

On the Weight Distribution of the Extended Quadratic Residue Code of Prime 137

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

Fixed and Mobile Communications Research

University of Plymouth

Plymouth, PL4 8AA, United Kingdom

Post-print of 7th International ITG Conference on Source and Channel Coding, Ulm, 14–16 January 2008

Abstract

The Hamming weight enumerator function of the formally self-dual even, binary extended quadratic residue code of prime $p = 8m + 1$ is given by Gleason's theorem for singly-even code. Using this theorem, the Hamming weight distribution of the extended quadratic residue is completely determined once the number of codewords of Hamming weight j A_j , for $0 \leq j \leq 2m$, are known. The smallest prime for which the Hamming weight distribution of the corresponding extended quadratic residue code is unknown is 137. It is shown in this paper that, for $p = 137$ $A_{2m} = A_{34}$ may be obtained without the need of exhaustive codeword enumeration. After the remainder of A_j required by Gleason's theorem are computed and independently verified using their congruences, the Hamming weight distributions of the binary augmented and extended quadratic residue codes of prime 137 are derived.

1 Introduction

The Hamming weight distribution of a linear error correcting code is of practical and theoretical interest. It provides a great deal of information on the code capability in detecting errors and in correcting errors or erasures. The complexity of computing the Hamming weight distribution of a code is exponential. In general, the computation requires one to enumerate all codewords of the code; or to enumerate all codewords of the dual and apply the MacWilliams identity.

Since the birth of coding theory, various algebraic error correcting codes have been discovered. One classic family of such codes is the family of quadratic residue (QR) codes, which has rich mathematical structure and good error correcting capability. Despite having these advantages, the construction of its algebraic decoder is non trivial. Due to the existence of rich mathematical structure, there are considerable restrictions on the weight

structure of this family of codes and therefore it is not necessary to enumerate all codewords or those of the dual in computing the Hamming weight distribution. In fact, by knowing a fraction of the Hamming weight distribution, the complete distribution can be obtained. Recently, this method has been used by Gaborit *et al* [1] to obtain the Hamming weight distributions of binary extended QR codes of primes 73, 89, 97, 113 and 127¹. In our previous work [2, 3], we have evaluated the Hamming weight distributions of the extended QR codes of primes 151 and 167. The smallest prime for which the Hamming weight distribution of the corresponding extended QR code is not known in 137 and in this paper, its Hamming weight distribution is evaluated. We show that even smaller fraction of the Hamming weight distribution is sufficient to derive the complete Hamming weight distribution.

The remainder of this paper is organised as follows. Section 2 gives the definition and notation that we use in this paper—including a brief recall of the binary QR codes. Section 3 discusses the modular congruence of the number of codewords of a given Hamming weight and the Hamming weight distribution of the extended QR code of prime 137 is derived in Section 4.

2 Definition and Notation

Let \mathbb{F}_2^n be a space of vector of length n whose elements take value over \mathbb{F}_2 (binary field). An $[n, k, d]$ binary linear code \mathcal{C} of length n , dimension k and minimum Hamming distance d , is a k -dimensional subspace of \mathbb{F}_2^n . Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, the scalar product of these two vectors is defined as $\mathbf{x} \cdot \mathbf{y} = \sum_{j=0}^{n-1} x_j y_j \pmod{2}$. Given a code \mathcal{C} , the dual code is defined as $\mathcal{C}^\perp = \{\mathbf{c}^\perp \mid \mathbf{c} \cdot \mathbf{c}^\perp = 0 \text{ for all } \mathbf{c} \in \mathcal{C} \text{ and } \mathbf{c}^\perp \in \mathbb{F}_2^n\}$. The hull of a code \mathcal{C} is defined as $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp$.

