New Ring-Linear Codes from Geometric Dualization

Michael Kiermaier, Johannes Zwanzger

New Ring-Linear Codes from Geometric Dualization

Michael Kiermaier* and Johannes Zwanzger

Institut für Mathematik, Universität Bayreuth, 95440 Bayreuth, Germany
{michael.kiermaier,johannes.zwanzger}@uni-bayreuth.de
http://codes.uni-bayreuth.de

1 Introduction

1.1 History

In the 1960s and 1970s the Nordstrom-Robinson-Code [30] and subsequently the infinite series of the Preparata- [31], Kerdock- [21], Delsarte-Goethals- [6] and Goethals-Codes [7] were discovered. Apart from a few corner cases, all of these codes are non-linear binary block codes that have higher minimum distance than any known comparable (having equal size and length) linear binary code. We will call such codes *better-than-known-linear* or *BTKL*. In [26, Research Problem (15.4)] the question was raised if the Preparata and Kerdock codes are better than any comparable linear binary code (*better-than-linear*, *BTL*[1]). For the Preparata series this was shown in [2]. Of the remaining above mentioned series still only the smaller codes are proven to be BTL.

Later the striking discovery was made [28,12] that all these codes can be constructed as images of certain $\mathbb{Z}_4$-linear codes under the Gray map. Since then, a lot of research has been done on $\mathbb{Z}_4$-linear codes and on linear codes over more general finite rings. However, the examples on BTL- or BTKL-codes found since then are comparatively sparse. They include Gray images of QR-codes over $\mathbb{Z}_4$, the two Calderbank-McGuire-codes [3,4] and some quasi-cyclic codes over $\mathbb{Z}_4$ [1][2]. Two further examples [13,22] come from a hyperoval in the projective Hjelmslev plane over the 16-element Galois ring $\mathrm{GR}(16,4)$ where a similar Gray map allows the comparison with $\mathbb{F}_4$-linear codes.

1.2 Overview

Our aim is the construction of new ring-linear BTL- and BTKL-codes. The class of base rings are the Galois rings $\mathrm{GR}(4^r,4)$ of characteristic 4, which include $\mathbb{Z}_4$ as its smallest and most important member. All these rings come with a

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

[1] While BTL is a hard property of a binary block code, BTKL only describes the current state of knowledge.

[2] We would like to mention that Ex. 5 and 6 in [1] are not BTKL due to recently found linear binary codes.

generalized Gray map which allows the comparison with $\mathbb{F}_q$-linear codes. Associated with these rings are the Hjelmslev geometries, and the central tool for the construction is geometric dualization [18]. Roughly speaking, it gives us the possibility to compute the parameters of a code which was constructed out of another code by selecting the information words of codewords of certain symmetrized weights and putting them as columns into a generator matrix.

Our first construction dualizes the $\mathbb{Z}_4$-linear preimages of the Kerdock codes. It turns out that the resulting codes can be extended while preserving their minimum distance. The final series $\hat{\mathcal{K}}^*_{r+1}$ of $\mathbb{Z}_4$-linear codes has high minimum Lee distance, the first two members are BTL-codes. For the second construction we start with a series related to the Kerdock codes we call *Teichmüller codes*, the result is a 2-parameter-series $\mathcal{T}^*_{r,k}$. Both series $\hat{\mathcal{K}}^*_{r+1}$ and $\mathcal{T}^*_{r,k}$ consist of homogeneous 3-weight codes and have the property that the largest part of the codewords are minimum weight words. We also compute the symmetrized weight enumerator of the codes which enables us to derive the parameters of residuals.

The generalized Gray map translates our codes into ordinary, generally nonlinear codes in the Hamming space. For moderate lengths, the online tables [9] can be used for the comparison with classical linear codes. In this way, we get the BTL- and BTKL-codes summarized in the table below. They are either new or give an alternative construction to already known code parameters. A preliminary report on this research containing the series $\hat{\mathcal{K}}^*(r+1)$ was published in [24].

