

# On the Minimum Distance of Some Families of $\mathbb{Z}_{2^k}$ -linear Codes\*

F. Galand

INRIA Rocquencourt, Projet CODES, Le Chesnay, France  
and GREYC, University of Caen, Caen, France.  
Fabien.Galand@inria.fr

## Abstract

With the help of a computer, we obtain the minimum distance of some codes belonging to two families of  $\mathbb{Z}_{2^k}$ -linear codes: the first is the generalized Kerdock codes which aren't as good as the best linear codes and the second is the Hensel lift of quadratic residue codes. In the latter, we found new codes with same minimum distances as the best linear codes of same length and same cardinality. We give a construction of binary codes starting with a  $\mathbb{Z}_{2^k}$ -linear code and adding cosets to it, increasing its cardinality and keeping the same minimum distance. This construction allows to derive a non trivial upper bound on cardinalities of  $\mathbb{Z}_{2^k}$ -linear Codes.

## 1 Introduction

The article of Hammons *et al.*, [1], gives a construction of Kerdock codes as images by the Gray map of linear codes over the ring of integers modulo 4,  $\mathbb{Z}_4$  (see also [2]). Such codes are called  $\mathbb{Z}_4$ -linear. The point is that the Gray map is a translation-invariant isometric mapping from  $\mathbb{Z}_4$  with Lee metric, to  $\text{GF}(2)^2$  with Hamming metric.

One can define a generalization of the Lee metric, called homogeneous metric (see [3]) over the ring of integers modulo  $2^k$ ,  $\mathbb{Z}_{2^k}$ , by the weight function

$$w_L(a) = \begin{cases} 0 & \text{if } a = 0, \\ 2^{k-2} & \text{if } a \neq 2^{k-1}, \\ 2^{k-1} & \text{if } a = 2^{k-1}. \end{cases}$$

The nice feature of this metric is that we know a translation-invariant isometric mapping (see [4]) from  $\mathbb{Z}_{2^k}$  to a subset of  $\text{GF}(2)^{2^{k-1}}$ , namely the Reed-Muller

---

\*in proceedings of the 15th AAECC International Symposium, Springer-Verlag, LNCS 2643, 2003, p. 235 – 243.

code of length  $2^{k-1}$  and order 1,  $\text{RM}(1, k-1)$ . This mapping is called the generalized Gray map,  $\Psi$  and is defined by

$$\Psi(a) : (y_1, \dots, y_{k-1}) \mapsto a_k + \sum_{i=1}^{k-1} a_i y_i ,$$

where  $a = \sum a_i 2^i \in \mathbb{Z}_{2^k}$  and  $a_i \in \text{GF}(2)$ . With this mapping, binary codes can be constructed from codes over  $\mathbb{Z}_{2^k}$  by taking their images with the generalized Gray map. The binary images have same cardinalities as codes over  $\mathbb{Z}_{2^k}$  and their minimum Hamming distances are the minimum homogeneous distances of the codes over  $\mathbb{Z}_{2^k}$ . Moreover, if the code over  $\mathbb{Z}_{2^k}$  is linear, its binary image  $C$  is distance-invariant, that is all its cosets of the form  $c + C$ , with  $c \in C$  have the same distance distribution. We call  $\mathbb{Z}_{2^k}$ -linear the codes equal to images by the generalized Gray map of linear codes over  $\mathbb{Z}_{2^k}$ .

With the generalized Gray map came a natural generalization of Kerdock codes, which can be better than the best linear codes. In the Section §3, we address the issue of their minimum distance with the help of a computer. We show that these codes are not good for short lengths.

The Hensel lift to  $\mathbb{Z}_4$  of quadratic residue codes is known to give good binary codes [5, 6, 7, 8]. We study their Hensel lift to  $\mathbb{Z}_{2^k}$ , still using a computer. We obtain new results for several codes. In particular we find a  $\mathbb{Z}_{16}$ -linear code whose parameters are equal to those of the best known linear code.

Finally, in [8], Duursma *et al.* use the union of 2 cosets of a  $\mathbb{Z}_8$ -linear code to construct a bigger code with same length and minimum distance. We generalize this construction to  $\mathbb{Z}_{2^k}$ , the number of cosets which are used depending on  $k$  and on the parameters of the  $\mathbb{Z}_{2^k}$ -linear code. This construction yields a non trivial upper bound on the cardinalities of  $\mathbb{Z}_{2^k}$ -linear codes.

