AALBORG UNIVERSITY

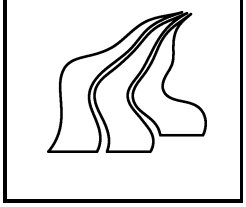
On lower existence bounds for the asymptotic parameters of $\mathbb{Z}_{2^l}-$linear codes

by

Bo Hove and Christian Thommesen

December 2003 R-2003-23

DEPARTMENT OF MATHEMATICAL SCIENCES
AALBORG UNIVERSITY
Fredrik Bajers Vej 7 G ▪ DK - 9220 Aalborg Øst ▪ Denmark
Phone: +45 96 35 80 80 ▪ Telefax: +45 98 15 81 29
URL: www.math.auc.dk/research/reports/reports.htm



ISSN 1399–2503 ▪ On-line version ISSN 1601–7811

On lower existence bounds for the asymptotic parameters of $\mathbb{Z}_{2^l}-$linear codes

Bo Hove Christian Thommesen*

December 15, 2003

Abstract

Recently $\mathbb{Z}_4-$linear codes has been generalized to the so called $\mathbb{Z}_{2^l}-$linear codes. By considering $\mathbb{Z}_{2^l}-$linear codes as concatenated codes we derive lower bounds on their minimum distance and error exponents.

Keywords: $\mathbb{Z}_{2^l}-$linear codes, concatenated codes, Gilbert-Varshamov bound, error exponent, weight distribution.

I Introduction

In [1], [2], [3] concatenated codes with fixed inner code and the outer code randomly selected is analyzed. For these codes a lower existence bound on the asymptotic parameters is derived and this bound is compared to the Gilbert-Varshamov bound. Furthermore an upper bound on the weight distribution of these codes is determined and this bound is then used to examine the error performance of the codes when used on the $q-$ary symmetric channel with symbol to symbol error probability $p/(q-1)$ and decoded by the maximum likelihood rule.

In this paper we perform a similar analysis of the so called $\mathbb{Z}_{2^l}-$linear codes (defined in [4]) which are a generalization of $\mathbb{Z}_4-$linear codes. To perform this analysis we consider $\mathbb{Z}_{2^l}-$linear codes as concatenated codes (described in Section I-C). To carry out this analysis we need to

*Bo Hove is with Thisted Gymnasium DK-7700 Thisted, Denmark and Christian Thommesen is with the Department of mathematical sciences, Aalborg University DK-9220 Aalborg Ø, Denmark.

define some basic concepts and show a few preliminary results and this is the contents of the rest of the introduction. First, in Section I-A, we state some results from [2] which are important to our analysis. Then, in Section I-B, we discuss Galois rings ($\mathbb{Z}_{2^l}$ is a Galois ring) and linear codes over Galois rings. Finally we introduce $\mathbb{Z}_{2^l}-$linear codes.

I-A Concatenated codes with fixed inner code and random outer code

In this section we recall results from [2]. The coding scheme for concatenated codes with fixed inner code and random outer code is as follows.

The outer encoding is given by a $K \times N$ generator matrix G_0 for the outer $[N, K]$ code over $\mathbb{F}_{q^k}$. The inner encoding is given by a $k \times n$ generator matrix G_I for the inner $[n, k]$ code over $\mathbb{F}_q$. Hence, the resulting coding scheme defines the encoding for an $[nN, kK]$ code over $\mathbb{F}_q$ where the $q-$ary rate is

$$R = \frac{kK}{nN}. \tag{1}$$

By fixing G_I, i.e. the inner code, and selecting G_0 randomly from the uniform distribution on all $K \times N$ matrices over $\mathbb{F}_{q^k}$ an ensemble of concatenated codes is obtained.

For a given $[n, k]$ inner code with Hamming weight distribution $\boldsymbol{A} = [A_0, A_1, \ldots, A_n]$ a discrete random variable X is defined such that $p(X = i) = \frac{1}{q^k} A_i,\ i = 1, 2, \ldots, n$. Also define $\tau = \tau(\delta)$ such that

$$E(q^{-\tau(X-n\delta)}) = \min_{t \geq 0} E(q^{-t(X-n\delta)}). \tag{2}$$

Now we can state the following bound.

Theorem 1 *If R is given by (1) and τ by (2), then for*

$$nR < -\log_q(E(q^{-\tau(X-n\delta)})),$$

concatenated codes with rate R and fractional minimum distance at least δ exist.

Remark: The bound in Theorem 1 is compared to the Gilbert-Varshamov bound. It follows that for $k = n$, i.e. the inner code is the all word code, the bound in Theorem 1 is identical to the Gilbert-Varshamov bound.

I-B Linear codes over Galois rings

A Galois ring R is defined to be a finite commutative local ring with unity, where the maximal ideal m is given by $m = pR$, p a prime number. The characteristic then is p^l for some $l \in \mathbb{N}$, and the residue class field is $GF(p^j)$ where $j \in \mathbb{N}$. Except for an isomorphism, R is uniquely determined by p^l and j ([6]), and we will let $R = GR(p^l, j)$ denote the Galois ring of characteristic p^l and residue class field $GF(p^j)$.

The set of $n-$tuples over R, R^n, is an $R-$module and a linear code over R is defined as any $R-$submodule of R^n. In this paper we need to consider linear codes over R in the following setup. We define an $[n, k]$ linear code over R by an arbitrary $k \times n$ generator matrix G with entries from the Galois ring R, and such that the the information sequence $\boldsymbol{x} \in R^k$ is encoded into $\boldsymbol{y} = \boldsymbol{x}G$.

