J. Korean Math. Soc. **44** (2007), No. 5, pp. 1139–1162

OPTIMAL LINEAR CODES OVER $\mathbb{Z}_m$

STEVEN T. DOUGHERTY, T. AARON GULLIVER, YOUNG HO PARK, AND JOHN N. C. WONG

ABSTRACT. We examine the main linear coding theory problem and study the structure of optimal linear codes over the ring $\mathbb{Z}_m$. We derive bounds on the maximum Hamming weight of these codes. We give bounds on the best linear codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$ of lengths up to 6. We determine the minimum distances of optimal linear codes over $\mathbb{Z}_4$ for lengths up to 7. Some examples of optimal codes are given.

1. Introduction

The main coding problem for linear codes (in one of its forms) is to find the largest minimum weight for any linear code with a given length and cardinality over a given alphabet. The problem is widely studied for codes over fields but not for codes over rings. Over the past decade codes over rings have gained in importance for both practical and theoretical reasons. Codes over $\mathbb{Z}_4$ have been particularly of interest and we give special attention to those codes here. In general, the question is to find the maximum number of elements that can fit in a space where the distance between those elements is a maximum. Of course, these are two conflicting aims, namely, adding more vectors generally requires that the minimum distance between vectors reduces. This question has many applications outside of mathematics in information theory and many applications inside of mathematics, for example, in the study of lattices and designs. In this paper we shall survey the major results necessary for studying this question, add new results and solve the question using the results and computation for some small lengths.

Some families of codes are of particular interest because they are often the optimal codes for a particular set of parameters. For example, Maximum Distance Separable (MDS) codes and Maximum Distance with respect to Rank (MDR) codes are very useful in examining this fundamental question. We shall examine these codes as well.

We shall begin with some definitions. For any undefined terms from coding theory see [20] or [21]. For a more elementary introduction see [18]. For general

Received October 28, 2006.
2000 *Mathematics Subject Classification.* 94B05, 94B65.
Key words and phrases. linear codes, optimal codes, codes over rings.

results on codes over finite rings see [25]. A code C of length n is a subset of $\mathbb{Z}_m^n$. If the code is a submodule then we say that the code is linear. In this work all codes are assumed to be linear unless specified otherwise. The ambient space is attached with the standard inner product, i.e., $[v, w] = \sum v_i w_i$. We define the orthogonal to the code C by $C^\perp = \{v \mid [v, w] = 0 \text{ for all } w \in C\}$. The Hamming distance between two vectors is the number of coordinates in which they disagree. The minimum Hamming distance of a code, denoted by $d_H(C)$, is the smallest distance between any two distinct vectors. The Hamming weight of a codeword is the number of non-zero coordinates in the vector. For linear codes $d_H(C)$ coincides with the smallest non-zero Hamming weight in the code. Other weights will be defined later for various rings, for a given weight X we define $d_X(C)$ as the minimum weight of a non-zero vector for that weight. As usual we use $[n, k, d]$ to refer to a linear code of length n, rank k and minimum Hamming weight d and we use (n, M, d) to refer to a code (possibly non-linear) that has length n, M elements and minimum Hamming distance d.

For linear codes it is obvious that the minimum Hamming distance is the same as the minimum Hamming weight. Two codes are said to be equivalent if one can be formed from the other by permuting the coordinates and changing the signs of coordinates. This differs from the definition for codes over fields, which allows the more general multiplication of coordinates by units.

For a code C, the weight enumerator of the code for a given weight X is defined by

$$W_X(C) = \sum_{c \in C} x^{wt(c)},$$

where $wt(c)$ denotes the weight of the codeword c.

If $C = C^\perp$, a code is said to be self-dual. All self-dual codes over $\mathbb{Z}_4$ up to length 15 and some codes of length 16 have been classified [5, 23, 15]. All self-dual codes over $\mathbb{Z}_8$ up to length 6 and some codes of length 8 have been classified [6]. All self-dual codes over $\mathbb{Z}_9$ up to length 8 have been classified [2]. Beyond these codes, no classification of codes over $\mathbb{Z}_m$ has appeared in the literature, except for the optimal rate 1/2 codes over $\mathbb{Z}_4$ for lengths up to 8 [17].

2. Types and ranks

Unlike codes over fields we do not have dimension for codes over rings so we need to use their rank and type, which we shall now describe. We know from [12] that any finitely generated submodule of $\mathbb{Z}_m^n$ is isomorphic to

$$\mathbb{Z}_m/f_1\mathbb{Z}_m \oplus \mathbb{Z}_m/f_2\mathbb{Z}_m \oplus \cdots \oplus \mathbb{Z}_m/f_s\mathbb{Z}_m, \tag{1}$$

where f_i are positive integers with $f_1 \mid f_2 \mid \cdots \mid f_n \mid m$. For such a submodule C of $\mathbb{Z}_m^n$, define the *rank* of C as $|\{i \mid f_i \neq 1\}|$ and the free rank as $|\{i \mid f_i = m\}|$. We say that the code is a free code if the free rank is equal to the rank.

For codes over $\mathbb{Z}_{p^e}$ it is easy to produce a generator matrix from which we can read the rank. Any linear code over $\mathbb{Z}_{p^e}$ has a generator matrix which can

be put in the following form:

$$(2)\qquad \begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,s+1} \\ 0 & pI_{k_2} & pA_{2,3} & pA_{2,4} & \cdots & \cdots & pA_{2,s+1} \\ 0 & 0 & p^2 I_{k_3} & p^2 A_{3,4} & \cdots & \cdots & p^2 A_{3,s+1} \\ \vdots & \vdots & 0 & \ddots & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & p^{e-1} I_{k_s} & p^{e-1} A_{s,s+1} \end{pmatrix},$$

where $A_{i,j}$ are matrices in $\mathbb{Z}_{p^{e-i+1}}$. Note that this has appeared in incorrect forms often in the literature. Here the rank is simply the number of rows of the generator matrix. In this case the type is $\{(1)^{k_1}, (p)^{k_2}, (p^2)^{k_3}, \ldots, (p^{e-1})^{k_e}\}$ and has $\prod_{i=1}^{e} p^{(e-i+1)k_i}$ elements. The rate of a code over $\mathbb{Z}_m$ is $\frac{\log_m(|C|)}{n}$, for codes over $\mathbb{Z}_{p^e}$ this is realized as $\frac{k_1 + \frac{k_2}{p} + \cdots + \frac{k_{e-1}}{p^{e-1}}}{n}$.

It is not always possible for a matrix to be placed in this form for codes over $\mathbb{Z}_m$. For example, the code generated by $(3, 22)$ over $\mathbb{Z}_{36}$ cannot be put into this form, see [19] for a detailed study of this question. It does however generate a free code, even though it cannot be put into a form with a unit in the first coordinate. This is because of the following proposition.

Proposition 2.1. *Let* $v = (v_1, \ldots, v_n) \in \mathbb{Z}_m^n$ *and let* $d = \gcd(v_1, \ldots, v_n, m)$. *Then* $|\langle v \rangle| = \frac{m}{d}$.

Proof. First we see that $\frac{m}{d} v = 0$ so there are at most $\frac{m}{d}$ elements generated by v. Moreover $\frac{m}{d}$ is the smallest γ such that $\gamma v = 0$. Otherwise $\gamma v_i = 0$ for all i and $\frac{m}{\gamma}$ divides v_i for all i and $\frac{m}{\gamma} > d$ which is a contradiction since d is the greatest common divisor.

Assume $0 < \alpha < \beta < \frac{m}{d}$ and $\alpha v = \beta v$ then $(\alpha - \beta)v = 0$ which implies $\alpha - \beta = 0$ or $\alpha - \beta > \frac{m}{d}$. It must be that $\alpha - \beta = 0$ so $\alpha = \beta$. □

The situation for the generator matrices of codes over $\mathbb{Z}_m$ is much different than for codes over fields and even for codes over $\mathbb{Z}_{p^e}$. First we do not have the usual properties of linear independence since we have a module and not a vector space. Secondly, we do not have a form which is as easily described as the case for $\mathbb{Z}_{p^e}$.

We say that the codewords $v_1, \ldots, v_k$ generate C if every vector of C is a linear combination of the v_i, i.e., each $v \in C$ is of the form $\sum a_i v_i$ where $a_i \in \mathbb{Z}_m$. It is not as easy to describe a minimal generating set (basis) in this case. For a full description of the many nuances of this problem see [19].

