq^{r_0-1}\}$, $i \in S'$, $r_0 \mid r$, be a cyclotomic coset mod p. We define C_{2i} to be the set consisting of all integers $2a$, with $a \in C'_i$. Furthermore, we introduce for each $i \in S'$, a set consisting of the integers $a \in C'_i$ when a is odd and $a + p$ when a is even. If i is odd, we call this set C_i and if i is even C_{i+p}. It is clear that C_i and C_{i+p} only contain odd integers which are less than $2p$.

Lemma 37

(i) *C_{2i} is a cyclotomic coset mod $2p$ for all $i \in S'$;*

(ii) *C_i and C_{i+p} are cyclotomic cosets mod $2p$ for all $i \in S'$;*

(iii) *if* $a \in C_i$, *then modulo 2p,* $2a \in C_{2i}$;

(iv) *the cyclotomic cosets in* (i) *together with the cyclotomic cosets in* (ii) *constitute the complete family of* $2\kappa + 2$ *cyclotomic cosets mod* $2p$, *and their indices constitute the index set S*;

(v) *the cyclotomic cosets in* (i) *correspond to irreducible polynomials contained in* $\Phi_p(x)$ *and those in* (ii) *to irreducible polynomials contained in* $\Phi_{2p}(x)$;

(vi) *if* $P_i(x)$ *is an irreducible factor of* $\Phi_p(x)$, *then* $P_{i+p}(x)$ *is an irreducible factor of* $\Phi_{2p}(x)$ *and vice versa, for all* $i \in S'$ *and* $P_{i+p}(x) = (-1)P_i(-x)$;

(vii) *if* C_{j+p}, $j \in S$ *and j odd, is the set of integers* $a \in C_j$ *for a even, and* $a + p$ *for a odd, then the family* $\{C_{j+p} : j \in S\}$ *is the same as the family* $\{C_{2i} : i \in S'\}$ *as defined in* (*i*);

(viii) $C_{2i} = C_{i+p}$, *and hence* $P_{2i}(x) = P_{i+p}(x)$, *for all* $i \in S'$, *if and only if* $2 \in C_1$.

Proof

(i) The integers a and b are both elements of the cyclotomic class C_i' if and only if $b = aq^j \mod p$ for some j. It follows immediately that this is equivalent to $2b = 2aq^j \mod 2p$, or equivalently, a and b are in the same cyclotomic coset mod $2p$. Since all r elements of C_{2i} are different, the statement now follows.

(ii) Take two integers a and b from $C_{i'}$. If both are odd, then $b = aq^j \mod p$ for some j, or equivalently $b = aq^j + kp$. Since a, b, q and p are odd, k must be even and therefore $b = a\, q^j \mod 2p$. If both a and b are even, the proof is similar. Now, assume a is odd and b is even. We know that $b = aq^j + kp$ with k odd. Hence, $b + p = aq^j + (k+1)p$, and so $b + p = a\, q^j \mod 2p$.

(iii) This relationship is immediately clear from the definitions of C_i and C_{2i}.

(iv) Since all cosets have size r and since their intersections are all empty, they form a family of 2κ different cyclotomic cosets mod $2p$ Together with C_0 and C_p, they form a complete family of $2\kappa + 2$ cosets mod $2p$.

(v) Assume ζ is a primitive $2p^{th}$ root of unity. Then ζ^2 is a p^{th} root of unity. The ζ-powers with an exponent in C_{2i} are all powers of ζ^2 and therefore zeros of $\Phi_p(x)$. The ζ-powers with an exponent in $C_{i'}$ can all be written as $\zeta^p \zeta^{2j}$ for some j. Since $\zeta^p = -1$, these powers are zeros of $\Phi_p(-x) = \Phi_{2p}(x)$.

(vi) This follows from $P_{i+p}(x) = \prod_{j \in C_{i+p}} (x - \zeta^j) = \prod_{j \in C_i} (x + \zeta^j) = (-1)^r P_i(-x)$;

(vii) The family of cosets C_i for *i* even and C_{i+p} for i odd, is precisely the family of cyclic cosets containing the even integers mod $2p$;

(viii) We have the following equivalencies $P_{2i}(x) = P_{i+p}(x) \leftrightarrow C_{2i} = C_{i+p} \leftrightarrow 2i \in C_{i+p} \leftrightarrow 2 \in C_1$. □

Remark 38
It may occur that the index i of the cyclotomic coset C_i is not the smallest integer in this coset. If so, we maintain *i* as index of that coset (remember our conventions of indexing cyclotomic cosets). Due to this agreement we have that S' is a subset of the complete set of indices *S*, though the family of cosets indexed by the elements of S' is not a subfamily of the complete family of cosets mod $2p$.

It follows from Lemma 37 that the irreducible polynomials $P_{i_1}(x)$, $P_{i_2}(x),\ldots,$ $P_{i_\kappa}(x)$ can be identified with the polynomials $P_i(x)$, $i \in S'\setminus\{0\}$, and that the polynomials $P_{i_{\kappa+1}}(x)$, $P_{i_{\kappa+2}}(x),\ldots..,P_{i_{2\kappa(}}(x)$ correspond with the polynomials $P_{i+p}(x)$, $i \in S'\setminus\{0\}$. It follows that the choice for the indices i_j, such that $P_{i_{\kappa+j}}(x) = (-1)^r P_{i_j}(-x)$, for $1 \le j \le \kappa$, can be accomplished by taking $i_{\kappa+j} = i_j + p$, since $\zeta^p = -1$ if ζ is a primitive $2p^{th}$ root of unity. Another immediate consequence of Lemma 37 (vi) and of the property $\Phi_{2p}(x) = \Phi_p(-x)$ is that

$$p_{i_j,1} = -p_{i_{\kappa+j},1}, \quad 1 \le j \le \kappa. \tag{45}$$

The polynomials (cyclonomials) $c_{i_{\kappa+j}}(x)$, $1 \le j \le \kappa$, for the case $n = 2p$, can be obtained from the polynomials $c'_{i_j}(x)$, $i_j \in S'\setminus\{0\}$, for the case $n = p$, by means of the relation

$$c_{i_{\kappa+j}}(x) = c'_{i_j}(x^{p+1}), \quad 1 \le j \le \kappa. \tag{46}$$

In the specific case that $2 \in C'_1$, and hence $2 \in C_{1+p}$, we may replace x^{p+1} by x^2. Remember that if *j* takes on the values 1, 2, …, κ, the index i_j of the polynomial $c'_{i_j}(x)$ runs through the set $S'\setminus\{0\}$. From the construction of the cyclotomic cosets C_i mod $2p$, $i \in S'\setminus\{0\}$, it follows that $c_{i_j}(x)$ is obtained from the polynomial $c'_{i_j}(x)$ by adding p to the exponents of the even powers of x, and leaving invariant the odd powers. In a formal way this can be expressed by the relation

$$c_{i_j}(x) = x^p c'_{i_j}(x^{p+1}), \quad 1 \le j \le \kappa, \tag{47}$$

as one can verify quite easily, by handling these polynomials mod $x^{2p} - 1$.
The next theorem expresses the idempotents $\theta_i(x)$ and $\vartheta_i(x)$ for the case $n = 2p$ in terms of the cyclonomials and idempotents for the case $n = p$.

Theorem 39

(i) *The idempotent generator* $\vartheta_i(x) = 1 - \theta_i(x)$ *of the code* $C_{2p,q,t}^{-i}$, $i \in S \cap U_{2p}$, *is determined by the expression*

$$\theta_i(x) = (2p)^{-1}[r(1-x^p) - \sum_{j=1}^{\kappa} p_{i_j,i,1}(x^p - 1)c_{i_j}^{'}(x^{p+1})];$$

(ii) *If* $\theta_i^{'}(x)$ *is the idempotent corresponding to column i of the matrix* M' *for* $n = p$, *then*

$$\theta_i(x) = -2^{-1}(x^p - 1)\theta_i^{'}(x^{p+1});$$

(iii) *If* $\vartheta_i^{'}(x)$ *is the idempotent generator of the GR-code* $C_{p,q,t}^{-i}$, *then*

$$\vartheta_i(x) = 2^{-1}[1 + x^p - (x^p - 1)\vartheta_i^{'}(x^{p+1})].$$

Proof
The expressions follow immediately from Theorem 32 and from the relations (45), (46) and (47). □

Example 40
Take $n = 10$ and $q = 3$. It follows that $r = 4$, $\kappa = \varphi(10)/4 = 1$. The cyclotomic cosets mod 10 are $C_0 = \{0\}$, $C_1 = \{1,3,7,9\}$, $C_2 = \{2,4,6,8\}$, $C_5 = \{5\}$, and the corresponding polynomials are $P_0(x) = x - 1$, $P_1(x) = x^4 - x^3 + x^2 - x + 1$, $P_2(x) = x^4 + x^3 + x^2 + x + 1$, $P_5(x) = x + 1$.
The matrix M is equal to

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 5 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 2 \\ 5 \end{matrix}.$$

Since $t = \kappa = 1$, there is only one generalized residue code $C_{10,3,1}^{1}$, generated by its minimal polynomial $P_1(x)$. Here, the cyclotomic cosets are self-inverse, and therefore the idempotent generator of this code $C_{10,7,1}^{1}$ is determined by the column with label 1. First we find

$$\theta_1(x) = 10^{-1}(c_0(x) + c_1(x) - c_2(x) - c_5(x)) = 1 + x + x^3 + x^7 + x^9 - x^2 - x^4 - x^6 - x^8 - x^5,$$

and next

$$\vartheta_1(x) = 1 - \theta_1(x) = -x^9 + x^8 - x^7 + x^6 + x^5 + x^4 - x^3 + x^2 - x\,.$$

Now, we shall compute these idempotents by applying parts (ii) and (iii) of Theorem 39. The cyclotomic cosets are $C_0\{0\}$, $C_1 = \{1,2,3,4\}$. The *GR*-code $C^1_{5,3,1}$ is generated by $P_1(x) = x^4 + x^3 + x^2 + x + 1$. .

The matrix M' is a 2×2 -submatrix of M, which is obtained by taking the first two columns and the first and third row of M

$$M' = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

From Theorem 32 it follows straightforwardly that $\theta_1'(x) = -1 + x + x^2 + x^3 + x^4$, and hence $\vartheta_1'(x) = -x^4 - x^3 - x^2 - x - 1$. When substituting these expressions in the formulas of Theorem 39 (ii) and (iii) respectively, and using that $2^{-1} = -1$ in $GF[3]$, one obtains the same results for $\theta_1(x)$ and $\vartheta_1(x)$ as before. □

7. The case $n = p^\lambda$.

Next, we take $n = p^\lambda$ and q a prime power such that $(p,q) = 1$.
In order to deal with this case, we need the following lemma.

