On the Weight Enumerators of Duadic and Quadratic Residue Codes

Philippe Gaborit, Carmen-Simona Nedeloaia
LACO, Université de Limoges
123, Av. A. Thomas,
87000 Limoges, France
Email: gaborit@unilim.fr, carmen.nedeloaia@unilim.fr
and
Alfred Wassermann
Mathematisches Institut, Universität Bayreuth
95440 Bayreuth, Germany
Email: alfred.wassermann@uni-bayreuth.de

Version 1.5 – October 2, 2003

Abstract

In this paper we compute the weight enumerators of various quadratic residue codes over $\mathbf{F}_2$ and $\mathbf{F}_3$, together with certain codes of related families like the duadic and the quadratic double circulant codes. We use a parallel algorithm to find the number of codewords of a given (not too high) weight, from which we deduce by usual classical methods for self-dual and isodual codes over $\mathbf{F}_2$ and $\mathbf{F}_3$ their associated, previously unknown, weight enumerators. We compute weight enumerators for lengths as high as 152 for binary codes and 96 for ternary codes.

1 Introduction

The family of duadic codes which contains the quadratic residue codes was introduced in [9] by Leon, Masley and Pless and their minimum distance (for lengths up to 241) was considered in [17] using a probabilistic algorithm to compute their minimum distance. Another interesting family related to quadratic residue codes, the quadratic double circulant (QDC) codes, was introduced by Pless over $\mathbf{F}_3$ [**?**] and by Karlin [8] over $\mathbf{F}_2$ and was later generalized by Gaborit over F_q in [7].

The families of duadic codes and especially the family of quadratic residue codes and QDC codes contain many codes with the best known parameters. For some cases when these codes are extremal self-dual codes, the weight distribution is fixed, but for many other cases when the codes are not extremal or not self-dual, only the minimum distance is known and not the complete weight distribution. In this paper we are interested in the weight distribution of these codes. We give in particular the weight distributions of binary extended quadratic residue (XQR) codes up to length 152 (except length 138). We also give the weight distribution of some binary QDC and duadic codes with good minimum distance. The weight distributions of the best known ternary self-dual QDC and XQR codes for lengths up to 96 are also given.

Our results mainly rely on the computation of the number of codewords of not too high weights for these codes. This is done through a parallel algorithm based on a well known counting method for self-dual codes, which runs faster than the MAGMA system [3]. We then apply classical techniques to deduce their weight enumerators.

Note that by comparison the weight distribution of BCH codes are known up to length 128 [6], although until now the weight distributions of the binary XQ_{73} and XQ_{89} were not known.

The paper is organized as follows: in Section 2 and 3 we explain our notation and briefly recall the duadic and quadratic double circulant codes constructions. In Section 4 we recall the classical methods to compute the weight enumerators of self-dual or even formally self-dual codes, in Section 5 we give an algorithm to compute the number of codewords of linear $[n, k, d]$ codes with the property that $n = 2k$. In Section 6 we give the number of codewords of low weight for the codes we consider and finally we list in Section 7 the weight enumerators of all binary quadratic residue codes of length up to 152 (except length 138) and some QDC codes, as well as all ternary self-dual or QDC codes of lengths between 72 and 96.

2 Definition and notation

A linear code $C[n, k]$ of length n and dimension k over the Galois field with q elements $\mathbf{F}_q$ is a linear subspace of dimension k in $\mathbf{F}_q^n$. An element of C is called a codeword. The (Euclidean) scalar product is understood with respect to the form: $x \cdot y = \sum x_i y_i$. The dual of a code C is denoted by $C^\perp$. A code C is said (Euclidean) self-dual if and only if $C = C^\perp$ for the Euclidean scalar product. Two codes over $\mathbf{F}_q$ are said to be *monomially equivalent* if they differ only from a monomial transformation (i.e. a permutation of the coordinates followed by a multiplication of the coordinates by a nonzero element of $\mathbf{F}_q$).

The (Hamming) weight $w(x)$ of a codeword $x = (x_1, ..., x_n)$ is the number of its nonzero coordinates and the minimum distance $d(C)$ of a code C is defined by: $d(C) = \min\{w(x-y) | x, y \in C\}$. The weight enumerator W_C of a code C is $W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$, where A_i is the number of codewords of C of weight i. There are two kind of binary self-dual codes. A self-dual code is said to be of Type II (or doubly-even self-dual) if all its Hamming weights are a multiple of four. Else, it is said to be of Type I (or singly-even self-dual). Note that the length of a Type II code is a multiple of eight. A ternary self-dual code is said to be Type III if all its Hamming weights are a multiple of three.

A code which has the same weight enumerator as its dual is said to be *formally self-dual (fsd)*. If C is equivalent to its dual then C is said to be *isodual*.

