A new series of $\mathbb{Z}_4$-linear codes of high minimum Lee distance derived from the Kerdock codes

Michael Kiermaier* and Johannes Zwanzger

***Abstract*— A new series of $\mathbb{Z}_4$-linear codes of high minimum Lee distance is given. It is derived from the $\mathbb{Z}_4$-linear representation of the Kerdock codes. The Gray image of the smallest of these codes is a nonlinear binary $(114, 2^8, 56)$-code, and in the second smallest case the Gray image is a nonlinear binary $(1988, 2^{12}, 992)$-code. Both codes have at least twice as many codewords as any linear binary code of equal length and minimum distance.**

I. Introduction

A. Kerdock Codes

In [5], Kerdock introduced a class of nonlinear binary codes of very high minimum Hamming distance. Later it was discovered [8], [1] that the Kerdock codes can be described as images of $\mathbb{Z}_4$-linear codes $\hat{K}(r+1)$, $r \geq 3$ odd, under the Gray map. For the smallest cases $r = 3$ and $r = 5$ it is known that the Kerdock codes have at least twice as many codewords as any linear binary code of equal length and minimum distance. In [7, Research Problem (15.4)] the question was raised if this is true for all Kerdock codes. This question is still open.

B. Idea of the new construction

Our aim is to construct a new series of good $\mathbb{Z}_4$-linear codes from the codes $\hat{K}(r+1)$. The rough idea for the construction is the following: We fix a generator matrix $\hat{G}_{r+1}$ of $\hat{K}(r+1)$ and define S as a set of projective representatives of all information words x such that $x\hat{G}_{r+1}$ is a codeword of a certain symmetrized weight. Now the vectors in S are put as columns into a matrix A_{r+1}, and the code generated by A_{r+1} is denoted by $C(r+1)$. It turns out that it is possible to append a column only consisting of zeros and 2s to the matrix A_{r+1} such that all minimum weight codewords of $C(r+1)$ get extended by symbols 2. By appending a suitable number of such columns, the minimum weight is raised to match the second smallest weight in $C(r+1)$. Almost all codewords of the resulting code $\hat{C}(r+1)$ are codewords of minimum Lee weight, which indicates that $\hat{C}(r+1)$ has very good error correcting properties. The Gray images of the two smallest codes $\hat{C}(4)$ and $\hat{C}(6)$ have at least twice as many codewords as any linear binary code of equal length and minimum distance.

M. Kiermaier is with the Department of Mathematics, University of Bayreuth, 95440 Bayreuth, Germany michael.kiermaier@uni-bayreuth.de

J. Zwanzger is with the Department of Mathematics, University of Bayreuth, 95440 Bayreuth, Germany johannes.zwanzger@uni-bayreuth.de

*Supported by Deutsche Forschungsgemeinschaft under Grant No. WA 1666/4-1.

C. Outline of the paper

In Section II a brief introduction to $\mathbb{Z}_4$-linear codes is given. For a deeper treatment the reader is referred to [4, Chapter 12]. In Section III the series of the codes $\hat{C}(r+1)$ is constructed and their parameters are determined. The main tool for the computation of the parameters is the duality construction in [3] for multisets of points in projective Hjelmslev geometries. For the theory of projective Hjelmslev geometries and the connection to coding theory over rings see [2] and the references cited there. Finally in Section IV we have a closer look at the two smallest codes $\hat{C}(4)$ and $\hat{C}(6)$ of the series.

II. $\mathbb{Z}_4$-linear codes

For a positive integer n, a $\mathbb{Z}_4$*-linear code* C of length n is a submodule of the free module $\mathbb{Z}_4^n$.