In order to derive a Gilbert-Varshamov type bound we divide the set of information sequeces $\boldsymbol{x} \in R^k \setminus \{\mathbf{0}\}$ into the following subsets

$$
\begin{aligned}
X_1 &= \{\boldsymbol{x} = (x_1, x_2, \ldots, x_k) | \text{ at least one } x_i \text{ is a unit } \} \qquad (3)\\
X_2 &= \{\boldsymbol{x} = (x_1, x_2, \ldots, x_k) | \ \boldsymbol{x} \in (pR)^k \text{ and at least one } x_i = pu, \text{ where } u \text{ is a unit}\}\\
&\vdots\\
X_s &= \{\boldsymbol{x} = (x_1, x_2, \ldots, x_k) | \ \boldsymbol{x} \in (p^{s-1}R)^k \text{ and at least one } x_i = p^{s-1}u, \text{ where } u \text{ is a unit}\}\\
&\vdots\\
X_l &= \{\boldsymbol{x} = (x_1, x_2, \ldots, x_k) | \ \boldsymbol{x} \in (p^{l-1}R)^k \text{ and } \boldsymbol{x} \neq \mathbf{0}\}.
\end{aligned}
$$

Note that $\#X_1 = p^{ljk} - p^{(l-1)jk}$, $\#X_2 = p^{(l-1)jk} - p^{(l-2)jk}, \ldots, \#X_s = p^{(l-s+1)jk} - p^{(l-s)jk}, \ldots, \#X_l = p^{jk} - 1$.

To derive the Gilbert-Varshamov type bounds we need the following lemma.

Lemma 2 *Given arbitrary $\boldsymbol{x} \in X_i, \boldsymbol{y} \in (p^{i-1}R)^n$. Then the linear equation system $\boldsymbol{y} = \boldsymbol{x}G$, with the elements of the $(k \times n)$ matrix G as the unknown, always has solutions, and the number of solutions is independent of $\boldsymbol{x}$ and $\boldsymbol{y}$.*

Proof: We have to prove that there always is a solution and that there are the same number of solutions independent of the choice of $\boldsymbol{x} \in X_i, \boldsymbol{y} \in (p^{i-1}R)^n$ (of course i is fixed).

For fixed $\boldsymbol{x} \in X_i$, consider the mapping from the set of $k \times n$ matrices over R, $M_{k,n}(R)$, into $(p^{i-1}R)^n$, given by $G \mapsto \boldsymbol{x}G$.
The mapping is easily checked to be surjective, and since it is a homomorphism from the additive group of $M_{k,n}(R)$ into the additive group of $(p^{i-1}R)^n$, for fixed $\boldsymbol{y} \in (p^{i-1}R)^n$ the number of matrices G such that $\boldsymbol{x}G = \boldsymbol{y}$ is $\#M_{k,n}(R)/\#(p^{i-1}R)^n$ which is independent of $\boldsymbol{x}$ and $\boldsymbol{y}$. ■

I-B.1 A Gilbert-Varshamov type bound for linear codes over Galois rings

Combining Lemma 2 and the setup for linear codes over Galois rings given in this section with the technique from [8] it is straightforward to show a Gilbert-Varshamov type bound for linear codes over Galois rings. However, this bound does not guarantee existence of better linear codes over $GR(p^l, j)$ than the usual Gilbert-Varshamov bound for linear codes over the residue class field $GR(p^j)$. Details can be seen in [5].

I-C $\mathbb{Z}_{2^l}-$linear codes

In [4] the concept of $\mathbb{Z}_4-$linear codes are generalized to $\mathbb{Z}_{2^l} = GR(2^l, 1)$, i.e. a generalization of the Gray map is introduced. Thus, by this map binary (nonlinear) codes are obtained from linear codes over $\mathbb{Z}_{2^l}$ and these codes are denoted $\mathbb{Z}_{2^l}-$linear codes.

We consider $\mathbb{Z}_{2^l}-$linear codes as concatenated codes where the outer code is a randomly selected linear code over $\mathbb{Z}_{2^l}$ and the inner code is fixed, and given by the generalized Gray map. Doing this we can use the approach from [1], [2], [3] where concatenated codes with fixed inner code and randomly selected outer codes are considered.

First we give the definition of the generalized Gray map from [4], and then we state an important property of this map which is, that the mapping is distance preserving.

Definition 3 *[4] Let $l \geq 2$ and let $b \in \mathbb{Z}_{2^l}$ with binary expansion $\sum_{i=1}^{l} b_i 2^{i-1}$. The image of b, $\mathcal{G}(b)$, is the following boolean function on $GF(2)^{l-1}$*

$$\mathcal{G}(b) : (v_1, v_2, \ldots, v_{l-1}) \mapsto b_l + \sum_{i=1}^{l-1} b_i v_i.$$

In this definition we naturally identify a boolean function on $GF(2)^{l-1}$ with a word in $GF(2)^{2^{l-1}}$ such that $\mathcal{G}$ is a mapping from $\mathbb{Z}_{2^l}$ to $GF(2)^{2^{l-1}}$. From Definition 3 it also follows that $\mathcal{G}$ is a

mapping from $\mathbb{Z}_{2^l}$ to $\mathcal{R}(1, l-1)$, the first order binary Reed-Muller code of length 2^{l-1}. As usual we extend $\mathcal{G}$ coordinatewise to a mapping from $\mathbb{Z}_{2^l}^n$ to $(GF(2)^{2^{l-1}})^n$. Finally, when $l = 2$ it follows directly that $\mathcal{G}$ equals the usual Gray map.

Theorem 4 *[4] Let a, b be two elements of $\mathbb{Z}_{2^l}$. The Hamming distance between $\mathcal{G}(a)$ and $\mathcal{G}(b)$ equals the Hamming weight of $\mathcal{G}(a-b)$.*

Remark: By this theorem, the distance distribution of a $\mathbb{Z}_{2^l}-$linear code equals its weight distribution.

II A Gilbert-Varshamov type bound for $\mathbb{Z}_{2^l}-$linear codes

Now we introduce the concatenated coding scheme which will be used to determine a Gilbert-Varshamov type bound for $\mathbb{Z}_{2^l}-$linear codes.