Lemma 41
Let p be a prime and q be some prime power with $(p,q) = 1$ *. Let furthermore a be some positive integer. For p odd and* $a \geq 1$ *or for p even and* $a \geq 2$*, the inequality* $ord_{p^{a+1}}(q) > ord_{p^a}(q)$ *implies* $ord_{p^{a+i-1}}(q) = p^{i-1} ord_{p^a}(q)$*, for all* $i \geq 1$.

Proof
(i) First we consider the case p odd. For our convenience, we assume $a = 1$, and so the condition of the Lemma is $\text{ord}_{p^2}(q) > \text{ord}_p(q)$.

Let $r := \text{ord}_p(q)$. We shall prove by mathematical induction the following set of relations:

$$\text{ord}_{p^i}(q) = rp^{i-1}, \quad q^{rp^{i-1}} = 1 + k_i p^i, \quad (k_i, p) = 1, \tag{48}$$

for all $i \geq 1$. From the condition $\text{ord}_{p^2}(q) > \text{ord}_p(q)$, it follows that we can write $q^r = 1 + kp$, with $(k,p) = 1$. So, (48) holds for $i = 1$, by definition of r and by taking $k_1 = k$.
Next, we assume that the relations (48) are true for some fixed integer $i \geq 1$. Then $q^{rp^{i-1}} = 1 + k_i p^i$, for some integer k_i with $(k_i, p) = 1$. It follows that

$$q^{rp^i} = (1 + k_i p^i)^p = \sum_{l=0}^{p} \binom{p}{l} (k_i p^i)^l$$
$$= 1 + k_i p^{i+1} + \sum_{l=2}^{p-1} \binom{p}{l} (k_i p^i)^l + k_i p^{pi}.$$

Since $p \mid \binom{p}{l}$ for all $l \in \{2,3,.....,p-1\}$, all terms in the summand are divisible by p^{i+2}. Moreover, since p is odd, we have $pi \geq 3i \geq i+2$, and so the last term in the rhs is also divisible by p^{i+2}. Therefore, we can write $q^{rp^i} = 1 + k_{i+1} p^{i+1}$ with $(k_{i+1}, p) = 1$, or equivalently, $\text{ord}_{p^{i+1}}(q) \mid rp^i$. So, if $e := \text{ord}_{p^{i+1}}(q)$, we have $rp^i = ey$ for some integer y. We also know that $e = xrp^{i-1}$ for some integer x. Combining these two equalities gives $xy = p$, so either $x = 1$ or $x = p$. But $x = 1$ yields $\text{ord}_{p^{i+1}}(q) = \text{ord}_{p^i}(q) = rp^{i-1}$, which contradicts (48). Hence, $\text{ord}_{p^{i+1}}(q) = rp^i$. So, the relations (48) also hold for $i+1$. Due to the principle of mathematical induction, the relations (48) hold for all $i \geq 1$. The equality of the Lemma now follows immediately.
For values $a > 1$ the proof is completely similar.

(ii) Next, we consider the case $p = 2$, and we take $a = 2$.
Let $r' := \text{ord}_{2^2}(q)$. The condition of the Lemma yields $\text{ord}_{2^3}(q) > \text{ord}_{2^2}(q)$. We shall prove by induction that for all $i \geq 1$

$$\text{ord}_{2^{i+1}}(q) = r'2^{i-1}, \quad q^{r'2^{i-1}} = 1 + k_i 2^{i+1}, \quad (k_i, 2) = 1. \tag{49}$$

For $i = 1$ these relations are true, because of the definition of r'.
Assume (49) holds for a certain value of $i \geq 1$. Then $q^{r'2^{i-1}} = 1 + k_i 2^{i+1}$ with $(k_i, 2) = 1$. It follows that

$$q^{r'2^i} = (1 + k_i 2^{i+1})^2 = 1 + k_i 2^{i+2} + k_i^2 2^{2i+2} = 1 + k_{i+1} 2^{i+2}, \quad (k_{i+1}, 2) = 1.$$

Since $i \geq 1$, this implies $\text{ord}_{2^{i+2}}(q) \mid r'2^i$. Therefore, if $e' := \text{ord}_{2^{i+2}}(q)$, we can write $r'2^i = e'y$. We also have $e' = xr'2^{i-1}$. Hence, $xy = 2$, and so $x = 1$ or $x = 2$. But $x = 1$ gives $\text{ord}_{2^{i+2}}(q) = r'2^{i-1} = \text{ord}_{2^{i+1}}(q)$ which contradicts (49). So $x = 2$ and hence (49) also holds for $i+1$, and by induction for all $i \geq 1$.
For values $a > 2$ the proof is completely similar.
□

Remark 42
The above result can also be derived from [2, Lemma 3.34]. Actually, Lemma 41 is a special case of the lemma in [2].

Remark 43
The case $p = 2$, $q = 3$ shows that the condition $a \geq 2$ is necessary, since $\text{ord}_{2^2}(3) = 2 > \text{ord}_{2^1}(3) = 1$, but $\text{ord}_{2^3}(3) = 2 \neq 4$.

As usual we have $r := \text{ord}_n(q) = \text{ord}_{p^\lambda}(q)$. Moreover, we define u:=$\text{ord}_p(q)$. In this case the factorization of $x^n - 1$ into cyclotomic polynomials is as follows

$$x^n - 1 = x^{p^\lambda} - 1 = (x-1)\Phi_p(x)\Phi_{p^2}(x).....\Phi_{p^\lambda}(x). \tag{50}$$

The cyclotomic polynomial $\Phi_p(x)$ is the product of $\nu := \varphi(p)/u = (p-1)/u$ monic polynomials of degree u which are irreducible over $GF(q)$, say

$$\Phi_p(x) = P_1(x)P_2(x).....P_\nu(x). \tag{51}$$

Similarly, $\Phi_{p^b}(x)$ is the product of $\kappa_b := \varphi(p^b)/r_b = p^{b-1}(p-1)/r_b$ irreducible polynomials

$$\Phi_{p^b}(x) = F_1(x)F_2(x).....F_{\kappa_b}(x), \tag{52}$$

which are all of degree r_b, while $r_b = \text{ord}_{p^b}(q)$, $r_1 = u$ and $r_\lambda = r$.
We now distinguish between p is odd and $p = 2$. If p is odd and if $\text{ord}_{p^2}(q) > \text{ord}_p(q)$, it follows from Lemma 41 (i) that

$$r_b = up^{b-1},\ 1 \leq b \leq \lambda, \tag{53}$$

and hence

$$r/u = n/p. \tag{54}$$

As a consequence we have that (cf. [1, Section 4]) $\kappa = \kappa_b = \nu$, and moreover that the polynomials $F_i(x)$ can be identified with $P_i(x^{n/p})$, for $1 \leq i \leq \kappa$. Hence, the cyclotomic polynomials in (52) can be factorized into irreducible polynomials over $GF(q)$ as follows

$$\Phi_{p^b}(x) = P_1(x^{p^{b-1}})P_2(x^{p^{b-1}}).....P_\kappa(x^{p^{b-1}}), \tag{55}$$

for all b, $1 \le b \le \lambda$. Changing the notation of the labels as introduced in (2), we now write

$$\Phi_{p^b}(x) = \prod_{i \in S'\setminus\{0\}} P_i(x^{p^{b-1}}) . \tag{56}$$

In eq. (56) i runs through the $t(=\kappa)$ different values of the set $S'\setminus\{0\} = \{i_1, i_2, ..., i_\kappa\}$, where S' stands for the set of indices of the cyclotomic cosets mod p. This notation expresses the one-to-one relationship between the cyclotomic cosets mod p with respect to q, and the irreducible factors of $\Phi_{p^b}(x)$ in $GF(q)[x]$. The polynomials $P_i(x^{p^{b-1}})$ are all of degree r_b for a fixed value of b. In particular, the polynomials $P_i(x^{p^{\lambda-1}})$, $i \in S'\setminus\{0\}$, which are of degree $r_\lambda = r$, are the minimal generators of the generalized residue codes $C^i_{p^\lambda,q,t}$, with $t = \kappa$.

These considerations also hold for $p = 2$, if we require $\text{ord}_{2^3}(q) > \text{ord}_{2^2}(q) > \text{ord}_2(q)$ (cf. Lemma 41). Therefore, from now on we assume that $\text{ord}_{p^2}(q) > ord_p(q)$ and additionally, if $p = 2$ that $\text{ord}_{2^3}(q) > \text{ord}_{2^2}(q)$. We shall denote this condition by (*).

The columns of the matrix M which correspond to the polynomials $P_i(x^{p^{\lambda-1}})$, $i \in S'\setminus\{0\}$, determine the idempotent generators of the *GR*-codes $C^i_{p^\lambda,q,t}$. In general, we shall label the columns of M by

$$0, i_1^\lambda, i_2^\lambda, ..., i_\kappa^\lambda, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_\kappa^{\lambda-1}, ..., i_1^1, i_2^1, ..., i_\kappa^1, \tag{57}$$

with $i_1^\lambda = 1$, and such that the indices $i_1^b, i_2^b, ..., i_\kappa^b$ indicate the κ irreducible polynomials $P_i(x^{p^{b-1}})$, $i \in S'\setminus\{0\}$, for $1 \le b \le \lambda$. The indices in (57) form the complete set S of indices of the cyclotomic cosets mod p^λ.

The following lemma will enable us to establish the one-to-one relationship between the irreducible polynomials over $GF(q)$ which are contained in $x^{p^\lambda} - 1$ and the cyclotomic cosets mod p^λ with respect to q.

Lemma 44

Let condition (*) *hold. If* $C_i = \{i, iq, ..., iq^{r_b - 1}\}$ *is a cyclotomic coset mod* p^b *with respect to q and of size* r_b, *then* $pC_i = \{pi, piq, ..., piq^{r_b - 1}\}$ *is a cyclotomic coset mod* p^{b+1}, *also of size* r_b, *while it is a cyclotomic coset mod* p^b *of size* r_b / p, *for* $1 \le b \le \lambda$, *if one replaces integers which occur more than once by just one of these.*

The proof is straightforward and is omitted. According to the rule agreed upon in Section 3, we denote this cyclotomic coset mod p^b by C_{ip} (cf. eq. (26) and Lemma 20). Now, we consider the cyclotomic cosets in (57) indexed by $i_1^\lambda, i_2^\lambda, ..., i_\kappa^\lambda$. Since these are cosets mod p^λ, it follows from Lemma 44 that $i_j^\lambda p = i_j^{\lambda-1}$, for $1 \le j \le \kappa$.
More generally, it follows for $1 \le b \le \lambda$ that

$$i_j^\lambda p^{b-1} = i_j^{\lambda-b+1}, \ 1 \le j \le \kappa, \tag{58}$$

$$i_j^\lambda = i_j, \ 1 \le j \le \kappa, \tag{59}$$

where the integers i_j, $1 \le j \le \kappa$, are the non-zero indices of the cyclotomic cosets mod p, i.e. the elements of $S' \setminus \{0\}$.
The cyclotomic cosets with indices $i_1^b, i_2^b, ..., i_\kappa^b$ are of size $r / p^{\lambda-b} = r_b$, and so these cosets correspond to the irreducible polynomials $P_i(x^{p^{b-1}})$, $1 \le i \le \kappa$, which have degree r_b, for all b, $1 \le b \le \lambda$. In particular we may assume that the cyclotomic coset C_i mod p^λ corresponds to the polynomial $P_i(x^{p^{\lambda-1}})$ for all $i \in \{i_1^\lambda, i_2^\lambda, ..., i_\kappa^\lambda\}$.