The Hamming weight of a vector $\mathbf{v} \in \mathbb{F}_2^n$, denoted by $wt_H(\mathbf{v})$, is the number of its non zero coordinates and the minimum Hamming distance of \mathcal{C} is simply the smallest Hamming weight of all codewords in \mathcal{C} . Throughout this paper, we deal exclusively with Hamming space and for convenience, the word ‘‘Hamming’’ shall be omitted. The weight enumerator function of \mathcal{C} is given by

$$A_{\mathcal{C}}(z) = \sum_{j=0}^n A_j z^j \tag{1}$$

where z is an indeterminate and A_j is the number of codewords of weight j . The distribution of A_j for $0 \leq j \leq n$ is called the weight distribution of a code.

Given a vector $\mathbf{v} \in \mathbb{F}_2^n$ of even weight, if $wt_H(\mathbf{v}) \equiv 0 \pmod{4}$, it is termed doubly-even; otherwise $wt_H(\mathbf{v}) \equiv 2 \pmod{4}$ and it is termed singly-even. An even code is one which has codewords of even weight only. A code \mathcal{C} is called self-dual if $\mathcal{C} = \mathcal{C}^\perp$. A self-dual code may be doubly-even if the weight of all codewords is divisible by 4 or singly-even if there are

¹The Hamming weight distribution of that of prime 151 is also given in [1], but we have shown that this result has been incorrectly reported, refer to [2] for the detailed discussion.

codewords whose weight is congruent to 2 (mod 4). In addition to self-dual code, there also exists formally self-dual code. A code \mathcal{C} is termed formally self-dual if $\mathcal{C} \neq \mathcal{C}^\perp$ but $A_{\mathcal{C}}(z) = A_{\mathcal{C}^\perp}(z)$.

2.1 Quadratic Residue Codes

In this subsection, a brief summary of QR codes over \mathbb{F}_2 is given [4]. Binary QR codes are cyclic codes of prime length p where $p \equiv \pm 1 \pmod{8}$. Let Q and N be sets of quadratic residue and non quadratic residue modulo p respectively. Given a prime p , there are four QR codes denoted by \mathcal{Q}_p , \mathcal{N}_p , $\overline{\mathcal{Q}}_p$ and $\overline{\mathcal{N}}_p$. If α is a primitive p -root of unity, the generator polynomial of the $[p, (p+1)/2, d-1]$ augmented QR codes \mathcal{Q}_p and \mathcal{N}_p contains roots whose exponents are element of Q and N respectively. The $[p, (p-1)/2, d]$ expurgated QR codes $\overline{\mathcal{Q}}_p$ and $\overline{\mathcal{N}}_p$ contain, in their generator polynomial, α^0 in addition to the roots of the respective augmented QR codes. Note that \mathcal{Q}_p (resp. $\overline{\mathcal{Q}}_p$) is permutation equivalent to \mathcal{N}_p (resp. $\overline{\mathcal{N}}_p$).

If $p \equiv -1 \pmod{8}$, $\mathcal{Q}_p^\perp = \overline{\mathcal{Q}}_p$ and as such the $[p+1, (p+1)/2, d]$ extended QR code $\hat{\mathcal{Q}}_p$ is self-dual and doubly-even. For $p \equiv 1 \pmod{8}$, $\mathcal{Q}_p^\perp = \overline{\mathcal{N}}_p$ and therefore $\hat{\mathcal{Q}}_p \neq \hat{\mathcal{Q}}_p^\perp$ but $A_{\hat{\mathcal{Q}}_p}(z) = A_{\hat{\mathcal{Q}}_p^\perp}(z)$ implying the corresponding extended QR code is formally self-dual.

In this paper, we are interested in the QR codes where $p \equiv 1 \pmod{8}$, in particular $p = 137$. Since the extended code is formally self-dual, the restrictions on the weight structure imposed by Gleason's theorem for singly-even code applies. This implies that for a given prime $p = 8m+1$, the weight enumerator function $A_{\hat{\mathcal{Q}}_p}(z)$ is given by [5]

$$A_{\hat{\mathcal{Q}}_p}(z) = \sum_{j=0}^m K_j (1+z^2)^{4m-4j+1} \{z^2(1-z^2)^2\}^j \quad (2)$$

for some integer K_j . Equation (2) shows that the complete weight distribution can be derived once the first m even terms of A_j ($A_0 = 1$ by definition) are known. Note that $\hat{\mathcal{Q}}_p$ is an even code and thus $A_j = 0$ for odd integer j .