II-A The concatenated coding scheme

The outer encoding: The outer encoder maps each information sequence $\boldsymbol{x} = [x_1, x_2, \ldots x_K] \in \mathbb{Z}_{2^l}^K$ into a codeword $\boldsymbol{y} = [y_1, y_2, \ldots, y_N] \in \mathbb{Z}_{2^l}^N$ given by

$$\boldsymbol{y} = \boldsymbol{x}G, \tag{4}$$

where G is a $K \times N$ matrix over $\mathbb{Z}_{2^l}$.

The inner encoding: By the inner encoding the codeword $\boldsymbol{y}$ is mapped into a codeword $\boldsymbol{c} = [c_1, c_2, \ldots, c_N] \in (\mathbb{Z}_2^{2^{l-1}})^N$, where $c_i = \mathcal{G}(y_i)$ and $\mathcal{G}$ is given by Definition 3. Thus the symbols c_i of the word $\boldsymbol{c}$ in the concatenated code are words in the binary first order Reed-Muller code of length 2^{l-1} with Hamming weight distribution $\boldsymbol{A} = [A_1, A_2, \ldots, A_{2^{l-1}}]$, where $A_0 = A_{2^{l-1}} = 1$, $A_{2^{l-2}} = 2^l - 2$ and the remaining A_i's equals 0. Therefore we obtain a concatenated code of length $2^{l-1}N$ of size at most $(2^l)^K$.

Randomization: A random ensemble of concatenated codes is obtained by fixing the inner encoding, as given above, and selecting G randomly from the uniform distribution of all $K \times N$ matrices over $\mathbb{Z}_{2^l}$.

Consider (4) where $\boldsymbol{x} \in \mathbb{Z}_{2^l}^K \setminus \{0\}$ and $\boldsymbol{y} \in \mathbb{Z}_{2^l}^N$ are fixed, i.e. we consider a linear equation system with the elements of G as unknown. By Lemma 2 the number of solutions to (4) only depends on whether $\boldsymbol{x}$ is in $X_1, X_2, \ldots$ or X_k (the X_i's, with $R = \mathbb{Z}_{2^l}$, are defined in (3)). In the following we use the approach from [1], [2], [3]. However, here we have to divide into different cases according to whether $\boldsymbol{x}$ is in $X_1, X_2, \ldots$ or X_l. Then the "worst" case determines the result.

To derive the bound we need a corollary of the following lemma.

Lemma 5 *Let $\boldsymbol{x} \in X_i$ be a fixed information sequence. Then the symbols $c_1, c_2, \ldots, c_N$ of $\boldsymbol{c}$, the corresponding codeword in the concatenated code, are independently and uniformly distributed over a linear subcode of $\mathcal{R}(1, l-1)$ of size 2^{l-i+1} and weight distribution $A_0 = A_{2^{l-1}} = 1$ and $A_{2^{l-2}} = 2^{l-i+1} - 2$.*

Proof: When $\boldsymbol{x} \in X_i$ the symbols $y_1, y_2, \ldots, y_N$ of the outer codeword $\boldsymbol{y}$ are independent and identically distributed over $2^{i-1}\mathbb{Z}_{2^l}$. Thus, in the binary expansion of $y_j,\ y_j = \sum_{h=1}^{l} y_{j,h} 2^{h-1}$, we have that $y_{j,1} = y_{j,2} = \cdots = y_{j,i-1} = 0$. Recall $\mathcal{G}(y_j) : (v_1, v_2, \ldots, v_{l-1}) \mapsto y_{j,l} + \sum_{h=1}^{l-1} y_{j,h} v_h$ (Definition 3) and that $\mathcal{G}(0) = \mathbf{0},\ \mathcal{G}(2^{l-1}) = \mathbf{1}$ (in $\mathcal{R}(1, l-1)$). Consequently, when $\boldsymbol{x} \in X_i$, the symbols $c_1, c_2, \ldots c_N$ of the corresponding codeword $\boldsymbol{c}$ in the concatenated code are independently and uniformly distributed over a linear subcode of $\mathcal{R}(1, l-1)$ of size 2^{l-i+1}. Clearly the weight distribution of this subcode is $A_0 = A_{2^{l-1}} = 1$ and $A_{2^{l-2}} = 2^{l-i+1} - 2$. ■

From Lemma 5 we immediately obtain the following corollary.

Corollary 6 *Let $\boldsymbol{x} \in X_i$ be a fixed information sequence. Then the Hamming weight of the corresponding codeword in the concatenated code is a stochastic variable*

$$W_i = Z_{1,i} + Z_{2,i} + \cdots + Z_{N,i},$$

where $Z_{j,i} \sim Z_i,\ j = 1, 2, \ldots, N$ are independently and identically distributed. Z_i is given by

$$P(Z_i = 0) = P(Z_i = 2^{l-1}) = \frac{1}{2^{l-i+1}},\ P(Z_i = 2^{l-2}) = \frac{2^{l-i+1} - 2}{2^{l-i+1}}.$$

Example: Consider $\mathbb{Z}_{2^l} = \mathbb{Z}_8$. In this case, the probability distribution of the stochastic variables Z_i given in Corollary 6 are

$$P(Z_1 = 0) = P(Z_1 = 4) = 1/8,\ P(Z_1 = 2) = 3/4$$
$$P(Z_2 = 0) = P(Z_2 = 4) = 1/4,\ P(Z_2 = 2) = 1/2$$
$$P(Z_3 = 0) = P(Z_3 = 4) = 1/2.$$

II-B The bound

We define the rate, in bits, of the ensemble of concatenated codes ($\mathbb{Z}_{2^l}-$linear codes) by

$$R = \frac{lK}{2^{l-1}N}. \tag{5}$$

Hence $2^{2^{l-1}NR}$ equals the number of information sequences $\boldsymbol{x} \in \mathbb{Z}_{2^l}^K$.