## 2 Background

### 2.1 Galois Rings

We recall basic facts about Galois rings ([9, 1]) since we will need them to define generalized Kerdock codes in §3.

Galois rings are finite rings isomorphic to quotient rings  $\mathbb{Z}_{p^k}[X]/(P)$  where  $p$  is a prime and  $P$  is a unitary polynomial such that  $P \pmod{p}$  is an irreducible polynomial with coefficients in  $\text{GF}(p)$ . We denote  $\text{GR}(p^k, m)$  the Galois ring isomorphic to  $\mathbb{Z}_{p^k}[X]/(P)$  where  $P$  has degree  $m$ . The set of roots of  $X^{p^m-1} - 1$  is a cyclic multiplicative group of order  $p^m - 1$ . Adding 0 to this group, we get the Teichmuller set,  $\mathcal{T} = \{0, \zeta, \dots, \zeta^{p^m-1}\}$  with  $\zeta$  a generator of the cyclic group. If we choose for  $P$  a polynomial such that  $P \pmod{p}$  is primitive, then we can take  $\zeta = X \pmod{P}$ . The quotient ring  $\text{GR}(p^k, m)/(p)$  is simply the field  $\text{GF}(p^m)$  and the Teichmuller set is a set of representatives of the equivalence classes of  $\text{GR}(p^k, m)$  modulo  $p$ .

As with finite fields, the automorphism group of  $\text{GR}(p^k, m)$  is cyclic of order  $m$ , and generated by a particular element  $\sigma$ , the Frobenius map, which coincides

with the power function exponent  $p$  on the Teichmuller set and with identity on the subring  $\mathbb{Z}_{p^k}$ . Using the additive representation of the elements of  $\text{GR}(p^k, m)$  (the elements are polynomials over  $\mathbb{Z}_{p^k}$  in  $\zeta$  of degree strictly less than  $m$ ),  $\sigma$  is defined by

$$\sigma(\alpha) = \sum_{i=0}^{m-1} a_i \zeta^{i p} ,$$

for every  $\alpha = \sum a_i \zeta^i$ . Over the ring  $\text{GR}(p^k, m)$  one can define a trace mapping,  $\text{Tr}: \text{GR}(p^k, m) \rightarrow \mathbb{Z}_{p^k}$ , which is the sum over all the automorphisms,

$$\text{Tr}(\alpha) = \sum_{j=0}^{m-1} \sigma^j(\alpha).$$

This mapping is a linear form over  $\text{GR}(p^k, m)$ . Moreover, every linear form over  $\text{GR}(p^k, m)$  has the form  $x \mapsto \text{Tr}(\alpha x)$  for some  $\alpha \in \text{GR}(p^k, m)$ .

## 2.2 Hensel Lift and Cyclic Codes

The Hensel lift can be viewed as a toolbox for constructing cyclic codes over  $\mathbb{Z}_{2^k}$  from binary cyclic codes. We focus on cyclic codes of odd length  $n$  over  $\mathbb{Z}_{2^k}$  which are free modules. These codes are ideals of  $\mathbb{Z}_{2^k}[X]/(X^n - 1)$  generated by a polynomial  $g^{(k)}$  dividing  $X^n - 1$ . Such polynomials can be obtained by Hensel lifting from binary polynomials dividing  $X^n - 1$ , more precisely, if  $f$  divides  $X^n - 1$  in  $\text{GF}(2)$ , then there exists a unique unitary polynomial  $f^{(k)}$  of  $\mathbb{Z}_{2^k}[X]$  dividing  $X^n - 1$  such that  $f^{(k)} = f \pmod{2}$ .

In the sequel a cyclic code over  $\mathbb{Z}_{2^k}$  obtained this way will be referred to as Hensel lift of the binary code (for properties of (cyclic) codes over  $\mathbb{Z}_{p^k}$  see [10, 11]).