No.	gen. Gray image	construction	status	already known?
1	$(58, 2^7, 28)_2$	residual of $\hat{\mathcal{K}}^*_3$ in E	BTL	[25]
2	$(60, 2^8, 28)_2$	residual of $\mathcal{T}^*_{2,5}$ in A	BTL	[1, Ex. 4]
3	$(114, 2^8, 56)_2$	$\hat{\mathcal{K}}^*_3$	BTL	new
4	$(180, 2^9, 88)_2$	residual of $\mathcal{T}^*_{2,5}$ in C	BTKL	new
5	$(244, 2^9, 120)_2$	res. of code No. 7 in $(122, 120, 0)$	BTKL	new
6	$(372, 2^{10}, 184)_2$	$\mathcal{T}^*_{2,5}$	BTL	new
7	$(484, 2^{10}, 240)_2$	residual of $\hat{\mathcal{K}}^*_5$ in B	BTKL	new
8	$(1988, 2^{12}, 992)_2$	$\hat{\mathcal{K}}^*_5$	BTL	new
9	$(504, 4^6, 376)_4$	$\mathcal{T}^*_{4,3}$	BTKL	[22]

2 Galois rings

Here a brief introduction to Galois rings is given. For details, see for example [27].

Let p be prime and m be a positive integer. Let $f \in \mathbb{Z}_{p^m}[X]$ be a monic polynomial of degree $r \geq 1$, such that its image modulo p is irreducible in $\mathbb{F}_p[X]$. The ring $\mathbb{Z}_{p^m}[X]/(f)$ is called the *Galois ring* $\mathrm{GR}(p^{mr}, p^m)$ of order p^{mr} and characteristic p^m. It can be shown that up to ring isomorphism, the definition does not depend on the exact choice of f. In the case $m = 1$, R is the finite field $\mathbb{F}_{p^m}$.

$R = \mathrm{GR}(p^{mr}, p^m)$ is a local ring with the unique maximal ideal Rp, which is principal. The *residue class field* R/pR is isomorphic to $\mathbb{F}_q$ with $q = p^r$. The unit group R^* of order $q(q-1)$ has a unique subgroup of order $q-1$, its set of *Teichmüller units* which will be denoted by T^*. If the defining polynomial f of R is chosen as the Hensel lift of a primitive polynomial in $\mathbb{Z}_p[X]$ of degree r, $X + (f)$ is a generator of T^*. Furthermore, $T = T^* \cup \{0\}$ is called set of *Teichmüller elements* in R. T forms a set of representatives of the *residue class field*.

$\mathrm{GR}(p^{mr}, p^m)$ is a subring of $\mathrm{GR}(p^{ms}, p^m)$ if and only if r divides s. In this way, for any positive integer k, $\mathrm{GR}(q^{mk}, p^m)$ is a free R-module of rank k, and we can identify the elements of $\mathrm{GR}(q^{mk}, p^m)$ with vectors in R^k. This identification gives rise to the isomorphism $R^k \cong \mathrm{GR}(q^{mk}, p^m)$ as R-modules, providing an additional multiplicative structure on the vectors in R^r.

We define the *period* $\pi(x)$ of a Galois ring element $x \in R$ as the smallest non-negative integer s such that $xp^s = 0$. It holds that $\pi(x) = 0$ if and only if $x = 0$ and $\pi(x) = m$ if and only if x is a unit in R.

3 Linear codes over Galois rings

Here the basic notions of the theory of linear codes over Galois rings are given. For a deeper discussion the reader is referred to [15,17]. A good source for the theory of $\mathbb{Z}_4$-linear codes is [20, Chapter 12].

Let p be a prime, r be a positive integer, $q = p^r$, $R = \mathrm{GR}(q^m, p^m)$ and n be a positive integer. A subset $\mathcal{C}$ of R^n is called a *block code over R of length n*. If $\mathcal{C}$ is a submodule of the R-module R^n, $\mathcal{C}$ is an *R-linear code*.