Let C be a self-dual or formally self-dual code of length n and minimum distance $d(C)$, then bounds are known for the minimum distance [18], depending on q. A Type II code satisfies $d(C) \leq 4\lfloor \frac{n}{24} \rfloor + 4$. For Type I codes we have

$$d(C) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4, & \text{if } n \neq 22 \pmod{24}, \\ 4\lfloor \frac{n}{24} \rfloor + 6, & \text{if } n = 22 \pmod{24}. \end{cases}$$

For binary formally self-dual codes: $d(C) \leq 2\lfloor \frac{n}{8} \rfloor + 2$. The minimum distance of a self-dual ternary code C satisfies: $d(C) \leq 3\lfloor \frac{n}{12} \rfloor + 3$. A self-dual code meeting one of the previous bounds according to its self-duality is said to be *extremal*. A code is called *optimal* if it has the highest known minimum weight for its length and dimension.

3 Background on duadic, quadratic residue codes and quadratic double circulant codes

3.1 Duadic codes and quadratic residue codes

Duadic codes were introduced by Leon, Masley and Pless in [9]. In the following we recall basic facts about duadic codes and quadratic residue codes. More details can be found in [16] and [17].

Duadic codes are a special family of cyclic codes. We suppose the reader is familiar with cyclic codes and their idempotents (see [11] for more details).

We consider the usual ideal ring $R_n = \mathbf{F}_q[x]/(x^n - 1)$, with columns labeled by $\{0, 1, \ldots, n-1\}$. For any integer a less than n such that $\gcd(a, n) = 1$ we can define a permutation μ_a, called a *multiplier*, by

$$\mu_a : i \longrightarrow ai \pmod{n}, \quad i \in \{0, 1, \ldots, n-1\}.$$

A word $y = (y_0, y_1, \cdots, y_{n-1})$ is even-like if $\sum_{i=0}^{n-1} y_i = 0$ in $\mathbf{F}_q$, and odd-like else. A code is said to be *even-like* if all its vectors are even-like and *odd-like* provided it contains at least one odd-like vector. The set $\mathcal{E}$ of even-like vectors in R_n forms an $[n,\, n-1]$ cyclic code whose dual code $\mathcal{E}^\perp$ is the repetition code with generating idempotent $j(x) = \frac{1}{n}(1 + x + x^2 + \ldots + x^{n-1})$. So $\mathcal{E}$ has generating idempotent $1 - j(x)$.

Duadic codes are defined in terms of idempotents. They come in two pairs: one even-like pair and one odd-like pair. Let $C_1 = \langle e_1(x)\rangle$ and $C_2 = \langle e_2(x)\rangle$, where $e_1(x)$ and $e_2(x)$ are the even-like idempotents associated to the cyclic codes C_1 and C_2. Then C_1 and C_2 form a pair of even-like duadic codes provided:

$$e_1(x) + e_2(x) = 1 - j(x),$$

and provided there is a multiplier μ_a such that

$$C_1\mu_a = C_2 \quad \text{and} \quad C_2\mu_a = C_1.$$

This implies in particular that $C_1 \cap C_2 = \{\mathbf{0}\}$, $C_1 + C_2 = \mathcal{E}$, n is odd and C_1 and C_2 each have dimension $\frac{n-1}{2}$. Associated to C_1 and C_2 is the pair of odd-like duadic codes $D_1 = \langle 1 - e_2(x)\rangle$ and $D_2 = \langle 1 - e_1(x)\rangle$.

Duadic codes can also be defined in terms of q-cyclotomic cosets. Let C_1 and C_2 be a pair of even-like duadic codes with defining set $T_1 = \{0\} \cup S_1$ and $T_2 = \{0\} \cup S_2$, where S_1 and S_2 are a union of q-cyclotomic cosets. Since μ_a interchanges C_1 and C_2, and since C_1 and C_2 have dimension $\frac{n-1}{2}$, we have:

$$S_1\mu_a = S_2,\ S_2\mu_a = S_1,\ S_1 \cap S_2 = \emptyset \quad \text{and} \quad S_1 \cup S_2 = \{1, 2, \cdots, n-1\}.$$

In that case one says that the pair S_1 and S_2 forms *a splitting of n given by μ_a.*

Then the three following results are true [16]:

1) Duadic codes of length n over $\mathbf{F}_q$ exist if and only if there is a multiplier which gives a splitting of n and if and only if q is a square modulo n.

2) Binary duadic codes of length n exist if and only if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where p_i is prime and $p_i \equiv \pm 1 \pmod 8$ for $1 \le i \le r$. Ternary duadic codes of length n exist if and only if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where p_i is prime and $p_i \equiv \pm 1 \pmod{12}$ for $1 \le i \le r$.

3) Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be a pair of odd-like duadic codes of length n over $\mathbf{F}_q$. It is possible to define a special extension which is used for duadic codes. Assume that there is a solution $\gamma \in \mathbf{F}_q$ to the equation $1 + \gamma^2 n = 0$. And for C a linear code, define $\widetilde{C} = \{\tilde{\mathbf{c}}\} = c_0 c_1 \cdots c_{n-1} c_\infty$ where $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$.

Then:

(i) If μ_{-1} gives the splitting for $\mathcal{D}_1$ and $\mathcal{D}_2$, then $\widetilde{\mathcal{D}_1}$ and $\widetilde{\mathcal{D}_2}$ are self-dual.

(ii) If $\mathcal{D}_1\mu_{-1} = \mathcal{D}_1$, then $\widetilde{\mathcal{D}_1}$ and $\widetilde{\mathcal{D}_2}$ are dual of each other. Moreover, for binary codes, if $\widetilde{\mathcal{D}_1}$ is self-dual then $\widetilde{\mathcal{D}_1}$ is Type II if $n \equiv -1 \pmod 8$ and Type I if $n \equiv +1 \pmod 8$.

Quadratic residue codes of length n over $\mathbf{F}_q$, when they exist for a given n and a given q, correspond to the particular case where S_1 and S_2 are respectively the sets of non null quadratic residues and non quadratic residues modulo n.

3.2 Quadratic double circulant codes

Quadratic double circulant codes were first introduced by Pless in [14] over $\mathbf{F}_3$ (see also Beenker [1]) and by Karlin in [8] over $\mathbf{F}_2$. They were generalized later over $\mathbf{F}_q$ (q a power of a prime number) by the first author in [7].

Let $\mathcal{K}$ be $\mathbf{F}_2$ or $\mathbf{F}_3$, let r, s and t be elements of $\mathcal{K}$ and let p be a prime. We set the matrix $Q_p(r,s,t)$ to be the $p \times p$ matrix on $\mathcal{K}$ labeled on its rows and its columns by $0, 1, 2, \ldots, p-1$, and with components q_{ij}. The entries q_{ij} are defined in terms of quadratic residues and by the function χ (which is not necessarily a character) defined on $\mathbf{F}_p$ by $\chi(0) = r$, $\chi(i) = s$ if i is a quadratic residue in $\mathbf{F}_p$ and $\chi(i) = t$ else. Then we let q_{ij} equals to $\chi(j-i)$. Note that the matrix $Q_p(r,s,t)$ is circulant.

For any α, β and γ in $\mathcal{K}$, the $[2p+2, p+1]$ double circulant code with the following generator matrix is a quadratic double circulant code:

$$\mathcal{B}_p(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0\cdots 0 & \alpha & \beta\cdots\beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_p(r,s,t) \\ 0 & & \gamma & \end{array}\right)$$

Now we set $\epsilon = 1$ if $p = 4k+1$ and $\epsilon = -1$ if $p = 4k+3$. Unless otherwise specified we always consider $\beta = 1$, $\gamma = \epsilon \cdot \beta$ and $\alpha = r$.

The previous matrix is said to be *bordered* quadratic double circulant, another *pure* quadratic double circulant also exists [7]. The codes with generator matrices $\mathcal{B}_p(r,s,t)$ may be self-dual or isodual depending on the different parameters.

4 Computing weight enumerators

Computing the weight enumerator of a code is in general a difficult problem. Meanwhile in some cases the homogeneous weight enumerator belongs to a certain algebraic ring. So that the weight enumerator of the code can be computed from the number of codewords of given ‘not too high’ weights. In this paper we consider four kind of codes: Type II codes, Type I codes, even formally self-dual binary codes and ternary self-dual codes. We recall in this section how to compute their weight enumerator from certain of their coefficients A_i (see [18] for more details on self-dual codes and their weight enumerators). In particular for Type I codes we precise up to which weight it is necessary to compute the number of codewords for both the code and its shadow, to deduce the weight enumerator. We see that in fact this weight is very close from the necessary weight for Type II codes.

4.1 Type II codes

The weight enumerator of Type II codes can be computed through Gleason theorem [18], which stands that the homogeneous weight enumerator of a Type II code belongs to the ring $\mathbb{C}[P_8, P_{24}]$, with $P_8 = x^8 + 14x^4y^4 + y^8$ and $P_{24} = x^4y^4(x^4 - y^4)^4$:

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/24 \rfloor} a_i (x^8 + 14x^4y^4 + y^8)^{\frac{n}{8}-3i} \{x^4y^4(x^4 - y^4)^4\}^i.$$

and therefore it is sufficient to know the $\lfloor n/24 \rfloor + 1$ first coefficients A_{4i} (i.e. up to $A_{4\lfloor n/24 \rfloor}$, A_0 is always equal to 1) to deduce the weight enumerator exactly. It means that the knowledge of the number of codewords of weights (roughly) up to $n/6$ of a Type II code permits to know the total weight enumerator. More precisely the choice of the polynomial P_{24} implies that the linear system of the i first A_{4i} terms has a unique solution in terms of the i first a_i.