## 3 Generalized Kerdock Codes and Their Parameters

The Kerdock code of length  $2^{m+1}$  ( $m$  odd) is known to be the image by the Gray map of affine functions over  $\text{GR}(4, m)$  (viewed as a  $\mathbb{Z}_4$ -module) restricted to the Teichmuller set (cf. [1]). This led to define generalized Kerdock codes  $\mathcal{K}(k, m)$  as the image by his generalized Gray map of affine functions over  $\text{GR}(2^k, m)$  (viewed as a  $\mathbb{Z}_{2^k}$ -module) restricted to the Teichmuller set, write  $\text{AF} = \{x \mapsto \text{Tr}(\alpha x) + b \mid \alpha \in \text{GR}(2^k, m), b \in \mathbb{Z}_{2^k}\}$  the set of affine functions,

$$\mathbf{K}(k, m) = \left\{ \left( \mathbf{c}(0), \mathbf{c}(1), \mathbf{c}(\zeta), \dots, \mathbf{c}(\zeta^{2^m-2}) \right) \mid \mathbf{c} \in \text{AF} \right\}$$

the set of  $2^m$ -tuples corresponding to restrictions of affine functions to the Teichmuller set, then  $\mathcal{K}(k, m) = \Psi(\mathbf{K}(k, m))$  (see [4]). Thus, these codes are of lengths  $2^{k+m-1}$  and cardinality  $2^{k(m+1)}$ . We have the following lower bound on the minimum distance  $\delta$

**Proposition 1** (Carlet [4, §IV Cor. 1])

$$\delta \geq 2^{m+k-2} - 2^{k+\lceil \frac{m}{2^{k-1}} \rceil - 4} \cdot \left\lfloor 2^{\frac{m}{2}+2-\lceil \frac{m}{2^{k-1}} \rceil} (2^{k-1} - 1) \right\rfloor . \quad (1)$$

*Cyclic Structure of Generalized Kerdock Codes.* We proved that generalized Kerdock codes are related to cyclic codes over  $\mathbb{Z}_{2^k}$  (recall that over  $\mathbb{Z}_{2^k}$  we can define duality with respect to the usual inner product).

**Proposition 2** *The code  $\mathbf{K}(k, m)$  is the dual of an extended cyclic code over  $\mathbb{Z}_{2^k}$ . Moreover, if  $k \leq m$ , then  $\mathbf{K}(k, m)$  is an extended cyclic code over  $\mathbb{Z}_{2^k}$ .*

*Proof.*

Due to length constraint we refer to [12]. □

*Generalized Preparata Codes.* Kerdock codes ( $k = 2$ ) are related to Preparata codes, their  $\mathbb{Z}_4$ -duals: the Gray image of dual of  $\mathbf{K}(2, m)$  is a Preparata code (cf. [1]) in the sense it has the same parameters and weight distribution. A natural generalization of Preparata codes is

**Definition 1** *The generalized Preparata code,  $\mathcal{P}(k, m)$ , is the generalized Gray image of the dual of  $\mathbf{K}(k, m)$ .*

*Minimum distance.* Carlet asked for the accuracy of the lower bound (1), particularly in the case  $k = 3$ , since for this value of  $k$ , it is close to the minimum distance of the dual of 3-error correcting BCH code of the same length (parameters of this dual are  $[2^{m+2} - 1, 3m + 6, 2^{m+1} - 2^{(m+3)/2}]$ ). With the help of a computer we computed some minimum distances of generalized Kerdock codes. The results are in Table 1 (notation  $\{n, k, d\}$  means length  $n$ , cardinality  $2^k$  and minimum distance  $d$ ). In fact, when possible we computed the whole weight distribution of the code  $\mathbf{K}(k, m)$ , and we used the MacWilliams identities (over  $\mathbb{Z}_{2^k}$ ) to get the weight distribution of its dual, leading to minimum distance of generalized Preparata Codes (see Table 2). Comparing this with Brouwer's table of the best linear codes show (see Table 3 and [13]), except for the case  $k = m = 3$ , generalized Kerdock and Preparata codes are not as good as the best linear codes for the parameters we were able to compute. Moreover, the bound seems tight, so it is very likely that duals of BCH codes are better than generalized Kerdock codes and we check it is actually true for the parameters we computed: they are shorter, bigger and with larger minimum distance.