The generator matrix form and the rank can be quite different for codes over $\mathbb{Z}_m$ than for the case for code over a field or over $\mathbb{Z}_{p^e}$. For example, consider the code generated by the vector $(2, 3)$ in $\mathbb{Z}_6^2$. By the previous proposition we have that $|\langle (2,3) \rangle| = 6$. Hence the rank is 1 but $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ also generates this code but would appear to have rank 2 by examining the generator matrix, it

does not have rank 2 however. Moreover, the second matrix cannot be brought into the form of the first matrix by elementary row operations. We can however describe the type. Namely if a code is of the form

$$\mathbb{Z}_m/f_1\mathbb{Z}_m \oplus \mathbb{Z}_m/f_2\mathbb{Z}_m \oplus \cdots \oplus \mathbb{Z}_m/f_n\mathbb{Z}_m, \tag{3}$$

then the code is said to be of *type* $\{(a_1)^{k_1}, (a_2)^{k_2}, (a_3)^{k_3}, \ldots, (a_s)^{k_s}\}$, where $a_1 < a_2 < \cdots < a_s < m$ and $a_1 = 1$, and has $\prod_{i=1}^{s}(\frac{m}{a_i})^{k_i}$ elements, where $a_i = \frac{m}{f_i}$ and $k_i = |\{j \mid f_j = f_i\}|$. For a description of the generator matrix see [19]. We can say that if a code has rank r then there exists a basis with r elements for that code by the above description. It follows that a code over $\mathbb{Z}_m$ of rank k is a free code if and only if the code has m^k elements and has rank k.

If C is a linear code of type $\{(a_1)^{k_1}, (a_2)^{k_2}, (a_3)^{k_3}, \ldots, (a_s)^{k_s}\}$ then $C^{\perp}$ is a linear code of type $\{1^{n-\sum k_i}, (\frac{m}{a_s})^{k_s}, \ldots, (\frac{m}{a_3})^{k_3}, (\frac{m}{a_2})^{k_2}\}$, see [19]. This gives that $|C||C^{\perp}| = m^n$.

If a set of vectors satisfies the usual definition of linear independence, i.e., $\sum \alpha_i v_i = 0$ implies $\alpha_i = 0$ for all i, then we note that the code generated by these vectors is a free code. A linear code can also be described in terms of its parity check matrix H, i.e., $v \in C$ if and only if $Hv^T = 0$. Similar to codes over fields we have the following.

The minimum Hamming weight of C is d if and only if any $d-1$ of the columns of H are linearly independent but some d are not. This follows from the following argument. Let L_i be the columns of the parity check matrix H. There exists a vector $v \in C$ of weight d if and only if $\sum \alpha_i L_i = 0$ where there are precisely d non-zero α_i. Hence if no $d-1$ are linearly dependent but some d are then the minimum weight of C is d.

However the result is not true if the columns are only independent in the sense that a linear combination of the vectors summing to 0 implies the coefficients are non-units, since a single column can be independent in this sense but be a multiple of a divisor of m and then C can have minimum distance 1 without there being an all zero column in H.

The well known Singleton bound for codes over any alphabet of size m (see [21] for example) gives that

$$d_H(C) \leq n - \log_m(|C|) + 1. \tag{4}$$

For linear codes it is also shown in [12] that

$$d_H(C) \leq n - \text{rank(C)} + 1. \tag{5}$$

This is a stronger bound in general unless the linear code is a free code in which case the bounds coincide.

We recall the following definition. If C is a code over $\mathbb{Z}_m$ of length n with $d_H(C) = n - \text{rank(C)} + 1$, then we say that C is a Maximum Distance with respect to Rank (MDR) code and if the rank is equal to the free rank then we

say that it is a Maximum Distance Separable (MDS) code. For a full description of these codes see [12].

3. Chinese remainder theorem

We shall describe how to use the Chinese Remainder Theorem to construct codes over $\mathbb{Z}_m$ where m is not a prime power.

Let $\Psi_r : \mathbb{Z}_m^n \to \mathbb{Z}_r^n$ with r dividing m, with

$$\Psi_r(c_1, \ldots, c_n) = (c_1 \pmod r, \ldots, c_n \pmod r).$$

If $m = \prod q_i^{e_i}$ where q_i is a prime with $q_i \neq q_j$, $i \neq j$ then define $\Psi : \mathbb{Z}_m^n \to \oplus \mathbb{Z}_{q_i^{e_i}}^n$ by

$$\Psi(c_1, \ldots, c_n) = (\Psi_{q_1^{e_1}}(c_1, \ldots, c_n), \Psi_{q_2^{e_2}}(c_1, \ldots, c_n), \ldots, \Psi_{q_k^{e_k}}(c_1, \ldots, c_n)).$$

The Chinese Remainder Theorem gives that the inverse map is a module isomorphism. Let $C_1, C_2, \ldots, C_k$ be codes where C_i is a code over $\mathbb{Z}_{q_i^{e_i}}$, and define the code

$$CRT(C_1, C_2, \ldots, C_k) = \{\Psi^{-1}(v_1, v_2, \ldots, v_k) \mid v_i \in C_i\}.$$

The code $CRT(C_1, C_2, \ldots, C_k)$ is called the Chinese product of codes C_1, C_2, $\ldots$, C_k. It is easy to see that $|CRT(C_1, C_2, \ldots, C_k)| = \prod_{i=1}^k |C_i|$. For a full description of these codes see [7] and [12].

Denote $\operatorname{supp}(v_1, v_2, \ldots, v_n) = \{j \mid v_j \neq 0\}$.

Lemma 3.1. *Suppose $m = rs$ with $(r, s) = 1$. Let $v \in \Psi_r(C)$. If $u \in C$ such that $\Psi_r(u) = v$ and $\Psi_s(u) = 0$, then* $\operatorname{supp}(v) = \operatorname{supp}(u)$. *In particular,* $wt(u) = wt(v)$.

Proof. We have $u = v + rw$ for some w. Clearly if $u_i = 0$, then $v_i = \Psi_r(u_i) = 0$. Conversely suppose $v_i = 0$. Then $u_i = rw_i$ and $\Psi_s(u)_i = rw_i = 0 \pmod s$. Since $(r, s) = 1$, this implies that $w_i = 0 \pmod s$. Thus $u_i = 0 \pmod m$, i.e., $u_i = 0$. □

Lemma 3.2. *Let $C = CRT(C_1, C_2, \ldots, C_k)$, then $d_H(C) = \min\{d_{C_i}\}$.*

Proof. By Lemma 3.1 if $v \in C_i$ then applying the CRT to v and the all 0 vector produces a vector with the same Hamming weight as v. Hence we have that $d_H(C)$ can be at most $\min\{d_{C_i}\}$. If there were a non-zero vector w in C with weight less than this, its projection to some $\mathbb{Z}_{q_i^{e_i}}$ would be a non-zero vector with weight less than the smallest of all the minimum weights of C_i, which is a contradiction. □

It is clear that any code over $\mathbb{Z}_m$ is the Chinese product of codes over rings with prime power cardinality. Hence we see that the fundamental questions of coding theory need to be examined over $\mathbb{Z}_{p^e}$ and then the results can be used to describe the more general case. Specifically, the best minimum weight possible for a code over $\mathbb{Z}_m$ is determined by the best possible minimum weights of codes over prime power rings.

4. MDS and MDR codes

We shall examine the structure MDS and MDR codes. These codes, when they exist, must be optimal since they meet the Singleton bound. Some of the results in this section were first shown in a different form in our paper [10].

Lemma 4.1. *If C is a linear MDS code over $\mathbb{Z}_m$ of rank r and type $\{a_1^{k_1}, a_2^{k_2}, \ldots, a_s^{k_s}\}$ then $k_i = 0$ for $i > 1$.*

Proof. If $k_i > 0$ for any $i > 1$ then $|C| < m^r$. The bound given in (5) prevents the code from meeting the bound given in (4). □

This means that any linear code that is MDS must be a free code.

Let $v \in C \subset \mathbb{Z}_{p^e}^n$ where C is an MDS code, then $p^{e-1}v$ has Hamming weight less than or equal to the Hamming weight of v. Hence the minimum weight vectors of C either have no coordinates with a multiple of p^{e-1} in them or they consist entirely of coordinates with a multiple of p in them.

