1

A Database of $\mathbb{Z}_4$ Codes

NUH AYDIN AND TSVETAN ASAMOV

Abstract

There has been much research on codes over $\mathbb{Z}_4$, sometimes called quaternary codes, for over a decade. Yet, no database is available for best known quaternary codes. This work introduces a new database for quaternary codes. It also presents a new search algorithm called genetic code search (GCS), as well as new quaternary codes obtained by existing and new search methods.

Keywords: *Quaternary codes, binary codes, cyclic codes, quasicyclic codes, genetic code search.*

1. INTRODUCTION

One of the main problems of coding theory is to construct codes with best possible parameters. There are databases of best known codes over small finite fields. For many years the online table [9] has been the primary source of the records of the best known codes over small fields. Recently, it is announced that this table is discontinued due to the existence of [15] which often has more explicit information on constructions. The computer algebra system MAGMA [8] has such a database too. Moreover, a table of best known binary non-linear codes is available at [18].

For over a decade there has been intensive research on codes over $\mathbb{Z}_4$, integers modulo 4, sometimes called quaternary codes. The term "quaternary code" has been used both for codes over $\mathbb{Z}_4$ and for codes over $\mathbb{F}_4$, the finite field with 4 elements. In this paper, we shall use the term exclusively for $\mathbb{Z}_4$ codes. Among other results, some good quaternary codes have been constructed [10],[7],[23], and [5]. Self-dual codes over $\mathbb{Z}_4$ of length up to 9 are classified in [11], and this is extended to length 15 in [14] (16 for Type II codes in [20]). Rains has classified optimal self-dual codes over $\mathbb{Z}_4$ in [22]. A large number of self-orthogonal quasi-twisted (QT) $\mathbb{Z}_4$ codes have also been constructed [17]. Despite all this research, no database of best known quaternary codes is available. The development of such a table has been started in [5]. We now have compiled a database of quaternary codes. It is available at

J. of Combinatorics, Information & System Sciences Vol. **34** (2009) No. 1-4, pages 1-12

Corresponding author email:

http://Z4Codes.info/ and it is being updated continually. Unlike the tables at [15], we do not overwrite the existing entries when they are improved but rather keep both the old and the new results. This strategy is chosen primarily based on the fact that several different metrics on quaternary codes, i.e. Hamming, Euclidean and Lee distance, have been considered by the researchers. Moreover, for the sake of easier communication, we have decided to provide researchers with administrative privileges that would allow them to add their new results to the table, as well as edit the existing entries. Accounts can be acquired by contacting the database editors via email.

In addition to the creation of the database, we have also devised and implemented some search algorithms to find new quaternary codes. The paper also describes and reports the results of these searches. One of the search methods we consider in this paper is the further exploration of the class of quasi-cyclic codes, which has been the source of many of the new codes discovered in recent years. The other method is called the "progressive dimension growth" (PDG) which is introduced recently in [4] for fields. In our work, it is modified for the ring $\mathbb{Z}_4$ and the Lee metric. Finally, extending some of the ideas behind PDG, we implemented a new algorithm called "genetic code search" (GCS) that has produced better results than PDG over $\mathbb{Z}_4$. The following sections give more information about the algorithms We have used MAGMA for all computations.

2. BASIC FACTS ON QUATERNARY CODES

A *code* C of length n over $\mathbb{Z}_4$ is a subset of $\mathbb{Z}_4^n$. C is a *linear code* over $\mathbb{Z}_4$ if it is an additive subgroup of $\mathbb{Z}_4^n$, hence a submodule of $\mathbb{Z}_4^n$. In this paper we will consider only linear codes over $\mathbb{Z}_4$. An element of C is called a *codeword* and a *generator matrix* is a matrix whose rows generate C. The *Hamming weight* $w_H(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_4^n$ is $|\{i : x_i \neq 0\}|$. The *Lee weight* $w_L(x)$ of a vector x is $\sum_{i=1}^{n} \min\{|x_i|, |4 - x_i|\}$.

