

# Some Results on the Weight Distributions of the Binary Double-Circulant Codes Based on Primes

C. Tjhai, M. Tomlinson, R. Horan, M. Ahmed and M. Ambroze

Fixed and Mobile Communications Research,

University of Plymouth, Plymouth PL4 8AA, UK

email:{ctjhai,mtomlinson,rhoran,mahmed,mambroze}@plymouth.ac.uk

*Preprint of the 10<sup>th</sup> IEEE International Conference on Communications Systems, 30 Oct – 1 Nov 2006, Singapore*

## Abstract

This paper presents a more efficient algorithm to count codewords of given weights in self-dual double-circulant and formally self-dual quadratic double-circulant codes over GF(2). A method of deducing the modular congruence of the weight distributions of the binary quadratic double-circulant codes is proposed. This method is based on that proposed by Mykkeltveit, Lam and McEliece, *JPL. Tech. Rep.*, 1972, which was applied to the extended quadratic-residue codes. A useful application of this modular congruence method is to provide independent verification of the weight distributions of the extended quadratic-residue and quadratic double-circulant codes. Using this method in conjunction with the proposed efficient codeword counting algorithm, we are able

- i) to give the previously unpublished weight distributions of the [76, 38, 12] and [124, 62, 20] binary quadratic double-circulant codes;
- ii) to prove that the [168, 84, 24] extended quadratic-residue and quadratic double-circulant codes are inequivalent; and
- iii) to provide corrections to the published results on the weight distributions of the binary extended quadratic-residue code of prime 151, and the number of codewords of weights 30 and 32 of the binary extended quadratic-residue code of prime 137.

## 1 Introduction

Binary self-dual codes form an important class of codes due to their powerful error-correcting capabilities and their rich mathematical structure. As such, this family of codes has been a subject of extensive research for many years. Much of this work is on their classification and the search for the extremal codes [1]. Many binary self-dual codes are codes with the highest

known minimum distance. Recently, van Dijk *et al.* [2], constructed two inequivalent binary self-dual codes of length 160 that have higher minimum distance than the previously known half-rate codes of that length.

Closely related to the self-dual codes are the double-circulant codes. Many good binary self-dual codes can be constructed in double-circulant form. An interesting family of binary, double-circulant codes, which includes self-dual and formally self-dual codes, is the family of codes based on primes. A classic paper for this family was published by Karlin [3] in which double-circulant codes based on primes congruent to  $\pm 1$  and  $\pm 3$  modulo 8 were considered. Moore's PhD work [4] investigated the class which is congruent to 3 modulo 8, and his work was later extended by Gulliver *et al.* [5] to longer codes. An extensive discussion on these two types of circulant is also given by MacWilliams *et al.* [6]. The prime-based double-circulant codes can also be constructed over non binary fields, e.g. see Pless [7] and Beenker [8] for  $\text{GF}(3)$ , and Gaborit [9] for the generalisation to prime fields. The weight distributions of double-circulant codes based on primes congruent  $\pm 1$  modulo 8, of lengths from 74 to 152 (except 138), i.e. binary extended Quadratic Residue (QR) codes, may be found in [10], as well as those based on primes congruent to  $\pm 3$  modulo 8, of lengths 108 and 120.

This paper considers the weight distributions of the binary double-circulant codes based on primes, and it is organised as follows. Section 2 introduces the notation and gives a review of double-circulant codes based on primes congruent to  $\pm 1$  and  $\pm 3$  modulo 8. Section 3 presents an improved algorithm to compute the number of codewords of given weight in certain double-circulant codes. In order to count codewords of given weight, this algorithm requires the enumeration of less codewords than a recently published technique [10, 2]. Based on the fact that the extended QR codes are invariant under the projective special linear group, Mykkeltveit *et al.* [11] developed a technique to deduce the modular congruences of the number of codewords of a given weight in these codes. In Section 4, we describe the automorphism group of the family of double circulant codes with primes congruent to  $\pm 3$  modulo 8 which contains the projective special linear group. Accordingly, we show that, with some modifications, the modular congruence method of Mykkeltveit is also applicable to these double-circulant codes. Using this method in conjunction with that given in Section 3, we compute the weight distributions of the quadratic double-circulant codes of lengths 76 and 124. It has been observed that, for some primes, there exist two double-circulant codes from different constructions which have the same parameters, but it is not known if the two codes are equivalent. Section 6 discusses two such codes of length 168, and using the techniques presented in Section 4, determines that these codes are inequivalent. In Section 5, we prove that some of the results reported by Gaborit *et al.* [10] on the extended QR code of length 138 and 152 are incorrect, and provide corrections to these results. Section 7 concludes the paper.

## 2 Background and Notation

Let  $\mathbb{F}_2^n$  denote the space of vectors of length  $n$  with elements in  $\text{GF}(2)$ . A binary linear code is a  $k$ -dimensional linear subspace of  $\mathbb{F}_2^n$ . We denote  $[n, k, d]$

as a binary linear code of length  $n$ , dimension  $k$  and minimum distance  $d$ . The weight enumerator function of a code is defined as  $A(z) = \sum_{i=0}^n A_i z^i$ , where  $A_i$  denotes the number of codewords of weight  $i$ . If  $\mathcal{C}$  is a binary linear code, its dual code  $\mathcal{C}^\perp$  is defined as  $\mathcal{C}^\perp = \{w \in \mathbb{F}_2^n \mid \sum_{i=0}^{n-1} v_i w_i = 0 \pmod{2}, \text{ for all } v \in \mathcal{C}\}$ .

A code is called self-dual iff  $\mathcal{C} = \mathcal{C}^\perp$ . A self-dual code is called Type II, or *doubly even*, if all codeword weights are divisible by 4; otherwise it is called Type I, or *singly even*. A Type II self-dual code has a length that is divisible by 8. A code is called formally self-dual (fsd) if its weight enumerator is equal to that of its dual. A self-dual, or fsd, code is called *extremal* if its minimum distance is the highest possible for the given parameters.

