Minimal Distances in Generalized Residue Codes

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)
A.J. van Zanten A.J.vanZanten@uvt.nl
Department of Communication and Informatics, University of Tilburg, The Netherlands
S.M. Dodunekov stedo@math.bas.bg
Institute Of Mathematics And Informatics, Bulgarian Academy of Sciences, Bulgaria.

Abstract. A general type of linear cyclic codes is introduced as a straightforward generalization of quadratic residue codes, e-residue codes, generalized quadratic residue codes and polyadic codes. A generalized version of the well-known square-root bound for odd-weight words is derived.

1 Introduction

Quadratic residue codes or QR-codes form a special type of linear cyclic codes of prime length p (odd) over a finite field (cf. [7] or other textbooks). Binary QR-codes with $q = 2$ or $q = 2^l$ are the best studied quadratic residue codes by far. Also ternary QR-codes are studied occasionally. These are sometimes called *Pless symmetry codes* (cf. [8]). For $q > 3$ quadratic residue codes are not studied very closely. Pless in [9] introduced so-called Q-codes which contain as a subclass quadratic residue codes over GF(4). Van Lint and MacWilliams in [13] generalize the concept of quadratic residue codes to codes with prime power length $n = p^m$ over arbitrary fields GF(q), $(p, q) = 1$. These codes are called *generalized quadratic residue codes* or GQR-codes. Berlekamp in [1, Section 15.2] defines *e-residue codes*, which for $e = 2$ are identical to quadratic residue codes. In an e-residue code, the role played by the quadratics in GF(q) is now adopted by the e-powers in this field. Like in the case of QR-codes, the code length of e-codes is always an odd prime.

A different kind of generalization of QR-codes form the *duadic codes* which are introduced by Leon, Masley and Pless in [5]. Instead of quadratics and nonquadratics, one considers two arbitrary disjunct subfamilies S_1 and S_2 of the family S of cyclotomic cosets mod n, such that $S_1 \cup S_2 = S$. The length of the codes in [5] is equal to $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$, where each p_i is prime and congruent to $\pm 1 \mod 8$. The codes in [5] are further generalized for other splittings of S, giving rise to *triadic codes* in [11] and to *m-adic* or *polyadic codes* in [2] and [12]. The codes in [2] are of prime length and those in [11] and in [12] of prime power length. In Sections 2 and 3 we shall introduce a new family of linear cyclic codes $C^i_{n,q,t}$, which we call *generalized residue codes* (*GR-codes*). These are codes over an arbitrary field $\mathrm{GF}(q)$ having an arbitrary length n, $(n,q)=1$. A third parameter t is a divisor of $\varphi(n)$ and is related to the number of subfamilies into which S is split. In this sense the codes $C^i_{n,q,t}$ generalize all codes mentioned earlier in this text. The index i runs from 1 until t, and labels t equivalent versions of a GR-code with fixed values of the parameters n, q and t. In Section 4, we derive a generalization of a well-known theorem on minimal distances in quadratic and in generalized quadratic codes.

The contents of this contribution is based on a paper of the third author in [3]. For more properties and examples of GR-codes,we refer to [4].

2 Preliminaries

Let $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$ and let q be a prime power such that $(n,q)=1$. Let furthermore $r = \mathrm{ord}_n(q)$ be the multiplicative order of $q \mod n$, i.e. r is the least integer satisfying $q^r \equiv 1 \pmod n$. Let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial over the field of rationals $\mathbb{Q}$. Then $\Phi_n(x)$ divides $x^n - 1$ and we can write