A. The Lee metric

The *Lee weight* $w_{\mathrm{Lee}} : \mathbb{Z}_4 \to \mathbb{Z}$ maps 0 to 0, the units 1 and 3 to 1 and the zero divisor 2 to 2. It is extended to $\mathbb{Z}_4^n$ by summing up the Lee weights component-wise. Furthermore, the *Lee distance* $d_{\mathrm{Lee}} : \mathbb{Z}_4^n \times \mathbb{Z}_4^n \to \mathbb{Z}$ is defined by $d_{\mathrm{Lee}}(x, y) = w_{\mathrm{Lee}}(x-y)$. It is a metric on $\mathbb{Z}_4^n$. For a code C the polynomial

$$\sum_{c\in C} X^{w_{\mathrm{Lee}}(c)} \in \mathbb{Z}[X]$$

is called the *Lee weight enumerator*. The minimum Lee distance $d = d_{\mathrm{Lee}}(C)$ over all pairs of distinct codewords of a code C is called *minimum Lee distance* of C. If additionally C has length n, we call C a $\mathbb{Z}_4$-linear $(n, \#C, d)$-code or a $\mathbb{Z}_4$-linear code of parameters $(n, \#C, d)$. Like linear codes over finite fields, $\mathbb{Z}_4$-linear codes are distance-invariant. This implies that the minimum Lee distance equals the minimum Lee weight among all non-zero codewords.

B. The Gray map

The *Gray map* $\mathbb{Z}_4 \to \mathbb{F}_2^2$ is defined by

$$\begin{cases} 0 & \mapsto (0,0) \\ 1 & \mapsto (0,1) \\ 2 & \mapsto (1,1) \\ 3 & \mapsto (1,0) \end{cases}.$$

Coordinate-wise application yields the extended Gray map $\mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$. It is an isometry from $(\mathbb{Z}_4^n, d_{\mathrm{Lee}})$ to $(\mathbb{F}_2^{2n}, d_{\mathrm{Ham}})$, where d_{Ham} denotes the Hamming distance. So the Gray image of a $\mathbb{Z}_4$-linear $(n, \#C, d)$-code C is a – generally non-linear – binary $(2n, \#C, d)$-code, and the Hamming weight enumerator of the Gray image of C coincides with the Lee weight enumerator of C. For that reason, besides length and size the minimum Lee weight is the most important parameter of a $\mathbb{Z}_4$-linear code.

Like in classical coding theory over finite fields, one of the main goals is to find a $\mathbb{Z}_4$-linear code for given length and size whose minimum Lee distance is as large as possible. As a special case of linear codes over finite chain rings, a table of $\mathbb{Z}_4$-linear codes of high minimum Lee distance can be found in [11].

A further weight of interest is the *symmetrized weight* counting the number of zeros, symbols 2 and units in a codeword. The *symmetrized weight enumerator* collects this information for all codewords of a given code. While often denoted by a homogeneous polynomial in three indeterminants, in this article we will give the symmetrized weight enumerators by listing the occurring symmetrized weights as the rows of a table.

Two $\mathbb{Z}_4$-linear codes are called *equivalent*, if one can be mapped to the other by a combination of permuting the coordinates and multiplying some coordinates in all codewords by -1. Two equivalent codes have the same symmetrized weight enumerator.

C. Galois rings

Let $f \in \mathbb{Z}_4[X]$ be a monic polynomial of degree $r \geq 1$, such that its image modulo 2 is irreducible in $\mathbb{F}_2[X]$. The ring $\mathbb{Z}_4[X]/(f)$ is called the *Galois ring* $\mathrm{GR}(2^{2r}, 4)$ of order 2^{2r} and characteristic 4. It can be shown that up to ring isomorphism, the definition does not depend on the exact choice of f.

Each element of $\mathrm{GR}(2^{2r}, 4)$ has a unique representative of degree at most $r-1$. By the coefficients of this representative, each element of $\mathrm{GR}(2^{2r}, 4)$ will be identified with a vector in $\mathbb{Z}_4^r$. This identification gives rise to the isomorphism $\mathbb{Z}_4^r \cong \mathrm{GR}(2^{2r}, 4)$ as $\mathbb{Z}_4$-modules, providing an additional multiplicative structure on the vectors in $\mathbb{Z}_4^r$.