The Hamming and Lee distances $d_H(x, y)$ and $d_L(x, y)$ between two vectors x and y are $w_H(x - y)$ and $w_L(x - y)$, respectively. The minimum Hamming and Lee weights, d_H and d_L, of C are the smallest Hamming and Lee weights, respectively, amongst all non-zero codewords of C.

The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is the coordinate-wise extension of the function from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by $0 \to (0, 0), 1 \to (1, 0), 2 \to (1, 1), 3 \to (0, 1)$. The image, $\phi(C)$, under the Gray map of a linear code C over $\mathbb{Z}_4$ of length n is a (in general non-linear) binary code of length $2n$. The Gray map is an isometry from $(\mathbb{Z}_4^n, w_L)$ to $(\mathbb{Z}_2^{2n}, w_H)$. Therefore, the minimum Hamming weight of $\phi(C)$ is equal to the minimum Lee weight of C.

Two codes are said to be *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called *permutation-equivalent.* Any linear code C over $\mathbb{Z}_4$ is permutation-equivalent to a code with generator matrix G of the form

$$G = \begin{bmatrix} I_{k_1} & A_1 & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2A_2 \end{bmatrix}, \tag{1}$$

where A_1, A_2, B_1, and B_2 are matrices with entries 0 or 1 and I_k is the identity matrix of order k. Such a code has size $4^{k_1}2^{k_2}$. The code is a free module if and only if $k_2 = 0$. If C has length n and minimum Lee weight d_L, then it is referred to as an $[n, 4^{k_1}2^{k_2}, d_L]$-code.

2.1 CYCLIC CODES OVER $\mathbb{Z}_4$

A cyclic code over $\mathbb{Z}_4$ is a $\mathbb{Z}_4$-linear code which is invariant under cyclic shifts where the cyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ over $\mathbb{Z}_4$ is the m-tuple $(x_{m-1}, x_0, \ldots, x_{m-2})$. Similarly to the case of finite fields, cyclic codes over $\mathbb{Z}_4$ of length n are ideals in the ring $\frac{\mathbb{Z}_4[x]}{\langle x^n-1\rangle}$ under the usual identification of vectors with polynomials. Although algebraically cyclic codes have the same structure over fields and over $\mathbb{Z}_4$ (ideals in a factor ring), the fact that $\mathbb{Z}_4[x]$ is not a unique factorization domain makes it more challenging to find all cyclic codes over $\mathbb{Z}_4$. For instance, computer algebra systems (such as Magma and Maple), cannot directly provide factorizations of $x^n - 1$ for an arbitrary n. When n is odd, it is easier to obtain a factorization of $x^n - 1$ and hence to find all cyclic codes of length n. For an even n, the situation is much harder. In fact, the factorization is not unique in that case. In this paper we consider only cyclic codes of odd length over $\mathbb{Z}_4$. For the case of odd n some of the most important facts about ideals of the relevant ring and the factorization of $x^n - 1$ are summarized below, and they can be found in [21], [25] or [27]. For the case of even n, we refer the reader to [1],[2], and [3].

For an odd positive integer n, $x^n - 1$ can be factored into a product of finitely many pairwise coprime basic irreducible polynomials over $\mathbb{Z}_4$. Also, this factorization is unique up to ordering of the factors [21, 27]. In fact, we have the following: if $f_2(x) | (x^n - 1)$ in $\mathbb{Z}_2[x]$ then there is a unique, monic polynomial $f(x) \in \mathbb{Z}_4[x]$ such that $f(x) | (x^n - 1)$ in $\mathbb{Z}_4[x]$ and $\overline{f(x)} = f_2(x)$, where $\overline{f(x)}$ denotes the reduction of $f(x)$ modulo 2 [27]. The polynomial $f(x)$ is called the Hensel lift of $f_2(x)$. There are well–known methods of finding this polynomial, such as Graeffe's method [27]. Therefore, there is a one–to–one correspondence between irreducible factors of $x^n - 1$ over $\mathbb{Z}_2$ and irreducible factors of $x^n - 1$ over $\mathbb{Z}_4$.