## 4 Hensel lift of Binary Quadratic Residue Codes

The idea was to lift good binary cyclic codes to  $\mathbb{Z}_{2^k}$ , we choose binary quadratic residue codes,  $\text{QR}(n)$ , since they fulfill this criteria. Codes obtained by Hensel lift of their generating polynomial to  $\mathbb{Z}_4$  had been studied for several lengths, see [5] ( $n = 17, 23$ ), [6] ( $n = 31, 47$ ), [7] ( $n = 31$ ). The codes of [5] are as good as the best linear codes and those of [6] are better (for same length and cardinality).

Table 1: Parameters of  $\mathcal{K}(k, m), \{2^{(m+k-1)}, k(m+1), \delta\}$  .

$m \setminus k$	2	3	4	5
3	{16, 8, 6}	{32, 12, 10}	{64, 16, 20}	{128, 20, 40}
4	{32, 10, 12}	{64, 15, 20}	{128, 20, 40}	{256, 25, 80}
5	{64, 12, 28}	{128, 18, 44}	{256, 24, 88}	{512, 30, 176}
6	{128, 14, 56}	{256, 21, 96}	{512, 28, 192}	{1024, 35, 384}
7	{256, 16, 120}	{512, 24, 212}	{1024, 32, 424}	
8	{512, 18, 240}	{1024, 27, 440}		
9	{1024, 20, 496}	{2048, 30, 928}		
10	{2048, 22, 992}	{4096, 33, 1888}		

$m \setminus k$	6	7	8
3	{256, 24, 80}	{512, 28, 160}	{1024, 32, 320}
4	{512, 30, 160}		

Table 2: Parameters of  $\mathcal{P}(k, m), \{2^{(m+k-1)}, k(2^m - (m+1)), \delta\}$  .

$m \setminus k$	2	3	4	5
3	{16, 8, 6}	{32, 12, 10}	{64, 16, 20}	{128, 20, 40}
4	{32, 22, 4}	{64, 33, 8}	{128, 44, 16}	{256, 55, 32}
5	{64, 52, 6}	{128, 78, 10}	{256, 104, 20}	{512, 130, 40}
6	{128, 114, 4}	{256, 171, 8}	{512, 228, 16}	
7	{256, 240, 6}	{512, 360, 10}	{1024, 480, 20}	
8	{512, 494, 4}	{1024, 741, 8}		
9	{1024, 1004, 6}	{2048, 1506, 10}		
10	{2048, 2026, 4}			

$m \setminus k$	6	7
3	{256, 24, 80}	{512, 28, 160}
4	{512, 66, 64}	

Table 3: Extract from (Binary) Brouwer's table: bound on the best minimum distance for linear codes of the same length and the same cardinality than  $\mathcal{K}(k, m)$  (left) and  $\mathcal{P}(k, m)$  (right).

$m \setminus k$	2	3	4	5	6	$m \setminus k$	2	3	4	5	6
3	5	10	24	48-53	100-114	3	5	10	24	48-53	100-114
4	12	24	48-53	100-114		4	5	12-14	28-38	68-96	
5	25-26	48-54	100-114			5	5	16-22	46-71		
6	56-57	112-116				6	5	24-34			
7	113-120					7	5				

Table 4: Bound (1) and true minimum distance  $\delta$  of  $\mathcal{K}(3, m)$ .

$m$	3	4	5	6	7	8	9	10
$\delta$	10	20	44	96	212	440	928	1888
bound (Prop. 1)	0	8	32	80	190	416	892	1856
error (%)	-	60	27.3	16.7	10.4	5.5	3.9	1.7

Duursma *et al.* lifted QR(23) to  $\mathbb{Z}_8$  and thus got a code better than previously known codes (linear or not). It is the only example of a good code obtained by Hensel lift to  $\mathbb{Z}_{2^k}$  with  $k > 2$ . But the authors didn't stop at this point, they used a union of 2 cosets to construct a bigger code. We will go back to this in the next section.