Now we examine the probability that a code in the ensemble has a fractional Hamming weight of at most δ. Let P_δ denote the probability that a code in the ensemble has minimum Hamming weight at most $2^{l-1}N\delta$. To each of the $2^{2^{l-1}NR}$ information sequences we have the event M_m :"the codeword corresponding to message m has weight at most $2^{l-1}N\delta$". Hence, by the union bound and Corollary 6

$$\begin{aligned} P_\delta &\leq \sum_{m=1}^{2^{2^{l-1}NR}} P(M_m) = \sum_{i=1}^{l} \#X_i P(Z_{1,i} + Z_{2,i} + \cdots + Z_{N,i} \leq 2^{l-1}N\delta) \\ &\leq \sum_{i=1}^{l} 2^{\frac{2^{l-1}(l-i+1)}{l}RN} E(2^{-t_i(W_i - 2^{l-1}N\delta)}) \\ &= \sum_{i=1}^{l} (2^{\frac{2^{l-1}(l-i+1)}{l}R} E(2^{-t_i(Z_i - 2^{l-1}\delta)}))^N \text{ for every } t_i \geq 0,\ i = 1, 2, \ldots, l. \end{aligned}$$

Let $\tau_i = \tau_i(\delta)$ be chosen such that

$$E(2^{-\tau_i(Z_i - 2^{l-1}\delta)}) = \min_{t_i \geq 0} E(2^{-t_i(Z_i - 2^{l-1}\delta)}) \text{ for } i = 1, 2, \ldots, l. \tag{6}$$

Then we have

Theorem 7 *Let R be given by (5) and τ_i by (6). Then for*

$$\frac{2^{l-1}(l-i+1)}{l} R < -\log_2(E(2^{-\tau_i(Z_i - 2^{l-1}\delta)})) \text{ for } i = 1, 2, \ldots, l,$$

and N sufficiently large there exist $\mathbb{Z}_{2^l}-$linear codes with rate R and fractional minimum distance at least δ.

Note, for $\delta_i \leq \frac{2^l-1}{2^l}$ we have by Chernoff's theorem for large deviations that

$$\lim_{N\to\infty} \frac{\log(P(Z_{1,i} + Z_{2,i} + \cdots + Z_{N,i} \leq 2^{l-1}N\delta))}{N} = \log(E(2^{-\tau_i(Z_i - 2^{l-1}\delta_i)})). \tag{7}$$

Consequently, by using random technique together with the union bound for minimum weight, no better than Theorem 7 can be obtained asymptotically, where the inner code is given by the generalized Gray map in Definition 3.

For each $i = 1, 2, \ldots, l$ we can derive a parametric form of the bound in Theorem 7. When $\tau_i = \tau_i(\delta)$ is used as parameter for the $(R_i, \delta_i)-$curve given by

$$R_i = -\frac{l}{(l-i+1)2^{l-1}} \log_2(E(2^{-\tau_i(Z_i - 2^{l-1}\delta_i)})) \text{ for } i = 1, 2, \ldots, l, \tag{8}$$

we obtain by (6)

$$E((Z_i - 2^{l-1}\delta_i)2^{-\tau_i(Z_i - 2^{l-1}\delta_i)}) = 0 \text{ for } i = 1, 2, \ldots, l. \tag{9}$$

A parametric form then is

$$\begin{aligned} &(R_i, \delta_i) = \\ &\left(-\frac{l}{(l-i+1)2^{l-1}} \left(\tau_i \frac{E(Z_i 2^{-\tau_i Z_i})}{E(2^{-\tau_i Z_i})} + \log_2(E(2^{-\tau_i Z_i})) \right), \frac{1}{2^{l-1}} \frac{E(Z_i 2^{-\tau_i Z_i})}{E(2^{-\tau_i Z_i})} \right) \end{aligned} \tag{10}$$

for $i = 1, 2, \ldots, l$.

By the form in (10) we obtain $(R_i, \delta_i)-$plots, where the "worst" plot determines the quality of the $\mathbb{Z}_{2^l}-$linear codes guaranteed to exist by Theorem 7. In the case $\mathbb{Z}_{2^l} = \mathbb{Z}_8$ we obtain the $(R_i, \delta_i)-$plots shown in figure 1 where we also plot the Gilbert-Varshamov bound for binary codes.

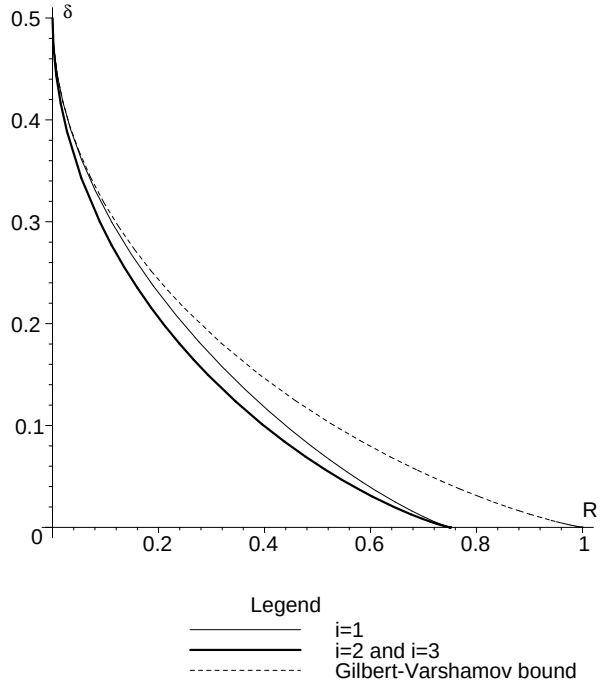


Figure 1: $(R_i, \delta_i)-$plots for $\mathbb{Z}_8-$linear codes

As seen in Figure 1 the cases $i = 2$ and $i = 3$ coincide and give the worst condition on (R, δ). In Figure 1 note also that for small rates, results very close to the Gilbert-Varshamov bound can be obtained.

In the following we prove that in general, for $\mathbb{Z}_{2^l}$, the cases $i = l - 1$ and $i = l$ coincide.