As a class, double-circulant codes are  $[n, k]$  codes, where  $k = n/2$ , whose generator matrix  $G$  consists of two circulant matrices. A circulant matrix  $R$  is a square  $m \times m$  matrix in which each row (resp. column) is a cyclic shift of the adjacent row (resp. column). Such a matrix  $R$  is completely characterised by a polynomial formed from its first row,  $r(x) = \sum_{i=0}^{m-1} r_i x^i$ , which is called the *defining polynomial*, and the algebra of polynomials modulo  $x^m - 1$  is isomorphic to that of circulants.

Double-circulant codes can be put into two classes, namely *pure*, and *bordered double-circulant*, codes, whose generator matrices  $G_p$  and  $G_b$  are shown in (1) and (2) respectively, where  $I_k$  is the  $k$ -dimensional identity matrix, and  $\alpha \in \{0, 1\}$ . For the purpose of this paper, we consider the bordered case only and, unless otherwise stated, we shall assume that the term double-circulant codes refers to (2).

$$G_p = \begin{array}{|c|c|} \hline I_k & R \\ \hline \end{array} \quad (1),$$

$$G_b = \begin{array}{|c|ccc|c|} \hline & 1 & \dots & 1 & \alpha \\ \hline & & & & 1 \\ I_k & & R & & \vdots \\ & & & & 1 \\ \hline \end{array} \quad (2)$$

Two binary linear codes,  $\mathcal{A}$  and  $\mathcal{B}$ , are *equivalent* if there exists a permutation  $\pi$  on the coordinates of the codewords which maps the codewords of  $\mathcal{A}$  onto codewords of  $\mathcal{B}$ . We shall write this as  $\mathcal{B} = \pi(\mathcal{A})$ . If  $\pi$  transforms  $\mathcal{C}$  into itself, then we say that  $\pi$  fixes the code, and the set of all permutations of this kind form the automorphism group of  $\mathcal{C}$ , denoted as  $\text{Aut}(\mathcal{C})$ . MacWilliams *et al.* [6] gives some conditions on the equivalence of double-circulant codes, which are restated for convenience in the lemma below.

**2.1 Lemma.** Let  $\mathcal{A}$  and  $\mathcal{B}$  be double-circulant codes with generator matrices  $[I|A]$  and  $[I|B]$  respectively. Let the polynomials  $a(x)$  and  $b(x)$  be the defining polynomials of  $A$  and  $B$ . The codes  $\mathcal{A}$  and  $\mathcal{B}$  are equivalent if any of the following conditions hold: i)  $B = A^T$ , or ii)  $b(x)$  is the reciprocal of  $a(x)$ , or iii)  $a(x)b(x) = 1 \pmod{x^m - 1}$ , or iv)  $b(x) = a(x^u)$  where  $m$  and  $u$  are relatively prime.

For the purpose of this paper, we call the double-circulant codes based on prime congruent to  $\pm 1$  modulo 8 the  $[p + 1, \frac{1}{2}(p + 1), d]$  extended quadratic residue (QR) codes, i.e.  $p \equiv \pm 1 \pmod{8}$ ; and, following [9], those based on prime congruent to  $\pm 3$  modulo 8 the  $[2(p + 1), p + 1, d]$  quadratic double-circulant codes, i.e.  $p \equiv \pm 3 \pmod{8}$ .

## 2.1 Extended Quadratic Residue Codes as Double-Circulants

The following is a summary of the extended QR codes as double-circulant codes [3, 6, 12]. Let  $p$  be a prime congruent to  $\pm 1$  modulo 8 and let  $Q$  and  $N$  be the sets of quadratic residues and non residues modulo  $p$  respectively. Binary QR codes are cyclic codes of length  $p$  over  $\text{GF}(2)$ . For a given  $p$ , there exists four QR codes:  $\bar{Q}, \bar{N}$  which are equivalent and have dimension  $\frac{1}{2}(p-1)$ , and  $Q, N$  which are equivalent and have dimension  $\frac{1}{2}(p+1)$ . The  $[p+1, \frac{1}{2}(p+1)]$  extended quadratic residue code, denoted by  $\hat{Q}$  (resp.  $\hat{N}$ ), is obtained by annexing an overall parity check to  $Q$  (resp.  $N$ ). If  $p \equiv -1 \pmod{8}$ ,  $\hat{Q}$  (resp.  $\hat{N}$ ) is Type II; otherwise it is fsd.

It is well-known that  $\text{Aut}(\hat{Q})$  contains the projective special linear group  $\text{PSL}_2(p)$  [6]. If  $r$  is a generator of the cyclic group  $Q$  then  $\sigma : i \rightarrow ri \pmod{p}$  is a member of  $\text{PSL}_2(p)$ . Given  $n \in N$ , the cycles of  $\sigma$  can be written as

$$(\infty)(n, nr, nr^2, \dots, nr^t)(1, r, r^2, \dots, r^t)(0) \quad (3)$$

where  $t = \frac{1}{2}(p-3)$ . Due to this property,  $G$ , the generator matrix of  $\hat{Q}$ , can be arranged into circulants as shown in (4).

$$G = \begin{array}{c} \infty \\ \beta \\ \vdots \\ \beta r^t \end{array} \begin{array}{|c|c|c|c|} \hline & \infty & n & \dots & nr^t & 1 & \dots & r^t & 0 \\ \hline & 1 & 1 & \dots & 1 & 1 & \dots & 1 & 1 \\ \hline & 0 & & & & & & & 1 \\ \hline & \vdots & & L & & & R & & \vdots \\ \hline & 0 & & & & & & & 1 \\ \hline \end{array} \quad (4)$$

The rows  $\beta, \beta r, \dots, \beta r^t$  in the above generator matrix contain

$$\bar{e}_\beta(x), \bar{e}_{\beta r}(x), \dots, \bar{e}_{\beta r^t}(x),$$

where  $\bar{e}_i(x) = x^i e(x)$  whose coordinates are arranged in the order of (3). Note that, if  $p \equiv 1 \pmod{8}$ , then  $\alpha=1, \beta=n$  and the idempotent  $e(x) = \sum_{n \in N} x^n$ ; otherwise  $\alpha=0, \beta=1$  and  $e(x) = 1 + \sum_{n \in N} x^n$ . If  $L$  is non-singular, (4) can be transformed to (2). For many  $\hat{Q}$ ,  $L$  is invertible and Karlin [3] has shown that  $p = 73, 97, 127, 137, 241$  are the known cases where the canonical form (2) cannot be obtained. In addition to form (2),  $G$  can also be transformed to (1), and Jenson [12] has shown that, for  $7 \leq p \leq 199$ , except  $p = 89, 167$ , the canonical form (1) exists.