Following this work, we lifted generating polynomial of QR( $n$ ) for  $n = 17, 23, 31, 47$  to  $\mathbb{Z}_8$  and  $\mathbb{Z}_{16}$ , extended the resulting codes by a parity-check symbol, then computed their minimum distance with computer assistance. Results are shown in Table 5, bold (resp. italic) is for codes better than (resp. as good as) the best linear ones and \* is only an upper bound on minimum distance. Note that extended lift to  $\mathbb{Z}_8$  of QR for length 31 and 47 and extended lift to  $\mathbb{Z}_{16}$  of QR(31) reach the parameters of best linear codes.

Table 5: Parameters of generalized Gray image of extended Hensel lift of QR( $n$ ) (left) and minimum distance of the best known linear codes of same length and size (right).

$n$	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{16}$	$n$	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{16}$
17	{36, 18, 8}	{72, 27, 16}	{144, 36, 32}	17	8	19	38
23	{48, 24, <i>12</i> }	{96, 36, <b>24</b> }	{192, 48, <i>48</i> }	23	<i>12</i>	<b>20</b>	<i>48</i>
31	{64, 32, <b>14</b> }	{128, 48, <i>28</i> }	{256, 64, <i>56*</i> }	31	<b>12</b>	<i>28</i>	62
47	{96, 48, <b>18</b> }	{192, 72, <i>36</i> }		47	<b>16</b>	<i>36</i>	

\*: only an upper bound

## 5 Constructing Binary Codes Using $\mathbb{Z}_{2^k}$ -linear Codes

By definition of the generalized Gray map  $\Psi$ , the images of codes of length  $n$  over  $\mathbb{Z}_{2^k}$  are subsets of  $\text{RM}(1, k-1)^n$ .

Let  $\mathcal{C} \subset \text{RM}(r, m)^n$  be a binary code of minimum distance  $d$ . If we can find cosets of  $\mathcal{C}$  at distance at least  $d$  from each other then, we can perform the union of these cosets, getting a code with same length and same minimum distance as  $\mathcal{C}$ , but with larger cardinality. We study below a construction of such cosets relying on non binary codes and possibility to find cosets of  $\text{RM}(r, m)$  far enough from each other.

Namely we are searching for a set  $T \subset (\text{GF}(2)^{2^m})^n$  such that the sum of any two elements is at Hamming distance at least  $d$  from the set  $\text{RM}(r, m)^n$ .

**Theorem 1** Let  $\mathcal{C} \subset \text{RM}(r, m)^n$  be a binary code of minimum distance  $d$ . Let  $S$  be a subset of  $\text{GF}(2)^{2^m}$  such that

$$\forall z \in \text{RM}(r, m), \forall (x, y) \in S \times S, x \neq y \quad w(x + y + z) \geq d_S ,$$

and  $T \subset S^n$  with

$$\forall (\mathbf{u}, \mathbf{v}) \in T \times T, \mathbf{u} \neq \mathbf{v}, \quad |\{i : u_i \neq v_i\}| \geq d_T .$$

If the inequality  $d_T \cdot d_S \geq d$  holds, then the cosets  $\mathbf{t} + \mathcal{C}$ ,  $\mathbf{t} \in T$ , are pairwise disjoint and the code  $\mathcal{G}$  of length  $n \cdot 2^m$  defined by

$$\mathcal{G} = \bigcup_{\mathbf{t} \in T} (\mathbf{t} + \mathcal{C})$$

is of cardinality  $|T| \cdot |\mathcal{C}|$  and minimum distance  $d$ .

*Proof.*

Let  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{b} = (b_1, \dots, b_n)$  be two distinct codewords of  $\mathcal{C}$ , with  $a_i, b_i$  in  $\text{RM}(r, m) \subset \text{GF}(2)^{2^m}$  and  $\mathbf{u} = (u_1, \dots, u_n)$ ,  $\mathbf{v} = (v_1, \dots, v_n)$  with  $u_i, v_i$  in  $S$ . Then,

$$w(\mathbf{a} + \mathbf{u} + \mathbf{b} + \mathbf{v}) = \sum_{i=0}^n w(a_i + u_i + b_i + v_i) .$$

We have the two following cases:

1.  $\mathbf{u} = \mathbf{v}$ , so  $\mathbf{a} + \mathbf{u}$  and  $\mathbf{b} + \mathbf{v}$  are in the same coset of  $\mathcal{C}$ , thus

$$w(\mathbf{a} + \mathbf{u} + \mathbf{b} + \mathbf{v}) = w(\mathbf{a} + \mathbf{b}) \geq d ;$$