Theorem 8 *Consider the curves given by the parametric form in (10). The curves given by* $i = l$ *and* $i = l - 1$ *coincide.*

Proof: By P_{δ_l} we denote the probability that the words in the concatenated code given by $\mathcal{G}(\boldsymbol{x}G)$, where $\boldsymbol{x} \in X_l$, have minimum weight at most $2^{l-1}N\delta_l$. Similarly, by $P_{\delta_{l-1}}$ we denote the probability that the words in the concatenated code given by $\mathcal{G}(\boldsymbol{x}G)$, where $\boldsymbol{x} \in X_{l-1}$, have minimum weight at most $2^{l-1}N\delta_{l-1}$.

Clearly,

$$\begin{aligned} P_{\delta_{l-1}} &\leq 2^{2K} P(Z_{1,l-1} + Z_{2,l-1} + \cdots + Z_{N,l-1} \leq 2^{l-1} N\delta_{l-1}) \quad (11) \\ P_{\delta_l} &\leq 2^{K} P(Z_{1,l} + Z_{2,l} + \cdots + Z_{N,l} \leq 2^{l-1} N\delta_l), \quad (12) \end{aligned}$$

where $Z_{i,j}$ is given by Corollary 6.

In the following we examine $P(Z_{1,l-1} + Z_{2,l-1} + \cdots + Z_{N,l-1} \leq 2^{l-1} N\delta_{l-1})$ and $P(Z_{1,l} + Z_{2,l} + \cdots + Z_{N,l} \leq 2^{l-1} N\delta_l)$.

First observe that $Z_{i,l}/2^{l-1},\ i = 1, 2, \ldots, N$, are independent stochastic variables which takes on the values 0 and 1, each with probability $1/2$. By this we obtain

$$P(Z_{1,l}/2^{l-1} + Z_{2,l}/2^{l-1} + \cdots + Z_{N,l}/2^{l-1} \leq N\delta_l) = \frac{1}{2^N} \sum_{j=0}^{N\delta_l} \left(\begin{array}{c} N \\ j \end{array} \right) \leq 2^{-N(1-H(\delta_l))}, \quad (13)$$

where $0 \leq \delta_l \leq 1/2$ and H is the binary entropy function.

Hence, by (12)

$$P_{\delta_l} \leq 2^K 2^{-N(1-H(\delta_l))} = 2^{K-N(1-H(\delta_l))}. \quad (14)$$

Now observe that $\frac{Z_{j,l-1}}{2^{l-2}} = Y_{2j-1} + Y_{2j}$, where $Y_m,\ m = 1, 2, \ldots, 2N$, are independent stochastic variables which takes on the values 0 and 1, each with probability $1/2$. Therefore

$$\begin{aligned} &P(Z_{1,l-1}/2^{l-2} + Z_{2,l-1}/2^{l-2} + \cdots + Z_{N,l-1}/2^{l-2} \leq 2N\delta_{l-1}) = \quad (15) \\ &P(Y_1 + Y_2 + \cdots + Y_{2N} \leq 2N\delta_{l-1}) = \frac{1}{2^N} \sum_{j=0}^{2N\delta_{l-1}} \left(\begin{array}{c} 2N \\ j \end{array} \right) \leq 2^{-2N(1-H(\delta_{l-1}))}, \end{aligned}$$

where $0 \leq \delta_{l-1} \leq 1/2$.

Hence, by (11)

$$P_{\delta_{l-1}} \leq 2^{2K} 2^{-2N(1-H(\delta_{l-1}))} = 2^{2(K-N(1-H(\delta_{l-1})))}. \quad (16)$$

To obtain $P_{\delta_{l-1}} < 1$ and $P_{\delta_l} < 1$ we observe, by (16) and (14), that $K - N(1 - H(\delta_l))$ and $K - N(1 - H(\delta_{l-1}))$ must be less than 0. Hence the two cases are asymptotically equivalent.

Now observe by (13) and (15) that

$$\begin{aligned} \lim_{N\to\infty} \frac{\log(P(Z_{1,l}/2^{l-1} + Z_{2,l}/2^{l-1} + \cdots + Z_{N,l}/2^{l-1} \leq N\delta_l))}{N} &= -(1 - H(\delta_l)), \\ \lim_{N\to\infty} \frac{\log(P(Z_{1,l-1}/2^{l-2} + Z_{2,l-1}/2^{l-2} + \cdots + Z_{N,l-1}/2^{l-2} \leq 2N\delta_{l-1}))}{2N} &= -(1 - H(\delta_{l-1})). \end{aligned}$$

Consequently, by using (7) and the limits above we obtain that for $i = l$ and $i = l-1$ the curves given by (10) coincide. ■

III Analysis of the bound

In this section we determine which of the cases $i = 1, 2, \ldots l$ actually determine the quality of the bound in Theorem 7. Furthermore we will compare this bound to the Gilbert-Varshamov bound for binary block codes. To perform the tasks described above we will use the MacWilliams identities.

Consider $\mathbb{Z}_{2^l}-$linear codes as concatenated codes given by the coding scheme in Section II-A. Let $A(z)$ be the weight distribution polynomial for the inner code, i.e. for first order Reed-Muller code of length 2^{l-1}. Thus

$$A(z) = \sum_{i=0}^{n} A_i z^i,\ A_0 = A_{2^{l-1}} = 1,\ A_{2^{l-2}} = 2^l - 2,\ A_i = 0 \text{ otherwise.} \tag{17}$$

Let $B(z) = \sum_{j=0}^{n} B_j z^j$ be the be the weight distribution polynomial for the dual code of the inner code, i.e. for $\mathcal{R}(l-3, l-1)$. By the MacWilliams identities we have

$$\frac{1}{2^l} A(z) = \sum_{j=0}^{n} B_j (1/2 + 1/2z)^{n-j} (1/2 - 1/2z)^j. \tag{18}$$

By substituting $z = 2^{-t}$ in (18) we obtain

$$E(2^{-tZ_1}) = \sum_{j=0}^{n} B_j (\frac{1}{2} + \frac{1}{2}2^{-t})^{n-j} (\frac{1}{2} - \frac{1}{2}2^{-t})^j, \tag{19}$$

where Z_1 is given by Corollary 6.

