Idempotent Generators of Generalized Residue Codes

A.J. van Zanten A.J.vanZanten@uvt.nl
Department of Communication and Informatics, University of Tilburg, The Netherlands
A. Bojilov a.t.bozhilov@uvt.nl,bojilov@fmi.uni-sofia.bg
Department of Communication and Informatics, University of Tilburg, The Netherlands (sabbatical from Faculty of Mathematics and Informatics, University of Sofia, Bulgaria)
S.M. Dodunekov stedo@math.bas.bg
Institute Of Mathematics And Informatics, Bulgarian Academy of Sciences, Bulgaria.

Abstract. A general method is developed for the construction of idempotent generators of GR-codes over GF(q) of length n. For $n \in \{p, 2p, p^k, 2p^k\}$, explicit expressions for these generators can be derived.

1 Introduction

For the conventions, preliminaries, definition and general setting of the family of generalized residue codes, we refer to Sections 1–3 of ref. [1]. We only repeat the main aspects of their definition. The factorization of $x^n - 1$ and of the n^{th} cyclotomic polynomial in GF(q) can be written as

$$x^n - 1 = (x-1)P(x)\Phi_n(x) = (x-1)P(x)P_1(x)P_2(x)\dots P_k(x), \qquad (1)$$

where the $P_i(x)$, $1 \le i \le k$, are irreducible polynomials over GF(q), with $kr = \varphi(n)$, $r = \mathrm{ord}_n(q)$. Let $H \subseteq \mathbb{U}_n$ be the subgroup $H = \langle q \rangle = \{1, q, q^2, \dots, q^{r-1}\}$ with cosets H_1 (= H), H_2,..., H_k, and let K be another subgroup of $\mathbb{U}_n$ of index t and containing H. The cosets of K in $\mathbb{U}_n$ are K_1 (= K), K_2,..., K_t, $k = st$. Let furthermore, ζ be a primitive n^{th} root of unity in some extension field of GF(q). Then we can write

$$P_i(x) = \prod_{l \in H_i} (x - \zeta^l), \qquad 1 \le i \le k. \qquad (2)$$

Finally, the t equivalent GR-codes $C^i_{n,q,t}$, $1 \le i \le t$, are defined as the cyclic codes generated by the polynomials

$$g^{(i)}(x) = \prod_{l \in K_i} (x - \zeta^l) = \prod_{k=1}^{s} P_{j_k}(x), \qquad 1 \le i \le t. \qquad (3)$$

2 Idempotent generators of cyclic codes

Let $g(x)$ be the minimal polynomial of a cyclic code C of length n over GF(q), and let $h(x)$ be its check polynomial. Then we have in the ring R_n^q that

$$g(x)h(x) = x^n - 1 = 0. \tag{4}$$

Definition 1. *Let C be a cyclic code. A polynomial $e(x) \in C$, of degree less than n, which is an identity of C is called the idempotent generator of C.*

This idempotent generator is unique and has the idempotency property

$$e^2(x) = e(x). \tag{5}$$

It is also well-known, that $e(x)$ can be obtained from the relation

$$a(x)g(x) + b(x)h(x) = 1, \tag{6}$$

which holds for certain polynomials $a(x)$ and $b(x)$ in R_n^q, since $\big(g(x), h(x)\big) = 1$. It follows immediately that

$$e(x) = a(x)g(x). \tag{7}$$

The polynomial $a(x)$ can of course be obtained by Euclid's algorithm. An alternative method for determining $e(x)$ is given by the rule

$$e(x) = n^{-1}xh'(x)g(x), \tag{8}$$

where $h'(x)$ stands for the formal derivative of the polynomial $h(x)$, and where n^{-1} is to be taken in GF(q). This expression can easily be proved by taking the formal derivative of (6). Its binary version can be found in [3, Ch. 8, Problem 17].

A third general approach for the computation of idempotent generators is provided by the following theorem, which is based on the inversion formula used in Lemma 7 of [3, Ch. 7].