## 2.2 Quadratic Double-Circulant Codes

Let  $p$  be a prime that is congruent to  $\pm 3$  modulo 8. A binary  $[2(p+1), p+1]$  quadratic double-circulant code, denoted by  $\mathcal{B}$ , can be constructed using the following defining polynomials

$$b(x) = \begin{cases} 1 + \sum_{r \in Q} x^r & \text{if } p \equiv 3 \pmod{8}, \text{ and} \\ \sum_{r \in Q} x^r & \text{if } p \equiv -3 \pmod{8}. \end{cases} \quad (5)$$

The generator matrix  $G$  of  $\mathcal{B}$  can be written as follows [6]

$$G = \begin{array}{c|ccc|ccc} & l_\infty & l_0 & \dots & l_{p-1} & r_\infty & r_0 & \dots & r_{p-1} \\ \hline 1 & & & & & 0 & & & \\ \vdots & & & & & \vdots & & & \\ 1 & & & & & 0 & & & \\ \hline 0 & 0 & \dots & 0 & & 1 & 1 & \dots & 1 \end{array} \quad (6)$$

which is equivalent to (2) with  $\alpha = 0$  and  $k = p + 1$ . If  $p \equiv 3 \pmod{8}$ ,  $\mathcal{B}$  is Type II; otherwise it is fsd with  $B = B^T$ . Codes of the form  $\mathcal{B}$  form an interesting family of double-circulant codes. In terms of self-dual codes, the family contains the largest extremal Type II code known,  $n = 136$ .

### 3 An Improved Algorithm To Count Codewords of Given Weight for Double-Circulant Codes

An algorithm to count codewords of given weight in half-rate codes, which have two full rank disjoint information sets is described in [2] and [10]. This algorithm requires the enumeration of

$$\binom{k}{w/2} + 2 \cdot \sum_{i=1}^{w/2-1} \binom{k}{i}$$

codewords in counting all codewords of weight  $w$ . We show in the following that, for self-dual double-circulant and fsd quadratic double-circulant codes, it is sufficient to enumerate

$$\sum_{i=1}^{w/2} \binom{k}{i}$$

codewords only.

Let  $\mathcal{C}_1$  and  $\mathcal{C}_2$  be a self-dual double-circulant, and a fsd quadratic double-circulant codes respectively, which has defining polynomial  $r(x)$ . We assume that  $\text{wt}(f(x))$  represents the weight of the polynomial  $f(x)$  and  $T_m(x)$  is a set of binary polynomials with degree at most  $m$ .

**3.1 Lemma.** Consider double-circulant codes of dimension  $k$ . Let  $u_i(x), v_i(x) \in T_{k-1}(x)$  for  $i = 1, 2$ , and  $e(x), f(x) \in T_{k-2}(x)$ . The number of weight  $w$  codewords of the forms  $c_1(x) = (u_1(x)|v_1(x))$  and  $c_2(x) = (v_2(x)|u_2(x))$  are equal, where

- i) for self-dual pure double-circulant codes,  $u_2(x) = u_1(x)^T$  and  $v_2(x) = v_1(x)^T$ ;
- ii) for self-dual bordered double-circulant codes,  $u_1(x) = (\epsilon|e(x))$ ,  $v_1(x) = (\gamma|f(x))$ ,  $u_2(x) = (\epsilon|e(x)^T)$  and  $v_2(x) = (\gamma|f(x)^T)$  where  $\gamma = \text{wt}(e(x)) \pmod{2}$ ;
- iii) for fsd pure double-circulant codes ( $p \equiv -3 \pmod{8}$ ),  $u_2(x) = u_1(x)^2$  and  $v_2(x) = v_1(x)^2$ ;

- iv) for fsd bordered double-circulant codes ( $p \equiv -3 \pmod{8}$ ),  $u_1(x) = (\epsilon|e(x))$ ,  $v_1(x) = (\gamma|f(x))$ ,  $u_2(x) = (\epsilon|e(x)^2)$ ,  $v_2(x) = (\gamma|f(x)^2)$  where  $\gamma = \text{wt}(e(x)) \pmod{2}$ .

**Proof.**

- i) Let  $G_1 = [I_k|R]$  and  $G_2 = [R^T|I_k]$  be the two full-rank generator matrices with mutually disjoint information sets of a self-dual pure double-circulant code. Assume that  $r(x)$  and  $r(x)^T$  are the defining polynomials of  $G_1$  and  $G_2$  respectively. Given  $u_1(x)$  as an input,  $G_1$  produces a codeword  $c_1(x) = (u_1(x)|v_1(x))$ , where  $v_1(x) = u_1(x)r(x)$ . Another codeword  $c_2(x)$  can be obtained from  $G_2$  by using  $u_1(x)^T$  as an input,  $c_2(x) = (v_1(x)^T|u_1(x)^T)$ , where  $v_1(x)^T = u_1(x)^T r(x)^T = (u_1(x)r(x))^T$ . Since the weight of a polynomial and that of its transpose are equal, for a given polynomial of degree at most  $k-1$ , there exists two distinct codewords of the same weight.
- ii) Let  $G_1$ , given by (2), and  $G_2$  be two full-rank generator matrices with pairwise disjoint information sets, of bordered self-dual double-circulant codes. It is assumed that the form of  $G_2$  is identical to that given by (6) with  $I_p = B^T$  and  $B = I_p$ . Let  $f(x) = e(x)r(x)$ , consider the following cases:

- (a)  $\epsilon = 0$  and  $\text{wt}(e(x))$  is odd, generator matrix  $G_1$  produces a codeword  $c_1(x) = (0|e(x)|1|f(x))$ . Applying  $(0|e(x)^T)$  as an information vector to generator matrix  $G_2$  yields another codeword  $c_2(x) = (1|e(x)^T r(x)^T|0|e(x)^T) = (1|f(x)^T|0|e(x)^T)$ .
- (b)  $\epsilon = 1$  and  $\text{wt}(e(x))$  is odd,  $G_1$  produces  $c_1(x) = (1|e(x)|1|f(x)+j(x))$ . Applying  $(1|e(x)^T)$  as an information vector to  $G_2$ , a codeword  $c_2(x) = (1|e(x)^T r(x)^T + j(x)|1|e(x)^T) = (1|f(x)^T + j(x)|1|e(x)^T)$ , is obtained.
- (c)  $\epsilon = 0$  and  $\text{wt}(e(x))$  is even,  $G_1$  produces a codeword  $c_1(x) = (0|e(x)|0|f(x))$ . Applying  $(0|e(x)^T)$  as an information vector to  $G_2$ , another codeword  $c_2(x) = (0|e(x)^T r(x)^T|0|e(x)^T) = (0|f(x)^T|0|e(x)^T)$  is produced.
- (d)  $\epsilon = 1$  and  $\text{wt}(e(x))$  is even, generator matrix  $G_1$  produces  $c_1(x) = (1|e(x)|0|f(x)+j(x))$ . Applying  $(1|e(x)^T)$  as an information vector to generator matrix  $G_2$  yields a codeword  $c_2(x)$  of the form  $(0|e(x)^T r(x)^T + j(x)|1|e(x)^T) = (0|f(x)^T + j(x)|1|e(x)^T)$ .

It is clear that in all cases,  $\text{wt}(c_1(x)) = \text{wt}(c_2(x))$  since  $\text{wt}(v(x)) = \text{wt}(v(x)^T)$  and  $\text{wt}(v(x)+j(x)) = \text{wt}(v(x)^T + j(x))$  for some polynomial  $v(x)$ . This means that given an information vector, there always exists two distinct codewords of the same weight.

- iii) Let  $G_1$ , given by (1) with  $R = I_p + Q$ , and  $G_2$ , given by (1) with  $I_k = I_p + N$  and  $R = I_p$ , be two full-rank generator matrices with pairwise disjoint information sets, of pure fsd double-circulant codes for  $p \equiv -3 \pmod{8}$ . Given  $u_1(x)$  as input,  $G_1$  produces a codeword  $c_1(x) = (u_1(x)|v_1(x))$ , where  $v_1(x) = u_1(x)(1+q(x))$ , where as  $G_2$  produces

a codeword  $c_2(x) = (v_2(x)|u_2(x))$ , where  $u_2(x) = u_1(x)^2$  and  $v_2(x) = u_1(x)^2(1 + n(x)) = u_1(x)^2(1 + q(x))^2 = v_1(x)^2$ . Since the weight of a polynomial and that of its square are the same over  $\mathbb{F}_2$ , the proof follows.

iv) Let  $G_1$ , given by (2) with  $B = R$ , and  $G_2$ , given by (6) with  $I_p = B^2$  and  $B = I_p$ , be two full-rank generator matrices with pairwise disjoint information sets, of bordered fsd double-circulant codes for  $p \equiv -3 \pmod{8}$ . Let  $f(x) = e(x)b(x)$ , consider the following cases:

- (a)  $\epsilon = 0$  and  $\text{wt}(e(x))$  is odd, generator matrix  $G_1$  produces a codeword  $c_1(x) = (0 | e(x) | 1 | f(x))$ . Applying  $(0 | e(x)^2)$  as an information vector to  $G_2$ , another codeword  $c_2(x) = (1 | e(x)^2 n(x) | 0 | e(x)^2)$  is obtained. Since  $e(x)^2 n(x) = e(x)^2 b(x)^2 = f(x)^2$ , the codeword  $c_2 = (1 | f(x)^2 | 0 | e(x)^2)$ .
- (b)  $\epsilon = 1$  and  $\text{wt}(e(x))$  is odd,  $G_1$  produces  $c_1(x) = (1 | e(x) | 1 | f(x) + j(x))$ . Applying  $(1 | e(x)^2)$  as an information vector to  $G_2$  yields a codeword  $c_2(x)$  which can be written as  $(1 | e(x)^2 n(x) + j(x) | 1 | e(x)^2) = (1 | f(x)^2 + j(x) | 1 | e(x)^2)$ .
- (c)  $\epsilon = 0$  and  $\text{wt}(e(x))$  is even,  $G_1$  produces a codeword  $c_1(x) = (0 | e(x) | 0 | f(x))$ . Applying  $(0 | e(x)^2)$  as an information vector to  $G_2$ , another codeword  $c_2(x) = (0 | e(x)^2 n(x) | 0 | e(x)^2) = (0 | f(x)^2 | 0 | e(x)^2)$  is produced.
- (d)  $\epsilon = 1$  and  $\text{wt}(e(x))$  is even,  $G_1$  produces  $c_1(x) = (1 | e(x) | 0 | f(x) + j(x))$ . Applying  $(1 | e(x)^2)$  as an information vector to  $G_2$  yields a codeword  $c_2(x)$  which can be written as  $(0 | e(x)^2 n(x) + j(x) | 1 | e(x)^2) = (0 | f(x)^2 + j(x) | 1 | e(x)^2)$ .

It is clear that in all cases,  $\text{wt}(c_1(x)) = \text{wt}(c_2(x))$  since  $\text{wt}(v(x)) = \text{wt}(v(x)^2)$  and  $\text{wt}(v(x) + j(x)) = \text{wt}(v(x)^2 + j(x))$  for some polynomial  $v(x)$ . This means that given an information vector, there always exists two distinct codewords of the same weight. ■

From Lemma 3.1, it follows that, in order to count codewords of weight  $w$ , the enumeration of  $\sum_{i=1}^{w/2} \binom{k}{i}$  codewords only is required and

$$A_w = a_{w/2} + 2 \sum_{i=1}^{w/2-1} a_i, \quad (7)$$

where  $a_i$  is the number of weight  $w$  codewords which have  $i$  non zeros in the first  $k$  coordinates.