Let C be an MDS code over $\mathbb{Z}_{p^e}$, which of course means that it is a free code, and let $C' = p^{e-1}C$, then by a result in [9] we have that $d_{C'} = d_C$. Let B be the code over $\mathbb{Z}_p$ formed by sending αp^{e-1} to α. We note that $|C'| = |B|$. It is well known that if C is an MDS code [12] then C is a free code with $|C| = (p^e)^k$. It follows that $|C'| = p^k$ and so B is an $[n, k, d]$ code. If C is MDS then we have $n - k + d = 1$ so B is an MDS code over $\mathbb{Z}_p$. This gives the following theorem.

Theorem 4.2. *If there exists an MDS code over $\mathbb{Z}_{p^e}$ of rank k and length n then there exists an MDS code over $\mathbb{Z}_p$ of dimension k and length n.*

Knowing that the only binary MDS codes are $R_n = \langle 111\cdots1\rangle$, $E_n = \langle 111\cdots1\rangle^{\perp}$, $\{0\}$, and $\mathbb{F}_2^n$, the natural corollary to this theorem is the following.

Corollary 4.3. *There are no non-trivial linear MDS codes over $\mathbb{Z}_{2^e}$.*

In [12] the following is shown:

Lemma 4.4. *If $C_{k_1}, C_{k_2}, \ldots, C_{k_s}$ are codes over $\mathbb{Z}_{k_1}, \mathbb{Z}_{k_2}, \ldots, \mathbb{Z}_{k_s}$ then if C_{k_i} is an MDR code for all i (not necessarily the same rank), then $CRT(C_{k_1}, C_{k_2}, \ldots, C_{k_s})$ is an MDR code.*

It is also shown that the converse of this is not true. This can happen because the projected code may have a lower rank. For example, a code over $\mathbb{Z}_6$ with generator matrix

$$\begin{pmatrix} I_3 & A_1 & A_2 \\ 0 & 2I_4 & 2A_3 \end{pmatrix} \tag{6}$$

has rank 7 but $\Psi_2(C)$ has rank 3.

However, if the code over $\mathbb{Z}_m$ is a free code with rank k, then for r dividing m, the code $\Psi_r(C)$ is a free code with rank k.

Lemma 4.5. *For any code C over $\mathbb{Z}_m$ and r dividing n, $d_H(C) \leq d_H(\Psi_r(C))$ unless $\Psi_r(C) \neq 0$.*

Proof. Take any nonzero $v_0 \in \Psi_r(C)$. Then there exists a $v \in C$ such that $v = v_0 + rw$ for some vector w. If $m = rs$, then $sv = sv_0 \in C$. Now we simply note that $wt_C(sv) = wt_C(sv_0) = wt_{\Psi_r(C)}(v_0)$, which proves the lemma. □

Lemma 4.6. *Suppose C is a free code of length n over $\mathbb{Z}_m$ and $m = rs$. Let $v_0 \in \mathbb{Z}_r^n \subset \mathbb{Z}_m^n$. Then $v_0 \in \Psi_r(C)$ if and only if $sv_0 \in C$.*

Proof. Suppose $v_0 \in \Psi_r(C)$. Then there exists some codeword $v \in C$ and a vector w such that $v_0 = v + rw$. Thus $sv_0 = sv \in C$. Conversely, suppose $sv_0 \in C$. Let $\varphi : \mathbb{Z}_m^n \to C \subset \mathbb{Z}_m^n$ be an isomorphism and $\varphi(e_i) = (g_{i1}, \ldots, g_{in})$. where the e_i are a standard basis for $\mathbb{Z}_m^n$. Then $C = \{uG \mid u \in \mathbb{Z}_m^n\}$ and the $n \times n$ matrix $G = (g_{ij})$ is invertible over $\mathbb{Z}_m$ since φ is an isomorphism. Let $sv_0 = uG$ for some $u \in \mathbb{Z}_m^n$. Then $sv_0 G^{-1} = u$, and hence we can write $u = su^*$, where $u^* \in \mathbb{Z}_r^n$. Now we have that $sv_0 = uG = su^*G$, which implies that $v_0 \equiv u^* \Psi_r(G) \pmod{r}$. Therefore $v_0 \in \Psi_r(C)$. □

Lemma 4.7. *Suppose C is a free code of length n over $\mathbb{Z}_m$ and $m = rs$. Then $d_H(\Psi_r(C)) = d_H(C)$ or $d_H(\Psi_s(C)) = d_H(C)$.*

Proof. Suppose $d_H(\Psi_r(C)) > d_H(C)$. Take $v \in C$ with $wt(v) = d_H(C)$. Since $wt(\Psi_r(v)) \leq wt(v) = d_H(C) < d_H(\Psi_r(C))$, we have $\Psi_r(v) = 0$, i.e., $v = rv_0$ for some $v_0 \in \mathbb{Z}_s^n$. By Lemma 4.6, $v_0 \in \Psi_s(C)$. Now $d_H(C) = wt(v) = wt(v_0) \geq d_H(\Psi_s(C)) \geq d_H(C)$. □

We have that $d_H(\Psi_r(C)) > d_H(C)$ if and only if the codewords of C of minimum weight all have the form rw for some vector w. Using this fact, it is easy to construct such codes. For example, let $C = \langle (6,6,0,0,0,0), (0,0,1,1,1,1) \rangle$ defined over $\mathbb{Z}_{12}$, then $d_H(\Psi_2(C)) = 4$ and $d_H(\Psi_6(C)) = 4$, while $d_H(C) = 2$. Therefore Lemma 4.7 does not hold for non-free codes.

Summarizing these results we have the following. Let C be a free code.

(i) If C is a code over $\mathbb{Z}_{p^m}$, then its projections $\Psi_{p^j}(C)$ all have the same minimum distance $d_H(C)$.

(ii) If C is a code over $\mathbb{Z}_m$, then its projections $\Psi_r(C)$ have minimum distance at least $d_H(C)$, and if $m = rs$ then one of $\Psi_r(C)$ and $\Psi_s(C)$ has minimum $d_H(C)$.

It follows that $d_H(\Psi_r(C)) \geq d_H(C)$. Hence, if C is an MDS code over $\mathbb{Z}_m$, then $\Psi_r(C)$ is an MDS code over $\mathbb{Z}_r$. This, together with Lemma 4.4 gives the following.

Theorem 4.8. *Let $m = \prod q_i^{e_i}$ where $q_i \neq q_j$, $i \neq j$. An MDS code of length n over $\mathbb{Z}_m$ exists if and only if an MDS code of length n exists over $\mathbb{Z}_{q_i^{e_i}}$.*

Of course there can be non-linear MDS codes when there are no linear ones. For example, it is well known that there exists a $(4, m^2, 3)$ code over $\mathbb{Z}_m$ if and only if there exists a pair of mutually orthogonal Latin squares (MOLS) of order m (see [18] for example). We know that there exists a pair of such squares for all values $m > 2$ except 6. Hence there are non-linear MDS codes over $\mathbb{Z}_m$ of length 4 for all $m \neq 2, 6$.

Theorem 4.9. *There are non-trivial MDS codes over all $\mathbb{Z}_{p^e}$ for $p > 2$.*

Proof. The code generated by

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

has $(p^e)^2$ elements and length 4. If $v_1 = (1,0,1,1)$ and $v_2 = (0,1,1,2)$ and $\alpha v_1 + \beta v_2$ has Hamming weight less than 3, then $\alpha + \beta = 0$ and $\alpha + 2\beta = 0$ giving that $\alpha = \beta = 0$ since the ring is not of characteristic 2. Hence the minimum weight is 3 and the code is MDS. □

Corollary 4.10. *There exist non-trivial MDS codes over all $\mathbb{Z}_m$, $m \neq 2^e$.*

Proof. Let $m = \prod q_i^{e_i}$ be the prime factorization of m. Simply apply the CRT map to non-trivial MDS codes over $\mathbb{Z}_{q_i^{e_i}}$. If $q_i = 2$ then the CRT of a trivial code with a non-trivial code still results in a non-trivial code. □

Let $m = \prod q_i$, $q_i \neq 2$, $q_i \neq q_j$, q_i prime.
For each q_i, $2 \leq r \leq q_i$, if $\{a_1, a_2, \ldots, a_{\ell-1}\} \subseteq \mathbb{Z}_q - \{0\}$, for each i.
Consider the following matrix.