Let $\mathcal{C}$ be a block code over R and $c \in R^n$ be a codeword. for $i \in \{0, \ldots, m\}$ we define $a_i(c)$ as the number of components of c of period i, and the *symmetrized weight* $w_{\mathrm{sym}}(c) = (a_0(c), \ldots, a_m(c))$. The *symmetrized weight enumerator* of $\mathcal{C}$ is

$$w_{\mathrm{sym}}(\mathcal{C}) = \sum_{c \in \mathcal{C}} \mathbf{X}^{w_{\mathrm{sym}}(c)} = \sum_{c \in \mathcal{C}} \prod_{i=0}^{m} X_i^{a_i(c)} \in \mathbb{Z}[X_0, \ldots, X_m].$$

Symmetrized weight enumerators will often be given as a table, where each line corresponds to a single monomial, listing the coefficient and the exponents of the respective polynomial indeterminates. The exponent of X_0 may be skipped, since it can be recovered from the length and the other exponents.

The *Hamming weight* of a codeword $c \in \mathcal{C}$ is the number of non-zero components $w_{\mathrm{Ham}}(c) = \sum_{i=1}^{m} a_i(c) = n - a_0(c)$. The *homogeneous weight* of a codeword $c \in \mathcal{C}$ is $w_{\mathrm{hom}}(c) = qa_1(c) + \sum_{i=2}^{m}(q-1)a_i(c)$. The *homogeneous weight enumerator* of $\mathcal{C}$ is $w_{\mathrm{hom}}(\mathcal{C}) = \sum_{c \in \mathcal{C}} X^{w_{\mathrm{hom}}(c)} = w_{\mathrm{sym}}(\mathcal{C})(1, q, q-1 \ldots, q-1)$. For $R = \mathbb{Z}_4$ the homogeneous weight is better known as the *Lee weight* w_{Lee}. Each of these weights has an associated distance function (d_{sym}, d_{Ham}, d_{hom} or d_{Lee}), mapping a pair of codewords (c_1, c_2) to the respective weight of $c_1 - c_2$.

The idea behind the homogeneous weight is that all non-zero ideals of R get the same average weight, which is $\gamma = q - 1$. It admits the *generalized Gray*

map, a distance preserving map $(R, d_{\mathrm{hom}}) \to (\mathbb{F}_q^{q^{m-1}}, q^{2-m} d_{\mathrm{Ham}})$, which allows the construction of – generally non-linear – codes over a q-ary alphabet from R-linear codes. For $m = 1$, w_{hom} is just $q w_{\mathrm{Ham}}$. For $m = 2$, the *Reed-Solomon map* γ_* in [29] is a suitable generalized Gray map. The homogeneous weight was introduced in [5] as a generalization of the Lee weight to integer residue rings $\mathbb{Z}_k$. For the case $k = p^2$, p prime, also a generalized Gray map was given. A more general notion of the homogeneous weight and the Gray map can be found in [19,10,11].

The *minimum homogeneous distance* $d_{\mathrm{hom}}(\mathcal{C})$ is the smallest homogeneous distance between two different codewords of $\mathcal{C}$. We say that $\mathcal{C}$ is a $(n, \#\mathcal{C}, d_{\mathrm{hom}}(\mathcal{C}))$-code or a $(n, \#\mathcal{C}, d_{\mathrm{hom}}(\mathcal{C}))_{\#R}$-code. For R-linear codes $\mathcal{C}$ we have that $d_{\mathrm{hom}}(\mathcal{C})$ equals the smallest non-zero homogeneous weight among the codewords.

Like in classical coding theory over finite fields, one of the main goals is to find a R-linear code for given length and size whose minimum homogeneous distance is as large as possible. As a special case of linear codes over finite chain rings, a table of R-linear codes of high minimum homogeneous distance can be found in [23].

Fact 1 ([8]) *Let $\mathcal{C}$ be an R-linear $(n, \#\mathcal{C}, d)$-code and $c \in \mathcal{C}$ with $\gamma w_{\mathrm{Ham}}(c) < d$. Puncturing $\mathcal{C}$ in the support of c yields the* residual *of $\mathcal{C}$ in c, which is an R-linear code with parameters $(n - w_{\mathrm{Ham}}(c), \quad \#\mathcal{C}/\#(Rc), \quad \geq d - \gamma w_{\mathrm{Ham}}(c))$.*

3.1 *R*-linear codes and projective Hjelmslev geometry

For the theory of projective Hjelmslev geometries see [16]. The connection to R-linear codes is described in [15,17].