4.2 Type I Codes

In that case Gleason theorem (which is valid more generally for even fsd codes) shows that the homogeneous weight enumerator belongs to the ring $\mathbb{C}[P_2, P_8']$ for $P_2 = x^2 + y^2$ and $P_8' = x^2y^2(x^2 - y^2)^2$:

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/8 \rfloor} a_i (x^2 + y^2)^{\frac{n}{2}-4i} \{x^2y^2(x^2 - y^2)^2\}^i.$$

Applying the same idea than for Type II codes would lead to the computation of the $\lfloor n/8 \rfloor + 1$ first coefficients A_{2i} of W_C, up to $A_{2\lfloor n/8 \rfloor}$ (with $2\lfloor n/8 \rfloor$ roughly equal to $n/4$). Fortunately, the introduction of the concept of the shadow [5] permits to consider only roughly $n/6$ coefficients.

Let C be a singly-even self-dual code and let C_0 be its doubly-even subcode, then the shadow S of C is defined as $S := {C_0}^{\perp} \setminus C$. In particular S is a coset of C (i.e. it exists $s \in S$ s.t. $S = s + C$). The weight enumerator of S is related to the weight enumerator of C through the coefficients a_i:

$$W_S(x,y) = \sum_{i=0}^{\lfloor n/8 \rfloor} a_i (-1)^i 2^{\frac{n}{2}-6i} (xy)^{\frac{n}{2}-4i} (x^4 - y^4)^{2i} = x^n + B_1 x^{n-1} y + \ldots + B_n y^n.$$

The preceding formula implies that the only possible nonzero coefficients of W_S are the B_i, $i \equiv ss \pmod 4$, with $ss = n/2 \pmod 4$. The particular form of the polynomial xy in the preceding formula also implies that the coefficients B_{ss+4i} for $0 \le i \le \lfloor n/8 \rfloor$ of W_S fix the coefficients $a_{\lfloor n/8 \rfloor - i}$ for $0 \le i \le \lfloor n/8 \rfloor$. Note that the weight enumerator of the shadow can be obtained as $W_S(x,y) = W_{C_0^{\perp}}(x,y) - W_C(x,y)$, with about the same complexity as computing the weight enumerator of C.

Now suppose one is able to compute the number of codewords of a rate 1/2 code up to weight $2m$, therefore one can deduce the coefficients $a_1, \ldots, a_m$. It remains to compute $a_{\lfloor n/8 \rfloor}, \ldots, a_{m+2}, a_{m+1}$ via the shadow code. This requires the computation of $B_{ss}, B_{ss+4}, \ldots, B_{ss+4(\lfloor n/8 \rfloor - m-1)}$ and implies $ss+4(\lfloor n/8 \rfloor - m - 1)$ being of order of $2m$, not greater. Therefore we obtain:

$$2m = \lceil (ss + 4\lfloor n/8 \rfloor - 4)/3 \rceil.$$

Therefore $2m$ is roughly equal to $n/6$, the same value than for Type II codes.

For instance consider a self-dual Type I code of length 90. The number of necessary coefficients a_i is $1 + \lfloor 90/8 \rfloor = 12$ (a_0 is always 1), $ss = 1$ and $2m = 14$. The number of codewords of weights $2, 4, \ldots, 14$ give the coefficients $a_1, a_2, \ldots, a_7$ and the number of codewords of the shadow of weights 1, 5, 9 and 13 give the coefficients a_{11}, a_{10}, a_9 and a_8. As an example, for the code of length 90 and $S_1 = \{0, 1, 3, 5, 13\}$ we obtain $B_1 = 1$, $B_5 = B_9 = 0$, $B_{13} = 89$.

4.3 Even formally self-dual codes

In that case, no shadow theory exists and only Gleason theorem is known as for singly-even self-dual codes, implying that for computing $W_C(x, y)$ one has to compute $\lfloor n/8 \rfloor + 1$ coefficients A_{2i} (therefore up to weight $2\lfloor n/8 \rfloor$, roughly $n/4$).

4.4 Ternary case

The weight enumerator of Type III codes can be computed through Gleason theorem for Type III codes which stands that the homogeneous weight enumerator of a Type III code belongs to the ring $\mathbb{C}[P_4, P_{12}]$, with $P_4 = x^4 + 8xy^3$ and $P_{12} = y^3(x^3 - y^3)^3$:

$$W_C(x, y) = \sum_{i=0}^{\lfloor n/12 \rfloor} a_i (x^4 + 8xy^3)^{\frac{n}{12} - 3i} \{y^3(x^3 - y^3)^3\}^i$$

and therefore it is sufficient to know the $\lfloor n/12 \rfloor + 1$ first coefficients A_{3i} (i.e. up to $A_{3\lfloor n/12 \rfloor}$) to deduce the weight enumerator exactly. It means that the knowledge of the weights of (roughly) up to $n/4$ of a Type III code permits to know the total weight enumerator.