When $\boldsymbol{x} \in X_i$ is a fixed information sequence the inner code, given by our coding scheme, is either $\mathcal{R}(1, l-1)$ or a linear subcode subcode of $\mathcal{R}(1, l-1)$ which we denote by $\mathcal{D}_j,\ j = 2, 3, \ldots l$. Thus we have a sequence of codes $\mathcal{R}(1, l-1), \mathcal{D}_2, \mathcal{D}_3, \ldots, \mathcal{D}_l$ and since $\mathbb{Z}_{2^l} \supset 2\mathbb{Z}_{2^l} \supset \cdots \supset 2^{l-1}\mathbb{Z}_{2^l}$ we obtain $\mathcal{R}(1, l-1) \supset \mathcal{D}_2 \supset \mathcal{D}_3 \supset \ldots \supset \mathcal{D}_l$. Hence the dual codes of the codes above have the property

$$\mathcal{R}(l-3, l-1) \subset \mathcal{D}_2^{\perp} \subset \mathcal{D}_3^{\perp} \subset \ldots \subset \mathcal{D}_l^{\perp}. \tag{20}$$

Now let B_j^i denote the number of words of weight j in $\mathcal{D}_i$. Then by (20) $B_j^i \leq B_j^{i-1}$. Furthermore

$$0 \leq \frac{1}{2} + \frac{1}{2}2^{-t} \wedge 0 \leq \frac{1}{2} - \frac{1}{2}2^{-t} \leq \frac{t}{2},\ t \geq 0. \tag{21}$$

Then it follows that

$$E(2^{-tZ_i}) \leq E(2^{-tZ_{i-1}}),\ t \geq 0,\ i \geq 2. \tag{22}$$

By (22) it follows that the bound given by Theorem 7 for Z_{i-1} is not above the bound for Z_i. Hence the quality of the bound in Theorem 7 is determined by the case $i = l$ (which equals the case $i = l - 1$ by Theorem 8).

III-A Our bound compared to the Gilbert-Varshamov bound

Consider the setup given in Section I-A but with the restriction that we only consider binary codes. Let $\mathcal{C}$ denote the inner (linear) code with weight distribution polynomium $A(z) = A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. As above, let $B(z) = B_0 + B_1 z + B_2 z^2 + \cdots + B_n z^n$ be the weight distribution polynomial for $\mathcal{C}^\perp$. Of course these polynomials are related by the MacWilliams identities as shown in (18). By substituting $z = 2^{-t}$ in (18) we obtain

$$E(2^{-tX}) = \sum_{j=0}^{n} B_j (\frac{1}{2} + \frac{1}{2}2^{-t})^{n-j} (\frac{1}{2} - \frac{1}{2}2^{-t})^j, \tag{23}$$

where X is the random variable defined in Section I-A. Since the all-word inner code has its dual equal to $\mathbf{0}$, i.e. $B_0 = 1$, we have

$$E(2^{-tX_0}) = (\frac{1}{2} + \frac{1}{2}2^{-t})^n, \tag{24}$$

where X_0 is a binomial distributed random variable with parameters n and $1/2$. Thus, we have

$$E(2^{-tX}) = E(2^{-tX_0}) + \sum_{j=d(\mathcal{C}^\perp)}^{n} B_j (\frac{1}{2} + \frac{1}{2}2^{-t})^{n-j} (\frac{1}{2} - \frac{1}{2}2^{-t})^j. \tag{25}$$

Now it follows from the remark in Section I-A, (25) and (21) that our bound in Theorem 7 is not above the Gilbert-Varshamov bound.

$\mathbb{Z}_4-$linear codes

Consider the case of $\mathbb{Z}_4-$linear codes. In this case the inner code is the all-word code. Therefore, by the remark in Section I-A and Theorem 8 it follows that, in the case of $\mathbb{Z}_4$, the bound in Theorem 7 equals the Gilbert-Varshamov bound. Thus, there exist $\mathbb{Z}_4-$linear codes meeting the usual Gilbert-Varshamov bound for binary codes.

Note, by [7] the only case where

- the inner code is the all word code
- the outer code is a linear code over any Galois ring
- Theorem 4 holds

is $\mathbb{Z}_4$.

IV Error performance

We derive a lower bound on the error performance of our coding scheme used for transmission over the binary symmetric channel with error probability p and decoded by the maximum likelihood rule. That is we derive a lower bound on the error performance of $\mathbb{Z}_{2^l}-$linear codes on the binary symmetric channel.

To derive this bound we use the following well known result.

Theorem 9 *Let $\mathcal{C}$ denote a sequence of translation invariant binary codes with rate R and weight distribution A_ω, $\omega \geq 0$. The code length is n and the minimum distance d equals δn.*

Assume that for n greater than some fixed constant, the number of codewords of a given weight $w = \omega n$ can be bounded above by $\frac{1}{n}\log(A_w) \leq \alpha(\omega)$.

Then the error probability of decoding the family $\mathcal{C}$, used on the binary symmetric channel with error probability p, is upper bounded by $P_{de}(\mathcal{C}, p) \leq 2^{-nE(R,p)}$ for n greater than the above constant where

$$E(R,p) = -\max_{\delta \leq \omega \leq 1}(\alpha(\omega) + \omega \log(\sqrt{(p(1-p))}).$$

To derive a lower bound on the error performance of $\mathbb{Z}_{2^l}-$linear codes we estimate the "average" weight distribution of $\mathbb{Z}_{2^l}-$linear codes. We consider the average number of vectors of weight

less than or equal to $2^{l-1}N\omega,\ 0 \leq \omega \leq 1$. First we introduce the random variable $I_{\boldsymbol{x}}(\omega),\ \boldsymbol{x} \in \mathbb{Z}_{2^l}^K$ by

$$I_{\boldsymbol{x}}(\omega) = \begin{cases} 1 \text{ if the Hamming weight of the word corresponding to } \boldsymbol{x} \text{ is less than or equal to } 2^{l-1}N\omega \\ 0 \text{ otherwise} \end{cases} \tag{26}$$

Then $\sum_{\boldsymbol{x} \in \mathbb{Z}_{2^l}^K} I_{\boldsymbol{x}}(\omega)$ equals the number of words in the $\mathbb{Z}_{2^l}-$linear code of weight less than or equal to $2^{l-1}N\omega,\ 0 \leq \omega \leq 1$. Thus, the average number of words of weight less than or equal to $2^{l-1}N\omega$ is
$E(\sum_{\boldsymbol{x} \in \mathbb{Z}_{2^l}} I_{\boldsymbol{x}}(\omega)) = \sum_{\boldsymbol{x} \in \mathbb{Z}_{2^l}^K} E(I_{\boldsymbol{x}}(\omega))$.