The rough idea is the following: Given a $(k \times n)$ generator matrix of an R-linear code such that each column contains a unit, the columns can be interpreted as an n-element multiset of points in the projective Hjelmslev geometry $\mathrm{PHG}(R, k-1)$. Vice versa, given a multiset of points in $\mathrm{PHG}(R, k)$ one can associate an R-linear code by putting coordinate vectors of the points as columns into a generator matrix. Up to isomorphism, these operations are inverse to each other.

Now assume that we have $m = 2$. The symmetrized weight enumerator of an R-linear code translates into the *spectrum* of a multiset of points, which counts for each hyperplane H the number of points on H, the number of points neighbor to H but not on H, and the number of points not neighbor to H. For a single hyperplane H, these numbers are called the type of H. Given a multiset of points in $\mathrm{PHG}(R, k)$, a new multiset of points can be defined by selecting the hyperplanes of certain types with a multiplicity depending on the type and interpreting these hyperplanes as a multiset of points in the dual geometry (which interchanges the role of points and hyperplanes). If the selection of the hyperplanes can be done in a linear way in the sense of [18], then the spectrum of the dualized point set can be computed out of the original spectrum and the distribution of the points to the point classes.

3.2 The Kerdock codes

For $r \geq 3$ odd the code $\mathcal{K}_{r+1}$ 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 $\mathcal{K}_{r+1}$ is the Kerdock code as originally defined in [21]. For simplicity, we will use the term *Kerdock-code* for $\mathcal{K}_{r+1}$, too.

Fact 2 *Let $r \geq 3$ be odd. The code $\mathcal{K}_{r+1}$ is a $\mathbb{Z}_4$-linear code with the parameters*

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

The symmetrized weight enumerator of $\mathcal{K}_{r+1}$ is:

	$\#codewords$	a_0	a_1	a_2	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

Proof. In [20, Theorem 17.2.6], the Lee weight enumerator of $\mathcal{K}_{r+1}$ is given. The proof actually shows that the symmetrized weight enumerator is of the claimed form.

3.3 The Teichmüller Codes

Let r be a positive integer, $q = 2^r$ and $R = \mathrm{GR}(4^r, 4) = \mathrm{GR}(q^2, 4)$. Let further $k \geq 3$ be an odd integer and $S = \mathrm{GR}(4^{rk}, 4) = \mathrm{GR}(q^{2k}, 4)$. In the following we consider R as a subring of S. The Teichmüller units of S are a cyclic group T of order $q^k - 1$. Its cyclic subgroup U of order $q - 1$ is the group of Teichmüller units of R.

Now we define the *Teichmüller code* $\mathcal{T}_{q,k}$ as the R-linear code generated by a generator matrix, whose columns are set of representatives of the factor group T/U read as elements of R^k.

Fact 3 *Let $k \geq 3$ be odd, r be a positive integer and $q = 2^r$. The code $\mathcal{T}_{q,k}$ is a $\mathrm{GR}(q^2, 4)$-linear code with the parameters*

$$\left(\frac{q^k - 1}{q - 1}, \quad q^{2k}, \quad q^k - q^{\frac{k-1}{2}}\right).$$

The symmetrized weight enumerator of $\mathcal{T}_{q,k}$ is:

	#codewords	a_0	a_1	a_2	w_{Lee}
A	$\frac{1}{2}q^{\frac{k+1}{2}}\left(q^{\frac{k-1}{2}}-1\right)\left(q^k-1\right)$	$\frac{q^{k-2}-1}{q-1}-q^{\frac{k-3}{2}}$	$q^{k-2}+q^{\frac{k-3}{2}}$	q^{k-1}	$q^k+q^{\frac{k-1}{2}}$
B	$\frac{1}{2}q^{\frac{k+1}{2}}\left(q^{\frac{k-1}{2}}+1\right)\left(q^k-1\right)$	$\frac{q^{k-2}-1}{q-1}+q^{\frac{k-3}{2}}$	$q^{k-2}-q^{\frac{k-3}{2}}$	q^{k-1}	$q^k-q^{\frac{k-1}{2}}$
C	q^k-1	$\frac{q^{k-1}-1}{q-1}$	q^{k-1}	0	q^k
D	1	$\frac{q^k-1}{q-1}$	0	0	0