5 An algorithm to compute the number of codewords of given weight

For the counting of codewords of a given weight w we use an algorithm which seems to belong to the folklore knowledge for self-dual codes.

If C is a linear $[n, k, d]$ code over $\mathrm{GF}(q)$ with $n = 2k$ we compute two generator matrices $G' = (I', A')$ and $G'' = (A'', I'')$ for C having disjoint information sets of full rank, i.e. the two diagonal matrices I' and I'' each have rank k. If C is self-dual G' and G'' always exist. For all non self-dual codes, we are considering here, G' and G'' also exist.

For $1 \leq i \leq k$ let G'_i and G''_i be the ith row of the generator matrices G' and G'', respectively. In order to determine the number of codewords of weight w in C we count

1. for all values of t with $1 \leq t \leq w/2$ and all possible choices of $a_i \in \mathrm{GF}(q) \setminus \{0\}$ the number of codewords c of weight w which are the linear combination of t rows of G':
$$c = a_1 G'_{i_1} + a_2 G'_{i_2} + \cdots + a_t G'_{i_t}\,,$$
2. for all values of t with $1 \leq t < w/2$ and all possible choices of $a_i \in \mathrm{GF}(q) \setminus \{0\}$ the number of codewords c of weight w which are the linear combination of t rows of G'':
$$c = a_1 G''_{i_1} + a_2 G''_{i_2} + \cdots + a_t G''_{i_t}\,.$$

This method was generalized by Zimmermann [2] to the computation of the minimum distance of linear codes for any values of k and n.

For a fixed selection $i_1 i_2 \ldots i_t$ of rows of a generator matrix all linear combinations $a_1 G'_{i_1} + a_2 G'_{i_2} + \cdots + a_t G'_{i_t}$ and $a_1 G''_{i_1} + a_2 G''_{i_2} + \cdots + a_t G''_{i_t}$ with $a_i \in \mathrm{GF}(q) \setminus \{0\}$, $1 \leq i \leq t$, have to be tested. Since we can fix $a_1 = 1$ this means that for each selection of t rows $(q-1)^{t-1}$ linear combinations have to be tested. The resulting number of codewords then has to be multiplied by $(q - 1)$.

The generating of all combinations of t rows $i_1 i_2 \ldots i_t$ out of k rows of the generator matrices G' and G'', respectively, is realized with the revolving door algorithm by Nijenhuis and Wilf [13]. It has the property that in each step only one row in $i_1 i_2 \ldots i_t$ is exchanged.

The resulting sequence of t-tuples has the interesting property that the combination $i_1 i_2 \ldots i_t$ of the rows of the generator matrix is visited after exactly
$$m = \binom{i_t + 1}{t} - \binom{i_{t-1} + 1}{t - 1} + \cdots + (-1)^t \binom{i_2 + 1}{2} - (-1)^t \binom{i_1 + 1}{1} - [t \text{ odd}]$$
other combinations have been visited, see Lüneburg [10]. This enables an easy parallelization of the problem: For $1 \leq t \leq w/2$ we divide the work of $\binom{k}{t}$ enumeration steps in $\lfloor \binom{k}{t} / T \rfloor$ chunks of size T. The rth job for $1 \leq r \leq \lfloor \binom{k}{t} / T \rfloor$ then starts at enumeration step $(r - 1) \cdot T$. With the above formula the corresponding combination of rows $i_1 i_2 \ldots i_t$ of the generator matrix can be determined easily. For the distribution of the jobs we used `autoson` by McKay [12].

This algorithm is much faster than the codeword counting method `NumberOfWords` of the Computer Algebra System MAGMA [3]. There, by default only one information set is used.

This means that with MAGMA $O(\binom{k}{w})$ codewords have to be enumerated, whereas in our case only $O(\binom{k}{w/2})$ enumeration steps are necessary. Then, the algorithm can be parallelized on arbitrarily many computers. We used up to 40 computers simultaneously. Moreover, our implementation seems to be at least twice as fast as the implementation of MAGMA, version V2.9-6.

6 Minimum Weights in Duadic Codes

In this section we list the number of codewords A_i necessary to compute the weight enumerators of the codes we consider. Note that an empty entry means that the given coefficient is not necessary to compute the weight enumerator.

We list the duadic codes through the set S_1 of their cyclotomic cosets following [17]. For each cyclotomic coset, only the smallest representative is given. All the codes listed here are inequivalent [17]. For length $n < 217$, only the equivalence of the two $[162, 81, 8]$ codes was previously unknown. We computed the number of codewords of weight 16 and we found 2665355, respectively 5378527, so these codes are inequivalent.