In the following we again divide into different cases according to whether $\boldsymbol{x}$ is in X_1 or X_2 or $\ldots$ or X_l.

Theorem 10 *For $0 \leq \omega \leq 1$ consider $E(\sum_{\boldsymbol{x} \in X_i} I_{\boldsymbol{x}}(\omega))$. Then*

$$\frac{\log(E(\sum_{\boldsymbol{x} \in X_i} I_{\boldsymbol{x}}(\omega)))}{2^{l-1}N} \leq \frac{l-1+i}{l}R + \frac{1}{2^{l-1}}(\log(E(2^{-\tau_i Z_i})) + \tau_i 2^{l-1}\omega),$$

where $i = 1, 2, \ldots, l$, Z_i is the random variable given in Corollary 6 and τ_i is chosen from the condition $E(2^{-\tau_i(Z_i - 2^{l-1}\omega)}) = \min_{t_i \geq 0} E(2^{-t_i(Z_i - 2^{l-1}\omega)})$.

Proof: First note that $E(I_{\boldsymbol{x}}(\omega)) = P(Z_{1,i} + Z_{2,i} + \cdots + Z_{N,i} \leq 2^{l-1}N\omega)$, where $Z_{j,i}$ is given by Corollary 6. Thus

$$\begin{aligned} E(\sum_{\boldsymbol{x} \in X_i} I_{\boldsymbol{x}}(\omega)) &= \sum_{\boldsymbol{x} \in X_i} E(I_{\boldsymbol{x}}) = \#X_i P(Z_{1,i} + Z_{2,i} + \cdots + Z_{N,i} \leq 2^{l-1}N\omega) \\ &\leq 2^{\frac{2^{l-1}(l-i+1)}{l}RN} E(2^{-t_i(W_i - 2^{l-1}N\omega)}) \\ &= (2^{\frac{2^{l-1}(l-i+1)}{l}R} E(2^{-t_i(Z_i - 2^{l-1}\omega)}))^N \text{ for every } t_i \geq 0. \end{aligned}$$

Now let $\tau_i = \tau_i(\omega)$ be chosen such that $E(2^{-\tau_i(Z_i - 2^{l-1}\omega)}) = \min_{t_i \geq 0} E(2^{-t_i(Z_i - 2^{l-1}\omega)})$. Then the result follows immediately. ■

By Theorem 10, for each $i = 1, 2, \ldots, l$ we have an upper bound on the exponent of the average number of codewords in $2^{i-1}\mathbb{Z}_{2^l}$ of weight less than or equal to $2^{l-1}N\omega$. By substituting these upper bounds in Theorem 9 we obtain a sequence of lower bounds where the worst case,

asymptotically for $N \to \infty$, determines the quality of the error performance of the $\mathbb{Z}_{2^l}-$linear codes guaranteed to exist by this theorem.

For each $i = 1, 2, \ldots, l$ we can, similarly as we did when considering Theorem 7, derive a parametric form of the bound in Theorem 10. We obtain

$$\left(\frac{\log(E(\sum_{\boldsymbol{x}\in X_i} I_{\boldsymbol{x}}(\omega)))}{2^{l-1}N}, \omega\right) =$$
$$\left(\frac{(l-i+1)}{l}R + \frac{1}{2^{l-1}}(\log(E(2^{-\tau_i}Z_i)) + \tau_i 2^{l-1}\omega), \frac{1}{2^{l-1}}\frac{E(Z_i 2^{-\tau_i Z_i})}{E(2^{-\tau_i Z_i})}\right) \text{ for } i = 1, 2, \ldots l.$$

By this parametric form we obtain the plots in Figure 2 and Figure 3 in the case of $\mathbb{Z}_4$ and $\mathbb{Z}_8$ respectively.