It can be shown that the unit group $\mathrm{GR}(2^{2r}, 4)^*$ of order $2^{2r} - 2^r$ has a unique subgroup T^* of order $2^r - 1$, called the set of *Teichmüller units* in $\mathrm{GR}(2^{2r}, 4)$. If the defining polynomial f of $\mathrm{GR}(2^{2r}, 4)$ is chosen as the Hensel lift of a primitive polynomial in $\mathbb{F}_2[X]$ of degree r, $X + (f)$ is a generator of T^*. Furthermore, $T = T^* \cup \{0\}$ is called set of *Teichmüller elements* in $\mathrm{GR}(2^{2r}, 4)$. T is a set of representatives of the *residue class field* $\mathbb{F}_{2^r}$ of $\mathrm{GR}(2^{2r}, 4)$, which is the factor ring of $\mathrm{GR}(2^{2r}, 4)$ modulo its unique nontrivial ideal $2\,\mathrm{GR}(2^{2r}, 4)$.

D. $\mathbb{Z}_4$-linear representation of the Kerdock codes

For $r \geq 3$ odd the code $\hat{K}(r+1)$ is defined as the $\mathbb{Z}_4$-linear code generated by the rows of the $((r+1) \times 2^r)$-matrix

$$\begin{pmatrix} \mathbf{t}_0 & \cdots & \mathbf{t}_{2^r-1} \\ 1 & \cdots & 1 \end{pmatrix},$$

where $\mathbf{t}_0, \ldots, \mathbf{t}_{2^r-1} \in \mathbb{Z}_4^r$ runs over the Teichmüller elements of $\mathrm{GR}(2^{2r}, 4)$ which are read as elements in $\mathbb{Z}_4^r$.

Up to a permutation of the coordinates, the Gray image of $\hat{K}(r+1)$ is the Kerdock code as originally defined in [5].

Fact 1: Let $r \geq 3$ be odd. The code $\hat{K}(r+1)$ is a $\mathbb{Z}_4$-linear code of parameters

$$(2^r, \quad 2^{2r+2}, \quad 2^r - 2^{\frac{r-1}{2}}).$$

The symmetrized weight enumerator of $\hat{K}(r+1)$ is shown in Table I.

Proof: In [4, Theorem 17.2.6], the Lee weight enumerator of $\hat{K}(r+1)$ is given. The proof actually shows that the symmetrized weight enumerator is of the claimed form. ■

III. The Construction of the Code $\hat{C}(r+1)$

A. The code $C(r+1)$

In the following let $r \geq 3$ be odd and $\hat{G}_{r+1} \in \mathbb{Z}_4^{(r+1)\times 2^r}$ be a generator matrix of $\hat{K}(r+1)$. Furthermore, we take S as a set of projective representatives of information words $x \in \mathbb{Z}_4^{r+1}$ such that $x\hat{G}_{r+1}$ is a codeword of symmetrized weight B in Table I. The vectors in C are put as columns into a matrix A_{r+1}, and the code generated by A_{r+1} is denoted by $C(r+1)$. The size of S and therefore the length of the code $C(r+1)$ is $2^{2r} - 2^r$.

The definition of the code $C(r+1)$ depends on the choice of the generator matrix $\hat{G}_{r+1}$, the choice of the representatives in S and the order of the columns in A_{r+1}. But all these different choices lead to equivalent codes.

Lemma 2: Let $r \geq 3$ be odd. The code $C(r+1)$ is a $\mathbb{Z}_4$-linear code of parameters

$$(2^{2r} - 2^r, \quad 4^{r+1}, \quad 2^{2r} - 2^r - 2^{\frac{r-1}{2}}).$$

The symmetrized weight enumerator of $C(r+1)$ is shown in Table II. Furthermore, the codewords of lines B, D, E and F in Table II form a submodule of $C(r+1)$ of index 2.

Proof: To compute the symmetrized weight enumerator of $C(r+1)$, projective Hjelmslev geometry is used. The symmetrized weight of a codeword corresponds to the *type* of a hyperplane H in the Hjelmslev geometry with respect to a multiset of points $\mathfrak{K}$, which is a triple counting the number of points in $\mathfrak{K}$ incident with H, not incident but neighbor to H, and not neighbor to H, respectively. The counterpart to the symmetrized weight enumerator of a code is the *spectrum* of $\mathfrak{K}$, which lists the numbers of hyperplanes of the single types.