All minimum distances in our tables are exact, and agreed with those computed probabilistically in [17], as well as the exact ones in [19]. In all the tables, notation 'I','II' or 'iso' means that the corresponding codes are Type I, Type II or isodual.

To save space we list in the next section only the total weight distributions of the extended quadratic residue codes and QDC codes in the binary and ternary case. The notation XQ_{n-1} is for the extended quadratic residue code of length n and $\mathcal{B}_p(r,s,t)$ is for the QDC code constructed as in section 3.2.

6.1 Binary Case

n	S_1	Type	Weights							
			10	12	14	16	18	20	22	24
74	0, 1, 3, 5, 11	I	73	876	876	163812	504576			
74	0, 1, 3, 5, 13	I	73	0	0	174324	515088			
74	0, 1, 5, 9, 17	iso	0	657	8103	86724	1061274			
74	XQ_{73}	iso	0	0	8103	89133	1093905			
90	0, 1, 3, 5, 13	I	0	89	0	18601	94963	4529833	14729055	
90	0, 1, 3, 5, 19	I	0	89	0	18601	94963	4529833	14729055	
90	0, 1, 3, 11, 33	iso	0	0	0	14685	203632	2910567	30374454	
90	XQ_{89}	iso	0	0	0	0	274120	2819520	30530115	
98	XQ_{97}	iso	0	0	0	28518	80801	931588	15038492	166982396

n	S_1	Type	Weights			
			20	22	24	26
108	$\mathcal{B}_{53}(0,1,0)$	iso	260442	5804136	74455407	746650008

n	S_1	Type	Weights						
			16	18	20	22	24	26	28
114	XQ_{113}	iso	25764	0	450870	2795394	36685789	468994974	4741799790
114	0, 1, 3	iso	0	4746	139216	2499560	38153885	473211004	4773745342

n	S_1	Type	Weights							
			4	6	8	10	12	14	16	18
120	$1, 13, 17, 21$	iso	119	0	6664	0	233240	0	6285818	8000132
120	$1, 7, 11, 51$	iso	0	476	595	476	97342	242760	621061	12995752
120	$1, 7, 13, 17$	iso	0	0	952	0	28560	0	787780	1000076
120	$1, 7, 11, 17$	iso	0	0	0	0	1428	0	1904	79968

	Weights					
	20	22	24	26	28	30
cont.	152410678	678868344	3828465501	26066879076	95327385454	618071235908
cont.	56207032	246474228	1749528837	8831883928	43093426089	214787987092
cont.	19046545	84857472	479437315	3275719188	12450412366	84684304628
cont.	366996	2950724	33511590	325076584	3231268047	29780853844

n	S_1	Type	Weights	
			16	20
120	$\mathcal{B}_{59}(0,0,1)$	II	0	71862
128	1, 3, 9, 11, 13, 15, 21, 27, 47	II	94488	0
128	1, 3, 5, 9, 11, 13, 15, 21, 27	II	127	23114
128	1, 3, 9, 13, 15, 19, 21, 29, 47	II	1143	59563
128	1, 3, 7, 9, 11, 13, 19, 21, 47	II	3048	57785
128	1, 3, 7, 9, 11, 13, 21, 27, 47	II	127	8890
128	1, 3, 5, 7, 9, 13, 19, 21, 29	II	1016	0
128	1, 3, 15, 21, 23, 27, 29, 47, 55	II	127	25781
128	1, 3, 5, 7, 9, 19, 21, 23, 29	II	127	14224
128	1, 3, 5, 7, 9, 11, 21, 23, 27	II	127	17780
128	1, 3, 7, 9, 11, 21, 23, 27, 47	II	1016	113792
128	1, 3, 7, 9, 11, 19, 21, 23, 47	II	381	36449
128	1, 3, 7, 9, 13, 21, 27, 29, 47	II	127	22225
128	1, 3, 5, 9, 15, 21, 23, 27, 29	II	889	23114
128	1, 3, 9, 13, 15, 21, 27, 29, 47	II	0	33782
128	1, 3, 5, 9, 13, 15, 21, 27, 29	II	0	26670
128	1, 3, 9, 15, 21, 23, 27, 29, 47	II	0	19558
128	1, 3, 9, 11, 15, 21, 23, 27, 47	II	0	14224
128	1, 3, 7, 9, 21, 23, 27, 29, 47	II	0	38227
128	1, 3, 5, 9, 13, 15, 19, 21, 29	II	0	22225
128	1, 3, 9, 11, 13, 15, 19, 21, 47	II	0	22225
128	1, 3, 9, 15, 19, 21, 23, 29, 47	II	0	21336
128	1, 3, 5, 9, 15, 19, 21, 23, 29	II	0	24892
128	1, 3, 11, 13, 15, 21, 27, 47, 55	II	0	21336
128	1, 3, 5, 7, 9, 11, 13, 19, 21	II	0	29337
128	1, 3, 5, 7, 11, 13, 21, 27, 55	II	0	14224
128	1, 3, 5, 7, 21, 23, 27, 29, 55	II	0	25781
128	1, 3, 5, 7, 9, 21, 23, 27, 29	II	0	25781
128	1, 3, 5, 7, 9, 13, 21, 27, 29	II	0	32004
128	XQ_{127}	II	0	56896
128	1, 3, 5, 7, 9, 11, 13, 21, 27	II	0	14224

n	S_1	Type	Weights						
			22	24	26	28	30	32	34
138	XQ_{137}	iso	321402	2356948	21533934	490138050	6648308245	77865259105	?