Next, we consider the matrix elements $\mu_{j,i}$, $i \in \{i_1^\lambda, i_2^\lambda, ..., i_\kappa^\lambda\}$. We know already that $\mu_{0,i} = r$ for these i-values. Furthermore, $p_{ij,1} = 0$ if $ij \notin \{i_1^1, i_2^1, ..., i_\kappa^1\}$, or since $i \in \{i_1^\lambda, i_2^\lambda, ..., i_\kappa^\lambda\}$, $p_{ij,1} = 0$ for all $j \notin \{i_1^1, i_2^1, ..., i_\kappa^1\}$. Hence, we obtain from (37) that $\mu_{j,i} = 0$ for all these indices. So, we only have to focus on elements $\mu_{j,i}$ with $j \in \{i_1^1, i_2^1, ..., i_\kappa^1\}$. We shall restrict ourselves to $i = i_1^\lambda$ =1). We remind the reader of the fact that the columns labeled by $i_2^\lambda, ..., i_\kappa^\lambda$ are permutations of column i_1^λ.

We are now ready to prove our next theorem. In that theorem, the set S^a is the set of the indices of the cyclotomic cosets mod p^a. So, S^λ is identical with S and S^1 with S'. For $a \le \lambda$ one can easily verify that S^a is a subset of S $(= S^\lambda)$ and that $S^a \cap U_{p^a}$ is a subset of $S \cap U_{p^\lambda}$. We emphasize that throughout the text of this section we assume that condition (*) holds.

Theorem 45
Let a be some integer with $1 \le a \le \lambda$ for p odd, and $2 \le a \le \lambda$ for p even. Let $i \in S^a \cap U_{p^a}$. Let $\vartheta_i^*(x)$, $i \in S \cap U_{p^\lambda}$, be the idempotent generator of the code $C^i_{p^\lambda,q,t}$, and let $\vartheta_i^{a*}(x)$ be the idempotent generator of the code $C^i_{p^a,q,t}$, $i \in S^a \cap U_{p^a}$. If $ord_{p^{a+1}}(q) > ord_{p^a}(q)$, then $\vartheta_i^*(x) = \vartheta_i^{a*}(x^{p^{\lambda-a}})$.

Proof

For our convenience we take p odd together with $a=1$.

From Theorem 32 we know that $\vartheta_i(x)=1-\theta_i(x)$ with $\theta_i(x)=n^{-1}\sum_{k\in S}-\frac{r}{m_{ik}}p_{ik,1}c_k(x)$, $n=p^{\lambda}$. Again for reasons of convenience, we assume $i=1$. We already argued that the only k-values that contribute in the expression for $\theta_i(x)$ are $k=0$ and $k\in\{i_1^1,i_2^1,.....,i_\kappa^1\}$.

From $i_k^1=i_k p^{\lambda-1}$ it follows that $m_{i_k^1}=m_{i_k}$, and hence, $\mu_{i_k^1,1}=-\frac{r}{m_{i_k}}p_{i_k,1}$. Because of the condition in the Theorem, we have $\frac{r}{u}=\frac{n}{p}=p^{\lambda-1}$, and so

$$n^{-1}\mu_{i_k^1,1}=-\frac{r}{nm_{i_k}}p_{i_k,1}=-\frac{u}{pm_{i_k}}p_{i_k,1}=p^{-1}\mu'_{i_k,1}.$$

Here, $\mu'_{i_k,1}$ is an element of the matrix M' for the case that the code length is equal to p. Since $c_{i_k^1}(x)=c_{i_k}(x^{p^{\lambda-1}})$, the statement in the Theorem now follows immediately for this case. For other *a*-values we apply Lemma 41, to obtain a completely similar proof. □

Remark 46

The above result can also be derived from the fact that $P_i(x^{p^{\lambda-1}})$ is the minimal generator of $C^i_{p^{a+\lambda-1},q,t}$, if $P_i(x)$ is the minimal generator of $C^i_{p^a,q,t}$.

Example 47

We take $n=27$ and $q=7$. So, $\mathrm{ord}_3(7)=1<\mathrm{ord}_9(7)=3$. Since $u=1$, it follows that $r:=\mathrm{ord}_{3^3}(7)=9$. The cyclotomic cosets mod 27 are

$C_0=\{0\}$, $C_1=\{1,7,22,19,25,13,10,16,4\}$, $C_2=\{2,14,17,11,23,26,19,5,8\}$,

$C_3=\{3,21,12\}$, $C_6=\{6,15,24\}$, $C_9=\{9\}$ and $C_{18}=\{18\}$.

We conclude that $\Phi_{27}(x)$ is the product of two irreducible polynomials over $GF(7)$ of degree 9, $\Phi_9(x)$ is the product of two irreducible polynomials of degree 3 and $\Phi_3(x)$ is the product of two irreducible polynomials of degree 1 all over $GF(7)$. Actually, we have

$$x^{27}-1=(x-1)\Phi_3(x)\Phi_9(x)\Phi_{27}(x)=(x-1)(x-2)(x-4)(x^3-2)(x^3-4)(x^9-2)(x^9-4).$$

This is in accordance with the formalism on p. 38, since $\mathrm{ord}_9(7)=3>\mathrm{ord}_3(7)=1$.

One can easily verify that the irreducible factors in the rhs correspond to the cyclotomic cosets by means of the indices in the following way:

$P_0(x) = x-1$, $P_1(x) = x^9 - 2$, $P_2(x) = x^9 - 4$, $P_3(x) = x^3 - 2$, $P_6(x) = x^3 - 4$, $P_9(x) = x - 2$ and $P_{18}(x) = x - 4$.

Using these facts, we derive the matrix elements of the column with index 1:

$\mu_{0,1} = m_1 = 9$, $\mu_{0,2} = m_2 = 9$, $\mu_{9,1} = -\frac{m_1}{m_9} p_{9,1} = -\frac{9}{1}(-2) = 18$,

$\mu_{18,1} = -\frac{m_1}{m_{18}} p_{18,1} = -\frac{9}{1}(-4) = 36$, while all other elements $\mu_{j,1}$ in this column vanish, because $p_{j,1} = 0$ for those elements. After having computed the elements of the other columns in a completely similar way and reducing mod 7, we finally find for M

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 6 & 9 & 18 \end{matrix} \\ \begin{pmatrix} 1 & 9 & 9 & 3 & 3 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 2 & 4 \\ 1 & 0 & 0 & 0 & 0 & 4 & 2 \\ 1 & 0 & 0 & 6 & 5 & 1 & 1 \\ 1 & 0 & 0 & 5 & 6 & 1 & 1 \\ 1 & 4 & 1 & 3 & 3 & 1 & 1 \\ 1 & 1 & 4 & 3 & 3 & 1 & 1 \end{pmatrix} \end{array} \begin{matrix} \\ 0 \\ 1 \\ 2 \\ 3 \\ 6 \\ 9 \\ 18 \end{matrix}.$$

From this matrix we derive the primitive idempotent generator

$$\begin{aligned} \theta_1(x) &= 27^{-1}(\mu_{0,2} c_0(x) + \mu_{9,2} c_9(x) + \mu_{18,2} c_{18,2}(x)) \\ &= -(2c_0(x) + c_9(x) + 4c_{18}(x)) \\ &= 3x^{18} + 6x^9 + 5. \end{aligned}$$

and similarly $\theta_2(x) = 6x^{18} + 3x^9 + 5$. The idempotent generators of $C^1_{27,7,2}$ and $C^2_{27,7,2}$ are $\vartheta_1(x) = 4x^{18} + x^9 + 3$ and $\vartheta_1^*(x) = \vartheta_2(x) = x^{18} + 4x^9 + 3$ and $\vartheta_2^*(x) = \vartheta_1(x) = 4x^{18} + x^9 + 3$, respectively. As one can verify, these generators can be obtained from the corresponding generators of the codes $C^i_{9,7,2}$ by substituting x^9 for x. □

Example 48

For $n = 2^3$ and $q = 3$, we have $r := \mathrm{ord}_{2^3}(3) = 2$ and $t = \kappa = \varphi(8)/2 = 2$. The cyclotomic cosets mod 2^3 are $C_0 = \{0\}$, $C_1 = \{1,3\}$, $C_2 = \{2,6\}$, $C_4 = \{4\}$, $C_5 = \{5,7\}$, implying $S = \{0,1,2,4,5\}$. The corresponding irreducible polynomials are respectively $P_0(x) = x - 1$,

$P_1(x) = x^2 - x - 1$, $P_2(x) = x^2 + 1$, $P_4(x) = x + 1$ and $P_5(x) = x^2 + x + 1$. The factorization of $x^8 - 1$ into cyclotomic polynomials is $x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$, with $\Phi_1(x) = P_0(x)$, $\Phi_2(x) = P_4(x)$, $\Phi_4(x) = P_2(x)$ and $\Phi_8(x) = P_1(x)P_5(x)$.
As one can see, the number of irreducible polynomials contained in $\Phi_4(x)$ (and in $\Phi_2(x)$) is less than the number of irreducible factors of $\Phi_8(x)$. This is due to the fact that the condition $\mathrm{ord}_{2^3}(3) > \mathrm{ord}_{2^2}(3)$ is not satisfied, since both are equal to 2.
The irreducible polynomials $P_1(x)$ and $P_5(x)$ are the minimal generators of the two equivalent *GR*-codes $C^1_{8,3,2}$ and $C^5_{8,3,2}$. Applying the expression (27) for the matrix elements $\mu_{j,i}$, $i, j \in S$, we find for the matrix M

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 5 & 2 & 4 \end{matrix} \\ \begin{pmatrix} 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 0 & -1 \\ 1 & -1 & 1 & 0 & -1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 5 \\ 2 \\ 4 \end{matrix}.$$

The primitive idempotent generators corresponding to the columns with labels 1 and 5 are respectively

$$\theta_1(x) = 8^{-1}(-c_0(x) + c_1(x) - c_5(x) + c_4(x)) = x^7 + x^5 - x^4 - x^3 - x + 1,$$

$$\theta_5(x) = 8^{-1}(-c_0(x) - c_1(x) + c_5(x) + c_4(x)) = -x^7 - x^5 - x^4 - x^3 - x + 1.$$