3 Congruence of the Number of Codewords of a Given Weight

It is known in the literature that the automorphism group of $\hat{\mathcal{Q}}_p$, denoted by $\text{Aut}(\hat{\mathcal{Q}}_p)$, contains the projective special linear group $\text{PSL}_2(p)$ [4]. This linear group is generated by a set of permutations on the coordinates $(\infty, 0, 1, \dots, p-1)$ of the form $y \rightarrow (ay+b)/(cy+d)$ where $a, b, c, d \in \mathbb{F}_p$, $y \in \mathbb{F}_p \cup \{\infty\}$ and $ad-bc=1$. This set of permutations may be produced by the transformations² $S: y \rightarrow y+1$ and $T: y \rightarrow -y^{-1}$. The knowledge of the automorphism group of a code may be exploited to characterise the weight distribution of the code.

²In some cases, we can see that, in addition to S and T , the transformation $V: y \rightarrow \rho^2 y$ where ρ is a generator of \mathbb{F}_p also generates the desired permutation of $\text{PSL}_2(p)$. However, strictly speaking, V is redundant since $V = TS^\rho TS^\mu TS^\rho$ where $\mu = \rho^{-1} \pmod{p}$.

Let $\text{Aut}(\hat{Q}_p) \supseteq \text{PSL}_2(p) = \mathcal{H}$, the number of weight j codewords A_j can be categorised into two classes: one which contains all weight j codewords that are invariant under some element of \mathcal{H} and another which contains the rest. Given a codeword of \hat{Q}_p that is not invariant under some element of \mathcal{H} , applying all $|\mathcal{H}| = \frac{1}{2}p(p^2 - 1)$ permutations will result in $|\mathcal{H}|$ distinct codewords of \hat{Q}_p . In other words, the latter class forms orbits of size equal to the cardinality of $\text{PSL}_2(p)$. Let $A_j(\mathcal{H})$ denote the number of weight j codewords which are invariant under some element of \mathcal{H} , we may write

$$\begin{aligned} A_j &= n_j \cdot |\mathcal{H}| + A_j(\mathcal{H}) \\ &\equiv A_j(\mathcal{H}) \pmod{\frac{1}{2}p(p^2 - 1)} \end{aligned} \quad (3)$$

for $n_j \in \mathbb{Z}^* = \{0\} \cup \mathbb{Z}^+$ i.e. non negative integer. Since $|\mathcal{H}|$ can be factorised as $\mathcal{H} = \prod_i q_i^{e_i}$ where q_i is a prime and e_i is a positive integer, it is shown in [6] that $A_j(\mathcal{H})$ may be obtained by applying the Chinese Remainder Theorem to $A_j(S_{q_i}) \pmod{q_i^{e_i}}$ for all primes q_i that divide $|\mathcal{H}|$. Note that S_{q_i} is the Sylow- q_i -subgroup of \mathcal{H} and $A_j(S_{q_i})$ is the number of codewords of weight j fixed by some element of S_{q_i} .

For each prime q_i , in order to compute $A_j(S_{q_i})$, the subcode which is invariant under some element of S_{q_i} needs to be obtained. For odd primes q_i , S_{q_i} is cyclic and there exists $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{H}$, for some integers a, b, c, d , which generates cyclic permutation of order q_i . Thus, it is straightforward to obtain the invariant subcode and the corresponding $A_j(S_{q_i})$. On the other hand, if $q_i = 2$, S_2 is a dihedral group of order 2^s , where s is the highest power of 2 that divides $|\mathcal{H}|$, and $A_j(S_2)$ is given by [6]