n	S_1	Type	Weights	
			20	24
152	1, 3, 5, 11, 17	II	1661	315590
152	1, 3, 5, 11, 15	II	755	290675
152	XQ_{151}	II	28690	717230
152	1, 3, 7, 11, 15	II	0	253680

6.2 Ternary Case

n	S_1	Weights		
		18	21	24
72	XQ_{71}	357840		
84	XQ_{83}	0	2368488	
84	$\mathcal{B}_{41}(0,1,-1)$	0	1259520	
88	$\mathcal{B}_{43}(1,1,-1)$	0	635712	
96	$\mathcal{B}_{47}(0,1,-1)$	0	0	15358848

7 Weight Distributions

In each of the following tables, the weight distribution of the code C is given as shown hereafter (for Type II codes). In that case only the A_{4i} are given, starting from $i = 0$. Moreover, in the binary case, we only give the first half of the distribution because $A_i = A_{n-i}$ for $n/2 < i \leq n$. For Type I or isodual codes, we only mention A_i, with $i \equiv 0 \pmod 2$ since they the all-one word and for ternary case we mention all the A_i, with $i \equiv 0 \pmod 3$.

C $[n,k,d]$		
A_0	A_{12}	$\ldots$
A_4	A_{16}	$\ldots$
A_8	A_{20}	$\ldots$

7.1 Binary Codes

XQ_{73} $[74,37,14]$						
1	0	0	1093905	254815041	6824006274	24737670308
0	0	8103	8481140	961185963	13019584383	
0	0	89133	53285328	2871214319	19988042838	

XQ_{89} $[90,45,18]$					
1	0	0	249109665	136522171665	3403264592178
0	0	274120	1650476520	402352364565	4842229755990
0	0	2819520	8806726665	983530112015	5773480681050
0	0	30530115	38261417997	2001805012350	

XQ_{97} $[98,49,16]$				
1	0	931588	50926874040	17462837266490
0	0	15038492	233809599765	33526663755928
0	0	166982396	894066458642	54576674050892
0	28518	1358454930	2860927585152	75458314701252
0	80801	9150616832	7695094033816	88704970251121

$\mathcal{B}_{53}(0,1,0)\,[108,54,20]$					
1	0	260442	48988609776	72678166237737	2057126174405640
0	0	5804136	296249593887	192293022909528	2564427604488075
0	0	74455407	1505946930696	436002802265628	2759782492680368
0	0	746650008	6456853758147	849260837522448	
0	0	6776021115	23472658198080	1423731100290057	

$\mathrm{XQ}_{113}\,[114,57,16]$					
1	0	450870	40222705272	130792381305999	9146861126267592
0	0	2795394	282354497019	410299386601373	13906428976796370
0	0	36685789	1670741392215	1108537936510704	18376732004342040
0	25764	468994974	8378734842802	2586605780563854	21121413533212377
0	0	4741799790	35791510616904	5223754097520833	

7.2 Doubly-Even Binary Codes

$\mathcal{B}_{59}(0,0,1)\,[120,60,20]$					
1	0	38266515	18824858869630	30531593455793640	335200293307691448
0	0	6114942900	397449398883096	116023986363853260	
0	71862	475562216745	4630515150103920	257257754706576195	

$\mathrm{XQ}_{127}\,[128,64,20]$					
1	0	12886944	18071400219840	94116098389459776	4051982879111857536
0	0	2935906752	552526728803616	549827720843995776	5193576979998072614
0	56896	320496430380	9491105395362624	1920594821540759360	

$\mathrm{XQ}_{151}\,[152,76,20]$				
1	0	39390352685	542987434102295230	2949674479653927921105
0	28690	5498418925790	9222363801666354938	8446025592483033745430
0	717230	430930711970510	98458872937411257395	15840564760239843844500
0	164250450	19714914844819780	670740325520625252110	19527364659006039947448

7.3 Ternary Codes

$\mathrm{XQ}_{71}\,[72,36,18]$				
1	0	3526708233024	33060319439473536	354030140213568
0	357840	59355639700560	44727780092682960	15690598310400
0	29772288	607803719012256	34777050459847488	230439513024
0	2688809760	3798836081510400	14918073393482560	701366400
0	125992569472	14443540225111008	3328268946790464	242112