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

Since this equality holds in $\mathbb{Z}[x]$, it also holds in $\mathbb{Z}_p[x]$, and hence we may consider $\Phi_n(x)$ as a polynomial over $\mathrm{GF}(q)$. More in particular, we shall consider polynomials over $\mathrm{GF}(q)$ as elements of the polynomial ring $R_n = \mathrm{GF}(q)[x]/(x^n-1)$ For the degree of $\Phi_n(x)$ we can write (cf. [6, Theorem 2.47])

$$\deg \Phi_n(x) = \varphi(n) = rk \tag{2}$$

for some integer k, and we have the following factorization in $\mathrm{GF}(q)[x]$

$$\Phi(x) = P_1(x)P_2(x)\dots P_k(x), \tag{3}$$

where all polynomials $P_i(x)$ have degree r and are irreducible over $\mathrm{GF}(q)$. We also introduce the multiplicative group of the ring $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, represented by

$$G = \mathbb{U}_n = \{\bar{a} \in \mathbb{Z}_n \mid (a,n) = 1\}. \tag{4}$$

The minimal subgroup $H \le G$ containing q is the cyclic group generated by q, i.e.

$$H = \langle q \rangle = \{1, q, q^2, \dots, q^{r-1}\}. \tag{5}$$

Since the factorgroup G/H has order k, we can write

$$G = H_1 \cup H_2 \cup \dots \cup H_k, \tag{6}$$

where the cosets H_i are non-intersecting cyclotomic classes defined by $H_i = x_i H$, with representative elements $x_1 = 1$, x_2,…,x_k. If ζ is a primitive n^{th} root of unity in some appropriate extension field of GF(q), we may define the irreducible (over GF(q)) polynomials $P_i(x)$, $1 \leq i \leq k$, as

$$P_i(x) = \prod_{l \in H_i} (x - \zeta^l). \tag{7}$$

Finally, we choose a subgroup K of G of index t , such that

$$H \leq K \leq G. \tag{8}$$

It follows that $k = st$ for some integer s, and furthermore that

$$|G| = \varphi(n) = rk = rst, \quad |K| = rs, \quad |H| = r, \tag{9}$$

and by relabeling the H-cosets

$$K = H_1 \cup H_2 \cup \cdots \cup H_s. \tag{10}$$

Here, H_1 is the same coset as H_1 in (6). The cosets of K in G are K_1 ($= K$), K_2,…, K_t.

3 Definition of generalized residue codes

With respect to the chosen subgroup K we now define polynomials

$$g^{(i)}(x) = \prod_{l \in K_i} (x - \zeta^l) = \prod_{k=1}^{s} P_{j_k}(x), \qquad 1 \leq i \leq t, \tag{11}$$

where the indices $j_1, j_2, \ldots j_s$ form a subset of $\{1, 2, \ldots, k\}$. It will be obvious that the polynomials in (11) are of degree rs, that they have their coefficients in GF(q) and that

$$\prod_{i=1}^{t} g^{(i)}(x) = \Phi_n(x). \tag{12}$$

Definition 1. *The generalized residue code $C^i_{n,q,t}$ of length n over* GF(q) *and based on the subgroup K of $\mathbb{U}_n$ of index t, is the cyclic code generated by the polynomial $g^{(i)}(x)$, for any $i \in \{1, 2, \ldots, t\}$. If the group K is identical to a subgroup $\mathbb{U}^m_n \leqq \mathbb{U}_n$, where m is minimal with respect to this property, we shall alternatively speak of an m-residue code.*

The following properties of generalized residue codes can easily be proved.

Theorem 1. *For any set of fixed values for n, q and t, the following relations hold:*

(i) the GR-codes $C^i_{n,q,t}$, $1 \le i \le t$, all have dimension $n - \dfrac{\varphi(n)}{t}$; moreover, they are equivalent, and hence they have the same minimum distance;

(ii) $\bigcap\limits_{i=1}^{t} C^i_{n,q,t} = \big(\Phi_n(x)\big)$;

(iii) if $t \ge 2$, then $\sum\limits_{i=1}^{t} C^i_{n,q,t} = R_n$.

In the theory of the group $\mathbb{U}_n$ it is proved that this group is cyclic if and only if n equals 2, 4, p^k or $2p^k$ for any odd prime p. Based on this property the next theorem can be proved.