(7)
$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 0 \\ a_1 & a_2 & \cdots & a_{\ell-1} & 0 & 0 \\ a_1^2 & a_2^2 & \cdots & a_{\ell-1}^2 & 0 & 0 \\ & & \vdots & & & \\ a_1^{r-2} & a_2^{r-2} & \cdots & a_{\ell-1}^{r-2} & 0 & 0 \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_{\ell-1}^{r-1} & 0 & 1 \end{pmatrix}$$

This matrix is a parity check matrix for an $[\ell+1, \ell+1-r, r+1]$ MDS code over $\mathbb{Z}_{q_i}$.

Theorem 4.11. *Let $m = \prod q_i$, $q_i \neq 2$, $q_i \neq q_j$, q_i prime. If $2 \leq \mu \leq \min\{q_i\}$ then there exists an MDS code over $\mathbb{Z}_m$ for all m, $2 \leq m \leq \mu$.*

Proof. Apply the CRT map to the MDS codes over $\mathbb{Z}_{q_i}$, which have the parity check matrix given in (7), as long as $m \leq \mu$. □

In [14], MDS codes over $\mathbb{Z}_m$ are related to a combinatorial structure by showing that there exists a set of s mutually orthogonal Latin k hypercubes of order m if and only if there exists a $[k+s, n^k, s+1]$ MDS code over $\mathbb{Z}_m$.

5. Torsion codes over $\mathbb{Z}_{p^e}$ of length n

Let C be a code over $\mathbb{Z}_{p^e}$. We make a similar definition to the one given in [11] and in [22]. Namely we define the following codes over the field $\mathbb{Z}_p$. For $1 \leq i \leq e$ define

(8)
$$Tor_i(C) = \{v \pmod p \mid p^i v \in C\}$$

and

$$Res(C) = Tor_0(C) = \{v \mid \text{there exists } u \text{ with } v + pu \in C\}. \tag{9}$$

Given a generator matrix over $\mathbb{Z}_{p^e}$ of the form:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,e-1} \\ 0 & pI_{k_1} & pA_{1,2} & \cdots & pA_{1,e-1} \\ 0 & 0 & p^2 I_{k_2} & \cdots & p^2 A_{2,e-1} \\ \vdots & & & & \\ 0 & 0 & \cdots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e-1} \end{pmatrix}, \tag{10}$$

the code $Tor_i(C)$ is the code over $\mathbb{Z}_p$ generated by:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,e-1} \\ 0 & I_{k_1} & A_{1,2} & \cdots & A_{1,e-1} \\ \vdots & & & & \\ 0 & \cdots & I_{k_i} & \cdots & A_{i,e-1} \end{pmatrix}. \tag{11}$$

We can compute the cardinality of C in general by

$$|C| = \prod_{j=0}^{e-1} \left(\frac{(p)^e}{(p)^j}\right)^{k_j} = (p)^{\sum_{j=0}^{e-1}(e-j)k_j}. \tag{12}$$

Given a code C over $\mathbb{Z}_{p^e}$ we have that

$$|Tor_i(C)| = \prod_{j=0}^{i} |p|^{k_j}, \tag{13}$$

and using (12) gives

$$\prod_{s=0}^{e-1} |Tor_s(C)| = \prod_{s=0}^{e-1} \prod_{j=0}^{i} |p|^{k_j} = \prod_{s=0}^{e-1} (p)^{\sum_{j<i} k_i} = (p)^{\sum (e-j)k_j} = |C|. \tag{14}$$

Hence we have the following theorem:

Theorem 5.1. *For a code C over $\mathbb{Z}_{p^e}$ we have that*

$$|C| = \prod_{s=0}^{e-1} |Tor_s(C)|.$$

If the code is free then rank(Tor$_0$(C)) = rank(C). Let T_i be the generator matrix of $Tor_i(C)$ and let R_i be the rows of T_i. We have that a generating set of C is

$$\{R_0, pR_1, \ldots, p^{e-1}R_{e-1}\}.$$

The following lemma can be found in the proof of Theorem 4.2 (iii) of [22].

Lemma 5.2. *If C is a code over $\mathbb{Z}_{p^e}$ then* $\min\{d_H(Tor_i(C))\} \geq d_H(C)$.

Proof. If $v \in Tor_i(C)$ then there is a vector with the same Hamming weight in C, namely $p^i v$ which gives the result. □

Let C be a linear code over $\mathbb{Z}_m$ where $C = CRT(C_1, \ldots, C_s)$, then the minimum weight of C is less than or equal to the minimum weight of $Tor_i(C_j)$ for all i, j.

The next theorem follows from the results of this section.

Theorem 5.3. *The maximum attainable minimum weight of a code over $\mathbb{Z}_m$ with $m = \prod_{i=1}^{s} q_i^{e_i}$, where q_i is a prime and $q_i \neq q_j$ for $i \neq j$, is bounded above by the best attainable weights of its component codes over prime order fields, $\mathbb{F}_{q_i}$.*

6. Bounds for linear codes

For a code C over $\mathbb{Z}_m$ the standard sphere packing bound still applies, namely an $(n, M, 2t+1)$ code satisfies

$$M\left(\binom{n}{0} + \binom{n}{1}(m-1) + \cdots + \binom{n}{t}(m-1)^t\right) \leq m^n.$$

The standard proof applies. The Plotkin bound for codes over any finite Frobenius ring was generalized in [16] and the Griesmer bound was generalized in [24].

Consider a code C over $\mathbb{Z}_{p^e}$ with a generator matrix of the form given in (2). Let C_i be the code generated by

$$(15) \qquad \begin{pmatrix} 0 & \cdots & p^i I_{k_{i+1}} & p^i A_{i+1,i+2} & p^i A_{i+1,i+3} & \cdots & p^i A_{i+1,s+1} \end{pmatrix}.$$

The elements in the vectors of C_i are all multiples of p^i. Let $\Phi_{p^i} : C_i \to \mathbb{Z}_{\frac{p^e}{p^i}}$ by $\Phi_{p^i}(jp^i) = j$.

Lemma 6.1. *Given the above construction, $\Phi_{p^i}(C_i)$ is a linear code over $\mathbb{Z}_{p^{e-i}}$ of length $n - \sum_{j<i} k_j$ and rank k_i with the same Hamming weight distribution as C_i.*

Proof. The proof is straightforward noticing that the initial coordinates with 0 in them have been deleted. □

This lemma shows that if there is a vector of Hamming weight h in C then there is a corresponding vector with the same Hamming weight in a code $\Phi_{p^i}(C_i)$ over $\mathbb{Z}_{p^{e-i}}$. Let $A_{p^e}(n, r)$ be the highest minimum weight possible for a linear code over $\mathbb{Z}_{p^e}$ of rank r and $A_{p^e}(n, \{k_1, k_2, \ldots, k_s\})$ be the highest minimum weight possible for a linear code over $\mathbb{Z}_{p^e}$ of type $\{k_1, k_2, \ldots, k_s\}$. Then we have the following theorem.

Theorem 6.2. $A_{p^e}(n, \{k_1, k_2, \ldots, k_s\}) \leq \min\{A_{p^{e-i}}(n - \sum_{j<i} k_j, k_i)\}$.

Let $A_m(n, r)$ be the highest minimum weight possible for a linear code over $\mathbb{Z}_m$ of length n and rank k. First, the following lemma is clear.

Lemma 6.3. *If $r_1 < r_2$, then $A_m(n, r_2) \leq A_m(n, r_1)$.*

Theorem 6.4. *Let $m = \prod_i p_i^{a_i}$ be the factorization of m into prime factors. Then*

$$A_m(n, r) = \max A_{p_i^{a_i}}(n, r).$$

Proof. For a code C over $\mathbb{Z}_m$, we know that $d_H(C) = \min_i d_H(\Psi_{p_i^{a_i}}(C))$. By a result of [19], the rank of C is the maximum of the ranks of $\Psi_{p_i^{a_i}}(C)$.