Proof. In [14, Example II.3], it was shown that the corresponding *Teichmüller point set* $\mathfrak{T}_{q,k}$ in the projective Hjelmslev geometry $\mathrm{PHG}(R,k-1)$ is a 2-intersection set with respect to point-hyperplane intersections, and the intersection numbers are $(q^{k-2}-1)/(q-1)-q^{(k-3)/2}$ and $(q^{k-2}-1)/(q-1)+q^{(k-3)/2}$. Each point class of $\mathrm{PHG}(R,k)$ contains exactly 1 point of $\mathfrak{T}_{q,k}$. A double counting argument gives the spectrum of $\mathfrak{T}_{q,k}$, and from this the symmetric weight enumerator of $\mathcal{T}_{q,k}$ can be derived.

In the planar case $k=3$, the Teichmüller point sets are exactly the hyperovals discussed in [13,16]. In the case $q=2$ we have $\#U=1$, and the Teichmüller codes are just the Kerdock codes shortened in a single coordinate and therefore very good codes. But also the generalized Gray image of $\mathcal{T}_{3,4}$ is a BTKL-code. Its parameters $(84,4^6,60)_4$ were first given in [13].

4 Dualization of the Kerdock codes

4.1 The code $\mathcal{K}^*_{r+1}$

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

Lemma 4 *Let $r\geq 3$ be odd. The code $\mathcal{K}^*_{r+1}$ is a $\mathbb{Z}_4$-linear code with parameters*

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

The symmetrized weight enumerator of $\mathcal{K}^*_{r+1}$ shown below. The codewords of lines B, D, E and F form a submodule of $\mathcal{K}^*_{r+1}$ of index 2.

	#codewords	a_1	a_2	w_{Lee}
A	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-2}-2^{\frac{r-3}{2}}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^r-2^{\frac{r-1}{2}}$
B	$2^{2r+1}-2^{r+1}$	$2^{2r-2}-2^{r-1}$	2^{2r-1}	$2^{2r}-2^r$
C	2^{r+1}	$2^{2r-2}+2^{\frac{3r-3}{2}}-2^{r-2}-2^{\frac{r-3}{2}}$	$2^{2r-1}-2^{r-1}$	$2^{2r}-2^r+2^{\frac{3r-1}{2}}-2^{\frac{r-1}{2}}$
D	2^r-1	2^{2r-1}	0	2^{2r}
E	2^r	$2^{2r-1}-2^{r-1}$	0	$2^{2r}-2^r$
F	1	0	0	0

Proof. The construction corresponds to the duality construction in [18]. Following this article, we define the function τ by setting

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

Dualizing the associated point set $\mathfrak{K}$ in $\mathrm{PHG}(\mathbb{Z}_4, r)$ with this function τ yields a new point set $\mathfrak{K}^*$, which generates $\mathcal{K}^*_{r+1}$. The formula in [18] yields the spectrum of $\mathfrak{K}^*$ and subsequently the symmetrized weight enumerator of $\mathcal{K}^*$. The submodule statement follows from the fact that the point classes not containing any point of $\mathfrak{K}_{r+1}$ form the neighbor class of a hyperplane in $\mathrm{PHG}(r, \mathbb{Z}_4)$.

4.2 The code $\hat{\mathcal{K}}^*_{r+1}$

Now we define $\hat{\mathcal{K}}^*_{r+1}$ as an extension of $\mathcal{K}^*_{r+1}$ by $2^{\frac{r-3}{2}}$ coordinates in the following way: The codewords corresponding to the lines B, D, E and F in the symmetrized weight enumerator of $\mathcal{K}^*_{r+1}$ 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 $\mathcal{K}^*_{r+1}$ is raised to match the second smallest Lee weight $2^{2r} - 2^r$ (lines B and E).