## 4 Number of Codewords of Given Weights in Quadratic Double-Circulant Codes

Let  $Q$  and  $N$  be the sets of quadratic residue and non residue modulo  $p$  respectively. The linear group  $\text{PSL}_2(p)$  is generated by the set of all permutations to the coordinates  $(\infty, 0, 1, \dots, p-1)$  of the form  $y \rightarrow (ay+b)/(cy+d)$

where  $a, b, c, d \in \text{GF}(p)$ ,  $y \in \text{GF}(p) \cup \{\infty\}$  and  $ad - bc = 1$ . It can be shown that this form of permutation is generated by  $S : y \rightarrow y+1$ ,  $V : y \rightarrow \rho^2 y$  and  $T : y \rightarrow -\frac{1}{y}$  transformations, where  $\rho$  is a primitive element of  $\text{GF}(p)$ . In fact,  $V$  is redundant, since  $V = TS^\rho TS^\mu TS^\rho$ , where  $\mu \in \text{GF}(p)$  is the multiplicative inverse of  $\rho$ . Consider the coordinates  $(\infty, 0, 1, \dots, p-1)$ , the transformation  $S$  leaves the coordinate  $\infty$  invariant and introduces a cyclic shift to the rest of the coordinates. Let  $R_i$  and  $L_i$  denote the  $i$ th row of the right and left circulants of (6) respectively,  $J$  and  $J'$  denote the last row of the right and left circulant of (6) respectively. Using the arguments in [6], it can be shown that  $T(R_0) = R_0 + J$ ,  $T(R_s) = R_{-1/s} + R_0$ ,  $T(R_t) = R_{-1/t} + R_0 + J$ ,  $T(L_0) = L_0 + J'$ ,  $T(L_s) = L_{-1/s} + L_0$  and  $T(L_t) = L_{-1/t} + L_0 + J'$  for  $p \equiv 3 \pmod{8}$ , and  $T(R_0) = R_0$ ,  $T(R_s) = R_{-1/s} + J$ ,  $T(R_t) = R_{-1/t} + R_0$ ,  $T(L_0) = L_0$ ,  $T(L_s) = L_{-1/s} + J'$  and  $T(L_t) = L_{-1/t} + L_0$  for  $p \equiv -3 \pmod{8}$ , where  $s \in Q$  and  $t \in N$ . This establishes the following theorem on  $\text{Aut}(\mathcal{B})$  [6, 9].

**4.1 Theorem.** The automorphism group of the  $[2(p+1), p+1, d]$  binary quadratic double-circulant codes contains  $\text{PSL}_2(p)$  applied simultaneously to both circulants.

The knowledge of  $\text{Aut}(\mathcal{B})$  can be exploited to deduce the modular congruence of  $A_i$  of  $\mathcal{B}$ . If  $\mathcal{H} \subseteq \text{Aut}(\mathcal{B})$ , then  $A_i$  of  $\mathcal{B}$  can be categorised into two classes: one which contains all weight  $i$  codewords that are invariant under  $\mathcal{H}$  and the other which contains the rest. The latter class forms orbits of size  $|\mathcal{H}|$ , the order of  $\mathcal{H}$ .

For  $\mathcal{B}$ , we shall choose  $\mathcal{H} = \text{PSL}_2(p)$ , which has order  $\frac{1}{2}p(p^2 - 1)$ . Each  $A_i$  of  $\mathcal{B}$  can be written as  $A_i \equiv n_i \cdot |\mathcal{H}| + A_i(\mathcal{H})$ , where  $A_i(\mathcal{H})$  is the number of weight  $i$  codewords in a subcode fixed by some elements of  $\mathcal{H}$ . Since  $|\mathcal{H}| = \prod_j q_j^{e_j}$ , where  $q_j$  are distinct primes,  $A_i(\mathcal{H}) \pmod{|\mathcal{H}|}$  can be obtained by applying the Chinese-Remainder-Theorem to  $A_i(S_{q_j}) \pmod{q_j^{e_j}}$  for all  $q_j$  that divides  $|\mathcal{H}|$ , where  $S_{q_j}$  is the Sylow- $q_j$ -subgroup of  $\mathcal{H}$ . In order to compute  $A_i(S_{q_j})$ , we can find the subcode of  $\mathcal{C}$  that is fixed by  $S_{q_j}$ , and compute the number of codewords of weight  $i$  in this subcode.

In order to obtain the subcode fixed by  $S_{q_j}$  for all primes  $q_j$  that divide  $|\mathcal{H}|$ , the following method can be used. Let  $c_{l_i}$  (resp.  $c_{r_i}$ ) and  $c_{l_{i'}}$  (resp.  $c_{r_{i'}}$ ) denote the  $i$ th coordinate and  $i$ th permuted coordinate, with the respect to the permutation  $Z_{q_j}$ , in the left (resp. right) circulant form respectively. The invariant subcode can be obtained by solving a set of linear equations consisting of the parity-check matrix of  $\mathcal{B}$ ,  $c_{l_i} + c_{l_{i'}} = 0$  and  $c_{r_i} + c_{r_{i'}} = 0$  for all  $i \in \text{GF}(p) \cup \{\infty\}$ . The solution is a matrix of rank  $r > (p+1)$ , which is the parity-check matrix of the  $[2(p+1), 2(p+1) - r]$  invariant subcode.

Following [6], we represent an element of  $\text{PSL}_2(p)$  by a  $2 \times 2$  matrix  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , where  $a, b, c, d \in \text{GF}(p)$  and  $ad - bc = 1$ . For each odd prime  $q_j$ ,  $S_{q_j}$  is a cyclic group which can be generated by some  $Z_{q_j} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PSL}_2(p)$  of order  $q_j$ . Because  $S_{q_j}$  is cyclic, it is straightforward to obtain the invariant subcode, from which we can compute  $A_i(S_{q_j})$ .

On the other hand, the case of  $q_j = 2$  is more complicated. For  $q_j = 2$ ,  $S_2$  is a dihedral group of order  $2^{m+1}$ , where  $m+1$  is the maximum power of 2 that divides  $|\mathcal{H}|$ . According to Burnside [13], for  $p \equiv \pm 3 \pmod{8}$ , the highest power of 2 that divides  $|\mathcal{H}|$  is  $2^2$  and hence,  $m = 1$ . Accordingly,

there are 3 subgroups of order 2 in  $S_2$ , namely  $H_2 = \{1, P\}$ ,  $G_2^0 = \{1, T\}$  and  $G_2^1 = \{1, PT\}$  where  $P, T \in \text{PSL}_2(p)$ ,  $P^2 = T^2 = 1$  and  $TPT^{-1} = P^{-1}$ . Let  $T = \begin{bmatrix} 0 & 1 \\ p-1 & 0 \end{bmatrix}$ , which has order 2. It can be shown that any order 2 permutation,  $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , has  $b = c$  and  $a, d \in \text{GF}(p)$  such that  $ad - bc = 1$ .