The idempotent generators of $C^1_{8,3,2}$ and $C^5_{8,3,2}$ are respectively

$$\vartheta_1^*(x) = \vartheta_5(x) = 1 - \theta_5(x) = x^7 + x^5 + x^4 + x^3 + x,$$

and

$$\vartheta_5^*(x) = \vartheta_1(x) = 1 - \theta_1(x) = -x^7 - x^5 + x^4 + x^3 + x. \qquad \square$$

Example 49
Next, we take $n = 2^4$ and $q = 3$. Now we have $r := \mathrm{ord}_{2^4}(3) = 4$ and $\kappa = \varphi(16)/4 = 2$.
The cyclotomic cosets are $C_0 = \{0\}$, $C_1 = \{1,3,9,11\}$, $C_2 = \{2,6\}$, $C_4 = \{4,12\}$, $C_5 = \{5,15,13,7\}$, $C_8 = \{8\}$, $C_{10} = \{10,14\}$, and the corresponding irreducible polynomials

are $P_0(x) = x-1$, $P_1(x) = x^4 - x^2 - 1$, $P_2(x) = x^2 - x - 1$, $P_4(x) = x^2 + 1$,
$P_5(x) = x^4 + x^2 - 1$, $P_8(x) = x + 1$ and $P_{10}(x) = x^2 + x - 1$.
For the same reason as in the previous example, the number of irreducible factors in $\Phi_8(x)$ is unequal to the number of irreducible factors in $\Phi_4(x)$.
The factorization of $\Phi_{16}(x)$ into two irreducible polynomials of degree $r = 4$ is $\Phi_{16}(x) = (x^4 - x^2 - 1)(x^4 + x^2 - 1)$. These polynomials are the defining polynomials of the equivalent *GR*-codes $C^1_{16,3,2}$ and $C^5_{16,3,2}$. We now have sufficient data to compute the elements of the matrix M. Using again (27), we find the following elements in column 1: $\mu_{0,1} = 1$, $\mu_{2,1} = -1$, $\mu_{8,1} = -1$, $\mu_{10,1} = 1$, $\mu_{1,1} = \mu_{4,1} = \mu_{5,1} = 0$. So,

$$\theta_1(x) = 16^{-1}(c_0(x) - c_2(x) - c_8(x) + c_{10}(x)) = 1 - x^2 - x^6 - x^8 + x^{10} + x^{14},$$

$$\vartheta_1(x) = -x^{14} - x^{10} + x^8 + x^{10} + x^{14}.$$

Similarly, we find

$$\theta_5(x) = 16^{-1}(c_0(x) + c_2(x) - c_8(x) - c_{10}(x)) = 1 + x^2 + x^6 - x^8 - x^{10} - x^{14},$$

$$\vartheta_5(x) = x^{14} + x^{10} + x^8 - x^6 - x^2.$$

Indeed, the idempotent generators of $C^i_{2^4,3,2}$ can be obtained from those of $C^i_{2^3,3,2}$, $i \in \{1,5\}$, by replacing x by x^2. □

8. The case $n = 2p^\lambda$

Throughout the discussion of this case we assume again that condition (*) of p. 39 holds. We have the relations $r := \mathrm{ord}_{2p^\lambda}(q) = \mathrm{ord}_{p^\lambda}(q)$, $u := \mathrm{ord}_p(q)$, and $\kappa = \varphi(p)/u = p - 1/u$. In a similar way as in Sections 6 and 7, we derive that the factorization of $x^n - 1 = x^{2p^\lambda} - 1$ into cyclotomic polynomials now has the form

$$\begin{aligned} x^{2p^\lambda} - 1 &= \Phi_1(x)\Phi_2(x)\Phi_p(x)\Phi_{p^2}(x).....\Phi_{p^\lambda}(x)\Phi_{2p}(x)\Phi_{2p^2}(x).....\Phi_{2p^\lambda}(x) \\ &= (x-1)(x+1)\Phi_p(x)\Phi_{p^2}(x).....\Phi_{p^\lambda}(x)\Phi_p(-x)\Phi_{p^2}(-x).....\Phi_{p^\lambda}(-x), \end{aligned} \tag{60}$$

with

$$\Phi_{p^b}(x) = \prod_{i \in S' \setminus \{0\}} P_i(x^{p^{b-1}}), \tag{61}$$

for all b, $1 \le b \le \lambda$, and where the κ monic polynomials $P_i(x)$, $i \in S' \setminus \{0\}$, are the irreducible factors in $GF(q)[x]$ contained in $\Phi_p(x)$. Here, like in Section 7, S' stands

for the set of indices of the cyclotomic cosets mod p. The monic irreducible polynomials contained in $\Phi_{2p^\lambda}(x)$, which can be written as $(-1)^r P_i(-x^{p^{\lambda-1}})$, $i \in S'' \setminus \{0\}$, are the minimal generators of the *GR*-codes $C^i_{2p^\lambda,q,t}$ with $t = \kappa$. The columns of the matrix M which correspond to these polynomials determine the idempotent generators of these *GR*-codes.

Just like in Section 6, we now present a lemma which will enable us to establish the relationship between the above irreducible polynomials and the cyclotomic cosets mod $2p^\lambda$ with respect to *q*. In Lemma 50 the notation S stands again for the set of indices of cyclotomic cosets mod p^λ, while S'' denotes the set of such indices mod $2p^\lambda$. Similarly as in Section 6, we define that if $C_i = \{i, iq, ..., iq^{r_0-1}\}$, $i \in S$, $r_0 \mid r$, is a cyclotomic coset mod p^λ, then C_{2i} is the set consisting of all integers $2a$, $a \in C_i$. This set C_{2i} is a cyclotomic coset mod $2p^\lambda$. Furthermore, we introduce for each $i \in S$, a set consisting of the integers $a \in C_i$ when *a* is odd and $a + p^\lambda$ when *a* is even. If *i* is odd, we call this set again C_i, and if i is even C_{i+p^λ}. The sets C_i and C_{i+p^λ}, $i \in S$, together contain all odd positive integers which are less than $2p^\lambda$. The sets C_{2i}, $i \in S$, together contain all even nonnegative integers less than $2p^\lambda$.

Lemma 50

(i) *C_{2i} is a cyclotomic coset mod $2p^\lambda$ for any $i \in S$;*

(ii) *C_i and C_{i+p^λ} are cyclotomic cosets mod $2p^\lambda$ for all $i \in S$;*

(iii) *if $a \in C_i$, then mod $2p^\lambda$, $2a \in C_{2i}$;*

(iv) *the cyclotomic cosets in* (i) *and* (ii) *together constitute the complete family of $2\kappa + 2$ cyclotomic cosets mod $2p^\lambda$ and their indices constitute the index set S'';*

(v) *the cyclotomic cosets in* (i) *correspond to irreducible polynomials contained in $\Phi_{p^\lambda}(x)$ and those in* (ii) *to irreducible polynomials contained in $\Phi_{2p^\lambda}(x)$;*

(vi) *if $P_i(x)$ is an irreducible factor of $\Phi_{p^\lambda}(x)$, then $P_{i+p^\lambda}(x)$ is an irreducible factor of $\Phi_{2p^\lambda}(x)$ and vice versa, for all $i \in S$ and $P_{i+p^\lambda}(x) = (-1)^r P_i(-x)$;*

(vii) *if C_{j+p^λ}, $j \in S$ and j odd, is the set of integers $a \in C_j$ for a even and $a + p^\lambda$ for a odd, then the family $\{C_{j+p^\lambda} : j \in S\}$ is the same as the family $\{C_{2j} : j \in S\}$ defined in* (*i*);

(viii) *$C_{2i} = C_{i+p^\lambda}$, and hence $P_{2i}(x) = P_{i+p^\lambda}(x)$, for all $i \in S$, if and only if $2 \in C_1$.*

The proofs are similar to the proofs of Lemma 37.

Similarly to the labeling (57), we now introduce the following general labeling of the columns and rows of the matrix M (cf. the labeling in the cases $n = 2p$ and $n = p^\lambda$):

$$0, i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa}^{\lambda}, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_{\kappa}^{\lambda-1}, ..., i_1^1, i_2^1, ..., i_{\kappa}^1,$$
$$i_{\kappa+1}^{\lambda}, i_{\kappa+2}^{\lambda}, ..., i_{2\kappa}^{\lambda}, i_{\kappa+1}^{\lambda-1}, i_{\kappa+2}^{\lambda-1}, ..., i_{2\kappa}^{\lambda-1}, ..., i_{\kappa+1}^1, i_{\kappa+2}^1, ..., i_{2\kappa}^1, p^{\lambda} \qquad (62)$$

Together, the indices in (62) constitute the index set S'' of the cyclotomic cosets mod $2p^{\lambda}$. The mutual dependence of the indices in the first line of (62) is given by the relations (58) and (59). With respect to these relations, one should remember that the index of a cyclotomic coset is not uniquely determined, but can in principle be equal to any of the integers contained in that particular coset.

We choose the labels in (62) such that $i_1^b, i_2^b, ..., i_{\kappa}^b$ indicate in some order the κ monic irreducible polynomials $(-1)^{r_b} P_i(-x^{p^{b-1}})$, $i \in S''\backslash\{0\}$, contained in $\Phi_{2p^b}(x) = \Phi_{p^b}(-x)$, while $i_{\kappa+1}^b, i_{\kappa+2}^b, ..., i_{2\kappa}^b$ indicate the monic irreducible polynomials $P_i(x^{p^{b-1}})$, $i \in S''\backslash\{0\}$, contained in $\Phi_{p^b}(x)$, for $1 \le b \le \lambda$. In other words, we choose the indices such that $P_{i_j^b}(x) = (-1)^{r_b} P_{\kappa+i_j^b}(-x)$, for $1 \le j \le \kappa$, and hence $P_{i_j^b}(x) = P_{i_j}(x^{p^{b-1}}) = (-1)^{r_b} P_{\kappa+i_j^b}(-x)$. According to Lemma 50 (vi), this can be accomplished by taking $i_{\kappa+j} = i_j + p^{\lambda}$, for $1 \le j \le \kappa$, since $\zeta^{p^{\lambda}} = -1$ if ζ is a primitive $2p^{\lambda\ th}$ root of unity. We shall always take for ζ a zero of $P_{i_1^{\lambda}}(x) (= P_1(x^{p^{\lambda-1}}))$ as primitive $2p^{\lambda}$ root of unity, and so $i_1^{\lambda} = 1$. The final index p^{λ} in (62) indicates the column corresponding to the cyclotomic coset $C_{p^{\lambda}} = \{p^{\lambda}\}$.