2.  $\mathbf{u} \neq \mathbf{v}$ , so  $\mathbf{a} + \mathbf{u}$  and  $\mathbf{b} + \mathbf{v}$  are in different cosets, and we have

$$w(\mathbf{a} + \mathbf{u} + \mathbf{b} + \mathbf{v}) \geq \sum_{u_i \neq v_i} w(a_i + u_i + b_i + v_i) .$$

By linearity of  $\text{RM}(r, m)$ ,  $a_i + b_i$  is in  $\text{RM}(r, m)$  and the hypothesis on  $S$  leads to

$$w(\mathbf{a} + \mathbf{u} + \mathbf{b} + \mathbf{v}) \geq |\{i : u_i \neq v_i\}| \cdot d_S .$$

Since we have  $|\{i : u_i \neq v_i\}| \geq d_T$  and  $d_T \cdot d_S \geq d$ , we have  $w(\mathbf{a} + \mathbf{u} + \mathbf{b} + \mathbf{v}) \geq d$  and two different cosets are at distance at least  $d$ , in particular they are disjoint.

□

Now, we have to find sets  $S$  and  $T$  fulfilling the required hypothesis to get an effective construction. In view of Theorem 1, it is natural to take a concatenated code [14] for  $T$  and regard  $S$  as the inner code.

We start with  $S$ , using the well known construction of the Reed-Muller code  $\text{RM}(r+a, m)$  from  $\text{RM}(r, m)$  ([15, Chp. 13 §3]). Recall that  $\text{RM}(r+a, m)$  is the

union of  $2^l$  different cosets of  $\text{RM}(r, m)$ , with  $l = \binom{m}{r+a} + \binom{m}{r+a-1} + \dots + \binom{m}{r+1}$ . We take for  $S$  a set of coset representatives, so  $|S| = 2^l$  and it is easy to see  $d_S = 2^{m-r-a}$ , which is the minimum distance of  $\text{RM}(r+a, m)$ . To construct  $T$ , we use as an outer code, a code  $C$  of length  $n$  and minimum distance  $d_T \geq d/2^{m-r-a}$  over  $(GF)(2^l)$ , we choose a one to one mapping  $\varphi: GF(2^l) \rightarrow S$  and we define  $T$  by

$$T = \varphi(C) = \left\{ (\varphi(c_1), \dots, \varphi(c_n)) \mid (c_1, \dots, c_n) \in C \right\} .$$

Thus, we can apply Theorem 1. Note that the code  $\mathcal{G}$  we obtain this way is a subset of  $\text{RM}(r+a, m)^n$ , and so we can iterate the construction.

**Example 1** For  $\mathbb{Z}_8$  we have  $r = 1$ ,  $m = 2$ , and  $S = \{0000, 1000\}$ . If the  $\mathbb{Z}_8$ -linear code is  $\{96, 36, 24\}$ , we have only one possibility for  $C$ : the trivial binary code of length 24. This was used in [8].

*Bound on Cardinality of  $\mathbb{Z}_{2^k}$ -linear codes.* Since we can apply our construction, one can think intuitively that the subsets of  $\mathcal{C} \subset \text{RM}(1, k-1)^n$  aren't good codes, in particular for  $\mathbb{Z}_{2^k}$ -linear codes,  $k > 2$ . This can be formalized and yields to a bound on the cardinality of codes which are subsets of  $\text{RM}(r, m)^n$ .

**Corollary 1** Let  $\mathcal{C} \subset \text{RM}(r, m)^n$  be of minimum distance  $d$ . Then, we have the following bound on the cardinality of  $\mathcal{C}$  :

$$|\mathcal{C}| \leq \frac{A_{n \cdot 2^m}^d(2)}{A_n^{\lceil 2^{r+a-m} \cdot d \rceil}(2^l)} ,$$

where  $A_n^d(q)$  denote the maximum cardinality for a code of length  $n$  and minimum distance less or equal to  $d$  over  $GF(q)$  and  $l = \sum_{i=1}^a \binom{m}{r+i}$ .