Since all the columns of $\hat{G}_{r+1}$ contain at least one unit entry, we may consider the columns as a point set $\mathfrak{K}$ in the projective Hjelmslev Geometry $\mathrm{PHG}(r, \mathbb{Z}_4)$. By the symmetrized weight enumerator of $\hat{K}(r+1)$ from Fact 1 also the spectrum of $\mathfrak{K}$ is known. The construction of the code $C(r+1)$ geometrically corresponds to the duality construction discussed in [3]. Following this article, we define the function τ by setting

$$\alpha = 0, \quad \beta = \frac{1 + 2^{\frac{r-1}{2}}}{2^r} \quad \text{and} \quad \gamma = \frac{1 - 2^{\frac{r-1}{2}}}{2^r}$$

such that $\mathfrak{K}^\tau$ is the point set given by the vectors in S. By the formula in [3] we compute the spectrum of $\mathfrak{K}^\tau$, which translates into the symmetrized weight enumerator of $C(r+1)$ shown in Table II.

TABLE I

THE SYMMETRIZED WEIGHT ENUMERATOR OF $\hat{K}(r+1)$

	#codewords	#zeros	#symbols 2	#units	w_{Lee}
A	$2^{2r+1}-2^{r+1}$	$2^{r-2}+2^{\frac{r-3}{2}}$	$2^{r-2}-2^{\frac{r-3}{2}}$	2^{r-1}	$2^r-2^{\frac{r-1}{2}}$
B	$2^{2r+1}-2^{r+1}$	$2^{r-2}-2^{\frac{r-3}{2}}$	$2^{r-2}+2^{\frac{r-3}{2}}$	2^{r-1}	$2^r+2^{\frac{r-1}{2}}$
C	2^{r+1}	0	0	2^r	2^r
D	$2^{r+1}-2$	2^{r-1}	2^{r-1}	0	2^r
E	1	0	2^r	0	2^{r+1}
F	1	2^r	0	0	0

TABLE II

THE SYMMETRIZED WEIGHT ENUMERATOR OF $C(r+1)$

	#codewords	#zeros	#symbols 2	#units	w_{Lee}
A	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-2}+2^{\frac{r-3}{2}}$	$2^{2r-2}-2^{r-2}-2^{\frac{r-3}{2}}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^r-2^{\frac{r-1}{2}}$
B	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-1}$	$2^{2r-2}-2^{r-1}$	2^{2r-1}	$2^{2r}-2^r$
C	2^{r+1}	$2^{2r-2}-2^{\frac{3r-3}{2}}-2^{r-2}+2^{\frac{r-3}{2}}$	$2^{2r-2}+2^{\frac{3r-3}{2}}-2^{r-2}-2^{\frac{r-3}{2}}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^r+2^{\frac{3r-1}{2}}-2^{\frac{r-1}{2}}$
D	2^r-1	$2^{2r-1}-2^r$	2^{2r-1}	0	2^{2r}
E	2^r	$2^{2r-1}-2^{r-1}$	$2^{2r-1}-2^{r-1}$	0	$2^{2r}-2^r$
F	1	$2^{2r}-2^r$	0	0	0

For the computation it is important to recognize that all point classes in $\mathrm{PHG}(r,\mathbb{Z}_4)$ contain at most 1 point of $\mathfrak{K}$. Therefore, the 2^r points x in $\mathfrak{K}$ give $\mathfrak{K}(x)=\mathfrak{K}([x])=1$ (which yields line C in the table), and there are $2^{2r}-2^r$ points x in $\mathrm{PHG}(r,\mathbb{Z}_4)$ with $\mathfrak{K}(x)=0$, $\mathfrak{K}([x])=1$ (line A) and the same number of points with $\mathfrak{K}(x)=\mathfrak{K}([x])=0$ (line B). The remaining lines in the table arise as non-unit multiples of the codewords in lines A–C when switching back from the geometric to the coding theoretic point of view.

The point classes not containing any point of $\mathfrak{K}$ form the neighbor class of a hyperplane in $\mathrm{PHG}(r,\mathbb{Z}_4)$. Therefore, the codewords of the lines B, D, E and F together are a submodule of $C(r+1)$ of index 2. ■

B. The code $\hat{C}(r+1)$

Now we define $\hat{C}(r+1)$ as an extension of $C(r+1)$ by $2^{\frac{r-3}{2}}$ coordinates in the following way: The codewords corresponding to the lines B, D, E and F in Table II are extended by zeros and the codewords corresponding to the lines A and C are extended by symbols 2. In this way, the minimum Lee weight $2^{2r}-2^r-2^{\frac{r-1}{2}}$ (the codewords in line A) of $C(r+1)$ is raised to match the second smallest Lee weight $2^{2r}-2^r$ (lines B and E).