The columns of M with a label $i \in \{i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa}^{\lambda}\}$ determine the idempotent generators of the *GR*-codes $C^i_{2p^{\lambda},q,t}$. As for the matrix elements in these columns, we have similarly as in the case of $n = p^{\lambda}$, that $\mu_{j,i} = 0$ unless $j \in \{i_1^1, ..., i_{\kappa}^1, i_{\kappa+1}^1, ..., i_{2\kappa}^1\}$ or $j \in \{0, p^{\lambda}\}$. In particular, $\mu_{0,i} = r$ for these $i-$values and $\mu_{p^{\lambda},i} = -r$. It will be obvious that the indices (43) form a special case of (62) for $\lambda = 1$. We shall give an example to illustrate the above considerations.

Example 51

We take $n = 18 = 2.3^2$ and $q = 5$. Then we have $p = 3$, $\lambda = 2$, $u := \mathrm{ord}_3(5) = 2$, $\mathrm{ord}_9(5) = 6$ and $r := \mathrm{ord}_{18}(5) = 6$. It follows that $\kappa = \varphi(18)/r = 1$, so there is only one *GR*-code $C^1_{18,5,1}$.

To illustrate the relationship between the cyclotomic cosets mod 18 and mod 9, we first determine the latter cosets: $C_0 = \{0\}$, $C_1 = \{1,2,4,5,7,8\}$ and $C_3 = \{3,6\}$. Applying Lemma 50 (i), (ii) yields the cosets mod 18: $C_0 = \{0\}$,

$C_1 = \{1,5,7,11,13,17\}$, $C_2 (= C_{10}) = \{2,4,8,10,14,16\}$, $C_3 = \{3,15\}$, $C_6 (= C_{12}) = \{6,12\}$ and

$C_9 = \{9\}$. The labels i_j^{λ} of the rows and columns of M are $\lambda_1^2 = 1$, $\lambda_2^2 = 3$, $\lambda_2^1 = 2$ (or 10) and $\lambda_2^1 = 6$ (or 12).

The factorization of $x^{18} - 1$ into cyclotomic polynomials is

$$\begin{aligned} x^{18} - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_9(x)\Phi_{18}(x) \\ &= (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^3+1)(x^6-x^3+1). \end{aligned}$$

All these cyclotomic polynomials are irreducible in $GF(5)[x]$ and hence $P_0(x) = x - 1$, $P_1(x) = x^6 - x^3 + 1$, $P_2(x) = x^6 + x^3 + 1$, $P_3(x) = x^2 - x + 1$ $P_6(x) = x^2 + x + 1$, $P_9(x) = x + 1$, as one can easily verify.

For the matrix M we find

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 3 & 2 & 6 & 9 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 2 & 1 & 2 & 1 \\ 1 & 0 & 1 & 0 & 4 & 4 \\ 1 & 3 & 3 & 2 & 2 & 4 \\ 1 & 0 & 4 & 0 & 4 & 1 \\ 1 & 2 & 2 & 2 & 2 & 1 \\ 1 & 4 & 3 & 1 & 2 & 4 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 3 \\ 2 \\ 6 \\ 9 \end{matrix}.$$

The idempotent generator of $C_{18,5,1}^1$ is given by

$$\begin{aligned} \vartheta_1^*(x) = \vartheta_1(x) &= 1 - \theta_1(x) = 1 - 18^{-1}(c_0(x) + 3c_3(x) + 2c_6(x) + 4c_9(x)) \\ &= 1 - 2(1 - 2(x^3 + x^{15}) + 2(x^6 + x^{12}) - x^9) \\ &= -x^{15} + x^{12} + 2x^9 + x^6 - x^3 - 1. \end{aligned}$$

□

Example 52

Next, we take $n = 18$ and $q = 7$. Now, the polynomials $\Phi_3(x)$, $\Phi_6(x)$, $\Phi_9(x)$ and $\Phi_{18}(x)$ are no longer irreducible, and we can write

$$\begin{aligned} x^{18} - 1 &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_9(x)\Phi_{18}(x) \\ &= (x-1)(x+1)(x-4)(x-2)(x+4)(x+2)(x^3-4)(x^3-2)(x^3+4)(x^3+2), \end{aligned}$$

where the polynomials in the rhs are all irreducible in $GF(7)[x]$.

The cyclotomic cosets mod 9 are $C_0 = \{0\}$, $C_1 = \{1,4,7\}$, $C_2 = \{2,5,8\}$, $C_3 = \{3\}$ and $C_6 = \{6\}$. The corresponding irreducible polynomials are $P_0'(x) = x - 1$, $P_1'(x) = x^3 - 4$, $P_2'(x) = x^3 - 2$, $P_3'(x) = x - 4$ and $P_6'(x) = x - 2$.

Applying Lemma 50 (i) and (ii), we obtain the cyclotomic cosets mod 18:
$C_0 = \{0\}$, $C_1 = \{1,7,13\}$, $C_2 = \{2,8,14\}$, $C_5 = \{5,11,17\}$, $C_4 = \{4,10,16\}$, $C_3 = \{3\}$,
$C_6 = \{6\}$, $C_{12} = \{12\}$, $C_{15} = \{15\}$ and $C_9 = \{9\}$,
As primitive 18^{th} root of unity in some extension field of $GF(7)$ of degree 3, we take for ζ a zero of $x^3 + 4 = x^3 - 3$. Next, by applying $\zeta^3 = 3$, we find
$P_0(x) = x - 1$, $P_1(x) = x^3 - 3$, $P_2(x) = x^3 - 2$, $P_5(x) = x^3 + 2$, $P_4(x) = x^3 - 4$, $P_3(x) = x - 3$,
$P_6(x) = x - 2$, $P_{12}(x) = x + 3$, $P_{15}(x) = x + 2$ and $P_9(x) = x + 1$.
As one can verify, this set of irreducible polynomials can be obtained from those for $n = 9$, by taking $\{P_i^{'}(x) \mid i \in S'\backslash\{0\}\} \cup \{\pm P_i^{'}(-x) \mid i \in S'\backslash\{0\}\}$, where the signs in the second subset depend on the degree of the polynomial $P_i^{'}(-x)$ Hence, the indices $0, i_1^2, i_2^2, i_1^1, i_2^1, i_3^2, i_4^2, i_3^1, i_4^1, p^m$ of (62), have the values $0,1,5,3,15,4,2,12,6,9$, respectively. The idempotent generators of the *GR*-codes $C_{18,7,2}^i$, $i \in \{1,5\}$, are determined by the columns of the matrix M with label 1 and 5. The elements in these columns are (cf. (27)) $\mu_{j,i} = -\frac{m_i}{m_{ij}} p_{ij,1}$, with i equal to 1 and 5, respectively. We find for the corresponding column vectors $\mu_1 = (3,0,0,2,1,0,0,-2,-1,-3)^T$ and $\mu_5 = (3,0,0,1,2,0,0,-1,-2,-3)^T$. Hence, the idempotent generators of $C_{18,7,2}^1$ and $C_{18,7,2}^5$ are respectively

$$\begin{aligned}\vartheta_1^*(x) = 1 - \theta_5(x) &= 1 - 18^{-1}(3c_0(x) + c_3(x) + 2c_{15}(x) - c_{12}(x) - 2c_6(x) - 3c_9(x)) \\ &= 1 - 2(3 + x^3 + 2x^{15} - x^{12} - 2x^6 - 3x^9) \\ &= 3x^{15} + 2x^{12} - x^9 - 3x^6 - 2x^3 + 2\end{aligned}$$

and

$$\begin{aligned}\vartheta_5^*(x) = 1 - \theta_1(x) &= 1 - 18^{-1}(3c_0(x) + 2c_3(x) + c_{15}(x) - 2c_{12}(x) - c_6(x) - 3c_9(x)) \\ &= 1 - 2(3 + 2x^3 + x^{15} - 2x^{12} - x^6 - 3x^9) \\ &\quad -2x^{15} - 3x^{12} - x^9 + 2x^6 - 4x^3 + 2.\end{aligned}$$

For reasons of completeness, we finally present the complete matrix M:

$$M = \begin{array}{c} \begin{array}{cccccccccc} 0 & 1 & 5 & 3 & 15 & 4 & 2 & 12 & 6 & 9 \end{array} \\ \begin{pmatrix} 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 & 1 \\ 1 & 0 & 0 & 3 & -2 & 0 & 0 & -3 & 2 & -1 \\ 1 & 0 & 0 & -2 & 3 & 0 & 0 & 2 & -3 & -1 \\ 1 & 2 & 1 & -1 & -1 & -2 & -1 & 1 & 1 & -1 \\ 1 & 1 & 2 & -1 & -1 & -1 & -2 & 1 & 1 & -1 \\ 1 & 0 & 0 & -3 & 2 & 0 & 0 & -3 & 2 & 1 \\ 1 & 0 & 0 & 2 & -3 & 0 & 0 & 2 & -3 & 1 \\ 1 & -2 & -1 & 1 & 1 & -2 & -1 & 1 & 1 & 1 \\ 1 & -1 & -2 & 1 & 1 & -1 & -2 & 1 & 1 & 1 \\ 1 & -3 & -3 & -1 & -1 & 3 & 3 & 1 & 1 & -1 \end{pmatrix} \end{array} \begin{array}{c} 0 \\ 1 \\ 5 \\ 3 \\ 15 \\ 4 \\ 2 \\ 12 \\ 6 \\ 9 \end{array}$$

Notice that the 6^{th} column of M corresponds to the cyclotomic coset $C_{1+9} = C_{10} = C_4$, and the 7^{th} column to $C_{5+9} = C_{14} = C_2$.

Next, we present a theorem on the relationship between the idempotent generators of *GR*-codes of length $2p^{\lambda}$ and length $2p^{a}$ with $a \le \lambda$ which is similar to Theorem 45 . We shall need the following lemma.

Lemma 53
Let p be an odd prime and q some odd prime power with $(p,q)=1$. *Let furthermore a be some integer* ≥ 1. *The inequality* $ord_{2p^{a+1}}(q) > ord_{2p^{a}}(q)$ *implies* $ord_{2p^{a+i-1}}(q) = p^{i-1} ord_{2p^{a}}(q)$, *for all* $i \ge 1$.

The proof is similar to the first part of the proof of Lemma 41 . Like Lemma 41, the above result is also a special case of [2, Lemma 3.34] .

In the next theorem, the set S^a is the set of the indices of the cyclotomic cosets mod $2p^a$ for some $a \ge 1$, while S " is the set of such indices mod $2p^{\lambda}$. Similarly as in Section 7, S^a is a subset of S" and $S^a \cap U_{2p^a}$ is a subset of $S" \cap U_{2p^{\lambda}}$, if $a \le \lambda$.

Theorem 54
Let a be some integer satisfying $1 \le a \le \lambda$. *Let* $\vartheta_i^*(x)$, $i \in S" \cap U_{2p^{\lambda}}$, *be the idempotent generator of the GR-code* $C^i_{2p^{\lambda},q,t}$, *and let* $\vartheta_i^{a*}(x)$ *be the idempotent generator of* $C^i_{2p^{a},q,t}$,

$i \in S^a \cap U_{2p^a}$. *If* $ord_{2p^{a+1}}(q) > ord_{2p^a}(q)$, *then* $\vartheta_i^*(x) = \vartheta_i^{a*}(x^{p^{\lambda-a}})$.