$$A_j(S_2) \equiv (2^{s-1} + 1)A_j(H_2) - 2^{s-2}A_j(G_4^0) - 2^{s-2}A_j(G_4^1) \pmod{2^s}, \quad (4)$$

where H_2 and G_4^i , for $i = 0, 1$, are subgroups of order 2 and 4 respectively, which are contained in S_2 . Let $P \in \mathcal{H}$ of order 2^{s-1} and $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathcal{H}$ of order 2, it is shown in [6] that $H_2 = \{1, P^{2^{s-2}}\}$ and the non cyclic subgroup $G_4^i = \{1, P^{2^{s-2}}, P^i T, P^{2^{s-2}+i} T\}$.

4 The Weight Distribution

Following Gleason's theorem, see (2), the weight distribution of the binary extended QR code of prime 137 is given by

$$A_{\hat{Q}_{137}}(z) = \sum_{j=0}^{17} K_j (1+z^2)^{69-4j} (z^2 - 2z^4 + z^6)^j. \quad (5)$$

Since $A_0 = 1$ and the minimum distance of \hat{Q}_{137} is 22, only A_{2j} , for $11 \leq j \leq 17$, are required in order to deduce $A_{\hat{Q}_{137}}(z)$ completely. Note that each A_{2j} determines K_j for some integer j . However, following the idea in [6] which has been relatively forgotten, K_{17} may be determined without the need of exhaustively computing A_{34} as shown in this section.

Let us first deduce the modular congruence of A_{2j} , for $11 \leq j \leq 17$, of \hat{Q}_{137} . Some of these congruences have been given in the authors' previous

work [2], but are restated in the following to make the paper self-contained. For $p = 137$, it is clear that $|\mathcal{H}| = 2^3 \cdot 3 \cdot 17 \cdot 23 \cdot 137 = 1285608$. Let $P = \begin{bmatrix} 0 & 37 \\ 37 & 31 \end{bmatrix}$ and let $\begin{bmatrix} 0 & 1 \\ 136 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 136 & 6 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 136 & 11 \end{bmatrix}$ be generators of permutation of orders 3, 17 and 23 respectively. It is not necessary to find a generator that generates permutation of order 137 as it fixes the all zeros and all ones codewords only. Subcodes that are invariant under H_2 , G_4^0 , G_4^1 , S_3 , S_{17} and S_{23} are obtained and the number of weight $2j$, for $11 \leq j \leq 17$, codewords in these subcodes are then computed. The results are tabulated as follows, where k denotes the dimension of the corresponding subcode,

| | 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 |
| A_{34} | 343453 | 351 | 39 | 0 | 2 | 0 | 0 |

For $p = 137$, (4) becomes

$$A_{2j}(S_2) \equiv 5A_{2j}(H_2) - 2A_{2j}(G_4^0) - 2A_{2j}(G_4^1) \pmod{8}$$

and using this formulation, the following congruences

$$\begin{aligned} A_{22}(S_2) &= 2 \pmod{8} \\ A_{24}(S_2) &= 4 \pmod{8} \\ A_{26}(S_2) &= 6 \pmod{8} \\ A_{28}(S_2) &= 2 \pmod{8} \\ A_{30}(S_2) &= 0 \pmod{8} \\ A_{32}(S_2) &= 3 \pmod{8} \\ A_{34}(S_2) &= 5 \pmod{8} \end{aligned}$$

are obtained.

Combining all the above results using the Chinese-Remainder-Theorem, it follows that

$$\begin{aligned} A_{22} &= n_{22} \cdot 1285608 + 321402 \\ A_{24} &= n_{24} \cdot 1285608 + 1071340 \\ A_{26} &= n_{26} \cdot 1285608 + 964206 \\ A_{28} &= n_{28} \cdot 1285608 + 321402 \\ A_{30} &= n_{30} \cdot 1285608 + 428536 \\ A_{32} &= n_{32} \cdot 1285608 + 1124907 \\ A_{34} &= n_{34} \cdot 1285608 + 1143813 \end{aligned} \tag{6}$$

for some non negative integers n_{2j} .