Theorem 3: Let $r\geq 3$ be odd. The code $\hat{C}(r+1)$ is a $\mathbb{Z}_4$-linear code of parameters

$$(2^{2r}-2^r+2^{\frac{r-3}{2}},\quad 4^{r+1},\quad 2^{2r}-2^r).$$

The Lee weight enumerator of $\hat{C}(r+1)$ is

$$\begin{aligned}&1\\ &+(2^{2r+2}-2^{r+2}+2^r)\,X^{2^{2r}-2^r}\\ &+(2^r-1)\,X^{2^{2r}}\\ &+2^{r+1}\,X^{2^{2r}+2^{\frac{3r-1}{2}}-2^r}.\end{aligned}$$

The symmetrized weight enumerator of $\hat{C}(r+1)$ is shown in Table III.

Proof: By Lemma 2, the codewords of the lines B, D, E and F in Table II form a submodule of $C(r+1)$ of index 2. So the code $\hat{C}$ is indeed $\mathbb{Z}_4$-linear. The statements about length and size of $\hat{C}(r+1)$ are clear, and the symmetrized weight enumerator of $\hat{C}(r+1)$ can be easily computed from the symmetrized weight enumerator of $C(r+1)$ shown in Table II. ■

IV. EXAMPLES

A. $r=3$

The smallest Kerdock code $\hat{K}(4)$ is also known as the Octacode, and its Gray image is the Nordstrom-Robinson code. $\hat{K}(4)$ can also be seen as the smallest extended $\mathbb{Z}_4$-linear quadratic residue code. A possible generator matrix of $\hat{K}(4)$ is

$$\hat{G}_4=\begin{pmatrix}1&0&0&0&2&1&1&1\\0&1&0&0&1&2&1&3\\0&0&1&0&1&3&2&1\\0&0&0&1&1&1&3&2\end{pmatrix}.$$

The Lee weight enumerator of $\hat{K}(4)$ is

$$1+112X^6+30X^8+112X^{10}+X^{16}.$$

In order to construct the code $\hat{C}(4)$, we take projective representatives of the 112 information words of the codewords of Lee weight 10. The choice of the representatives is done according to the rule that the first unit entry equals 1. Taking these 56 representatives as columns of a matrix A_4 gives the matrix shown in Table IV without the last column. A_4 generates the code $C(4)$. Since all rows of A_4 have Lee weight 70 and therefore correspond to line C in Table II, the column $(2\ 2\ 2\ 2)^t$ is appended to A_4 according to the discussed extension rule. The resulting (57×4)-matrix shown in Table IV generates the code $\hat{C}(4)$.

By Theorem 3, $\hat{C}(4)$ is a $\mathbb{Z}_4$-linear code of length 57 and size 256, and the Lee weight enumerator of $\hat{C}(4)$ is

$$1+232X^{56}+7X^{64}+16X^{72}.$$

TABLE III

THE SYMMETRIZED WEIGHT ENUMERATOR OF $\hat{C}(r+1)$

	#codewords	#zeros	#symbols 2	#units	w_{Lee}
A	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-2}+2^{\frac{r-3}{2}}$	$2^{2r-2}-2^{r-2}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^{r}$
B	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-1}+2^{\frac{r-3}{2}}$	$2^{2r-2}-2^{r-1}$	2^{2r-1}	$2^{2r}-2^{r}$
C	2^{r+1}	$2^{2r-2}-2^{\frac{3r-3}{2}}-2^{r-2}+2^{\frac{r-3}{2}}$	$2^{2r-2}+2^{\frac{3r-3}{2}}-2^{r-2}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^{r}+2^{\frac{3r-1}{2}}$
D	$2^{r}-1$	$2^{2r-1}-2^{r}+2^{\frac{r-3}{2}}$	2^{2r-1}	0	2^{2r}
E	2^{r}	$2^{2r-1}-2^{r-1}+2^{\frac{r-3}{2}}$	$2^{2r-1}-2^{r-1}$	0	$2^{2r}-2^{r}$
F	1	$2^{2r}-2^{r}+2^{\frac{r-3}{2}}$	0	0	0