The proof is completely similar to the proof of Theorem 45.
We shall illustrate Theorem 54 by an example.

Example 55
Again we take $n = 18$ and $q = 7$. In the previous example we computed the idempotents of the *GR*-codes $C^i_{18,7,2}$, $i \in \{1,5\}$. Now, we shall do the same for the *GR*-codes $C^i_{6,7,2}$, $i \in \{1,5\}$. For $n = 6$ and $q = 7$, we have the cyclic cosets $C_0 = \{0\}, C_1 = \{1\}, C_2 = \{2\}$, $C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\}$. Notice that $S^1 = \{0,1,2,3,4,5\}$ is a subset of $S'' = \{0,1,5,3,15,2,4,12,,6,9\}$ and that $S^1 \cap U_6 = S'' \cap U_{18} = \{1,5\}$.
We can write

$$x^6 - 1 = (x-1)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1).$$

Since $u := \mathrm{ord}_6(7) = 1$ and $\kappa = 2/u = 2$, we can factorize $\Phi_6(x)$ in $GF(7)[x]$ as $x^2 - x + 1 = (x-3)(x+2)$. Similarly, we have $x^2 + x + 1 = (x-2)(x+3)$. For a primitive 6^{th} root of unity we choose $\zeta = 3$. Hence, $P_1'(x) = x - 3$, and consequently $P_2'(x) = x - 2$, $P_3'(x) = x + 1$, $P_4'(x) = x + 3$, $P_5'(x) = x + 2$ and $P_0'(x) = x - 1$.
Using the convention of labeling (62) and the definition of the matrix elements $\mu_{i,j}$ in (27), we obtain for the matrix M' in this case

$$M' = \begin{array}{c} \begin{matrix} 0 & 1 & 5 & 4 & 2 & 3 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & -2 & -3 & 2 & -1 \\ 1 & -2 & 3 & 2 & -3 & -1 \\ 1 & -3 & 2 & -3 & 2 & 1 \\ 1 & 2 & -3 & 2 & -3 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 5 \\ 4 \\ 2 \\ 3 \end{matrix}.$$

Hence,

$$\theta_1^{1*}(x) = \theta_5'(x) = 6^{-1}(1 - 2x + 3x^5 - x^3 - 3x^2 + 2x^4) = -3x^5 - 2x^4 + x^3 + 3x^2 + 2x - 1,$$

$$\vartheta_1^{1*}(x) = 3x^5 + 2x^4 - x^3 - 3x^2 - 2x + 2.$$

Since $\mathrm{ord}_{18}(7) = 3 > \mathrm{ord}_6(7) = 1$, we are allowed to apply Theorem 54 which yields

$$\vartheta_1^{\,*}(x) = 3x^{15} + 2x^{12} - x^9 - 3x^6 - 2x^3 + 2,$$

and which is identical to the expression for $\vartheta_1^*(x)$ in Example 52.
Similarly, we find

$$\vartheta_5^{1*}(x) = -2x^5 - 3x^4 - x^3 + 2x^2 - 4x + 2,$$

and again by Theorem 54

$$\vartheta_5^{\,*}(x) = -2x^{15} - 3x^{12} - x^9 + 2x^6 - 4x^3 + 2,$$

the same expression as found in Example 52.

Combining Theorems 39 and 54, would yield expressions for the idempotent generators of codes of length $2p^{\lambda}$ in terms of idempotent generators of codes of length p, when $a = 1$. We omit such expressions.

9. A few remarks on the unrestricted cases $n = p^{\lambda}$ and $n = 2p^{\lambda}$

In this section we briefly discuss the situation when condition (*) is not satisfied.

Example 56
Take $n = 5^2$ and $q = 7$. We now have $\text{ord}_5(7) = \text{ord}_{25}(7) = 4$ and $\text{ord}_{125}(7) = 20$. So, $r_1 = 4$, $r_2 = 4$ and $r_3 = 20$. Hence, the integer a in Lemma 41 cannot be taken equal to 1. Its minimal value is 2. Furthermore, $\kappa_1 = \varphi(5)/r_1 = 1$, $\kappa_2 = \varphi(25)/r_2 = 5$ and $\kappa_3 = \varphi(125)/r_3 = 5$.

The cyclotomic cosets mod 5 are $C_0 = \{0\}$ and $C_1 = \{1,2,4,3\}$ with corresponding irreducible polynomials (in $GF(7)[x]$) $P_0(x) = x - 1$ and $P_1(x) = x^4 + x^3 + x^2 + x + 1$. The second polynomial generates the *GR*-code $C_{5,7,1}^{1}$.

The cyclotomic cosets mod 25 are $C_0 = \{0\}$, $C_1 = \{1,7,24,18\}$, $C_2 = \{2,14,23,11\}$, $C_3 = \{3,21,22,4\}$, $C_6 = \{6,17,19,8\}$, $C_9 = \{9,13,16,12\}$ and $C_5 = \{5,10,20,15\}$. The irreducible polynomials corresponding to these cosets are respectively $P_0(x) = x - 1$, $P_1(x) = x^4 + 2x^3 + 4x^2 + 2x + 1$, $P_2(x) = x^4 + 4x^3 + 3x^2 + 4x + 1$, $P_3(x) = x^4 + 4x^3 + 4x + 1$, $P_6(x) = x^4 + 5x^3 + 5x^2 + 5x + 1$, $P_9(x) = x^4 + 6x^3 + 5x^2 + 6x + 1$ and $P_5(x) = x^4 + x^3 + x^2 + x + 1$.
From these data we derive the explicit form of the matrix *M*, which appears to be

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 6 & 9 & 5 \end{matrix} \\ \begin{pmatrix} 1 & 4 & 4 & 4 & 4 & 4 & 4 \\ 1 & -2 & -4 & -4 & -5 & -6 & -1 \\ 1 & -4 & -4 & -5 & -6 & -2 & -1 \\ 1 & -4 & -5 & -6 & -2 & -4 & -1 \\ 1 & -5 & -6 & -2 & -4 & -4 & -1 \\ 1 & -6 & -2 & -4 & -4 & -5 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 & 4 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 6 \\ 9 \\ 5 \end{matrix}.$$

The irreducible polynomials $P_1(x)$, $P_2(x)$, $P_3(x)$, $P_6(x)$ and $P_9(x)$ generate the *GR*-codes $C^i_{25,7,5}$, $i \in \{1,2,3,6,9\}$, while the columns with these indices determine the idempotent generators of these codes. So, similar to the notation (57), we now write $i_1^2 = 1$, $i_2^2 = 2$, $i_3^2 = 3$, $i_4^2 = 6$, $i_5^2 = 9$ and $i_1^1 = 5$.

We also investigate the relevant data in the case $n = 5^3$, $q = 7$.
The cyclotomic cosets mod 125 are $C_0 = \{0\}$,
$C_1 = \{1,7,49,93,26,57,24,43,51,107,124,118,76,32,99,68,111,82,74,18\}$,
$C_2 = 2C_1$, $C_3 = 3C_1$, $C_6 = 6C_1$, $C_9 = 9C_1$, $C_5 = \{5,35,120,90\}$, $C_{10} = \{10,70,115,55\}$,
$C_{15} = \{15,105,110,20\}$, $C_{30} = \{30,85,95,40\}$, $C_{45} = \{45,65,80,60\}$ and
$C_{25} = \{25,50,100,75\}$.
So, instead of labeling (57), we now have the following indices for the cyclotomic cosets

0, 1, 2, 3, 6, 9, 5, 10, 15, 30, 45, 25.

Similarly to the notation of (57), we denote these indices by $i_1^3 = 1$, $i_2^3 = 2$, $i_3^3 = 3$, $i_4^3 = 6$, $i_5^3 = 9$, $i_1^2 = 5$, $i_2^2 = 10$, $i_3^2 = 15$, $i_4^2 = 30$, $i_5^2 = 45$, $i_1^1 = 25$. The irreducible polynomials corresponding to the cyclotomic cosets are respectively $P_0(x)(= x-1)$, $P_1(x^5)$, $P_2(x^5)$, $P_3(x^5)$, $P_6(x^5)$, $P_9(x^5)$, $P_5(x)$, $P_{10}(x)$, $P_{15}(x)$, $P_{30}(x)$, $P_{45}(x)$ and $P_{25}(x)$. From $r :=$ $\text{ord}_{5^3}(7) = 20$ and $\varphi(5^3) = 5^2(5-1) = 100$, it follows that $\kappa = 100/20 = 5$. Taking $t = \kappa$, gives that the 5 columns of M labeled by 1, 2, 3, 6 and 9 determine the idempotent generators of the *GR*-codes $C^i_{5^3,7,5}$, $i \in \{1,2,3,6,9\}$. □

The previous example suggests the following extension of Lemma 44 which only holds if condition (*) is satisfied, i.e. if $\text{ord}_{p^2}(q) > \text{ord}_p(q)$ and additionally $\text{ord}_{2^3}(q) > \text{ord}_{2^2}(q)$ for $p = 2$.

Lemma 57

Let p be an arbitrary prime and q some prime power such that $(p,q) = 1$. *Let furthermore* $r_b := ord_{p^b}(q)$ *and* $\kappa_b := \varphi(p^b)/r_b$, *for* $b \geq 1$. *Then the following statements hold:*

(i) *if p is odd, there is an integer d,* $d \geq 1$, *with* $1 \leq r_1 = ... = r_d < r_{d+1} < r_{d+2} ....$, $r_{b+1} = pr_b$ *for* $b \geq d$, *and* $1 \leq \kappa_1 < .... < \kappa_d = \kappa_{d+1} = \kappa_{d+2} = ...$, $\kappa_{b+1} = p\kappa_b$ *for* $1 \leq b < d$;

(ii) *if p = 2, there is an integer d,* $d \geq 2$, *such that either*
$1 = r_1 = r_2 = ... = r_d < r_{d+1} < r_{d+2} < .... and\ 1 = \kappa_1 < \kappa_2 < .... < \kappa_d = \kappa_{d+1} = \kappa_{d+2} = ...$ *or*
$1 = r_1 < 2 = r_2 = ... = r_d < r_{d+1} < r_{d+2} < ....$ *and* $1 = \kappa_1 = \kappa_2 < .... < \kappa_d = \kappa_{d+1} = \kappa_{d+2} = ...$, *while* $r_{b+1} = 2r_b$ *for* $b \geq d$, *and* $\kappa_{b+1} = 2\kappa_b$ *for* $1 \leq b < d$ *and* $2 \leq b < d$ *respectively*;

(iii) *there are* κ_b *nonzero cyclotomic cosets mod* p^b *and of size* r_b *for* $b \geq 1$;

(iv) *to each cyclotomic coset* $C_i = \{i, qi, ..., q^{r_b - 1}i\}$ *mod* p^b *of size* r_b *with* $(i,p) = 1$, *there corresponds a cyclotomic coset* $C_i = \{i, qi, ..., q^{r_{b+1} - 1}i\}$ *mod* p^{b+1} *of size* r_{b+1}, *for* $b \geq 1$;

(v) *to each cyclotomic coset* $C_i = \{i, qi, ..., q^{r_c - 1}i\}$ *mod* p^b *of size* r_c, $1 \leq r_c \leq r_b$, *there corresponds a cyclotomic coset* $C_{pi} = \{pi, pqi, ..., pq^{r_c - 1}i\}$ *mod* p^{b+1}, *also of size* r_c, *for* $b \geq 1$.