Once the factorization of $x^n - 1$ over $\mathbb{Z}_4$ is obtained, the ideals of $R := \frac{\mathbb{Z}_4[x]}{\langle x^n - 1 \rangle}$ can be determined. For an odd positive integer n, any ideal I of the ring R has a generator of the form a $I = \langle f(x)h(x), 2f(x)g(x) \rangle$ where $f(x)g(x)h(x) = x^n - 1$ [21, 27]. Moreover, $|I| = 4^{\deg g(x)} 2^{\deg h(x)}$. It follows that the number of cyclic codes of length n is 3^r, where r is the number of irreducible factors of $x^n - 1$ [21].

Finally, it can be shown that any ideal of R, for an odd n, is a principle ideal, with a generator of the form $p(x) = f(x)h(x) + 2f(x)$ (or equivalently $p(x) = f(x)h(x) + 2f(x)g(x)$) where $f(x)$, $g(x)$, $h(x)$ are as above [21, 27].

Remark 1: When $x^n - 1$ has r irreducible factors over a field, the total number of cyclic codes is 2^r. We have a larger number over $\mathbb{Z}_4$ due to the existence of non–free codes (over a field all codes are free).

Remark 2: The generator polynomial $p(x)$ of an ideal of R described above does not necessarily divide $x^n - 1$. For example, let $n = 3$, $f(x) = 1$, and $h(x) = x - 1$, then $p(x) = x + 1$ and $p(x) \nmid (x^3 - 1)$. When $h(x) = 1$, $p(x) = 3f(x) = -f(x)$ does divide $x^n - 1$. It is shown in [7] that the cyclic code generated by $p(x)$ is a free module if and only if $p(x)$ divides $x^n - 1$.

2.2. Quasi-Cyclic Codes over $\mathbb{Z}_4$

Much research has focused on the class of quasi-cyclic (QC) and the related class of quasi-twisted (QT) codes, and many new codes over small finite fields have been discovered within these classes. Some of these results can be found in [6],[12, 13],[16] and [24]. In addition to the case of a field, QC codes over rings, especially over $\mathbb{Z}_4$, have been studied as well. QC codes over $\mathbb{Z}_4$ are first studied in [7], where a number of "good" quaternary codes are obtained. A quaternary linear code C with parameters $[n, 4^{k_1}2^{k_2}, d]$ (where d is the Lee weight) is called *good* if $d > d'$, where d' is the minimum distance of a best known binary linear code of length $2n$, and dimension $2k_1 + k_2$, i.e. if the Gray image of C has a larger minimum distance than the comparable binary linear code. Similarly, a quaternary code will be called *decent* if its Gray image has the same parameters as the best known binary code (i.e., if $d = d'$). The reason for this type of comparison is that even though the Gray image of a quaternary code is most likely non-linear, we do not have any other means of testing how good the parameters of a $\mathbb{Z}_4$ code are due to the facts that

a) the table [18] is much smaller than the tables for binary linear codes (it only goes up to minimum distance 29), and

b) there are no extensive tables of quaternary codes.

We believe that the table presented in this paper will meet a need in this area. The researchers are welcome to report and enter their codes to this database.

Next, we summarize some of the basic facts concerning the structures of QC codes. A more detailed treatment can be found in [6] for QC codes over fields, and in [7] for QC codes over $\mathbb{Z}_4$. A linear code over a ring is called $l-$QC if it is invariant under the cyclic shift by l positions. Algebraically, an $l-$QC code of length $n = ml$ over a ring R can be viewed as an $R[x]/\langle x^m - 1\rangle$ submodule of $(R[x]/\langle x^m - 1\rangle)^l$. Then an r-generator QC code is spanned by r elements of $(R[x]/\langle x^m - 1\rangle)^l$. In this paper, as is the case in most of the literature, we restrict ourselves to 1-generator QC codes. The following is a generalization of an important result about 1-generator QC codes [6], [7] that has been used in many of the recent work [12],[13]. The ring R can be a finite field or $\mathbb{Z}_4$.