Theorem 2. *If n is equal to 2, 4, p^k or $2p^k$, with p an odd prime, the group K of (8) with index t with respect to $\mathbb{U}_n$, is identical to the subgroup $\mathbb{U}_n^t$ consisting of all t-powers in G.*

We conclude that, if we restrict ourselves to n-values > 4, the GR-codes $C^i_{p^k,q,t}$ and $C^i_{2p^k,q,t}$ are t-residue codes for all i, $1 \le i \le t$. However, for other n-values there can also exist m-residue codes for certain values of m.

4 Minimal distances in GR-codes

In this section we consider polynomials $c^{(i)}(x) \in C^i_{n,q,t}$ of weight d (not necessarily the minimum weight of the code), and such that $x-1$ is not a divisor of this polynomial.

The following theorem can be considered as a generalization of a well-known result for QR-codes, GQR-codes and other generalizations of quadratic codes.

Theorem 3. *Let d be the weight of a polynomial $c^{(i)}(x) \in C^i_{n,q,t}$ such that $c^{(i)}(1) \ne 0$. If d_P is the weight of the polynomial $P(x)$ in (1), then $d_P d^t \ge n$.*

Proof. Let $c^{(1)}(x) \in C^1_{n,q,t}$ be a polynomial as described in the theorem. By suitable permutations of its coefficients, one can transform $c^{(1)}(x)$ into polynomials $c^{(2)}(x), \ldots, c^{(t)}(x)$ which also meet that description. As a consequence of Theorem 1, the product $P(x) \prod\limits_{i=1}^{t} c^{(i)}(x)$ is a nonzero multiple of $x^{n-1} + x^{n-2} + \cdots + 1$.

Let $P(1) \prod\limits_{i=1}^{t} c^{(i)}(1) = \alpha$, i.e. $P(x) \prod\limits_{i=1}^{t} c^{(i)}(x) \equiv \alpha \pmod{x-1}$. Using Chinese Reminder Theorem we conclude that

$$P(x)\prod_{i=1}^{t} c^{(i)}(x) \equiv \frac{\alpha}{n}(x^{n-1}+x^{n-2}+\cdots+1) \pmod{x^n-1}.$$

Since $P(x)\prod_{i=1}^{t} c^{(i)}(x)$ is a word with weight n ($\alpha \neq 0$) and since $\prod_{i=1}^{t} c^{(i)}(x)$ has at most d^t nonzero coefficients, the inequality follows immediately. □

We can even derive a stronger result in case that -1 is not an element of K, which can be seen as a generalization of a result of Assmus and Mattson (cf. ref. [10]).

Theorem 4. *Let d be the weight of a polynomial $c^{(i)}(x) \in C^i_{n,q,t}$ with $c^{(i)}(1) \neq 0$. If $-1 \notin K$, then $d_P(d^2-d+1)^{\frac{t}{2}} \geq n$.*

Proof. Since $-1 \notin K$, the integer -1 belongs to a coset different from $K_1 (= K)$. We shall denote this coset by K_{-1}. If $a \in G$ is neither in K_1 nor in K_{-1}, then a defines a coset K_a. Now $-a \notin K_a$, since this would imply $-1 \in K$. So, K_a and $K_{-a} = -aK$ are cosets different from K_1 and K_{-1}. Continuing in this way shows that the group G/K consists of cosets K_i and K_{-i} for $\frac{t}{2}$ different values i. In the context of this proof we label these cosets as K_i, K_{-i} with $i \in \{1, 2, \ldots, \frac{t}{2}\}$. Similarly, the corresponding polynomials (11) are denoted by $g^{(i)}(x)$, $g^{(-i)}(x)$ with again $i \in \{1, 2, \ldots, \frac{t}{2}\}$. For each fixed value i we write

$$\begin{aligned} g^{(i)}(x) &= \prod_{l\in K_i}(x-\zeta^l) = \prod_{m\in K}(x-\zeta^{im}) = x^{rs}\prod_{m\in K}(1-\zeta^{im}x^{-1}) \\ &= x^{rs}(-\zeta)^{i\sum\limits_{m\in K} m}\prod_{m\in K}(x^{-1}-\zeta^{-im}). \end{aligned}$$