Theorem 5 *Let $r \geq 3$ be odd. The code $\hat{\mathcal{K}}^*_{r+1}$ is a $\mathbb{Z}_4$-linear code with parameters*

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

The Lee weight enumerator of $\hat{\mathcal{K}}^*_{r+1}$ is

$$1 \; + \; (2^{2r+2} - 2^{r+2} + 2^r) X^{2^{2r} - 2^r} \; + \; (2^r - 1) X^{2^{2r}} \; + \; 2^{r+1} X^{2^{2r} + 2^{\frac{3r-1}{2}} - 2^r}.$$

The symmetrized weight enumerator of $\hat{\mathcal{K}}^*_{r+1}$ is:

	#codewords	a_1	a_2	w_{Lee}
A	$2^{2r+1} - 2^{r+1}$	$2^{2r-2} - 2^{r-2}$	$2^{2r-1} - 2^{r-1}$	$2^{2r} - 2^r$
B	$2^{2r+1} - 2^{r+1}$	$2^{2r-2} - 2^{r-1}$	2^{2r-1}	$2^{2r} - 2^r$
C	2^{r+1}	$2^{2r-2} + 2^{\frac{3r-3}{2}} - 2^{r-2}$	$2^{2r-1} - 2^{r-1}$	$2^{2r} - 2^r + 2^{\frac{3r-1}{2}}$
D	$2^r - 1$	2^{2r-1}	0	2^{2r}
E	2^r	$2^{2r-1} - 2^{r-1}$	0	$2^{2r} - 2^r$
F	1	0	0	0

Proof. By Lemma 4, the codewords of the lines B, D, E and F in the symmetrized weight enumerator of $\mathcal{K}^*_{r+1}$ form a submodule of $\mathcal{K}^*_{r+1}$ of index 2. So the code $\hat{\mathcal{K}}^*_{r+1}$ is indeed $\mathbb{Z}_4$-linear. The statements about length and size of $\hat{\mathcal{K}}^*_{r+1}$ are clear, and the symmetrized weight enumerator of $\hat{\mathcal{K}}^*_{r+1}$ can be easily computed from the symmetrized weight enumerator of $\mathcal{K}^*_{r+1}$.

4.3 Examples and Derived Codes

By Theorem 5 the Gray image of $\hat{\mathcal{K}}_4^*$ is a nonlinear binary code with the parameters $(114, 2^8, 56)$, which is BTL. The Gray image of the residual in a codeword of line E has the BTL-parameters $(58, 2^7, 28)$, Recently the authors constructed a $\mathbb{Z}_4$-linear code with these parameters using a hyperoval in the projective Hjelmslev plane over $\mathbb{Z}_4$ [25].

The Gray image of $\hat{\mathcal{K}}_6^*$ is a nonlinear $(1988, 2^{12}, 992)$-code. It was possible to show computationally that this code is BTL, details will be published elsewhere.

The Gray image of the residual of $\hat{\mathcal{K}}_6^*$ in a codeword of type B has the parameters $(484, 2^{10}, 240)$. This code is BTKL, since an $\mathbb{F}_2$-linear $[484, 10, 240]$-code would have a $\mathbb{F}_2$-linear residual with the parameters $[244, 9, 120]$ which is not known.

On the other hand, we can construct a $\mathbb{Z}_4$-linear code out of $\hat{\mathcal{K}}_6^*$ whose Gray image has these parameters: We checked computationally that every residual in a codeword of type B has the symmetrized weight enumerator

$$2X_0^{30}X_1^{92}X_2^{120} + 60X_0^{46}X_1^{76}X_2^{120} + 480X_0^{58}X_1^{56}X_2^{128} + 450X_0^{62}X_1^{60}X_2^{120} + 15X_0^{114}X_1^{128} + 16X_0^{122}X_1^{120} + X_0^{242}.$$

Taking again the residual in a codeword of symmetrized weight $(122, 120, 0)$ yields a $\mathbb{Z}_4$-linear code whose Gray image has the BTKL-parameters $(244, 2^9, 120)$.

5 Dualization of the Teichmüller codes

In the following let r be a positive integer, $q = 2^r$, $R = \mathrm{GR}(4^r, 4) = \mathrm{GR}(q^2, 4)$, $k \geq 3$ and G be a generator matrix of $\mathcal{T}_{q,k}$. Furthermore, we take S as a set of projective representatives of information words $x \in R^k$ such that xG is a codeword of $\mathcal{T}_{q,k}$ of symmetrized weight A. The vectors in S are put as columns into a matrix A, and the code generated by A is denoted by $\mathcal{T}_{q,k}^*$.