TABLE IV

GENERATOR MATRIX OF $\hat{C}(4)$

$$\begin{pmatrix} 1111 & 0222 & 0222 & 0222 & 1111 & 1111 & 1111 & 0222 & 0222 & 0222 & 1111 & 1111 & 1111 & 0222 & 2 \\ 0222 & 1111 & 2022 & 2022 & 1133 & 0222 & 0222 & 1111 & 1111 & 2022 & 1133 & 1133 & 0222 & 1111 & 2 \\ 2022 & 2022 & 1111 & 2202 & 2202 & 1133 & 2022 & 3113 & 2022 & 1111 & 1313 & 0222 & 3113 & 1133 & 2 \\ 2202 & 2202 & 2202 & 1111 & 0222 & 2202 & 3113 & 2022 & 3113 & 3113 & 2202 & 3113 & 1133 & 1313 & 2 \end{pmatrix}$$

Thus the Gray image of $\hat{C}(4)$ is a nonlinear binary code with the parameters $(114, 2^8, 56)$. By a Griesmer step, the existence of a linear binary $[114, 8, 56]$ would imply the existence of a linear binary $[58, 7, 28]$-code. But according to [9], no such code exists. Thus the Gray image of $\hat{C}(4)$ has at least twice as many codewords as any linear binary code of equal length and minimum distance.

While no linear binary $[58, 7, 28]$-code exists, we want to mention that there is a $\mathbb{Z}_4$-linear code whose Gray image is a nonlinear binary $(58, 2^7, 28)$-code. Recently the authors constructed such a code using a hyperoval in the projective Hjelmslev plane over $\mathbb{Z}_4$ [6].

Originally, the code $\hat{C}(4)$ was found by a heuristic approach similar to [10]. A subsequent analysis of the code revealed a clear structure and led to the construction of the series $\hat{C}(r+1)$.

B. $r = 5$

In the second smallest case $\hat{C}(6)$ is a $\mathbb{Z}_4$-linear code of length 994 and size 2^{12}, and the Lee weight enumerator of $\hat{C}(6)$ is

$$1 + 4000X^{992} + 31X^{1024} + 64X^{1120}.$$

The Gray image of $\hat{C}(6)$ is a nonlinear $(1988, 2^{12}, 992)$-code. It was possible to show that a linear binary $[1988, 12, 992]$-code does not exist, details will be published elsewhere. Thus also the Gray image of $\hat{C}(6)$ has at least twice as many codewords as any linear binary code of equal length and minimum distance.

Similar to the Kerdock series, it remains an open question if in this sense all the codes of the series $\hat{C}(r+1)$ are "better than linear".

REFERENCES

[1] Jr. A. Roger Hammons, P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, *The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[2] T. Honold, I. Landjev, *Linear Codes over Finite Chain Rings and Projective Hjelmslev Geometries*, Codes over Rings. Proceedings of the CIMPA Summer School Ankara, Turkey, 18–29 August 2008 (Patric Solé, ed.), World Scientific, 2009, pp. 60–123.

[3] T. Honold, I. Landjev, *The Dual Construction for Arcs in Projective Hjelmslev Planes*, submitted, 2010.

[4] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[5] A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187.

[6] M. Kiermaier, J. Zwanzger, *A non-free $\mathbb{Z}_4$-linear code of high minimum Lee distance*, submitted, 2010.

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

[8] A. A. Nechaev, *Kerdock code in a cyclic form*, Discrete Math. Appl. **1** (1991), 365–384.

[9] H. C. A. van Tilborg, *The smallest length of binary 7-dimensional linear codes with prescribed minimum distance*, Discrete Math., **33** (1981), 197–207.

[10] J. Zwanzger, *A heuristic algorithm for the construction of good linear codes*, IEEE Trans. Inform. Theory, **54** (2008), 2388–2392.

[11] J. Zwanzger, *Linear codes over finite chain rings*, http://www.mathe2.uni-bayreuth.de/20er/codedb/