Proof

Relations (i) and (ii) follow immediately from Lemma 41, (iii) is a consequence of the relations $\kappa_b = \varphi(p^b)/r_b$ and $\varphi(p^b) = p^{b-1}(p-1)$, (iv) follows from $r_{b+1} = r_b$ for $1 \leq b < d$, and from $r_{b+1} = pr_b$ for $b \geq d$ in (i), while relation (v) is obvious. □

Similar as eq. (52), the cyclotomic polynomial $\Phi_{p^b}(x)$ is the product of κ_b irreducible polynomials in $GF(q)[x]$, for $b \geq 1$, which are all of degree r_b, where the integers κ_b and r_b are as described in Lemma 57. For $b \geq d$, the irreducible polynomials $P_{i_j^b}(x)$ can be expressed in terms of the polynomials $P_{i_j^d}(x)$, according to

$$P_{i_j^b}(x) = P_{i_j^d}(x^{p^{b-d}}),$$

(63)

as a consequence of Lemma 57 (v). (Compare the remarks right after (57) about the polynomials $P_i(x^{p^{b-1}})$, $i \in S^{(1)} \setminus \{0\}$, where $d = 1$.) If $n = p^\lambda$, the columns of the matrix M, which correspond to these irreducible polynomials, can be labeled in general by

$$0, i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa_\lambda}^{\lambda}, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_{\kappa_{\lambda-1}}^{\lambda-1}, ..., i_1^1, i_2^1, ...i_{\kappa_1}^1 ,$$

(64)

with $i_1^{\lambda} = 1$. We remark that labeling (64) is the same as labeling (57) in case that condition (*) holds. In that case we have in Lemma 57 that $d = 1$ and hence $\kappa_1 = \kappa_2 = ... = \kappa_\lambda (=: \kappa)$. In the general case, the columns of M with labels $i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa_\lambda}^{\lambda}$ determine the idempotent generators of the κ_λ *GR*-codes $C^i_{p^\lambda, q, t}$, with $t = \kappa_\lambda$ and $i \in \{i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa_\lambda}^{\lambda}\}$.

In the case that $n = 2p^{\lambda}$, $\lambda \geq 1$, we have that $\Phi_{2p^b}(x) = \Phi_{p^b}(-x)$, $1 \leq b \leq \lambda$, is also the product of κ_b irreducible polynomials in $GF(q)[x]$, all of degree r_b, which can be obtained from those in $\Phi_{p^b}(x)$ by replacing x by $-x$. In this case the labeling of the matrix M can be accomplished by

$$0, i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa_\lambda}^{\lambda}, i_1^{\lambda-1}, i_2^{\lambda-1}, ..., i_{\kappa_{\lambda-1}}^{\lambda-1}, ..., i_1^1, i_2^1, ..., i_{\kappa_1}^1,$$
$$i_{\kappa_\lambda+1}^{\lambda}, i_{\kappa_\lambda+2}^{\lambda}, ..., i_{2\kappa_\lambda}^{\lambda}, i_{\kappa_{\lambda-1}+1}^{\lambda-1}, i_{\kappa_{\lambda-1}+2}^{\lambda-1}, ..., i_{2\kappa_{\lambda-1}}^{\lambda-1}, ..., i_{\kappa_1+1}^1, i_{\kappa_1+2}^1, ..., i_{2\kappa_1}^1, p^{\lambda} .$$

(65)

We choose the indices in the second row of (65) such that $P_{i_j^b}(x) = (-1)^{r_b} P_{\kappa_b + i_j^b}(-x)$, for $1 \leq b \leq \lambda$, (cf. also the remarks about the irreducible polynomials $P_i(x)$ on p. 46). Again the labels i_1^{λ}, i_2^{λ}, …., $i_{\kappa_1}^{\lambda}$ refer to generalized residue codes, i.e. the codes $C^i_{2p^\lambda, q, t}$, with $t = \kappa_\lambda$ and $i \in \{i_1^{\lambda}, i_2^{\lambda}, ..., i_{\kappa_1}^{\lambda}\}$.

For the special case that $t = \kappa_\lambda = 2$, we state and prove the following property.

Lemma 58

If $\kappa_\lambda = 2$*, then one has for the integer d in Lemma 57* :

(i) $d = 1$ *for odd p and* $\lambda \geq 1$;

(ii) $d = 2$ *and* $\lambda \geq 2$ *for* $p = 2$ *and* $q = 1 + 4l$*, l odd*;
$d = 2$ *and* $\lambda = 2$ *for* $q = 1 + 4l$*, l even*;

(iii) $d = 3$ *and* $\lambda \geq 3$ *for* $p = 2$ *and* $q = -1 + 4l$*, l odd*;
$d = 3$ *and* $\lambda = 3$ *for* $p = 2$ *and* $q = -1 + 4l$*, l even.*

Proof

(i) We shall show that for odd *p* and $\kappa_\lambda = 2$ we always have

$$\kappa_1 = \kappa_2 = ... = \kappa_\lambda = 2 .$$

Assume that this is not true. From Lemma 57 (i) it then follows that

$$1 = \kappa_1 < .... < \kappa_d = \kappa_{d+1} = ... = \kappa_\lambda = 2 .$$

Hence, $d = 2$ and $\kappa_2 = 2$. As a consequence we have $r_1 = \varphi(p)/1 = p-1$ and $r_2 = \varphi(p^2)/2 = p(p-1)/2$. From the first equality it follows that $q^{p-1} = 1 + kp$ and so since $p > 2$, $q^{p-1/2} = -1 + lp$, for certain integers *k* and *l*. But then we would have

$$q^{p(p-1)/2} = (-1+lp)^p = -\sum_{i=0}^{p} \binom{p}{i} (-lp)^i = -1 \mod p^2 .$$

This contradicts the relation $r_2 = p(p-1)/2$.

(ii) For $p = 2$ and $q = 1 + 4l$, *l* odd, one can easily show, by calculating the values of r_i, $i \geq 1$, and applying $r_i \kappa_i = 2^{i-1}$, that

$$1 = r_1 = r_2 < 2 = r_3 < r_4 < .... \text{ and } 1 = \kappa_1 < 2 = \kappa_2 = \kappa_3 = \kappa_4 = ...$$

If $q = 1 + 4l$, *l* even, one obtains similarly

$$1 = r_1 = r_2 = r_3 \leq r_4 \leq .... \text{ and } 1 = \kappa_1 < 2 = \kappa_2 < 4 = \kappa_3 \leq \kappa_4 \leq ....$$

The relations for *d* and λ now follow immediately.

(iii) In a similar way one obtains for $p = 2$ and $q = -1 + 4l$, *l* odd, that

$$1 = r_1 < 2 = r_2 = r_3 < 4 = r_4 < .... \text{ and } 1 = \kappa_1 = \kappa_2 < 2 = \kappa_3 = \kappa_4 = ... ,$$

While for $p = 2$ and $q = -1 + 4l$, *l* even, one finds

$$1 = r_1 < 2 = r_2 = r_3 = r_4 \leq r_5 \leq .... \text{ and } 1 = \kappa_1 = \kappa_2 < 2 = \kappa_3 < \kappa_4 \leq \kappa_5 \leq ....$$

Again, the relations for *d* and λ follow immediately. □

Example 59

We take $p = 2$ and $\lambda = 2$, so $n = 2^2$, and $q = 3$. So, we are in the first case of Lemma 58 (iii). The nonzero cyclotomic cosets mod 2^2 are $C_1 = \{1,3\}$, $C_2 = \{2\}$. Their sizes correspond to the orders $r_2 = \text{ord}_{2^2}(3) = 2$ and $r_1 = \text{ord}_{2^1}(3) = 1$, respectively.

Furthermore, we have $\kappa_1 = \varphi(2)/1 = 1$ and $\kappa_2 = \varphi(2^2)/2 = 1$.

So, in $GF(3)[x]$, $\Phi_2(x)$ factorizes into $\kappa_1 = 1$ irreducible polynomial of degree $r_1 = 1$ and $\Phi_4(x)$ into $\kappa_2 = 1$ irreducible polynomial of degree $r_2 = 2$. Indeed, we can write $x^{2^2} - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x-1)(x+1)(x^2+1)$. The labeling (64) becomes in this case $0, i_1^2, i_1^1 = 0,1,2$, and the corresponding polynomials are $P_1(x) = x^2 + 1$ and $P_2(x) = x + 1$.

Next, we take $\lambda = 3$. The nonzero cyclotomic cosets mod 2^3 are $C_1 = \{1,3\}$, $C_5 = \{5,7\}$, $C_2 = \{2,6\}$ and $C_4 = \{4\}$. The sizes correspond to the orders $r_3 = \text{ord}_{2^3}(3) = 2$, $r_2 = \text{ord}_{2^2}(3) = 2$ and $r_1 = \text{ord}_{2^1}(3) = 1$. We can write $x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$ $= (x-1)(x+1)(x^2+1)(x^4+1) = (x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$. For the labeling (64) we now have $0, i_1^3, i_2^3, i_1^2, i_1^1 = 0,1,5,2,4$ with corresponding irreducible polynomials $P_1(x) = x^2 + x - 1$, $P_5(x) = x^2 - x - 1$, $P_2(x) = x^2 + 1$, $P_4(x) = x + 1$.