Theorem 6 *The code $\mathcal{T}_{q,k}^*$ is a R-linear code with parameters*

$$\left(\frac{1}{2}q^{\frac{k-1}{2}}\left(q^{\frac{k-1}{2}}-1\right)\frac{q^k-1}{q-1},\quad q^{2k},\quad \frac{1}{2}\left(q^{2k-1}-q^{\frac{3k-1}{2}}-q^{k-1}\right)\right).$$

The symmetrized weight enumerator of $\mathcal{T}_{q,k}^*$ is:

	#codewords	a_1	a_2	w_{hom}
A	$q^{k+1}-q$	$\frac{1}{2}\left(q^{2k-3}-q^{k-2}\right)$	$\frac{1}{2}\left(q^{2k-2}-q^{\frac{3k-3}{2}}\right)$	$\frac{1}{2}\left(q^{2k-1}-q^{\frac{3k-1}{2}}+q^{\frac{3k-3}{2}}-q^{k-1}\right)$
B	$q^{2k}-q^{k+1}-q^k+q$	$\frac{1}{2}\left(q^{2k-3}-q^{k-2}-q^{\frac{3k-5}{2}}\right)$	$\frac{1}{2}\left(q^{2k-2}-q^{\frac{3k-3}{2}}\right)$	$\frac{1}{2}\left(q^{2k-1}-q^{\frac{3k-1}{2}}-q^{k-1}\right)$
C	q^k-1	$\frac{1}{2}\left(q^{2k-2}-q^{\frac{3k-3}{2}}\right)$	0	$\frac{1}{2}\left(q^{2k-1}-q^{\frac{3k-1}{2}}\right)$
D	1	$\frac{q^k-1}{q-1}$	0	0

Proof. The construction corresponds to the duality construction in [18]. Following this article, we define the function τ by setting

$$\alpha = \frac{1 + q^{\frac{k-1}{2}}}{2}, \quad \beta = -\frac{1}{2q^{\frac{k-3}{2}}}, \quad \gamma = 0.$$

Dualizing the associated point set $\mathfrak{T}$ in $\mathrm{PHG}(\mathbb{Z}_4, r)$ with this function τ yields a new point set $\mathfrak{T}^*$, which generates $\mathcal{T}^*_{q,r}$. The formula in [18] yields the spectrum of $\mathfrak{T}^*$ and subsequently the symmetrized weight enumerator of $\mathcal{T}^*$.

The code $\mathcal{T}^*_{2,3}$ equals $\mathcal{T}_{2,3}$. To see that the Gray image of $\mathcal{T}^*_{2,5}$ with the parameters $(372, 2^{10}, 184)_2$ is BTL, we look at the residual of a hypothetical $\mathbb{F}_2$-linear $[372, 10, 184]$-code. This would be an $\mathbb{F}_2$-linear $[188, 9, 92]$-code, and according to [9], such a code does not exist. Similarly, the residual of a hypothetical $\mathbb{F}_4$-linear $[504, 6, 376]$ code would be an $\mathbb{F}_4$-linear $[128, 5, 94]$-code, whose existence is not known. So the status of the Gray image of $\mathcal{T}^*_{4,3}$ which has the parameters $(504, 4^6, 376)_4$ is BTKL. The code $\mathcal{T}^*_{4,3}$ was first given in [22].

The Gray image of the residual of $\mathcal{T}^*_{2,5}$ in a codeword of symmetrized weight of type A is a non-linear $(60, 2^8, 28)$-code, which is BTL. In [1, Ex. 4] a quasi-cyclic $\mathbb{Z}_4$-linear construction for a code with these parameters was given. The Gray image of the residual of $\mathcal{T}^*_{2,5}$ in a codeword of symmetrized weight of type C is a non-linear $(180, 2^9, 88)$-code, which is a new example of a BTL-code.