Apart from subgroups of order 2,  $S_2$  also contains a non cyclic subgroup of order 4, which contains, apart from an identity, three permutations of order 2 [13], i.e. a Klein 4 group,  $G_4 = \{1, P, T, PT\}$ .

Following [11], it can be shown that, in order to compute  $A_i(S_2)$ , it is only necessary to consider the three subgroups of order 2 and  $G_4$ . However, all the three subgroups of order 2 are conjugate in  $\text{PSL}_2(p)$  and therefore, the subcodes fixed by  $G_2^0, G_2^1$  and  $H_2$  have identical weight distributions and consider either one of them, say  $G_2^0$ , is sufficient. Thus, the number of codewords of weight  $i$  in the subcodes fixed by  $S_2$  is

$$A_i(S_2) \equiv 3A_i(G_2^0) - 2A_i(G_4) \pmod{4}. \quad (8)$$

In summary, in order to deduce the modular congruence of the number of weight  $i$  codewords in  $\mathcal{B}$ , it is sufficient to compute the number of weight  $i$  codewords in the subcodes fixed by  $H_2, G_4$  and  $Z_q$  for all odd primes  $q$  that divide  $|\mathcal{H}|$ . The result follows by applying the Chinese-Remainder-Theorem to the number of weight  $i$  codewords in the subcodes.

As examples, we consider the weight distribution of the [76, 38, 12] and [124, 62, 20] fsd quadratic double-circulant codes, which were previously unknown. The weight enumerator of an fsd code is given by Gleason's theorem [1]

$$A(z) = \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} K_i (1+z^2)^{\frac{n}{2}-4i} (z^2 - 2z^4 + z^6)^i \quad (9)$$

for integers  $K_i$ . Hence, in order to compute  $A(z)$ ,  $A_{2i}$  for  $6 \leq i \leq 9$  and  $10 \leq i \leq 15$  have to be computed for the [76, 38, 12] and [124, 62, 20] codes respectively.

In the case of the [76, 38, 12] code,  $p = 37$  and  $|\text{PSL}_2(37)| = 2^2 \cdot 3^2 \cdot 19 \cdot 37 = 25308$ , and for the [124, 62, 20] code,  $p = 61$  and  $|\text{PSL}_2(61)| = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61 = 113460$ . The elements of  $\text{PSL}_2(p)$  which generate the required permutations are as follows  $P = \begin{bmatrix} 3 & 8 \\ 8 & 34 \end{bmatrix}$ ,  $T = \begin{bmatrix} 0 & 1 \\ 36 & 0 \end{bmatrix}$ ,  $Z_3 = \begin{bmatrix} 0 & 1 \\ 36 & 1 \end{bmatrix}$ ,  $Z_{19} = \begin{bmatrix} 0 & 1 \\ 36 & 3 \end{bmatrix}$  and  $Z_{37} = \begin{bmatrix} 0 & 1 \\ 36 & 35 \end{bmatrix}$  for  $p = 37$ , and  $P = \begin{bmatrix} 2 & 19 \\ 19 & 59 \end{bmatrix}$ ,  $T = \begin{bmatrix} 0 & 1 \\ 60 & 0 \end{bmatrix}$ ,  $Z_3 = \begin{bmatrix} 0 & 1 \\ 60 & 1 \end{bmatrix}$ ,  $Z_5 = \begin{bmatrix} 0 & 1 \\ 60 & 17 \end{bmatrix}$ ,  $Z_{31} = \begin{bmatrix} 0 & 1 \\ 60 & 5 \end{bmatrix}$ , and  $Z_{61} = \begin{bmatrix} 0 & 1 \\ 60 & 59 \end{bmatrix}$  for  $p = 61$ . The number of weight  $i$  codewords in various subcodes of dimension  $k$ , which are fixed by the  $\text{PSL}_2(p)$  permutations are

	$G_2^0$	$G_4$	$S_3$	$S_{19}$	$S_{37}$
$k$	20	12	14	2	2
$A_{12}$	21	3	3	0	0
$A_{14}$	0	0	0	0	0
$A_{16}$	153	11	24	0	0
$A_{18}$	744	20	54	0	0

and

	$G_2^0$	$G_4$	$S_3$	$S_5$	$S_{31}$	$S_{61}$
$k$	32	18	22	14	2	2
$A_{20}$	208	12	30	3	0	0
$A_{22}$	400	12	10	0	0	0
$A_{24}$	1930	36	50	0	0	0
$A_{26}$	8180	40	200	24	0	0
$A_{28}$	26430	140	620	48	0	0
$A_{30}$	84936	176	960	6	0	0

for  $p = 37$  and  $61$  respectively. By applying the Chinese-Remainder-Theorem, we have the following

$$\begin{aligned} A_{12} &= n_{12} \cdot 25308 + 2109 & A_{14} &= n_{14} \cdot 25308 \\ A_{16} &= n_{16} \cdot 25308 + 10545 & A_{18} &= n_{18} \cdot 25308 \end{aligned} \quad (10)$$

for the  $[76, 38, 12]$  code, and

$$\begin{aligned} A_{20} &= n_{20} \cdot 113460 + 90768 & A_{22} &= n_{22} \cdot 113460 + 75640 \\ A_{24} &= n_{24} \cdot 113460 + 94550 & A_{26} &= n_{26} \cdot 113460 + 83204 \\ A_{28} &= n_{28} \cdot 113460 + 71858 & A_{30} &= n_{30} \cdot 113460 + 68076 \end{aligned} \quad (11)$$

for the  $[124, 62, 20]$  code, where  $n_i$  are non negative integers.