Let G be the generator matrix of the half-rate code \hat{Q}_{137} . In order to efficiently count the number of codewords of weight $2j$, two full-rank generator matrices, say G_1 and G_2 , which have pairwise disjoint information sets

are required. These matrices can be easily obtained by performing Gaussian elimination on G to produce $G_1 = [I|A]$ and repeating the process on submatrix A to produce $G_2 = [B|I]$. For each of these full-rank matrices, we need to enumerate as many as

$$\sum_{i=0}^j \binom{69}{i}$$

codewords and count the number of those of weight $2j$. The efficiency of enumeration may be improved by employing the revolving door combination generator algorithm [7], which has the property that in two successive combination patterns, there is only one element that is exchanged. In addition to this, the revolving door algorithm also has a nice property that allows the enumeration to be realised on grid computer, see Appendix A.1. We have evaluated A_{2j} , for $11 \leq j \leq 16$, using a grid of approximately 1500 computers and the results are given below

$$\begin{aligned} A_{22} &= 321402 \\ A_{24} &= 2356948 \\ A_{26} &= 21533934 \\ A_{28} &= 490138050 \\ A_{30} &= 6648307504 \\ A_{32} &= 77865259035. \end{aligned} \tag{7}$$

Comparing (6) and (7), it can be clearly seen that³ $n_{22} = 0$, $n_{24} = 1$, $n_{26} = 16$, $n_{28} = 381$, $n_{30} = 5171$ and $n_{32} = 60566$. The non negative integer solutions of n_{2j} give an indication that the corresponding A_{2j} has been accurately computed.

We now show that A_{34} is known. It is worth noting that knowing A_{34} , based on the arguments on codeword counting given above, significantly reduces the complexity of computing $A_{\hat{Q}_{137}}(z)$. Consider Gleason's formulation given in (5), if we take its first derivative with respect to z , we have

$$\begin{aligned} \frac{d}{dz} A_{\hat{Q}_{137}}(z) &= \sum_{j=0}^{17} K_j (1+z^2)^{68-4j} (z^2 - 2z^4 + z^6)^{j-1} \\ &\quad \left\{ 2(69-4j)z(z^2 - 2z^4 + z^6) + \right. \\ &\quad \left. j(1+z^2)(2z - 8z^3 + 6z^5) \right\} \end{aligned} \tag{8}$$

³Note that A_{2j} , for $11 \leq j \leq 16$, have also been given in [1], however, A_{30} and A_{32} have been incorrectly reported as demonstrated in [2].

which may be expanded as

$$\begin{aligned}
\frac{d}{dz}A_{\hat{Q}_{137}}(z) &= (1+z^2)^{68}K_0+ \\
&\quad (1+z^2)^{64}\left\{130z(z^2-2z^4+z^6)+\right. \\
&\quad \left.(1+z^2)(2z-8z^3+6z^5)\right\}K_1+ \\
&\quad (1+z^2)^{60}(z^2-2z^4+z^6)\left\{122z(z^2-2z^4+z^6)+\right. \\
&\quad \left.2(1+z^2)(2z-8z^3+6z^5)\right\}K_2+ \\
&\quad \vdots \\
&\quad (z^2-2z^4+z^6)^{16}\left\{2z(z^2-2z^4+z^6)+\right. \\
&\quad \left.17(1+z^2)(2z-8z^3+6z^5)\right\}K_{17}.
\end{aligned} \tag{9}$$

From (9), we can see that the terms that involve K_j for $0 \leq j \leq 16$ become zero if we set $z = i = \sqrt{-1}$. Thus,

$$\begin{aligned}
\frac{d}{dz}A_{\hat{Q}_{137}}(z) \Big|_{z=i} &= 2i(i^2 - 2i^4 + i^6)^{17}K_{17} \\
&= -i2^{35}K_{17}.
\end{aligned} \tag{10}$$