References

1. Nuh Aydin and Dwijendra K. Ray-Chaudhuri, *Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes*, IEEE Trans. Inf. Theory **48** (2002), no. 7, 2065–2069.
2. A. E. Brouwer and L. M. G. M. Tolhuizen, *A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters*, Des. Codes Cryptogr. **3** (1993), 95–98.
3. A. R. Calderbank and Gary McGuire, *Construction of a $(64, 2^{37}, 12)$ code via Galois rings*, Des. Codes Cryptogr. **10** (1997), 157–165.
4. A. R. Calderbank, Gary McGuire, Vijay Kumar, and Tor Helleseth, *Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities*, IEEE Trans. Inf. Theory **42** (1996), no. 1, 217–226.
5. Ioana Constantinescu and Werner Heise, *A metric for codes over residue class rings*, Problems Inform. Transmission **33** (1997), 208–213.
6. P. Delsarte and J. M. Goethals, *Alternating bilinear forms over* GF_q, J. Combin. Theory Ser. A **19** (1975), no. 1, 26–50.
7. Jean-Marie Goethals, *Nonlinear codes defined by quadratic forms over* GF(2), Inform. and Control **31** (1976), no. 1, 43–74.
8. Marcus Greferath, Lecture at Cimpa-Unesco-Tübitak Summer School *Codes over Rings*, Middle East Technical University, Ankara, Turkey, August 2008
9. Markus Grassl, *Code Tables: Bounds on the parameters of various types of codes*, `www.codetables.de`.
10. Marcus Greferath and Stefan E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code.*, IEEE Trans. Inf. Theory **45** (1999), no. 7, 2522–2524.

11. ———, *Finite-ring combinatorics and MacWilliams' equivalence theorem*, J. Combin. Theory Ser. A **92** (2000), no. 1, 17–28.
12. 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. Inf. Theory **40** (1994), no. 2, 301–319.
13. Ludger Hemme, Thomas Honold, and Ivan Landjev, *Arcs in projective Hjelmslev spaces obtained from Teichmüller sets*, Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory 2000, 2000, pp. 4–12.
14. Thomas Honold, *Two-intersection sets in projective Hjelmslev spaces*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems, 2010, pp. 1807–1813.
15. Thomas Honold and Ivan Landjev, *Linear codes over finite chain rings.*, Electron. J. Combin. **7** (2000), #R11 (English).
16. Thomas Honold and Ivan Landjev, *On arcs in projective Hjelmslev planes*, Discrete Math. **231** (2001), no. 1–3, 265–278.
17. ———, *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.
18. ———, *The dual construction for arcs in projective Hjelmslev spaces*, Adv. Math. Commun. **5** (2011), no. 1, 11–21.
19. Thomas Honold and A. A. Nechaev, *Weighted modules and representations of codes*, Problems Inform. Transmission **35** (1999), no. 3, 205–223.
20. W. Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.
21. A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Inform. and Control **20** (1972), 182–187.
22. Michael Kiermaier and Axel Kohnert, *New Arcs in Projective Hjelmslev Planes Over Galois Rings*, Proceedings of the Fifth International Workshop on Optimal Codes and Related Topics 2007, 2007, pp. 112–119.
23. Michael Kiermaier and Johannes Zwanzger, *Online tables of linear codes over finite chain rings*, `codes.uni-bayreuth.de`.
24. ———, *A new series of $\mathbb{Z}_4$-linear codes of high minimum Lee distance derived from the Kerdock codes*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems, 2010, pp. 929–932.
25. ———, *A non-free $\mathbb{Z}_4$-linear code of high minimum Lee distance*, to appear in Advances in Mathematics of Communications, 2010.
26. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
27. Bernard R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.
28. A. A. Nechaev, *Kerdock code in a cyclic form*, Disc. Math. Appl. **1** (1991), no. 4, 365–384.
29. A. A. Nechaev and A. S. Kuzmin, *Linearly presentable codes*, Proceedings of the International Symposium on Information Theory and its Application (ISITA) 1996, 1996, pp. 31–34.
30. Alan W. Nordstrom and John P. Robinson, *An optimum nonlinear code*, Inform. and Control **11** (1967), no. 5–6, 613–616.
31. Franco P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Inform. and Control **13** (1968), no. 4, 378–400.