XQ_{83} [84, 42, 21]				
1	0	1352212685085528	26733400018682175840	14629832742157920
0	2368488	20473212184431552	29675353243188471504	381318300016752
0	284708592	202449078688331520	20292322166081839440	3368236422096
0	27749368752	1310283952206924240	8274112484895023040	6324380216
0	1592706743376	5538706800932028360	1923875803617010488	168
0	57955685753952	15191881867463438592	239704188855678792	

$\mathcal{B}_{41}(0, 1, -1)$ [84, 42, 21]				
1	0	1352235251475360	26733400409832932928	14629839379331400
0	1259520	20473152007392000	29675352917229507264	381316825089312
0	307996920	202449207639130560	20292322391745737760	3368469305376
0	27516485472	1310283726543025920	8274112355944224000	6301091888
0	1594181670816	5538707126890992600	1923875863794050040	1109136
0	57949048580472	15191881476312681504	239704166289288960	

$\mathcal{B}_{43}(1, 1, -1)$ [88, 44, 21]				
1	0	1294153960207680	149357302340678914944	2082732674601397104
0	635712	25036242546864384	244362022826028476160	138180567030830016
0	120126864	321440977188929664	256787210074634276928	4155805506743616
0	13724386368	2750936673293043840	169471411253708788224	46760218984160
0	973104610368	15702733362100701840	68144098773399841872	137405652384
0	44026206285264	59598753754070017344	16023500794040249664	41268480

$\mathcal{B}_{47}(0, 1, -1)$ [96, 48, 24]				
1	0	505749122830203648	19981992658967285787648	454433488827015168
0	15358848	7072363949850708480	19059746824746748028736	7545675935390208
0	2714166528	68123018965819051008	11815486076969836320768	43161251173632
0	277096863744	452631266154565769472	4635854691597632596608	53269682688
0	18611299710528	2071548979724323089408	1111643974252030120704	2075712
0	828013100655744	6502086773568887367168	155474680695461541888	
0	24803529161845248	13891892673289405272576	11895672055160067200	

References

[1] G. F. M. Beenker, "A note on Extended Quadratic Residue Codes over GF(9) and Their Ternary Images", *IEEE Trans. Inform. Theory* **30**, (1984), 403–405.

[2] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann, *Codierungstheorie – Konstruktion und Anwendung linearer Codes*, Springer, Heidelberg, 1998.

[3] W. Bosma and J. Cannon, *The Magma Computational Algebra System for Algebra, Number Theory and Geometry (Version 2.9).* University of Sydney, School of Mathematics and Statistics, Computational Algebra Group, May 2002.

[4] A. E. Brouwer, "Bounds on the size of linear codes", in *Handbook of Coding Theory*, ed. V.S. Pless and W.C. Huffman. Elsevier Science, North-Holland (1998), 295–461.

[5] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes", *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[6] Y. Desaki, T. Fujiwara and T. Kasami, "The Weight Distributions of Extended Binary Primitive BCH Codes of Length 128", *IEEE Trans. Inform. Theory* **43**, (1997), 1364–1371.

[7] P. Gaborit, "Quadratic Double Circulant Codes over Fields", *J. Combin. Theory Ser. A* **97** (2002), 85–107.

[8] M. Karlin, "New binary coding results by circulant", *IEEE Trans. Inform. Theory* **15** (1969), 81–92.

[9] J. Leon, J. Masley and V. Pless, "Duadic Codes", *IEEE Trans. Inform. Theory* **30** (1984), 709–714.

[10] H. Lüneburg, "Gray-Codes", *Abh. Math. Sem. Hamburg* **52** (1982), 208–227.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[12] B. D. McKay, "autoson—a distributed batch system for UNIX workstation networks (version 1.3)", Tech. Rep. TR-CS-96-03, Computer Science Department, Australian National University, 1996.

[13] A. Nijenhuis and H. S. Wilf, *Combinatorial Algorithms*, 2nd ed., Academic Press, New York, 1978.

[14] V. Pless, "Symmetry Codes over GF(3) and new five designs", *J. Combin. Theory Ser. A* **12** (1972), 119–142.

[15] V. Pless, "Q-Codes", *J. Combin. Theory Ser. A* **43** (1986), 258–276.

[16] V. Pless, W. C. Huffman and R. A. Brualdi, "An introduction to algebraic codes", in *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Elsevier-Science, North-Holland (1998), 3–139.

[17] V. Pless, J. Masley and J. Leon, "On weights in duadic codes", *J. Combin. Theory Ser. A* **44** (1987), 6–21.

[18] E. M. Rains and N. J. A. Sloane, "Self-dual codes", in *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Elsevier Science, North-Holland (1998), 177–294.

[19] M. H. M. Smid, "Duadic Codes", *IEEE Trans. Inform. Theory* **33** (1987), 432–433.