*Proof.*

Choose for  $C$  a code of length  $n$ , minimum distance  $\lceil 2^{r+a-m} \cdot d \rceil$  and maximal cardinality  $A_n^{\lceil 2^{r+a-m} \cdot d \rceil}(2^l)$  over  $GF(2^l)$ . Using for  $S$  a set of coset representatives of  $\text{RM}(r, m)$  in  $\text{RM}(r+a, m)$ , and applying Theorem 1 the code  $\mathcal{G}$  is of length  $n \cdot 2^m$  and minimum distance  $d$ . Therefor,  $|\mathcal{G}| \leq A_{n \cdot 2^m}^d(2)$ , since  $|\mathcal{G}| = |\mathcal{C}| \cdot |C|$ , we have the bound

$$|\mathcal{C}| \leq \frac{A_{n \cdot 2^m}^d(2)}{A_n^{\lceil 2^{r+a-m} \cdot d \rceil}(2^l)} .$$

□

Using the fact we can iterate the construction leads to the following

**Corollary 2** Let  $\mathcal{C} \subset \text{RM}(r, m)^n$  be of minimum distance  $d$ , and  $s_0 = r < s_1 < \dots < s_t \leq m$ . Then

$$|\mathcal{C}| \leq \frac{A_{n \cdot 2^m}^d(2)}{\prod_{j=1}^t A_n^{\lceil 2^{s_j-m} \cdot d \rceil}(2^{l_j})} , \quad (2)$$

$$\text{with } l_j = \sum_{i=s_{j-1}+1}^{s_j} \binom{m}{i}.$$

**Remark 1** We use for  $S$  a set of cosets representatives of  $\text{RM}(r, m)$  in  $\text{RM}(r+a, m)$  but, there exist other possibilities. For instance, when  $m$  is even and  $r = a = 1$  we can use a set of cosets representatives of  $\text{RM}(1, m)$  in the Kerdock code of length  $2^m$ . It leads to a smaller  $S$  (only  $2^m$  elements instead of  $2^{m(m-1)/2}$ ) but  $d_S$  is nearly twice as big ( $2^{m-1} - 2^{(m-2)/2}$  instead of  $2^{m-2}$ ). Of course, this yields different bounds.

*Asymptotic behavior of  $\mathbb{Z}_{2^k}$ -linear codes.* Recall the rate  $R$  of a  $(n, M, d)$  code over  $\text{GF}(q)$  is defined by  $R = \log_q(M)/n$ . Denote by  $UR(x)$  an asymptotic upper bound on the rate of binary codes of length  $n$  and minimum distance  $x \cdot n$ , for  $n \rightarrow \infty$  and denote by  $LR_q(x)$  an asymptotic lower bound on the maximum rate of codes of length  $n$  over  $\text{GF}(q)$  and minimum distance  $x \cdot n$ .

An asymptotic version of Corollary 2 is

**Corollary 3** Let  $R_m(x)$  be the asymptotic maximum rate for binary codes of length  $2^m \cdot n$ , minimal distance  $x \cdot 2^m \cdot n$  which are subsets of  $\text{RM}(1, m)^n$ . With notations of Corollary 2 we have

$$R_m(x) \leq UR(x) - \frac{1}{2^m} \sum_{j=1}^t l_j LR_{2^{l_j}}(x \cdot 2^{s_j})$$

*Proof.*

Taking logarithm of (2) and dividing by  $2^m \cdot n$ , we have

$$\frac{\log_2(|\mathcal{C}|)}{2^m \cdot n} \leq \frac{\log_2(A_{n \cdot 2^m}^d(2))}{2^m \cdot n} - \sum_{j=1}^t \frac{1}{2^m} \cdot \frac{\log_2(A_n^{\lceil 2^{s_j} \cdot d \rceil}(2^{l_j}))}{n}.$$

Thus, for  $x = d/(2^m \cdot n)$  fixed and  $n$  growing to infinity,

$$R_m(x) \leq UR(x) - \frac{1}{2^m} \sum_{j=1}^t \log_2(2^{l_j}) LR_{2^{l_j}}(x \cdot 2^{s_j}),$$

since  $x \cdot 2^{s_j}$  is the relative distance of the  $2^{l_j}$ -code of cardinality  $A_n^{\lceil 2^{s_j} \cdot d \rceil}(2^{l_j})$  and length  $n$ .