We use the algorithm in Section 3 to efficiently count codewords of the weights required by Gleason's theorem. Their weight distributions, which are symmetric with  $A_i = A_{n-i}$  and hence, only half terms are given, are

[76, 38, 12]					
$i$	$A_i$	$i$	$A_i$	$i$	$A_i$
0	1	22	53574224	32	19610283420
12	2109	24	275509215	34	33067534032
16	86469	26	1113906312	36	45200010670
18	961704	28	3626095793	38	50157375456
20	7489059	30	9404812736		
[124, 62, 20]					
$i$	$A_i$	$i$	$A_i$	$i$	$A_i$
0	1	32	199576556020	48	27906300869721380
20	90768	34	1489045613508	50	64924782329852000
22	529480	36	9466389337938	52	132248827882614296
24	10873250	38	51549138453256	54	236218089014480048
26	171180884	40	241551099887720	56	370432817595720572
28	2159102198	42	977979841051968	58	510493584341738312
30	22668808776	44	3433274842143012	60	618649064180799821
		46	10482288501057056	62	659543439108163376

Comparing the above  $A_i$  with (10) and (11), we immediately see that  $n_{12} = 0$ ,  $n_{14} = 0$ ,  $n_{16} = 3$  and  $n_{18} = 38$  for  $[76, 38, 12]$  code;  $n_{20} = 0$ ,  $n_{22} = 4$ ,  $n_{24} = 95$ ,  $n_{26} = 1508$ ,  $n_{28} = 19029$  and  $n_{30} = 199795$  for  $[124, 62, 20]$  code. Clearly (10) and (11) provide an independent check on the accuracy of the weight distributions.

## 5 Corrections to the Weight Distributions of the Extended Quadratic-Residue Codes

In this section, we demonstrate the importance of the modular congruence method in providing independent verification to the number of codewords of given weights enumerated exhaustively. We consider two cases of  $[p + 1, \frac{1}{2}(p + 1), d]$  code  $\hat{Q}$ , namely  $p = 137$  and  $p = 151$ . Note that, in the case of  $\hat{Q}$ , the method originally proposed in [11] is used.

## 5.1 Extended Quadratic-Residue Code of Prime 137

Gaborit *et al.* gave  $A_{2i}$ , for  $22 \leq 2i \leq 32$ , of  $\hat{Q}$  for  $p = 137$  in [10] and we will check the consistency of these results. For  $[p+1, \frac{1}{2}(p+1), d]$  code  $\hat{Q}$ , we know that  $\text{PSL}_2(p) \subseteq \text{Aut}(\hat{Q})$  and for  $p = 137$ , we have  $|\text{PSL}_2(p)| = 2^3 \cdot 3 \cdot 17 \cdot 23 \cdot 137 = 1285608$  and we need to compute  $A_{2i}(S_q)$ , where  $22 \leq 2i \leq 32$ , for all primes  $q$  dividing  $|\text{PSL}_2(p)|$ . Let  $P = \begin{bmatrix} 0 & 37 \\ 37 & 31 \end{bmatrix}$ ,  $T = \begin{bmatrix} 0 & 1 \\ 136 & 0 \end{bmatrix}$ ,  $Z_3 = \begin{bmatrix} 0 & 1 \\ 136 & 1 \end{bmatrix}$ ,  $Z_{17} = \begin{bmatrix} 0 & 1 \\ 136 & 6 \end{bmatrix}$ , and  $Z_{23} = \begin{bmatrix} 0 & 1 \\ 136 & 11 \end{bmatrix}$ . It is not necessary to find  $Z_p$  as it only fixes the *all zeros* and *all ones* codewords. The number of weight  $i$  codewords in various fixed subcodes of dimension  $k$  are

	$H_2$	$G_4^0$	$G_4^1$	$S_3$	$S_{17}$	$S_{23}$	$S_{137}$
$k$	35	19	18	23	5	3	1
$A_{22}$	170	6	6	0	0	0	0
$A_{24}$	612	10	18	46	0	0	0
$A_{26}$	1666	36	6	0	0	0	0
$A_{28}$	8194	36	60	0	0	0	0
$A_{30}$	34816	126	22	943	0	0	0
$A_{32}$	114563	261	189	0	0	0	0

and from the Chinese-Remainder-Theorem, we know that

$$\begin{aligned}
 A_{22} &= n_{22} \cdot 1285608 + 321402 & A_{28} &= n_{28} \cdot 1285608 + 321402 \\
 A_{24} &= n_{24} \cdot 1285608 + 1071340 & A_{30} &= n_{30} \cdot 1285608 + 428536 \\
 A_{26} &= n_{26} \cdot 1285608 + 964206 & A_{32} &= n_{32} \cdot 1285608 + 1124907
 \end{aligned} \tag{12}$$

for some integers  $n_i$ . Comparing these to the results in [10], we can immediately see that  $n_{22} = 0$ ,  $n_{24} = 1$ ,  $n_{26} = 16$ ,  $n_{28} = 381$ , and both  $A_{30}$  and  $A_{32}$  were incorrectly reported. By codeword evaluations, we have established that  $A_{30} = 6648307504$  ( $n_{30} = 5171$ ) and  $A_{32} = 77865259035$  ( $n_{32} = 60566$ ) in (12).

## 5.2 Extended Quadratic-Residue Code of Prime 151

For  $\hat{Q}$  of  $p = 151$ ,  $|\text{PSL}_2(p)| = 2^3 \cdot 3 \cdot 5^2 \cdot 19 \cdot 151 = 1721400$  and  $P = \begin{bmatrix} 1 & 42 \\ 42 & 104 \end{bmatrix}$ ,  $T = \begin{bmatrix} 0 & 1 \\ 150 & 0 \end{bmatrix}$ ,  $Z_3 = \begin{bmatrix} 0 & 1 \\ 150 & 1 \end{bmatrix}$ ,  $Z_5 = \begin{bmatrix} 0 & 1 \\ 150 & 27 \end{bmatrix}$ , and  $Z_{19} = \begin{bmatrix} 0 & 1 \\ 150 & 8 \end{bmatrix}$ . The number of weight  $i$  codewords in the various fixed subcodes of dimension  $k$  are

	$H_2$	$G_4^0$	$G_4^1$	$S_3$	$S_5$	$S_{19}$	$S_{151}$
$k$	38	20	19	26	16	4	1
$A_{20}$	38	2	0	25	15	0	0
$A_{24}$	266	4	4	100	0	0	0

and we have

$$A_{20} = 1721400n_{20} + 28690 \quad \text{and} \quad A_{24} = 1721400n_{24} + 717250.$$

It follows that  $A_{20}$  is correctly reported in [10], but  $A_{24}$  is incorrectly reported as 717230. Using the method in Section 3, we have established that  $A_{20} = 28690$  and  $A_{24} = 717250$ . Using Gleason's theorem for Type II codes [1], we give the corrected weight distribution of this code.