Let $d_{max} = A_{p_j^{a_j}}(n, r) = \max A_{p_i^{a_i}}(n, r)$. For $i \neq j$, choose C_i to be the repetition code $\langle 11 \cdots 1 \rangle$ over $\mathbb{Z}_{p_i^{a_i}}$ of rank 1 of length n, and take C_j to be the code of length n and rank r with minimum distance d_{max}. Then $C = CRT(\{C_i\}_i)$ has minimum distance d_{max}.

Suppose C is any code over $\mathbb{Z}_m$ of length n and rank r. Then there exists some j such that $\Psi_{p_j^{a_j}}(C)$ has rank r. Then

$$d_H(C) = \min_i d_H(\Psi_{p_i^{a_i}}(C)) \leq d_H(\Psi_{p_j^{a_j}}(C)) \leq A_{p_j^{a_j}}(n, r) \leq d_{max}.$$

This proves the theorem. □

We know from ([7]) that $CRT(C_1, C_2, \ldots, C_t)$ has cardinality $\prod |C_i|$ and has minimum Hamming weight $\min\{d_H(C_i)\}$. Let $B_m(n, M)$ be the highest minimum weight attainable from a code of length n over $\mathbb{Z}_m$ with M vectors.

This gives the following theorem:

Theorem 6.5. *If $m = \prod p_i^{a_i}$ is the factorization of m into prime power factors then*

$$B_m(n, Q) = \min\{B_{p_i^{a_i}}(n, Q_i)\}$$

where $\prod Q_i = Q$.

As an example of this theorem, it is clear that the best codes attainable for $\mathbb{Z}_6$ can be determined simply by examining the best binary and ternary codes. In general, the best codes attainable over $\mathbb{Z}_k$ can be determined by examining codes over the rings $\mathbb{Z}_{p^a}$ where p is a prime.

Let

$$M = M_r = \{w \in \mathbb{Z}_{p^e}^r \mid |\langle w \rangle| < p^e\} = p\mathbb{Z}_{p^e}^r.$$

Lemma 6.6. *Suppose $v_1, \ldots, v_{t-1} \in \mathbb{Z}_{p^e}^r$ are linearly independent. If $v_t \notin \langle v_1, \ldots, v_{t-1}, M \rangle$, then $v_1, \ldots, v_{t-1}, v_t$ are linearly independent.*

Proof. Let $\sum_{i=1}^{t} a_i v_i = 0$. If $a_t = 0$, then $a_i = 0$ for all i, and we are done. We assume that $a_t \neq 0$. If a_t is a unit, then $v_t \in \langle v_1, \ldots, v_{t-1} \rangle$, a contradiction. So suppose that $a_t = -\beta a$ for some divisor $a \neq 1, p^e$ of p^e and a unit β. Let $ab = p^e$. Then $\beta a v_t = \sum_{i=1}^{t-1} a_i v_i$. Multiplying both sides by b, we obtain $0 = \sum_{i=1}^{t-1} b a_i v_i$. Since $v_1, \ldots, v_{t-1}$ are linearly independent, we have that $ba_i = 0$ for all i. This means that $a \mid a_i$, say $a_i = ab_i$, for all i. Then $a(v_t - \sum_{i=1}^{t-1} b_i v_i) = 0$, i.e., $v_t = \sum_{i=1}^{t-1} b_i v_i + bw \in \langle v_1, \ldots, v_{t-1}, M \rangle$ for some w. This contradicts our assumption. □

Lemma 6.7. *If $v_1, \ldots, v_t \in \mathbb{Z}_m^r$ are linearly independent, then*

$$|\langle v_1, \ldots, v_t, M\rangle| = p^{(e-1)r+t}.$$

Proof. It is clear that

$$\langle v_1, \ldots, v_t, M\rangle = \{a_1v_1 + \cdots + a_tv_t + pw \mid 0 \leq a_i < p,\ w \in \mathbb{Z}_{p^e}^r\}.$$

Suppose that $a_1v_1 + \cdots + a_tv_t + pw = b_1v_1 + \cdots + b_tv_t + pu$. Then $(a_1 - b_1)v_1 + \cdots + (a_t - b_t)v_t + p(w - u) = 0$, which implies that $p^{e-1}(a_1 - b_1)v_1 + \cdots + p^{e-1}(a_t - b_t)v_t = 0$. By the linear independence, $p \mid a_i - b_i$, i.e., $a_i = b_i$ for all i. Since $|M| = p^{(e-1)r}$, the lemma is proved. □

Theorem 6.8. *Suppose*

$$\begin{pmatrix} n-1 \\ d-2 \end{pmatrix} < \frac{p^{n-k} - 1}{p^{d-2} - 1}.$$

Then there exists a free code over $\mathbb{Z}_{p^e}$ of length n and rank k with minimum distance d.

Proof. We shall construct an $(n-k)\times n$ parity check matrix H with the property that no $d-1$ columns are linearly dependent. The first column vector can be any vector $v_1 \notin M = M_r$, where $r = n - k$. Suppose we have chosen $t-1$ columns $v_1, v_2, \ldots, v_{t-1}$ so that no $d-1$ are linearly dependent. If

$$v_t \notin \cup\langle v_{i_1}, v_{i_2}, \ldots, v_{i_{d-2}}, M\rangle,$$

where the union is taken over all possible choices of $d-2$ columns from the $t-1$ columns, then no $d-1$ from the t columns $v_1, \ldots, v_t$ are linearly dependent. Such a vector v_t always exists if $|\cup\langle v_{i_1}, v_{i_2}, \ldots, v_{i_{d-2}}, M\rangle| < p^{er}$. We know that the size of this union is less than or equal to the number of ways of choosing $d-2$ columns from $t-1$ and multiplying by the size of the generated space and subtracting all but one copy of M which is common to all sets in the union. Then we have that for all $t \leq n$,

$$\begin{aligned}
&|\bigcup\langle v_{i_1}, v_{i_2}, \ldots, v_{i_{d-2}}, M\rangle| \\
&\leq \begin{pmatrix} t-1 \\ d-2 \end{pmatrix} |\langle v_1, v_2, \ldots, v_{d-2}, M\rangle| - \left(\begin{pmatrix} t-1 \\ d-2 \end{pmatrix} - 1\right)|M| \\
&\leq \begin{pmatrix} n-1 \\ d-2 \end{pmatrix} \left(p^{(e-1)r}p^{d-2} - p^{(e-1)r}\right) + p^{(e-1)r} \\
&= p^{(e-1)r}\left(\begin{pmatrix} n-1 \\ d-2 \end{pmatrix}(p^{d-2} - 1) + 1\right) \\
&< p^{er}.
\end{aligned}$$

This proves the theorem. □

Notice that the inequality is independent of e.

Consider the inequality $\begin{pmatrix} n-1 \\ d-2 \end{pmatrix} < \frac{p^{n-k}-1}{p^{d-2}-1}$. If $d > n-k+1$ then the right side of the equation is less than or equal to 1, so no codes with minimum weight greater than $n = k+1$ can exist. This is, of course, the well known Singleton bound. However, if $d = n-k+1$ we need

$$\begin{pmatrix} n-1 \\ n-k-1 \end{pmatrix} < \frac{p^{n-k}-1}{p^{n-k-1}-1}.$$

We see that $p < \frac{p^{n-k}-1}{p^{n-k-1}-1} < p+1$ and that $\begin{pmatrix} n-1 \\ n-k-1 \end{pmatrix}$ is a constant. This gives the following.

Theorem 6.9. *If* $p > \begin{pmatrix} n-1 \\ n-k-1 \end{pmatrix}$ *then there exists an MDS* $[n, k, n-k+1]$ *code over* $\mathbb{Z}_{p^e}$.

By the equivalence shown in [14] we have the following corollary.

Corollary 6.10. *For all* $p > \begin{pmatrix} n-1 \\ n-k-1 \end{pmatrix}$ *there exist* $n-k$ *Latin* k*-hypercubes of order* p^e.

Moreover using the Chinese Remainder Theorem we also have the following.

Corollary 6.11. *Let* $m = \prod p_i^{e_i}$ *with* $p_i \neq p_j$ *when* $i \neq j$. *If* $p_i > \begin{pmatrix} n-1 \\ n-k-1 \end{pmatrix}$ *then there exist* $[n, k, n-k+1]$ *MDS codes over* $\mathbb{Z}_m$.