Theorem 1. *Let $e(x) = e_{n-1}(x)x^{n-1} + e_{n-2}x^{n-2} + \cdots + e_0$ be the idempotent generator of a cyclic code C generated by its 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 $g(x)$.*

In the next section we shall present a method which provides us straightforwardly with an expression for idempotent generators in terms of the coefficients of the irreducible polynomials in (1). To this end, we also factorize the other cyclotomic polynomials in (1)

$$x^n - 1 = \prod_{i=1}^{l} P_i(x), \qquad P_0(x) = 1, \quad l \ge k. \tag{9}$$

We assume that the n^{th} primitive root ζ, together with ζ^q,...,$\zeta^{q^{m_1-1}}$ is a zero of $P_1(x)$. In general, the irreducible polynomial $P_s(x)$ has zeros ζ^s, ζ^{sq},...,$\zeta^{sq^{m_s-1}}$, where m_s is the size of the cyclotomic coset $C_s = \{s, sq, \ldots, sq^{m_s-1}\}$, $s \in S$, where S is the set of all indexes which indicate the cyclotomic cosets. So, there is a one-to-one correspondence between the cyclotomic cosets C_s and the irreducible polynomials

$$P_s(x) = x^{m_s} + p_{s,1}x^{m_s-1} + \cdots + p_{s,m_s}. \tag{10}$$

We adopt the convention that the index s of C_s denotes the least integer of the coset. On the other hand, there is also a one-to-one correspondence between the cosets C_s and the polynomials $c_s(x) \in R_n^q$, $s \in S$, defined by

$$c_s(x) = x^s + x^{sq} + \cdots + x^{sq^{m_s-1}}. \tag{11}$$

Furthermore, we shall make use of the multiset $C_s^{(i)} = \{is, isq, \ldots, isq^{m_s-1}\}$. One can easily prove that $C_s^{(i)} = n_s^i C_{is}$ for some positive integer $n_s^i = \dfrac{m_s}{m_i}$, and that

$$c_s(\zeta^i) = -n_s^i p_{is,1}. \tag{12}$$

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

$$\mu_{i,s} = c_s(\zeta^i) = -n_s^i p_{is,1}, \qquad i, s \in S. \tag{13}$$

In particular, we have $\mu_{0,s} = m_s$ and $\mu_{i,0} = 1$. It is well known and it can easily be shown that every idempotent generator $e(x)$ is a linear combination over GF(q) of the polynomials $c_s(x)$. We write for the idempotent generator of the code $\big(P_u(x)\big)$, $u \in S$

$$e_u(x) = \sum_{s \in S} \boldsymbol{\xi}_{u,s} c_s(x). \tag{14}$$

It is also well known that the idempotency property implies that $e(x)$ is the idempotent generator of a code C, if and only if $e(x)$ is equal to 0 for the zeros of the code and equal to 1 for the nonzeros. Therefore, the coefficients $\boldsymbol{\xi}_{u,s}$ in (14) are uniquely determined by the set of linear equations $\sum_{s \in S} \mu_{i,s}\boldsymbol{\xi}_{u,s} = e_u(\zeta^i)$, with $e_u(\zeta^i) = 0$ for $i = u$ and $e_u(\zeta^i) = 1$ for $i \neq u$. We now can write this set of equations, applying the equality (14), in matrix form as $M\boldsymbol{\xi}_u = \boldsymbol{\delta}_u$ with column vectors $\boldsymbol{\xi}_u$ and $\boldsymbol{\delta}_u$ of length $|S|$ and $\boldsymbol{\delta}_u$ having a zero on position u and ones everywhere else. Generalizing this approach yields the following theorem.

Theorem 2. *Let P_{i_1}, P_{i_2},...,P_{i_l} with $i_1, i_2, \ldots, i_l \in S$, be irreducible polynomials defined by* (10)*, and let C be the cyclic code generated by the product of these*

polynomials. Then the idempotent generator $e(x) = \sum_{s\in S} \boldsymbol{\xi}_s c_s(x)$ *is determined by the set of linear equations* $M\boldsymbol{\xi} = \boldsymbol{\delta}$*, where* $\boldsymbol{\delta}$ *is the column vector of length* $|S|$ *with zeros on the positions* $i_1, i_2, \ldots, i_l$*, and ones elsewhere.*

Theorem 3. *If* M^P *is the matrix obtained from* M *by interchanging the columns indexed by* s *and* $-s$*, for all* s*, then* $M^{-1} = n^{-1}M^P$*.*

Corollary 1. *The primitive idempotent generator corresponding to the cyclotomic coset* C_u*,* $u \in S$ *is given by* $\theta_u(x) = \frac{1}{n}\sum_{s\in S} \boldsymbol{\xi}_{u,s} c_s(x)$ *where* $\boldsymbol{\xi}_u$ *is equal to* $\boldsymbol{\mu}_{-u}$*, the column vector of* M *with index* $-u$*.*

For the proofs, we refer to [2]. The matrix M possesses a number of symmetry and orthogonality properties, the proofs of which can also be found in [2].