Theorem 2.1: *Let C be a 1-generator $l-$QC code of length $n = ml$ with a generator of the form*:

$$\boldsymbol{g(x)} = (f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x)) \tag{2}$$

where $g(x)|(x^m - 1), g(x), f_i(x) \in R[x]/\langle x^m - 1\rangle$, *and* $(f_i(x), h(x)) = 1$, $h(x) = \frac{x^m-1}{g(x)}$ *for all* $1 \le i \le l$. Then $l \cdot d \le d(C)$, *where d is the minimum distance of the cyclic code generated by $g(x)$, and $d(C)$ is the minimum distance of C. Moreover, the dimension of C is equal to the dimension of the cyclic code generated by $g(x)$.*

In terms of generator matrices, the QC codes can be characterized as follows.

Let

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ g_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ g_{m-2} & g_{m-1} & g_0 & \cdots & g_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ g_1 & g_2 & g_3 & \cdots & g_0 \end{bmatrix}_{m\times m} \tag{3}$$

An $(m \times m)$ matrix of the type G_0 is called a circulant matrix of order m or simply a circulant matrix.

It is well-known that the generator matrices of *QC* codes can be transformed into blocks of circulant matrices by a suitable permutation of columns. Therefore, any 1-generator QC code is permutation equivalent to a linear code generated by a matrix of the form

$$\begin{bmatrix} G_1 & G_2 & \ldots & G_l \end{bmatrix}_{m\times n}$$

where each G_k is a circulant matrix of the form (3).

2.3 A NEW QC $\mathbb{Z}_4$ CODE

Based on the search results for new codes over fields and over $\mathbb{Z}_4$, it is natural to search for new quaternary codes in the class of QC codes over $\mathbb{Z}_4$. Although this kind of search is carried out in [5],[7], and [23], a more complete search is still possible. For each odd integer m up to length 63, we produced all cyclic codes i.e., their generators, $p(x)$,(free or non-free), based on the results described in section II-A. We then searched for new QC codes of the form ($p(x)$, $p(x)f_1(x), \ldots, p(x)f_{l-1}$). In most cases we used $l = 2$ (in a few cases we also let $l = 3, 4$). Our search revealed a good (and new) quaternary QC code with parameters [86, $4^{15}2^0$, 55], whose Gray image (which is non-linear) is a binary (172, 2^{30}, 55)-code. The best known binary linear code of length 172, and dimension 30 has minimum distance 54. The generators and the Lee weight enumerator of this code are as follows:

$g(x) = x^{15} + 3x^{14} + 2x^{13} + 3x^{12} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + x^3 + 2x^2 + x + 3$, $f(x) = x^{28} + x^{27} + 3x^{26} + 2x^{25} + x^{24} + 2x^{22} + 3x^{21} + x^{20} + 3x^{19} + 2x^{18} + x^{17} + x^{16} + 2x^{15} + 3x^{14} + 2x^{13} + x^{12} + x^{11} + 2x^{10} + 3x^9 + x^8 + 3x^7 + 2x^6 + x^4 + 2x^3 + 3x^2 + x + 1$ $h(x) = 1$ so that $g(x)\,f\,(x)\,h\,(x) = x^{43} - 1$.