7. Codes over $\mathbb{Z}_4$

Linear codes over $\mathbb{Z}_4$ have received a great deal of attention since their introduction with respect to the Gray map. Here we consider optimal linear codes over this ring up to length 7.

We shall describe two maps to the binary field. The first is the standard Gray map, namely $\psi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ by $\psi(0) = 00$, $\psi(1) = 01, \psi(2) = 11, \psi(3) = 10$. This map is a non-linear weight preserving map.

The second map is $\Phi : 2\mathbb{Z}_4 \to \mathbb{F}_2$ by $\Phi(2) = 1, \Phi(0) = 0$.

There are three weights attached to vectors over $\mathbb{Z}_4$. The Hamming weight of a vector is the number of non-zero coordinates in the vector. The Lee weight of the vector is the Hamming weight of its image under the Gray map ψ. The Lee weight of a vector $v = (v_1, v_2, \ldots, v_n)$ over $\mathbb{Z}_4$ is also $\sum \min\{v_i, 4 - v_i\}$. The Euclidean weight of a vector $v = (v_1, v_2, \ldots, v_n)$ is $\sum \min\{v_i^2, (-v_i)^2\}$. We denote the minimum Hamming weight of a code C by $d_H(C)$, the minimum Lee weight by $d_L(C)$ and the minimum Euclidean weight by $d_E(C)$.

Lemma 7.1. *If* C *is a linear code over* $\mathbb{Z}_4$ *with no vectors having a 1 or 3 in them then* $\Phi(C)$ *is a binary linear code with the same Hamming weights as* C.

Any linear code over $\mathbb{Z}_4$ is permutation equivalent to a code with generator matrix

$$\begin{pmatrix} I_{k_1} & A_1 & A_2 \\ 0 & 2I_{k_2} & 2A_3 \end{pmatrix}, \tag{16}$$

where I_k is the k by k identity. A code of this form is said to be type $\{1^{k_1}, 2^{k_2}\}$. It has rank $k_1 + k_2$ and contains $4^{k_1}2^{k_2}$ elements. The rate of the code is $(k_1 + \frac{k_2}{2})/n$.

Lemma 7.2. *If C is a code over $\mathbb{Z}_4$ then $d_L(C) \leq 2d_H(C)$ and $d_E(C) \leq 4d_H(C)$.*

Proof. Given a vector with Hamming weight d the highest possible Lee weight is if its only non-zero coordinates are 2, and in this case it has Lee weight $2d$. The same applies for the Euclidean weight except that this vector has Euclidean weight $4d$. □

This bound is in fact rarely met since the Euclidean and Lee weight of a coordinate with a unit in them is 1. Hence vectors with small Hamming weight with few coordinates with a 2 in them produce vectors with small Euclidean and Lee weights. If there are minimum weight vectors with no coordinates with a 2 in them then $d_H(C) = d_L(C) = d_E(C)$.

For codes over $\mathbb{Z}_4$, Lemma 4.1 gives that if C is a linear MDS code of type $\{1^{k_1}, 2^{k_2}\}$ then $k_2 = 0$.

Corollary 4.3 gives that there are no non-trivial linear MDS codes over $\mathbb{Z}_4$.

Of course there are non-linear $\mathbb{Z}_4$ MDS codes. For example, a $[4, 4^2, 3]$ code is formed by a pair of MOLS of order 4.

In [13] the following bounds were given:

$$\left\lfloor \frac{d_E - 1}{4} \right\rfloor \leq n - \text{rank(C)}, \tag{17}$$

and

$$\left\lfloor \frac{d_L - 1}{2} \right\rfloor \leq n - \text{rank(C)}. \tag{18}$$

A code meeting the bound in (17) is MEDR, and a code meeting the bound in (18) MLDR.

Theorem 7.3. *If C is MEDR or MLDR then C is an MDR code.*

Proof. Follows from Lemma 7.2. □

Theorem 7.4. *There are no non-trivial MDR codes over $\mathbb{Z}_4$.*

Proof. Assume C is an MDR code of type $\{1^{k_1}, 2^{k_2}\}$ over $\mathbb{Z}_4$ with generator matrix given by (10).

Consider the code C' generated by

$$\begin{pmatrix} 2I_{k_1} & 2A_1 & 2A_2 \\ 0 & 2I_{k_2} & 2A_3 \end{pmatrix}. \tag{19}$$

Then $E = \Phi(C')$ is a binary linear code with minimum weight equal to the minimum weight of C. Moreover the dimension of E is $k = k_1 + k_2$. Hence E is a binary MDS code. □

Corollary 7.5. *There are no non-trivial MEDR or MLDR codes over* $\mathbb{Z}_4$.

Proof. If a code is maximum distance separable with respect to rank with any weight then it is MDR with respect to the Hamming weight, therefore it is trivial by the previous theorem. □

7.1. Optimal Linear Codes

The definition of equivalence was given in Section 1. Note that if a column is multiplied by an element other than ± 1 in $\mathbb{Z}_m$ (such as 2 in $\mathbb{Z}_4$), it can change the Lee and Euclidean weight distribution of the code, thus resulting in inequivalent codes.

We denote by $A_2(n, k)$ the maximum minimum weight for a binary code of length n and dimension k. We denote by $A_4(n, k_1, k_2)$ the maximum minimum weight for a linear $\mathbb{Z}_4$ code of type $\{1^{k_1}, 2^{k_2}\}$.

Theorem 6.2 gives that $A_4(n, k_1, k_2) \leq \min\{A_2(n, k_1), A_2(n - k_1, k_2)\}$.

Tables 1, 3, 5 and 7 were obtained by using the theoretical bounds established above. Tables 2, 4, 6 and 8 were obtained through an exhaustive search of all inequivalent codes. The search considered all possible generator matrices of the form (16), noting that in this case both A_1 and A_3 can be considered as binary matrices. Equivalent codes were eliminated by performing all possibly equivalence transformations on a selected matrix and removing the resulting matrices.

For $k_1 = 0$, the optimal codes are given by $2C_2$, where C_2 is an optimal binary code with the required length and dimension. Thus $d_E = 2d_L = 4d_H$, and so only codes with $k_1 > 0$ will be considered further. In addition, $d_E = d_L = d_H = 1$ when $k_1 = n$.

For $k_1 = 1, k_2 = 0$, the optimal codes can easily be characterized. For the Hamming weight, the highest weight is achieved by a binary repetition code. For the Lee weight, suppose all coordinates are nonzero, and let j be the number of coordinates with value 2 in the generator matrix. The number of ones is then $n - j$. The weight of this codeword is $2j + n - j = n + j$. The negation of this codeword has the same weight. The other nonzero codeword has weight $2(n - j)$. Equating these two weights gives $j = n/3$, and this equality has integer j when n is a multiple of 3. For $n = 3, j = 1$, and we have the generator matrix

$$(112).$$

This code has $d_L = 4$, and an optimal code of length $n = 3m$ has $d_L = 4m$. It is easily shown that $d_L = 4m + 1$ for $n = 3m + 1$ and $d_L = 4m + 2$ for $n = 3m + 2$. Now consider the Euclidean weight. The weight of the codeword with j 2's is now $4j + n - j = n + 3j$. The negation of this codeword has the

same weight. The other nonzero codeword has weight $4(n-j)$. Equating these two weights gives $j = 3n/7$, and this equality has integer j when n is a multiple of 7. For $n = 7, j = 3$, and we have the generator matrix

$$(1111222).$$

This code has $d_E = 16$, and an optimal code of length $n = 7m$ has $d_L = 16m$. It is easily shown that $d_E = 16m + 1$ for $n = 7m + 1$, $d_E = 16m + 4$ for $n = 7m + 2$, $d_E = 16m + 6$ for $n = 7m + 3$, $d_E = 16m + 8$ for $n = 7m + 4$, $d_E = 16m + 11$ for $n = 7m + 5$, and $d_E = 16m + 12$ for $n = 7m + 6$.