According to our notation, the rhs can be written as $bx^{rs}g^{(-i)}(x^{-1})$ where b must be an element of $\mathrm{GF}(q)$, since all coefficients of $g^{(i)}(x)$ and $g^{(-i)}(x)$ are in $\mathrm{GF}(q)$. Comparing the coefficients of x^0 in both polynomials gives $b = g^{(i)}(0)$.

Now, let $c^{(i)}(x) = a_i(x)g^{(i)}(x)$ be a polynomial in $C^i_{n,q,t}$ of weight d and degree e. Then $c^{(-i)}(x) = x^e c^{(i)}(x^{-1}) = a_{-i}(x)g^{(-i)}(x)$ with $a_{-i}(x) = x^e a_i(x)$ is a polynomial in $C^{-i}_{n,q,t}$ which has the same weight d. The polynomial $c^{(i)}(x)c^{(-i)}(x)$ is a polynomial in the intersection code $C^i_{n,q,t} \cap C^{-i}_{n,q,t}$ which cannot be the zero polynomial, since it is not divisible by $x-1$.

So, it has a positive weight which is at most equal to d^2-d+1. We can continue this process, since all codes $C^i_{n,q,t}$, $1 \leq i \leq \frac{t}{2}$, are equivalent and therefore all have a codeword of weight d. So, we end up with a polynomial

$\prod_{i=1}^{\frac{t}{2}} c^{(i)}(x)c^{(-i)}(x)$ which is in the intersection $\bigcap_{i=1}^{\frac{t}{2}} C^{i}_{n,q,t} \cap C^{-i}_{n,q,t}$ and which has a weight at most $(d^2 - d + 1)^{\frac{t}{2}}$. The inequality now follows from Theorem 1. $\square$

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, revised edition 1984, Aegean Park Press, Laguna Hills, Ca., 1984.

[2] Richard A. Brualdi and Vera S. Pless, Polyadic codes, *Discrete Applied Mathematics*, **25** (1-2), 3–17, 1989.

[3] S. M. Dodunekov, Residue codes, *Pliska Studia Matematika*, (**2**), 3–5, 1981.

[4] S.M. Dodunekov, A. Bojilov, and A.J. van Zanten, Generalized residue codes, TR 2010-001, TICC, Tilburg University, March 2010.

[5] Jeffrey S. Leon, John Myron Masley, and Vera Pless, Duadic codes, *IEEE Transactions on Information Theory*, **30** (5), 709–713, 1984.

[6] R. Lidl and H. Niederreiter, *Introduction to Finite Fields*, Cambridge University Press, Cambridge, 1986.

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

[8] Vera Pless, Symmetry codes over GF(3) and new five-designs, *Journal of Combinatorial Theory, Series A*, **12** (1), 119–142, 1972.

[9] Vera Pless, Q-codes, *Journal of Combinatorial Theory, Series A*, **43** (2), 258–276, 1986.

[10] Vera Pless, *Introduction to the Theory of Error-Correcting Codes*, Discrete Mathematics and Optimization. Wiley-Interscience, New York, 3rd edition, July 1998.

[11] Vera Pless and Joseph J. Rushanan, Triadic codes, *Linear Algebra and its Applications*, **98**, 415–433, 1988.

[12] Anuradha Sharma, Gurmeet K. Bakshi, and Madhu Raka, The weight distributions of irreducible cyclic codes of length 2^m, *Finite Fields and Their Applications*, **13** (4), 1086–1095, 2007.

[13] J. van Lint and F. MacWilliams, Generalized quadratic residue codes, *IEEE Transactions on Information Theory*, **24** (6), 730–737, Nov 1978.