Theorem 4. *For all* $i, j \in S$*, the matrix elements* $\mu_{i,j}$ *satisfy the following relations 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) $\sum_k m_k\mu_{k,i}\mu_{k,j} = nm_i\delta_{i,-j}$*;* *(iv)* $\sum_k m_k^{-1}\mu_{i,k}\mu_{j,k} = nm_i^{-1}\delta_{i,-j}$*.*

3 Idempotent generators of GR-codes

It will be clear that in case of GR-codes, the cyclotomic coset C_1 is equal to $H = \langle q\rangle$, while the cosets H_i of H are equal to those cyclotomic cosets C_i with $i \in S \cap \mathbb{U}_n$. So, for these i-values, we have $m_i = r$ $(= \mathrm{ord}_q(n))$. For the time being, we take $K = H$ for the construction of $t = \dfrac{\varphi(n)}{r}$ equivalent codes $C^i_{n,q,t} = \big(P_i(x)\big)$. In Section 1 the upper index i runs from 1 until t. Because of our relabeling in Section 2, we now assume that i runs through the set of the t different elements of $S \cap \mathbb{U}_n$. For the matrix elements of the i^{th} column of M we now have

$$\mu_{j,i} = -r\frac{p_{ij,1}}{m_{ij}}, \qquad i \in S \cap \mathbb{U}_n. \tag{15}$$

In the special case that also $j \in S \cap \mathbb{U}_n$, we may replace m_{ij} by $m_i = r$ in the rhs.

Theorem 5. *The idempotent generator of the GR-code* $C^i_{n,q,t}$*,* $i \in S \cap \mathbb{U}_n$*, is given by* $\vartheta_i(x) = 1 - \theta_i(x)$*, with* $\theta_i(x) = -n^{-1}\sum_{j\in S} rp_{ij,1}m_{ij}^{-1}c_j(x)$*.*

In order to determine all idempotent generators of the t equivalent codes $C^i_{n,q,t}$, it is sufficient to compute $\vartheta_1(x) = 1 - \theta_1(x)$, which corresponds to the column vector $\boldsymbol{\mu}_{-1}$ with components $\mu_{j,-1} = -rm_j^{-1}p_{-j,1}$. Due to the group

property of $\mathbb{U}_n$, one can easily verify that the components of any column vector $\boldsymbol{\mu}_i$, with $i \in S \cap \mathbb{U}_n$, form a permutation of those of $\boldsymbol{\mu}_{-1}$. We omit the details. We discuss briefly a few special subfamilies.

(i) In the special case $n = p$, p odd, one has that $\deg \Phi_p(x) = p - 1$. So, all cyclotomic cosets $\neq C_0$ have the same size $r = \mathrm{ord}_p(q)$ and all $k = \dfrac{p-1}{r}$ irreducible polynomials $P_i(x)$, $i \neq 0$, have degree r. It follows that $\mu_{i,j} = -m_j m_{ij}^{-1} p_{ij,1} = -p_{ij,1}$, for $i, j \in S/\{0\}$.

Example 1. *For $n = 13$ and $q = 3$, we find $r = 3$. The cyclotomic cosets are $C_0 = \{0\}$, $C_1 = \{1, 3, 9\}$, $C_2 = \{2, 5, 6\}$, $C_4 = \{4, 10, 12\}$, $C_7 = \{7, 8, 11\}$ and the corresponding 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.* (13) *we find the following matrix*

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

The primitive idempotent generator which corresponds to C_1 is equal to $\theta_1(x) = \sum_{s \in S} \mu_{s,-1} c_s(x) = \sum_{s \in S} \mu_{s,4} c_s(x) = -c_1(x) + c_2(x) - c_7(x)$. Finally, by applying Corollary 1 and substituting the expressions for $c_s(x)$, we obtain for $C^1_{13,3,4}$ the idempotent generator $\vartheta_1(x) = x^{11} + x^9 + x^8 + x^7 - x^6 - x^5 + x^3 - x^2 + x + 1$.