Since $\text{Aut}(\hat{Q}_p)$ is doubly-transitive, given A_{2j} of an extended QR code \hat{Q}_p , the number of codewords of weight $2j - 1$ and $2j$ in the augmented code Q_p are $\frac{2j}{p+1}A_{2j}$ and $\frac{p+1-2j}{p+1}A_{2j}$ respectively. Following [8], the weight enumerator function of Q_{137} may be written in terms of that of \hat{Q}_{137} as follows

$$A_{Q_{137}}(z) = A_{\hat{Q}_{137}}(z) + \left(\frac{1-z}{138}\right) \frac{d}{dz}A_{\hat{Q}_{137}}(z). \tag{11}$$

From (5), it is obvious that $A_{\hat{Q}_{137}}(z) \Big|_{z=i} = 0$ and therefore (11) becomes

$$A_{Q_{137}}(z) \Big|_{z=i} = -i \frac{1-i}{138} 2^{35} K_{17}. \tag{12}$$

The expurgated QR code \bar{Q}_{137} is an even code and following [4], $\bar{Q}_{137}^\perp = \mathcal{N}_{137}$. We can see that the exponents of the zeros of \bar{Q}_{137} are in the set $Q \cup \{0\}$, whereas those of \mathcal{N}_{137} are in the set N , and thus the hull of \bar{Q}_{137} has dimension zero. It follows from [9, Lemma 7.8.3 pp. 276] that the code \bar{Q}_{137} may be decomposed into an orthogonal sum of either 34 subcodes each consisting of three doubly-even and one singly-even codewords; or 33 subcodes each consisting of three doubly-even and one singly-even codewords, in addition to one subcode containing one doubly-even and three singly-even codewords. As a consequence, if W_w denotes the number of codewords of weight congruent to $w \pmod{4}$ in \bar{Q}_{137} , we have, see [9, Theorem 7.8.6 pp. 277]

$$W_0 - W_2 = \pm 2^{34}. \tag{13}$$

Note that this result also holds for \mathcal{Q}_{137} as $\overline{\mathcal{Q}}_{137}$ is the even weight subcode of \mathcal{Q}_{137} . Since all ones codeword $\mathbf{1}^p \in \mathcal{Q}_{137}$, it follows that

$$W_1 - W_3 = \pm 2^{34} \quad (14)$$

for the augmented QR code. Substituting z with \mathbf{i} in the weight enumerator function of \mathcal{Q}_{137} , we have

$$\begin{aligned} A_{\mathcal{Q}_{137}}(z) \Big|_{z=\mathbf{i}} &= A_0 + \mathbf{i}A_1 - A_2 - \mathbf{i}A_3 + \\ &\quad A_4 + \mathbf{i}A_5 - A_6 - \mathbf{i}A_7 + \\ &\quad \vdots \\ &\quad - A_{130} - \mathbf{i}A_{131} + A_{132} + \mathbf{i}A_{133} \\ &\quad - A_{134} - \mathbf{i}A_{135} + A_{136} + \mathbf{i}A_{137} \\ &= \left[\sum_{j \equiv 0 \pmod{4}} A_j - \sum_{j \equiv 2 \pmod{4}} A_j \right] + \\ &\quad \mathbf{i} \left[\sum_{j \equiv 1 \pmod{4}} A_j - \sum_{j \equiv 3 \pmod{4}} A_j \right] \\ &= [W_0 - W_2] + \mathbf{i}[W_1 - W_3] \end{aligned}$$

and thus, following (13) and (14),

$$A_{\mathcal{Q}_{137}}(z) \Big|_{z=\mathbf{i}} = \pm 2^{34}(1 + \mathbf{i}). \quad (15)$$