Let $p(x) = f(x)h(x) + 2f(x)$, then the polynomial $p(x)$ generates a free quaternary cyclic code with parameters [43, $4^{15}2^0$, 16]. The search revealed that with the choice of $f_1 = 2x^{13} + x^{12} + x^{10} + 2x^9 + 3x^8 + x^7 + 3x^6 + 3x^5 + 3x^4 + 2x^2 + x$, the 1-generator QC code generated by ($p(x)$, $p(x)f_1(x)$) has parameters [86, $4^{15}2^0$, 55]. Its Lee weight enumerator is given below where the bases are weights, and exponents are number of codewords of that weight

$$0^1 55^{774} 56^{1591} 57^{3698} 58^{5289} 59^{13244} 60^{24639} 61^{43602} 62^{74691}$$
$$63^{132870} 64^{233877} 65^{374100} 66^{614169} 67^{970854} 68^{1502291}$$
$$69^{2252598} 70^{3320202} 71^{4791318} 72^{6689811} 73^{9186262} 74^{12274866}$$
$$75^{15998236} 76^{20463442} 77^{25598416} 78^{31106974} 79^{36948696} 80^{43080625}$$
$$81^{48872424} 82^{54121520} 83^{58775152} 84^{62257851} 85^{64430426} 86^{65299285}$$
$$87^{64550138} 88^{62322437} 89^{58728454} 90^{54154888} 91^{48850752} 92^{42923718}$$
$$93^{37050520} 94^{31176720} 95^{25516630} 96^{20478707} 97^{16029368} 98^{12290346}$$
$$99^{9187466} 100^{6707312} 101^{4753392} 102^{3279137} 103^{2255178} 104^{498636}$$
$$105^{982292} 106^{634379} 107^{382872} 108^{227341} 109^{134590} 110^{76067}$$
$$111^{41452} 112^{21930} 113^{10578} 114^{6665} 115^{3440} 116^{1118} 117^{1032} 118^{172}$$
$$120^{129} 121^{86} 122^{86} 129^2.$$

3. QUATERNARY CODES FROM INVERSE GRAY MAP

The Gray map is usually used to obtain binary codes (usually non-linear) from quaternary codes (usually linear). However, we can also use its inverse to obtain quaternary codes (most likely non-linear) from a given binary code. If we take a binary code with parameters $[2n, 2k, d]$ then the inverse Gray map yields a quaternary code (which is most likely to be non-linear) with parameters $(n, 4^k, d)$. Taking advantage of existing databases for binary linear codes, we considered quaternary codes obtained this way from best known binary codes. This method contributed thousands of (non-linear) codes to the database.

4. GENETIC CODE SEARCH

It is well known that computing minimum distance of an arbitrary linear code is an NP-hard problem [26]. This result gives an insight about why there does not exist an efficient, general purpose search algorithm to find good linear codes. All known search methods/ algorithms for linear codes work well in some special cases. Recently, a new search algorithm has been introduced that works well for most parameter ranges over small fields [4]. In a large number of cases the algorithm produced linear codes with best known parameters, and in several cases generated new codes ("record breakers"). In our work we adopted this algorithm for the ring $\mathbb{Z}_4$ and the Lee metric. We refer the reader to [4] for further details. Originally, as implemented for the field case, PDG did not work very well for $\mathbb{Z}_4$. Therefore, we introduced changes inspired by genetic algorithms. We start off with an empty code and gradually expand it. At each step we examine multiple mutations of a single generator matrix. Thus GCS is not a typical genetic algorithm, in the sense that it operates on a single element and crossover between generator matrices is not considered. Here we present the details of GCS for free codes, i.e. $K = K_1$, $K_2 = 0$.

Initialize Set the input parameters and initialize sets and variables.

Set **N,K,T**;

Use the binary record table to determine D;

$BitShifts = \{1, 2, 3\}$;

$S = \{\}$;

$G = [0]$; $t = 1$; $k = 1$;

The length N and dimension K are the two input parameters. Based on their values we determine a desired Lee minimum distance D using the tables of best known binary codes. In addition, we also specify a small integer T, $1 \leq T \leq N - K$. Greater T implies a better chance for the construction of a good code but that benefit comes at the expense of increased computational time. The output of the algorithm is a linear code over $\mathbb{Z}_4$ of length N and minimum Lee distance $d \geq D$.