TABLE 1. Bounds on Optimal Codes over $\mathbb{Z}_4$ of Lengths 1-4

n	k_1	k_2	d_H	d_L	d_E
1	1	0	1	2	4
1	0	1	1	2	4
2	1	0	2	4	8
2	0	1	2	4	8
2	2	0	1	2	4
2	1	1	1	2	4
2	0	2	1	2	4
3	1	0	3	6	12
3	0	1	3	6	12
3	2	0	2	4	8
3	1	1	2	4	8
3	0	2	2	4	8
3	3	0	1	2	4
3	2	1	1	2	4
3	1	2	1	2	4
3	0	3	1	2	4
4	1	0	4	8	16
4	0	1	4	8	12
4	2	0	2	4	8
4	1	1	3	6	12
4	0	2	2	4	8
4	3	0	2	4	8
4	2	1	2	4	8
4	1	2	2	4	8
4	0	3	2	4	8
4	4	0	1	2	4
4	3	1	1	2	4
4	2	2	1	2	4
4	1	3	1	2	4
4	0	4	1	2	4

For other code parameters, we provide some examples below. A complete list of all optimal codes can be obtained from the second author. The classification of optimal rate 1/2 codes can be found in [17]. Here $\mathbb{Z}_4$ codes are denoted by $[n, k_1, k_2]$.

There is a unique optimal Lee weight $[7, 3, 0]$ code with $d_L = 6$ given by

$$G_{7,1} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 1 & 3 & 2 & 3 \end{pmatrix}.$$

This code has Lee weight enumerator

$$W_L(C_{7,1}) = 1 + 42x^6 + 7x^8 + 14x^{10}.$$

This code is self-orthogonal, but does not have a linear binary image.

TABLE 2. Optimal Code Distances for Lengths 1-4 over $\mathbb{Z}_4$

n	k_1	k_2	d_H	d_L	d_E
1	1	0	1	1	1
1	0	1	1	2	4
2	1	0	2	2	4
2	0	1	2	4	8
2	2	0	1	1	1
2	1	1	1	2	2
2	0	2	1	2	4
3	1	0	3	4	6
3	0	1	3	6	12
3	2	0	2	2	2
3	1	1	2	2	4
3	0	2	2	4	8
3	3	0	1	1	1
3	2	1	1	2	2
3	1	2	1	2	3
3	0	3	1	2	4
4	1	0	4	5	8
4	0	1	4	8	16
4	2	0	2	4	4
4	1	1	2	4	6
4	0	2	2	4	8
4	3	0	2	2	2
4	2	1	2	2	3
4	1	2	2	4	4
4	0	3	2	4	8
4	4	0	1	1	1
4	3	1	1	2	2
4	2	2	1	2	2
4	1	3	1	2	4
4	0	4	1	2	4

TABLE 3. Bounds on Optimal Codes over $\mathbb{Z}_4$ of Length 5

n	k_1	k_2	d_H	d_L	d_E
5	1	0	5	10	20
5	0	1	5	10	20
5	2	0	3	6	12
5	1	1	4	8	16
5	0	2	3	6	12
5	3	0	2	4	8
5	2	1	3	6	12
5	1	2	2	4	8
5	0	3	2	4	8
5	4	0	2	4	8
5	3	1	2	4	8
5	2	2	2	4	8
5	1	3	2	4	8
5	0	4	2	4	8
5	5	0	1	2	4
5	4	1	1	2	4
5	3	2	1	2	4
5	2	3	1	2	4
5	1	4	1	2	4
5	0	5	1	2	4

There is a unique optimal Lee weight $[7, 3, 3]$ code with $d_L = 4$ given by

$$G_{7,2} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix},$$

TABLE 4. Optimal Code Distances for Length 5 over $\mathbb{Z}_4$

n	k_1	k_2	d_H	d_L	d_E
5	1	0	5	6	11
5	0	1	5	10	20
5	2	0	3	4	6
5	1	1	3	5	8
5	0	2	3	6	12
5	3	0	2	3	3
5	2	1	2	4	4
5	1	2	2	4	8
5	0	3	2	4	8
5	4	0	2	2	2
5	3	1	2	2	3
5	2	2	2	2	4
5	1	3	2	4	4
5	0	4	2	4	8
5	5	0	1	1	1
5	4	1	1	2	2
5	3	2	1	2	2
5	2	3	1	2	3
5	1	4	1	2	4
5	0	5	1	2	4

TABLE 5. Bounds on Optimal Codes over $\mathbb{Z}_4$ of Length 6

n	k_1	k_2	d_H	d_L	d_E
6	1	0	6	12	24
6	0	1	6	12	24
6	2	0	4	8	16
6	1	1	5	10	20
6	0	2	4	8	16
6	3	0	3	6	12
6	2	1	4	8	16
6	1	2	3	6	12
6	0	3	3	6	12
6	4	0	2	4	8
6	3	1	3	6	12
6	2	2	2	4	8
6	1	3	2	4	8
6	0	4	2	4	8
6	5	0	2	4	8
6	4	1	2	4	8
6	3	2	2	4	8
6	2	3	2	4	8
6	1	4	2	4	8
6	0	5	2	4	8
6	6	0	1	2	4
6	5	1	1	2	4
6	4	2	1	2	4
6	3	3	1	2	4
6	2	4	1	2	4
6	1	5	1	2	4
6	0	6	1	2	4

and a unique optimal Lee weight $[7, 4, 1]$ code with $d_L = 4$ given by

$$G_{7,3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 \end{pmatrix}.$$

TABLE 6. Optimal Code Distances for Length 6 over $\mathbb{Z}_4$

n	k_1	k_2	d_H	d_L	d_E
6	1	0	6	8	12
6	0	1	6	12	24
6	2	0	4	6	8
6	1	1	4	6	11
6	0	2	4	8	16
6	3	0	3	4	6
6	2	1	4	4	8
6	1	2	3	5	8
6	0	3	3	6	12
6	4	0	2	3	3
6	3	1	2	4	4
6	2	2	2	4	6
6	1	3	2	4	8
6	0	4	2	4	8
6	5	0	2	2	2
6	4	1	2	2	2
6	3	2	2	2	4
6	2	3	2	4	4
6	1	4	2	4	6
6	0	5	2	4	8
6	6	0	1	1	1
6	5	1	1	2	2
6	4	2	1	2	2
6	3	3	1	2	3
6	2	4	1	2	4
6	1	5	1	2	4
6	0	6	1	2	4

Both codes have Lee weight enumerator

$$W_L(C_{7,2}) = 1 + 77x^4 + 168x^6 + 203x^8 + 56x^{10} + 7x^{12},$$

but only $C_{7,2}$ has a linear binary image (the unique optimal binary $[14, 9, 4]$ code).

There is a unique optimal Euclidean weight $[6, 2, 1]$ code with $d_E = 8$ given by

$$G_{6,1} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 1 & 2 & 3 & 1 \\ 0 & 0 & 2 & 0 & 2 & 0 \end{pmatrix}.$$

This code has Euclidean weight enumerator

$$W_E(C_{6,1}) = 1 + 27x^8 + 3x^{16} + x^{24}.$$

There are two optimal Euclidean weight $[7, 3, 0]$ codes with $d_E = 8$ given by

$$G_{7,4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix},$$

and

$$G_{7,5} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 1 & 3 & 2 & 3 \end{pmatrix}.$$

TABLE 7. Bounds on Optimal Codes over $\mathbb{Z}_4$ of Length 7

n	k_1	k_2	d_H	d_L	d_E
7	1	0	7	14	28
7	0	1	7	14	28
7	2	0	4	8	16
7	1	1	6	12	24
7	0	2	4	8	16
7	3	0	4	8	16
7	2	1	4	8	16
7	1	2	4	8	16
7	0	3	4	8	16
7	4	0	3	6	12
7	3	1	4	8	16
7	2	2	3	6	12
7	1	3	3	6	12
7	0	4	3	6	12
7	5	0	2	4	8
7	4	1	3	6	12
7	3	2	2	4	8
7	2	3	2	4	8
7	1	4	2	4	8
7	0	5	2	4	8
7	6	0	2	4	8
7	5	1	2	4	8
7	4	2	2	4	8
7	3	3	2	4	8
7	2	4	2	4	8
7	1	5	2	4	8
7	0	6	2	4	8
7	7	0	1	2	4
7	6	1	1	2	4
7	5	2	1	2	4
7	4	3	1	2	4
7	3	4	1	2	4
7	2	5	1	2	4
7	1	6	1	2	4
7	0	7	1	2	4

These codes have Euclidean weight enumerators

$$\begin{aligned} W_E(C_{7,4}) &= 1 + 27x^8 + 20x^{10} + 3x^{16} + 12x^{18} + x^{24}, \\ W_E(C_{7,5}) &= 1 + 42x^8 + 21x^{16}. \end{aligned}$$

The first code has a linear binary image (a [14,6,4] code), while the second code is self-orthogonal.