The next case is $\lambda = 4$. The nonzero cyclotomic cosets mod 2^4 are $C_1 = \{1,3,9,11\}$, $C_5 = \{5,15,13,7\}$, $C_2 = \{2,6\}$, $C_4 = \{4,12\}$, $C_8 = \{8\}$, $C_{10} = \{10,12\}$. The size of C_1 and C_5 is equal to $r_4 = \text{ord}_{2^4}(3) = 4$. Furthermore, $\Phi_{16}(x) = x^8 - 1 = (x^4 + x^2 - 1)(x^4 - x^2 - 1)$, where the two polynomials in the rhs are irreducible. Hence, $0, i_1^4, i_2^4, i_1^3, i_2^3, i_1^2, i_1^1 =$ 0,1,5,2,10,4,8 and the irreducible polynomials are $P_1(x) = x^4 + x^2 - 1$, $P_5(x) = x^4 - x^2 - 1$, $P_2(x) = x^2 + x - 1$, $P_{10}(x) = x^2 - x - 1$, $P_4(x) = x^2 + 1$ and $P_8(x) = x + 1$.
Notice that $P_1(x) = P_{i_1^4}(x) = P_{i_1^3}(x^{2^{4-3}}) = P_2(x^2)$ and similarly $P_5(x) = P_{10}(x^2)$, according to eq. (63) with $d = 3$ (cf. Lemma 58 (iii)). □

Example 60
Take $p = 2$, $\lambda = 4$ and $q = 5$. So, we are now in the second case of Lemma 58 (iii). We find $r_1 = 1$, $r_2 = 1$, $r_3 = 2$, $r_4 = 4$, and hence $\kappa_1 = 1$, $\kappa_2 = 2$, $\kappa_3 = 2$, $\kappa_4 = 2$, which shows that indeed $d = 2$. The cyclotomic cosets mod 2^4 are $C_1 = \{1,5,9,13\}$, $C_3 = \{3,15,11,7\}$, $C_2 = \{2,10\}$, $C_4 = \{4\}$, $C_6 = \{6,14\}$, $C_8 = \{8\}$, $C_{12} = \{12\}$. In $GF(5)[x]$ we have the following factorization into irreducible polynomials

$$\begin{aligned} x^{16} - 1 &= \Phi_1(x)\ \Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x) \\ &= (x-1)(x+1)(x+2)(x+3)(x^2+2)(x^2+3)(x^4+2)(x^4+3). \end{aligned}$$

The labeling (64) becomes $0, i_1^4, i_2^4, i_1^3, i_2^3, i_1^2, i_2^2, i_1^1 = 0,1,3,2,6,4,12,8$. The corresponding polynomials are $P_0(x) = x - 1$, $P_1(x) = x^4 + 2$, $P_3(x) = x^4 + 3$, $P_2(x) = x^2 + 2$, $P_6(x) = x^2 + 3$, $P_4(x) = x + 2$, $P_{12}(x) = x + 3$ and $P_8(x) = x + 1$. As one can see immediately, we have the following relations $P_1(x) = P_{i_1^4}(x) = P_{i_1^2}(x^{2^{4-2}}) = P_4(x^4)$, $P_3(x) = P_{i_2^4}(x) = P_{i_2^2}(x^{2^2}) = P_{12}(x^4)$, and similarly $P_2(x) = P_4(x^2)$, $P_6(x) = P_{12}(x^2)$.
These relations illustrate eq. (63), since $q = 1 + 4.1$ and $d = 2$ (cf. Lemma 58).

Next, we take $p = 2$, $\lambda = 5$, $q = 7$. For the r_i and κ_i, $1 \le i \le \lambda$, we find $r_1 = 1$, $r_2 = 2$, $r_3 = 2$, $r_4 = 2$, $r_5 = 4$ and $\kappa_1 = 1$, $\kappa_2 = 1$, $\kappa_3 = 2$, $\kappa_4 = 4$, $\kappa_5 = 4$. According to Lemma 57 (ii) we now have $d = 4$.
The nonzero cyclotomic cosets mod 2^5 are $C_1 = \{1,7,17,23\}$, $C_2 = \{2,14\}$, $C_3 = \{3,21,19,5\}$, $C_4 = \{4,28\}$, $C_6 = \{6,10\}$, $C_8 = \{8,24\}$, $C_9 = \{9,31,25,15\}$, $C_{11} = \{11,13,27,29\}$, $C_{12} = \{12,20\}$, $C_{16} = \{16\}$, $C_{18} = \{18,30\}$, $C_{22} = \{22,26\}$.
In $GF(7)[x]$ the factorization of $x^{32} - 1$ into irreducible polynomials is as follows

$$x^{32}-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x)\Phi_{32}(x)$$
$$=(x-1)(x+1)(x^2+1)(x^2-4x+1)(x^2+4x+1)\ (x^2+4x-1)(x^2-x-1)$$
$$=(x^2-4x-1)(x^2+x-1)\ (x^4+4x^2-1)\ (x^4-x^2-1)\ (x^4-4x^2-1)\ (x^4+x^2-1).$$

The correspondence between cyclotomic cosets and irreducible polynomials is as follows. If we choose as primitive 32^{th} root of unity a zero of $P_1(x) := x^4-x^2-1$, then
$P_9(x)=x^4+x^2-1,\ P_3(x)=x^4-4x^2-1,\ P_{11}(x)=x^4+4x^2-1,\ P_2(x)=x^2-x-1,$
$P_{18}(x)=x^2+x-1,\ P_6(x)=x^2-4x-1,\ P_{22}(x)=x^2+4x-1,\ P_4(x)=x^2+4x+1,$
$P_{12}(x)=x^2-4x+1, P_8(x)=x^2+1,\ P_{16}(x)=x+1.$
So, we have the following factorizations: $\Phi_{32}(x)=x^{16}+1=P_1(x)P_9(x)P_3(x)P_{11}(x)$,
$\Phi_{16}(x)=x^8+1=P_2(x)P_{18}(x)P_6(x)P_{22}(x)$, $\Phi_8(x)=x^4+1=P_4(x)P_{12}(x)$,
$\Phi_4(x)=x^2+1=P_8(x),\ \Phi_2(x)=x+1=P_{16}(x).$

The labeling (64) becomes

$$0,i_1^5,i_2^5,i_3^5,i_4^5,i_1^4,i_2^4,i_3^4,i_4^4,i_1^3,i_2^3,i_1^2,i_1^1=0,1,9,3,11,2,18,6,22,4,12,8,16\ .\qquad\square$$

Remark 61
The last case in Example 60 demonstrates that for $\lambda=5$ the value of κ_λ is not equal to 2. In case we had defined $\lambda=3$ (and $q=7$) in the previous example, we would have $\kappa_\lambda=\kappa_3=2$, and so we could apply the first part of Lemma 58 (ii), since $q=1+2.3$.

10. The *GR*-codes of length 21 over *GF*(4)

In this section we shall consider an example where the code length is not of type p^λ or $2p^\lambda$. In [1,Section 8] we derived the idempotent generators of the two *GR*-codes $C^i_{21,4,2}$, by a method related to the ones mentioned in Section 2. We now shall compute the same generators by means of the matrix *M*. Remember that the codes $C^i_{21,4,2}$ are not 2-residue codes, though *t* equals 2.

Example 62
We consider the case $n=21,\ q=4$ (cf. [1, Section 8]).
The cyclotomic cosets are

$C_0=\{0\},\ C_1=\{1,4,16\},\ C_2=\{2,8,11\},\ C_3=\{3,6,12\},\ C_5=\{5,17,20\},\ C_7=\{7\},$
$C_9=\{9,15,18\},\ C_{10}=\{10,13,19\},\ C_{14}=\{14\}.$

The irreducible polynomials corresponding to these cosets are respectively

$$P_0(x)=x+1,\ P_1(x)=x^3+\alpha x+1,\ P_2(x)=x^3+\alpha^2 x+1,\ P_3(x)=x^3+x^2+1,$$
$$P_5(x)=x^3+\alpha x^2+1,\ P_7=x+\alpha,\ P_9(x)=x^3+x+1,\ P_{10}(x)=x^3+\alpha^2 x^2+1,$$
$$P_{14}(x)=x+\alpha^2.$$

Since the sizes of all cyclotomic cosets are odd, the integers n_s^i are all equal to 1 in $GF(4)$, and so the matrix element $M_{i,s}$ is equal to $p_{is,1}$ for all $i,s\in S$. We find the following matrix.

$$M=\begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 5 & 7 & 9 & 10 & 14 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & \alpha & \alpha & 0 & \alpha^2 & \alpha^2 \\ 1 & 0 & 0 & 1 & \alpha^2 & \alpha^2 & 0 & \alpha & \alpha \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & \alpha & \alpha^2 & 0 & 0 & \alpha^2 & 1 & 0 & \alpha \\ 1 & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha & 1 & \alpha & \alpha^2 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & \alpha^2 & \alpha & 0 & 0 & \alpha & 1 & 0 & \alpha^2 \\ 1 & \alpha^2 & \alpha & 1 & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha \end{pmatrix} \end{array} \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 5 \\ 7 \\ 9 \\ 10 \\ 14 \end{matrix}.$$

For the code with minimal generator $g_1^{(1)}(x)=P_1(x)P_2(x)$, we obtain the idempotent generator $e_1^{(1)}(x)=\sum_{s\in S}\xi_s c_s(x)$, where the vector ξ is determined by

$$\xi=\varepsilon_0+M\varepsilon_5+M\varepsilon_{10}=\varepsilon_0+\mu_5+\mu_{10}=(1,1,1,0,0,1,0,0,1)^T.$$

The code generated by $g_1^{(2)}(x)=P_5(x)P_{10}(x)$ has the idempotent generator $e_1^{(2)}(x)$ with coefficient vector

$$\xi=\varepsilon_0+M\varepsilon_1+M\varepsilon_2=\varepsilon_0+\mu_1+\mu_2=(1,0,0,0,1,1,0,1,1)^T.$$

Similarly, we find for the coefficient vectors of the idempotent generators $e_2^{(1)}(x)$, $e_2^{(2)}(x)$, $e_3^{(1)}(x)$ and $e_3^{(2)}(x)$, respectively

$$\xi=\varepsilon_0+M\varepsilon_5+M\varepsilon_1=(1,\alpha,\alpha^2,1,\alpha,1,1,\alpha^2,1)^T,$$

$$\xi=\varepsilon_0+M\varepsilon_{10}+M\varepsilon_2=(1,\alpha^2,\alpha,1,\alpha^2,1,1,\alpha,1)^T,$$

$$\xi = \varepsilon_0 + M\varepsilon_5 + M\varepsilon_2 = (1, \alpha, \alpha^2, 1, \alpha^2, 0, 1, \alpha, 0)^T,$$

$$\xi = \varepsilon_0 + M\varepsilon_{10} + M\varepsilon_1 = (1, \alpha^2, \alpha, 1, \alpha, 0, 1, \alpha^2, 0)^T.$$

These six coefficient vectors yield the same idempotents as derived by a different method used in [1, Section 8]. □

Remark 63
We still investigate the question in which way the matrix M, as introduced in Section 3, is related to the character table of a finite abelian or nonabelian group.

References

1. S.M. Dodunekov, A. Bojilov and A.J. van Zanten, *Generalized Residue Codes*, TR 2010-001, TiCC, Tilburg University, www.uvt.nl/ticc

2. R.L. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications* (rev. ed.), Cambridge University Press, Cambridge 1997.

3. J.H. van Lint, *Coding Theory*, Springer-Verlag, New York, 1971.

4. J.H. van Lint and F.J. MacWilliams, *Generalized Quadratic Residue Codes*, IEEE Trans. Inf. Theory **24** (1978), 730 – 737.

5. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publ. Company, Amsterdam, 1977.