General GCS Algorithm

Initialize

while $((t \leq T)$ and $(k \leq K))$ **do**

$S = S \cup \{(K + kN), \ldots, ((k + 1)\, N - 1)\}$;

$G_{old} = [0]$; $G_{new} = [0]$;

$G_{temp} = [0]$; $G_{old}[k][k] = 1$;

$d = 1$;

Search for a suitable matrix G_{old}

if $(d \geq D)$ **then**

$G = G + G_{old}$;

$k = k + 1$;

end if

end while

The search for a suitable mutation matrix G_{old} presents the heaviest computational task. As the size of the set S increases with successive dimensions, so does the number of possible mutation matrices. This is a key difference between PDG and GCS. The process terminates either when a suitable mutation matrix is found or the specified level of T is reached.

Search for a suitable matrix G_{old}

```
while ((t ≤ T) and (d < D)) do
increment_t = true;
RedundancyShifts = The set of all subsequences
of BitShifts of length t;
Positions = The set of all subsets of S of size t;
for p in Positions do
 G_new = G_old;
 for r in RedundancyShifts do
  for i = 1 to t do
   G_new[p(i) ÷ N][(p(i) mod N) + 1] =
   = G_old[p(i) ÷ N][(p(i) mod N) + 1] + r(i);
 end for
 G_1 = G + G_new; C =< G_1 >;
 if (MinimumLeeWeight(C) > d) then
    d = MinimumLeeWeight(C);
    G_temp = G_new;
    increment_t = false;
    break p;
  end if
 end for
end for
G_old = G_temp;
if increment_t then
 t = t + 1;
end if
end while
```

Below is a table of small quaternary codes obtained with GCS whose Lee distances are equal to the minimum Hamming distances of the corresponding binary linear codes. We call such a code "decent". This is significant, considering that all binary linear codes up to length 32 are optimal. Based on our experience and the results from the literature, constructing decent codes is a challenging task. Besides, many of the decent $\mathbb{Z}_4$ codes may very well be regarded new.

Free decent quaternary linear codes.

N K_1
10 : 1, 2, 3, 4, 5, 6, 7, 8, 9
11 : 1, 3, 4, 7, 8, 9, 10
12 : 1, 2, 3, 4, 5, 8, 9, 10, 11
13 : 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12,
14 : 1, 2, 3, 6, 8, 10, 11, 12, 13
15 : 1, 2, 3, 4, 7, 9, 11, 12, 13, 14
16 : 1, 2, 6, 7, 8, 9
17 : 1, 2, 3, 4, 5
18 : 1, 2, 3
19 : 1, 2, 3
20 : 1, 2, 3, 4
21 : 1, 2, 3, 11
27 : 1, 2, 3

5. CONCLUSION AND FUTURE WORK

In this work, we introduce a new database of $\mathbb{Z}_4$ codes that is available online that can be conveniently updated by researchers. The database has been populated using several different search methods. We present a survey of some of the recent and promising methods to find new quaternary codes. Search with one of these methods has yielded a good quaternary code. We also introduce a new search method that has yielded many decent codes. We invite researches to search for new quaternary codes using known methods or devising new ones, and update the database with any new codes discovered. There is much room for improvement on this database.

REFERENCES

[1] Abualrub, T. and Siap, I. (2007). "Reversible cyclic codes over $\mathbb{Z}_4$," *Australasian Journal of Combinatorics*, vol 38, pp. 159-206.

[2] Abualrub, T. and Oehmke, R. (2003). "On the generators of $\mathbb{Z}_4$ cyclic code," *IEEE Trans. Inform. Theory*, vol 49, pp. 2126-2133.

[3] Blackford, T. (2003). "Cyclic codes over $\mathbb{Z}_4$ of oddly even length," *Disc. Appl. Math*, vol 128, pp. 27-46.

[4] Asamov, T. and Aydin, N. (2007). "A Search algorithm for linear codes: progressive dimension growth," *Des. Codes Cryptogr*., vol. 45, pp. 213-217.