There is a unique optimal Euclidean weight $[7, 4, 3]$ code with $d_E = 3$ given by

$$G_{7,6} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

TABLE 8. Optimal Code Distances for Length 7 over $\mathbb{Z}_4$

n	k_1	k_2	d_H	d_L	d_E
7	1	0	7	9	16
7	0	1	7	14	28
7	2	0	4	6	11
7	1	1	4	8	12
7	0	2	4	8	16
7	3	0	4	6	8
7	2	1	4	6	8
7	1	2	4	6	11
7	0	3	4	8	16
7	4	0	3	4	4
7	3	1	3	4	6
7	2	2	3	4	8
7	1	3	3	6	8
7	0	4	3	6	12
7	5	0	2	2	3
7	4	1	2	4	4
7	3	2	2	4	4
7	2	3	2	4	6
7	1	4	2	4	8
7	0	5	2	4	8
7	6	0	2	2	2
7	5	1	2	2	2
7	4	2	2	2	3
7	3	3	2	4	4
7	2	4	2	4	4
7	1	5	2	4	6
7	0	6	2	4	8
7	7	0	1	1	1
7	6	1	1	2	2
7	5	2	1	2	2
7	4	3	1	2	3
7	3	4	1	2	4
7	2	5	1	2	4
7	1	6	1	2	4
7	0	7	1	2	4

This code has Euclidean weight enumerator

$$\begin{aligned} W_E(C_{7,6}) &= 1 + 56x^3 + 119x^4 + 352x^7 + 357x^8 + 336x^{11} + 371x^{12} \\ &\quad + 224x^{15} + 147x^{16} + 56x^{19} + 21x^{20} + 7x^{24} + x^{28}, \end{aligned}$$

and has a linear binary image (a [14,11,2] code).

8. Codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$

Using the results we have attained so far we shall give the best linear codes (in terms of the Hamming distance) of a given length and given rank for codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$.

Any linear code over $\mathbb{Z}_8$ is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A_1 & A_2 & A_3 \\ 0 & 2I_{k_2} & 2A_4 & 2A_5 \\ 0 & 0 & 4I_{k_3} & 4A_6 \end{pmatrix}, \tag{20}$$

and any linear code over $\mathbb{Z}_9$ is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A_1 & A_2 \\ 0 & 3I_{k_2} & 3A_3 \end{pmatrix}, \tag{21}$$

where I_k is the k by k identity matrix.

Codes over $\mathbb{Z}_8$ have type $\{1^{k_1}, 2^{k_2}, 4^{k_3}\}$ and rank $k_1+k_2+k_3$. An $[n, k_1, k_2, k_3]$ $\mathbb{Z}_8$ code contains $8^{k_1}4^{k_2}2^{k_3}$ elements and has rate $(k_1 + \frac{k_2}{2} + \frac{k_3}{4})/n$.

An $[n, k_1, k_2]$ code over $\mathbb{Z}_9$ has type $\{1^{k_1}, 3^{k_2}\}$. It has rank $k_1 + k_2$ and contains $9^{k_1}3^{k_2}$ elements. The rate of this code is $(k_1 + \frac{k_2}{3})/n$.

Bounds on the Hamming weight of optimal codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$ up to length 6 for a given rank are given in Table 9. One may notice that these distances are equal to the bounds on binary and ternary codes. This is not surprising, as a construction which meets these bounds is $4G_2$ for $\mathbb{Z}_8$ and $3G_3$ for $\mathbb{Z}_9$, where G_2 and G_3 are generator matrices for optimal binary and ternary codes, respectively.

TABLE 9. Bounds on Optimal Codes

n	rank	$d_H - \mathbb{Z}_8$	$d_H - \mathbb{Z}_9$
1	1	1	1
2	1	2	2
2	2	1	1
3	1	3	3
3	2	2	2
3	3	1	1
4	1	4	4
4	2	2	3
4	3	2	2
4	4	1	1
5	1	5	5
5	2	3	3
5	3	2	2
5	4	2	2
5	5	1	1
6	1	6	6
6	2	4	4
6	3	3	3
6	4	2	2
6	5	2	2
6	6	1	1

References

[1] T. Abualrub and R. Oehmke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inform. Theory **49** (2003), no. 9, 2126–2133.

[2] J. M. P. Balmaceda, A. L. Rowena, and F. R. Nemenzo, *Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$*, Discrete Math. (to appear).

[3] T. Blackford, *Cyclic codes over Z_4 of oddly even length*, Discrete Appl. Math. **128** (2003), no. 1, 27–46.

[4] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes Cryptogr. **6** (1995), no. 1, 21–35.
[5] J. H. Conway and N. J. A. Sloane, *Self-dual codes over the integers modulo* 4, J. Combin. Theory Ser. A **62** (1993), no. 1, 30–45.
[6] S. T. Dougherty, T. A. Gulliver, and J. N. C. Wong, *Self-dual codes over* $\mathbb{Z}_8$ *and* $\mathbb{Z}_9$, Des. Codes Cryptogr. **41** (2006), no. 3, 235–249.
[7] S. T. Dougherty, M. Harada, and P. Sole, *Self-dual codes over rings and the Chinese remainder theorem*, Hokkaido Math. J. **28** (1999), no. 2, 253–283.
[8] S. T. Dougherty and S. Ling, *Cyclic codes over* $\mathbb{Z}_4$ *of even length*, Des. Codes Cryptogr. **39** (2006), no. 2, 127–153.
[9] S. T. Dougherty, S. Y. Kim, and Y. H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), no. 1-3, 123–135.
[10] S. T. Dougherty and Y. H. Park, *Codes over the p-adic integers*, Des. Codes Cryptogr. **39** (2006), no. 1, 65–80.
[11] ———, *On modular cyclic codes*, Finite Fields Appl. **13** (2007), no. 1, 31–57.
[12] S. T. Dougherty and K. Shiromoto, *MDR codes over* Z_k, IEEE Trans. Inform. Theory **46** (2000), no. 1, 265–269.
[13] ———, *Maximum distance codes over rings of order 4*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 400–404.
[14] S. T. Dougherty and T. A. Szczepanski, *Latin k-hypercubes*, submitted.
[15] J. Fields, P. Gaborit, J. S. Leon, and V. Pless, *All self-dual* Z_4 *codes of length* 15 *or less are known*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 311–322.
[16] M. Greferath, G. McGuire, and M. O'Sullivan, *On Plotkin-optimal codes over finite Frobenius rings*, J. Algebra Appl. **5** (2006), no. 6, 799–815.
[17] T. A. Gulliver and J. N. C. Wong, *Classification of Optimal Linear* $\mathbb{Z}_4$ *Rate 1/2 Codes of Length* ≤ 8, submitted.
[18] R. Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series. The Clarendon Press, Oxford University Press, New York, 1986.
[19] Y. H. Park, *Modular Independence and Generator Matrices for Codes over* $\mathbb{Z}_m$, submitted.
[20] W. C. Huffman and V. S. Pless, *Fundamentals of Error-correcting Codes*, Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003.
[21] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, Amsterdam, 1977.
[22] G. H. Norton and A. Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 1060–1067.
[23] V. Pless, J. S. Leon, and J. Fields, *All* Z_4 *codes of type II and length* 16 *are known*, J. Combin. Theory Ser. A **78** (1997), no. 1, 32–50.
[24] K. Shiromoto and L. Storme, *A Griesmer Bound for Linear Codes over Finite Quasi-Frobenius Rings*, Discrete Appl. Math. **128** (2003), no. 1, 263–274.
[25] J. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

STEVEN T. DOUGHERTY
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SCRANTON
SCRANTON, PA 18510, U. S. A.
E-mail address: doughertys1@Scranton.edu

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC
Victoria, BC V8W 3P6, Canada
E-mail address: agullive@ece.uvic.ca

Young Ho Park
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
E-mail address: yhpark@kangwon.ac.kr

John N. C. Wong
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC
Victoria, BC V8W 3P6, Canada