Equating (12) and (15),

$$-\mathbf{i} \frac{1 - \mathbf{i}}{138} 2^{35} K_{17} = \pm 2^{34}(1 + \mathbf{i}),$$

we arrive at

$$K_{17} = \mp 69. \quad (16)$$

Using (7), $A_{2j} = 0$ for $1 \leq j \leq 10$ and $A_0 = 1$, K_j for $0 \leq j \leq 16$ are determined. Substituting these into (5) and equating the coefficients of z^{34} with A_{34} , we have

$$A_{34} = 771068968296 + K_{17}. \quad (17)$$

Consider the case for $K_{17} = -69$, $A_{34} = 771068968227$. Comparing this A_{34} with the congruence given in (6), it follows that $n_{34} \notin \mathbb{Z}^*$ and hence this rules out the possibility of $K_{17} = -69$. If $K_{17} = 69$, however,

$$A_{34} = 771068968365 \quad (18)$$

and it follows that $n_{34} = 599769 \in \mathbb{Z}^*$, indicating that K_{17} is indeed 69.

Now we have determined A_{34} (and hence K_{17}) without exhaustively counting the number of codewords of weight 34 in $\hat{\mathcal{Q}}_{137}$. The weight distribution of $\hat{\mathcal{Q}}_{137}$ can be straightforwardly deduced from (5) and so is that of \mathcal{Q}_{137} from (11). The weight distributions of the augmented and also the extended QR code of prime 137 are tabulated in Table 1. Note that since the weight distributions are symmetrical, only the first half terms are tabulated.

Acknowledgements

The authors wish to thank the PlymGRID team of the University of Plymouth for providing the high performance computing resources.

References

- [1] P. Gaborit, C.-S. Nedeloaia, and A. Wassermann, “On the weight enumerators of duadic and quadratic residue codes,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 402–407, Jan. 2005.
- [2] C. Tjhai, M. Tomlinson, R. Horan, M. Ahmed, and M. Ambroze, “Some results on the weight distributions of the binary double-circulant codes based on primes,” in *Proc. 10th IEEE International Conference on Communications Systems*, (Singapore), 30 Oct.–1 Nov 2006.
- [3] C. Tjhai, M. Tomlinson, R. Horan, M. Ahmed, and M. Ambroze, “On the efficient codewords counting algorithm and the weight distribution of the binary quadratic double-circulant codes,” in *Proc. IEEE Information Theory Workshop*, (Chengdu, China), pp. 42–46, 22–26 Oct. 2006.
- [4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [5] 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.
- [6] 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.
- [7] A. Nijenhuis and H. S. Wilf, *Combinatorial Algorithms for Computers and Calculators*. Academic Press, London, 2nd ed., 1978.
- [8] J. H. van Lint, “Coding theory,” in *Lecture Notes in Mathematics No. 201*, Springer, Berlin, 1970.
- [9] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003. ISBN 0 521 78280 5.
- [10] H. Lüneburg, “Gray codes,” *Abh. Math. Sem. Hamburg*, vol. 52, pp. 208–227, 1982.
- [11] D. E. Knuth, *The Art of Computer Programming, Vol. 4: Fascicle 3: Generating All Combinations and Partitions*. Addison-Wesley, 3rd ed., 2005. ISBN 0 201 85394 9.

A Appendix

A.1 Parallel Realisation of Codeword Enumeration

In this appendix, a method to enumerate codewords in parallel is described and for a detailed description, refer to [7, 10, 11]. Let C_t^s denote the combination of t out of s elements with the combination pattern represented by an ordered set $a_t a_{t-1} \dots a_1$, where $a_1 < a_2 < \dots < a_{t-1} < a_t$. A pattern is said to have rank r if this pattern appears as the $(r+1)$ th element in the list of all C_t^s combinations. Here, it is assumed that the first element in the list of all C_t^s combinations has rank 0. The combination C_t^s , which follows the revolving door constraint and has an ordered set pattern, exhibits the following property

$$C_t^s \supset C_t^{s-1} \supset \dots \supset C_t^{t+1} \supset C_t^t.$$

Consequently, this implies that, for the revolving door combination patterns of the form $a_t a_{t-1} \dots a_1$, if those of fixed a_t are considered, the maximum and minimum ranks of such patterns are $\binom{a_t+1}{t} - 1$ and $\binom{a_t}{t}$ respectively.