[5] Aydin, N. and Gulliver, T. A. "Some good cyclic and quasi-twisted $\mathbb{Z}_4$- linear codes," to appear in *Ars Comb*.

[6] Aydin, N., Siap, I. and Ray-Chaudhuri, D. K. (2001). "The structure of 1-generator qasi-twisted codes and new linear codes," *Des. Codes Cryptogr*., vol. 24, pp. 313-326.

[7] Aydin, N. and Ray-Chaudhuri, D. (2002). "Quasi-Cyclic Codes over $\mathbb{Z}_4$ and Some New Binary Codes", *IEEE Trans. Inform. Theory*, vol. 48, pp. 2065-2069.

[8] Bosma, W., Cannon, J. J. and Playoust, C. (1997). The Magma algebra system I: The user language, *J. Symbolic Computation*, vol. 24, pp. 235-266.

[9] Brouwer, A. E., Linear code bound (online server), http://www.win.tue.nl/ aeb/voorlincod.html

[10] Calderbank, A. R. and McGuire, G. (1997). "Construction of a (64, 2^{37}, 12) code via Galois rings", *Des., Codes Cryptogr.*, vol. 10, pp. 157-165.

[11] Conway, J. H. and Sloane, N. J. A. (1993). "Self-dual codes over the integers modulo 4," *J. Combin. Theory, Ser. A*, vol. 62, pp. 31-45.

[12] Daskalov, R. and Hristov, P. (2003). "New quasi-twisted degenerate ternary linear codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2259-2263.

[13] Daskalov, R. and Hristov, P. "New binary one-generator quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 3001-3005, 2003.

[14] Fields, J., Gaborit, P., Leon, J. and Pless, V. (1998). "All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known," *IEEE Trans. Inform. Theory*, vol. 44, 1222-1228.

[15] Grassl, M. (Bounds on the minimum distance of linear codes) available at http://www.codetables.de

[16] Grassl, M. and White, G. (2005). "New Codes from Chains of Quasi-cyclic Codes," *Proceedings 2005 IEEE Int. Symposium on Inform. Theory*, pp. 2095-2099.

[17] Glynn, D. G., Gulliver, T. A. and Gupta, M. K. "On some quaternary self-orthogonal codes," *ARS Comb*., to appear.

[18] Litsyn, S., Table of non-linear binary codes [online], http://www.eng.tau.ac.il/~litysn/tableand/ index.html.

[19] MacWilliams, F. J. and Sloane, N. J. A. (1977). *The Theory of Error Correcting Codes*, North Holland, New York.

[20] Pless, V. S., Leon, J. S. and Fields J. (1997). "All $\mathbb{Z}_4$ codes of Type II and length 16 are known," *J. Combin. Theory, Ser. A* vol. 78, pp. 32-50.

[21] Pless, V. S. and Qian, Z. (1996). "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594-1600.

[22] Rains, E. M. (1999). "Optimal self-dual codes over $\mathbb{Z}_4$," *Disc. Math.*, vol. 203, 215-228.

[23] Siap, I., Abualrub, T. and Aydin, N. "Quaternary quasi-cyclic codes with even length components," to appear in *Mathematics and Computers in Simulation*.

[24] Siap, I., Aydin, N. and Ray-Chaudhuri, D. K. (2000). "New ternary quasi-cyclic codes with better minimum distances." *IEEE Trans. Inform. Theory*, vol. 46 , pp. 1554-1558.

[25] van Lint, J. H. (1999). *Introduction to Coding Theory*, Springer, New York.

[26] Vardy, A. (1997). "The intractability of computing the minimum distance of a code," *IEEE Trans Inform Theory* vol. 43, pp. 1757-1766.

[27] Wan, Z. (1997). *Quaternary Codes*, World Scientific, Singapore.

About the Authors

Nuh Aydin and Tsvetan Asamov
Department of Mathematics,
Kenyon College,
Gambier, OH 43022 USA