(ii) For $n = 2p$ and q an odd prime power, we have $\deg \Phi_{2p}(x) = \deg \Phi_p(x) = p - 1$, and the factorization $x^{2p} - 1 = (x-1)\Phi_2(x)\Phi_p(x)\Phi_{2p}(x)$, with $\Phi_2(x) = x + 1$. One can also easily prove that $\mathrm{ord}_{2p}(q) = \mathrm{ord}_p(q) = r$. Therefore, both $\Phi_{2p}(x)$ and $\Phi_p(x)$ are the product of $\dfrac{p-1}{2r}$ polynomials of degree r which are irreducible over $\mathrm{GF}(q)$. Let ζ be a primitive $2p^{\text{th}}$ root of unity in some extension field of $\mathrm{GF}(q)$ defined as a zero of one of the irreducible factors of $\Phi_{2p}(x)$. Then $\zeta^p = -1$ and hence it is the only zero of $\Phi_2(x)$. Furthermore, all other odd powers of ζ are zeros of $\Phi_2 p(x)$, while the positive even powers are zeros of $\Phi_p(x)$ (ζ^2 is primitive p^{th} root). Similarly as in (i), it follows that $\mu_{i,j} = -p_{ij,1}$, $i \notin \{0, p\}$, $\mu_{0,j} = r$, $\mu_{p,j} = -r$ for all $j \in S \cap \mathbb{U}_n$.

Example 2. *Take $n = 10$ and $q = 3$. The cyclotomic cosets are $C_0 = \{0\}$, $C_1 = \{1, 3, 7, 9\}$, $C_2 = \{2, 4, 6, 8\}$, $C_5 = \{5\}$, and the corresponding irreducible polynomials $P_0(x) = x - 1$, $P_1(x) = x^4 - x^3 + x^2 - x + 1$, $P_2(x) = x^4 + x^3 +$*

$x^2 + x + 1$, $P_5(x) = x + 1$. *The matrix* M *equals*

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

Since $C_{-1} = C_1$ *and* $10^{-1} = 1$ *in* GF(3), *the primitive idempotent* $\theta_1(x)$ *is equal to* $c_0(x) + c_1(x) - c_2(x) - c_5(x)$. *So,* $\vartheta_1(x) = 1 - \theta_1(x) = -x^9 + x^8 - x^7 + x^6 + x^5 + x^4 - x^3 + x^2 - x$.

(iii) The cases $n = p^k$ and $n = 2p^k$ can be dealt within in a similar way, since one can determine the integers m_i, $i \in S$, for all odd primes p (cf. [2]). We only give an example in this place.

Example 3. *Take* $n = 9$ *and* $q = 7$. *The cyclotomic classes 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 in* GF(7)$[x]$ *are respectively* $P_0(x) = x - 1$, $P_1(x) = x^3 - 2$, $P_2(x) = x^3 - 4$, $P_3(x) = x - 2$ *and* $P_6(x) = x - 4$. *For the matrix* M *we find*

$$M = \begin{pmatrix} 1 & 3 & 3 & 1 & 1 \\ 1 & 0 & 0 & 2 & 4 \\ 1 & 0 & 0 & 4 & 2 \\ 1 & -1 & -2 & 1 & 1 \\ 1 & -2 & -1 & 1 & 1 \end{pmatrix},$$

where rows and columns are indexed by 0, 1, 2, 3 and 6. The primitive idempotent generator $\theta_1(x)$ *is determined by the column vector* $\boldsymbol{\mu}_{-1} = \boldsymbol{\mu}_2$ *and hence, is equal to*

$$\theta_1(x) = 9^{-1}\big(3c_0(x) - 2c_3(x) - c_6(x)\big) = 3x^6 - x^3 - 2,$$

and the idempotent generator of $C^1_{9,7,2}$ *is*

$$\vartheta_1(x) = 1 - \theta_1(x) = 4x^6 + x^3 + 3.$$

References

[1] A. Bojilov, A.J. van Zanten and S.M. Dodunekov, Minimal distances in generalized residue codes, In *These Proceedings*.

[2] A. Bojilov, A.J. van Zanten and S.M. Dodunekov, Idempotents of cyclic codes, Technical report, TICC, Tilburg University, 2010. To be published.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland Mathematical Library*, North-Holland, 1977.