[152, 76, 20]			
$i$	$A_i$	$i$	$A_i$
0	1	48	542987434093298550
20	28690	52	9222363801696269658
24	717250	56	98458872937331749615
28	164250250	60	670740325520798111830
32	39390351505	64	2949674479653615754525
36	5498418962110	68	8446025592483506824150
40	430930711621830	72	15840564760239238232420
44	19714914846904500	76	19527364659006697265368

## 6 [168, 84, 24] Double-Circulant Codes

If  $2p + 1$  is a prime for  $p \equiv 3 \pmod{8}$ , there exists  $\hat{Q}$  and  $\mathcal{B}$  which have the same length  $2(p + 1)$  and dimension  $p + 1$ , and in some cases, the minimum distances are also the same. Some examples of such codes are the  $[8, 4, 4]$ ,  $[24, 12, 8]$  and  $[168, 84, 24]$  codes. Using Lemma 2.1, we found that, for the two former codes,  $\hat{Q}$  and  $\mathcal{B}$  are equivalent. We consider the  $[168, 84, 24]$  double-circulant codes in this section. Note that the minimum distance of  $\hat{Q}$  was shown to be 24 in [14] and that of  $\mathcal{B}$  was shown to be  $\leq 28$  in [5] and our computation confirms that it is 24.

The defining polynomials (in hexadecimal) of  $\hat{Q}$  and  $\mathcal{B}$  of length 168 are  $c6ac71e844bcd0c8ddd3c$  and  $d978c57f4ec8d015ce164$  respectively. Although these two polynomials have the same weight, the resulting double-circulant codes do not satisfy any condition in Lemma 2.1. The inequivalence of these codes can be deduced from their  $A(z)$ . Using the modular congruence method, it can be shown that

$$\bar{A}_{24} = 2328648n_{24} + 776216 \quad \text{and} \quad \hat{A}_{24} = 285852\hat{n}_{24},$$

where  $\bar{A}_{24}$  and  $\hat{A}_{24}$  are  $A_{24}$  of  $\hat{Q}$  and  $\mathcal{B}$  respectively. For integers  $\bar{n}_{24}, \hat{n}_{24} \geq 0$ ,  $\bar{A}_{24} \neq \hat{A}_{24}$  and thus, they are inequivalent.

## 7 Conclusions

We have presented a more efficient method of codeword counting algorithms for self-dual double-circulant and fsd quadratic double-circulant codes in addition to a method to deduce the modular congruence of the weight distributions of the quadratic double-circulant codes. This modular congruence method is derived from the classic technique proposed by Mykkeltveit *et al.* in 1972, which was applied to the extended QR codes. Using this method, we are able to deduce the inequivalence of the  $[168, 84, 24]$  extended QR and quadratic double-circulant codes, and also to correct the previously published results on the weight distribution of the  $[138, 69, 22]$  and  $[152, 76, 20]$  extended QR codes.

## Acknowledgements

We wish to thank the PlymGRID team of the University of Plymouth in providing high throughput computing resources.

## References

- [1] E. M. Rains and N. J. A. Sloane, “Self-Dual Codes,” in *Handbook of Coding Theory* (V. S. Pless and W. C. Huffman, eds.), Elsevier, North Holland, 1998. (Cited on pages 1, 9 and 11.)
- [2] M. van Dijk, S. Egner, M. Greferath, and A. Wassermann, “On two doubly even self-dual binary codes of length 160 and minimum weight 24,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 408–411, Jan. 2005. (Cited on pages 2 and 5.)
- [3] M. Karlin, “New binary coding results by circulants,” *IEEE Trans. Inf. Theory*, vol. 15, pp. 81–92, Jan. 1969. (Cited on pages 2 and 4.)
- [4] E. H. Moore, *Double Circulant Codes and Related Algebraic Structures*. Ph.D dissertation, Dartmouth College, USA, 1976. (Cited on page 2.)
- [5] T. A. Gulliver and N. Senkevitch, “On a class of self-dual codes derived from quadratic residue,” *IEEE Trans. Inf. Theory*, vol. 45, pp. 701–702, Mar. 1999. (Cited on pages 2 and 12.)
- [6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977. (Cited on pages 2, 3, 4, 5 and 8.)
- [7] V. Pless, “Symmetry codes over GF(3) and new five designs,” *J. Combin. Theory Ser. A*, vol. 12, pp. 119–142, 1972. (Cited on page 2.)
- [8] G. Beenker, “A note on extended quadratic residue codes over GF(9) and their ternary images,” *IEEE Trans. Inf. Theory*, vol. 30, pp. 403–405, Mar. 1984. (Cited on page 2.)
- [9] P. Gaborit, “Quadratic double circulant codes over fields,” *J. Combin. Theory Ser. A*, vol. 97, pp. 85–107, 2002. (Cited on pages 2, 3 and 8.)
- [10] P. Gaborit, C.-S. Nedeloaia, and A. Wassermann, “On the weight enumerators of duadic and quadratic residue codes,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 402–407, Jan. 2005. (Cited on pages 2, 5 and 11.)
- [11] J. Mykkeltveit, C. Lam, and R. J. McEliece, “On the weight enumerators of quadratic residue codes,” *JPL Technical Report 32-1526*, vol. XII, pp. 161–166, 1972. (Cited on pages 2, 9 and 10.)
- [12] R. Jenson, “A double circulant presentation for quadratic residue codes,” *IEEE Trans. Inf. Theory*, vol. 26, pp. 223–227, Mar. 1980. (Cited on page 4.)
- [13] W. Burnside, *Theory of Group of Finite Order*. Reprinted by Dover, New York, 2<sup>nd</sup>, 1911 ed., 1955. (Cited on pages 8 and 9.)

- [14] M. Grassl, “On the minimum distance of some quadratic residue codes,” in *Proc. IEEE International Symposium on Inform. Theory*, (Sorrento, Italy), p. 253, 25–30 Jun. 2000. (Cited on page 12.)