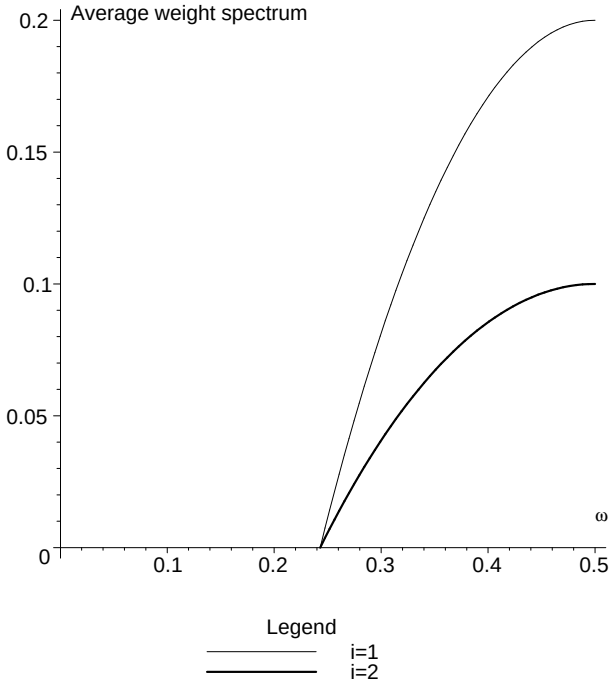


Figure 2: Average weight spectrum for $\mathbb{Z}_4-$linear codes

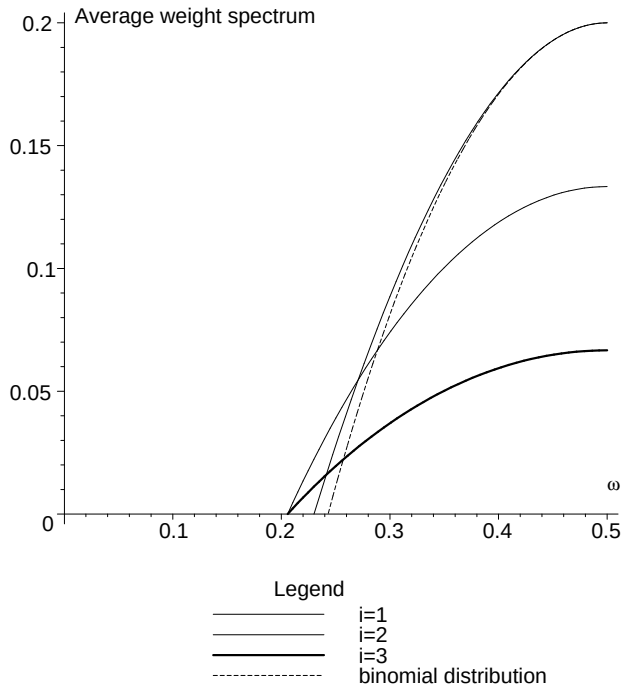


Figure 3: Average weight spectrum for $\mathbb{Z}_8-$linear codes

Combining the results of Theorem 10 and Theorem 9 we obtain the plots in Figure 4 and Figure 5 in the case of $\mathbb{Z}_4$ and $\mathbb{Z}_8$ respectively with error probability $p = 0.02$.

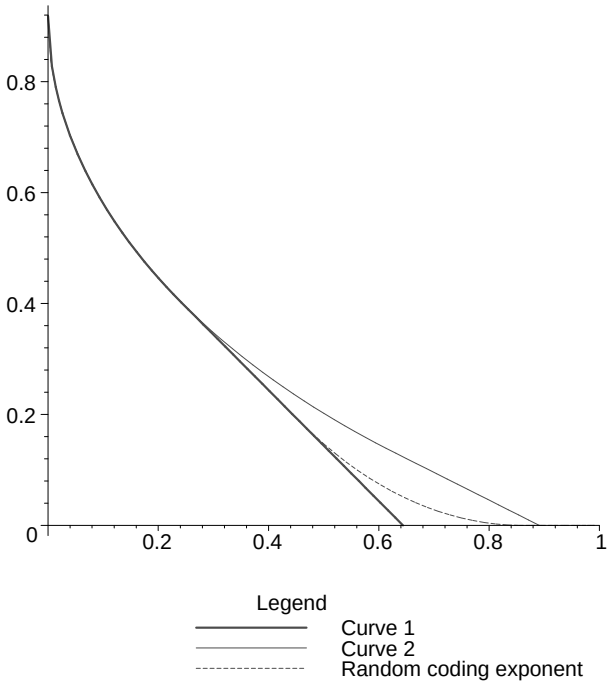


Figure 4: $(R, E(R, p))-$plot

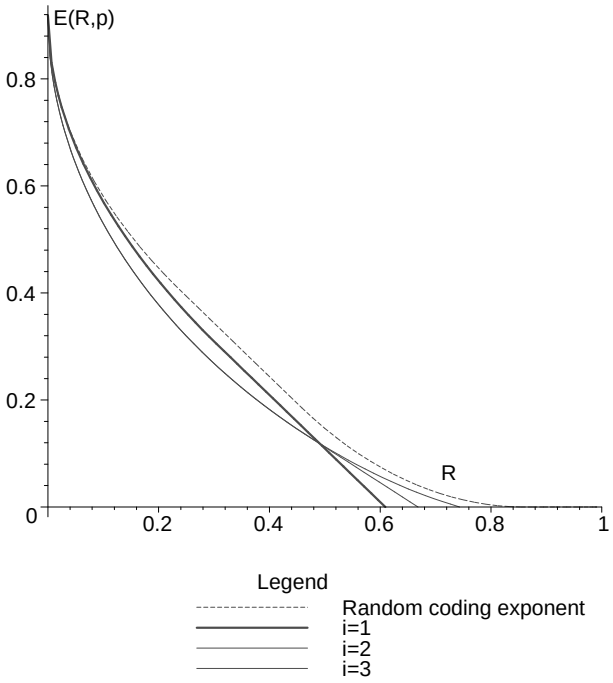


Figure 5: $(R, E(R,p))-$plot

References

[1] A. Barg, J. Justesen and C. Thommesen. Concatenated codes with fixed inner code and the outer code randomly selected. Technical Report, Department of mathematical sciences, Aalborg University, R-94-2016.

[2] A. Barg, J. Justesen and C. Thommesen. Concatenated codes with fixed inner code and the outer code randomly selected. Proceedings 1994 IEEE, International Symposium on Information Theory, page 476.

[3] A. Barg, J. Justesen and C. Thommesen. Concatenated codes with fixed inner code and random outer code. IEEE Trans. Inf. Theory, vol 47, no. 1, January 2001.

[4] Claude Carlet. $\mathbb{Z}_{2^k}-$linear codes. IEEE Trans. Inf. Theory, vol 44, no. 4, July 1998

[5] Bo Hove and Christian Thommesen. A Gilbert-Varshamov type bound for linear codes over Galois rings. Tech. Rep. R-98-2014, Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark.

[6] A.A. Nechaev. Kerdock codes in a cyclic form. Discrete Math. Appl. vol. 1, No. 4, pp. 364-384, 1991.

[7] A. Salgean-Mandache On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$". IEEE Trans. Inf. Theory, vol 45, no 6,1999, pp. 2146-2148.

[8] C. Thommesen. Existence of binary linear concatenated codes with Reed-Solomon codes as outer code, asymptotically meeting the Gilbert-Varshamov bound. IEEE Trans. Inf. Theory, vol 29, 1983, pp. 850-853