Asymptotic lower bound on  $A_n^\delta(q)$  is known, for exemple Gilbert-Varshamov bound states that

$$\lim_{n \rightarrow \infty} \frac{\log_q A_n^\delta(q)}{n} \geq 1 - H_q\left(\frac{\delta}{n}\right),$$

for fixed ratio  $\delta/n$  and with  $H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$ . On the other hand, we have Elias upper bound,

$$\lim_{n \rightarrow \infty} \frac{\log_2 A_n^\delta(2)}{n} \leq 1 - H_2\left(\frac{1}{2} \left(1 - \sqrt{1 - 2\frac{\delta}{n}}\right)\right),$$

still for fixed  $\delta/n$ . With those bounds and taking  $s_j = j + 1$ ,  $j \in [1, m - 1]$  in the previous corollary, we obtain

$$R_m(x) \leq 1 - H_2 \left( \frac{1}{2} (1 - \sqrt{1 - 2x}) \right) - \frac{1}{2^m} \sum_{i=2}^m l_i (1 - H_{2^i}(x \cdot 2^i))$$

with  $l_i = \binom{m}{i}$ .

## References

- [1] Hammons, R., Kumar, P., Calderbank, A., Sloane, N., Solé, P.: Kerdock, Preparata, Goethals and other codes are linear over  $\mathbb{Z}_4$ . *IEEE Transactions on Information Theory* **IT-40** (1994) 301–319
- [2] Nechaev, A.: Kerdock codes in a cyclic form. *Discrete Mathematics and Applications* **1** (1991) 365–384 (Translated from russian, *Diskretnaya Matematika*, vol. 1, n° 4, 1989, pp. 123–139).
- [3] Constantinescu, I., Heise, W.: A metric for codes over residue class rings. *Problems of Information Transmission* **33** (1997) 208–213 (Translated from russian, *Problemy Peredachi Informatsii*, vol. 33, n° 3, 1997, pp. 22–28).
- [4] Carlet, C.:  $\mathbb{Z}_{2^k}$ -linear codes. *IEEE Transactions on Information Theory* **IT-44** (1998) 1543–1547
- [5] Bonnecaze, A., Solé, P., Calderbank, A.: Quaternary quadratic residue codes and unimodular lattices. *IEEE Transactions on Information Theory* **IT-41** (1995) 366–377
- [6] Pless, V., Qian, Z.: Cyclic codes and quadratic residue codes over  $\mathbb{Z}_4$ . *IEEE Transactions on Information Theory* **IT-42** (1996) 1594–1600
- [7] Calderbank, A., McGuire, G., Kumar, P., Helleseth, T.: Cyclic codes over  $\mathbb{Z}_4$ , locator polynomials and Newton’s identities. *IEEE Transactions on Information Theory* **IT-42** (1996) 217–226
- [8] Duursma, I., Greferath, M., Litsyn, S., Schmidt, S.: A  $\mathbb{Z}_8$ -linear lift of the binary Golay code and a non-linear binary  $(96, 2^{37}, 24)$  code. *IEEE Transactions on Information Theory* **IT-47** (2001) 1596–1598
- [9] MacDonald, B.: *Finite Rings with Identity*. Dekker (1974)
- [10] Calderbank, A., Sloane, N.: Modular and  $p$ -adic cyclic codes. *Designs, Codes and Cryptography* **6** (1995) 21–35
- [11] Kanwar, P., López-Permouth, S.: Cyclic codes over the integers modulo  $p^m$ . *Finite Fields and Their Applications* (1997) 334–352
- [12] Galand, F.: Codes  $\mathbb{Z}_{2^k}$ -lineaires. Technical report, (INRIA) To appear.

- [13] Brouwer, A.: Bounds on the Size of Linear Codes. In: Handbook of Coding Theory. Volume 1. North-Holland (1998) 295–461.  
(<http://www.win.tue.nl/~aeb/voorlincod.html>).
- [14] Dumer, I.: Concatenated Codes and Their Multilevel Generalizations. In: Handbook of Coding Theory. Volume 2. North-Holland (1998) 1911–1988
- [15] MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. 3 edn. North-Holland (1996)