Let $\text{Rank}(a_t a_{t-1} \dots a_1)$ be the rank of the pattern $a_t a_{t-1} \dots a_1$, the revolving door combination also has the following recursive property on its rank,

$$\text{Rank}(a_t a_{t-1} \dots a_1) = \left[\binom{a_t+1}{t} - 1 \right] - \text{Rank}(a_{t-1} \dots a_1). \quad (19)$$

As an implication of this, if all $\binom{k}{t}$ codewords need to be enumerated, for some integers $k, t > 0$ and $k \geq t$, we can split the enumeration into $\lceil \binom{k}{t} / M \rceil$ blocks where in each block only at most M codewords need to be enumerated. In this way, the enumeration of each block can be done on a separate computer—allowing parallelism of codeword enumeration. We know that at the j th block, the enumeration would start from rank $(j-1)M$ and the corresponding pattern can be easily obtained by making use of (19) as well as the maximum and minimum ranks of the patterns of fixed a_t .

Table 1: The weight distributions of [137, 69, 21] augmented and [138, 69, 22] extended quadratic residue codes

| j | $Q_{137} = [137, 69, 21]$ | $\hat{Q}_{137} = [138, 69, 22]$ |
|-----|---------------------------|---------------------------------|
| 0 | 1 | 1 |
| 21 | 51238 | 0 |
| 22 | 270164 | 321402 |
| 23 | 409904 | 0 |
| 24 | 1947044 | 2356948 |
| 25 | 4057118 | 0 |
| 26 | 17476816 | 21533934 |
| 27 | 99448300 | 0 |
| 28 | 390689750 | 490138050 |
| 29 | 1445284240 | 0 |
| 30 | 5203023264 | 6648307504 |
| 31 | 18055712240 | 0 |
| 32 | 59809546795 | 77865259035 |
| 33 | 189973513945 | 0 |
| 34 | 581095454420 | 771068968365 |
| 35 | 1709208146190 | 0 |
| 36 | 4842756414205 | 6551964560395 |
| 37 | 13221982102853 | 0 |
| 38 | 34794689744350 | 48016671847203 |
| 39 | 88328700833460 | 0 |
| 40 | 216405317041977 | 304734017875437 |
| 41 | 511980845799941 | 0 |
| 42 | 1170241933257008 | 1682222779056949 |
| 43 | 2585374360137184 | 0 |
| 44 | 5523299769383984 | 8108674129521168 |
| 45 | 11414864729214318 | 0 |
| 46 | 22829729458428636 | 34244594187642954 |
| 47 | 44202380361406672 | 0 |
| 48 | 82879463177637510 | 127081843539044182 |
| 49 | 150535995889831600 | 0 |
| 50 | 264943352766103616 | 415479348655935216 |
| 51 | 451961780387038844 | 0 |
| 52 | 747475252178564242 | 1199437032565603086 |
| 53 | 1198781830242451728 | 0 |
| 54 | 1864771735932702688 | 3063553566175154416 |
| 55 | 2814110491202421488 | 0 |
| 56 | 4120661790689260036 | 6934772281891681524 |
| 57 | 5855675469990794812 | 0 |
| 58 | 8076793751711441120 | 13932469221702235932 |
| 59 | 10814690610004223000 | 0 |
| 60 | 14059097793005489900 | 24873788403009712900 |
| 61 | 17746731937729182608 | 0 |
| 62 | 21754058504313191584 | 39500790442042374192 |
| 63 | 25897686719588958304 | 0 |
| 64 | 29944200269524733039 | 55841886989113691343 |
| 65 | 33629639551783390742 | 0 |
| 66 | 36686879511036426264 | 70316519062819817006 |
| 67 | 38877142978140092004 | 0 |
| 68 | 40020588359850094710 | 78897731337990186714 |