GILBERT-VARSHAMOV TYPE BOUNDS FOR LINEAR CODES OVER FINITE CHAIN RINGS

FERRUH ÖZBUDAK
Department of Mathematics, Middle East Technical University
Inönü Bulvarı, 06531, Ankara, Turkey

PATRICK SOLÉ
CNRS, I3S, ESSI, BP 145, Route des Colles
06 903 Sophia Antipolis, France

(Communicated by Ivan Landjev)

Abstract. We obtain finite and asymptotic Gilbert-Varshamov type bounds for linear codes over finite chain rings with various weights.

1. Introduction

For some years, codes over rings have been especially interesting and many applications to communications and related areas have been found (cf. [4], [5], [8], [10], [12]). Recently in [7], the authors have established Gilbert-Varshamov type bounds for nonlinear codes with homogeneous weights over finite Frobenius rings.

In this paper we obtain Gilbert-Varshamov type bounds for linear codes over finite chain rings with various weights. We derive both finite and asymptotic versions of these bounds. Since there exist zero divisors, obtaining Gilbert-Varshamov type bounds for linear codes over finite chain rings requires further attention.

The paper is organized as follows. We give some definitions and fix some notation in the rest of this section. A finite Gilbert-Varshamov type bound is obtained in Section 2. We derive an asymptotic Gilbert-Varshamov type bound for a special weight, which has application to convolutional codes, in Section 3. Homogenous weights over arbitrary finite chain rings are considered in Section 4. Finally we obtain asymptotic Gilbert-Varshamov type bounds for Lee, Euclidean and PSK weights over the ring \( \mathbb{Z}_8 \).

We recall some definitions. Let \( \mathcal{R} \) be a finite chain ring with the maximal ideal \( < a > \) generated by \( a \in \mathcal{R} \). Let \( p^m \) be the cardinality of \( \mathcal{R} \), where \( p \) is a prime. Let \( t \) be the nilpotency of \( a \). We know that the chain
\[
\mathcal{R} = < a^0 > \supseteq < a > \supseteq \cdots \supseteq < a^{t-1} > \supseteq < a^t > = \{0\}
\]

consists of all ideals of \( \mathcal{R} \). Moreover \( t \) divides \( m \) and for each \( 0 \leq i \leq t \) the cardinality of the ideal \( < a^i > \) is \( p^{l(t-i)} \), where \( l = m/t \). Let \( q = p^t \). We refer to [9] for the details on chain rings.

Throughout the paper \( k \leq n \) are positive integers. Let \( \mathcal{R}^n \) be the set of all \( n \)-tuples over \( \mathcal{R} \). We consider \( \mathcal{R}^n \) as the left \( \mathcal{R} \)-module \( \mathcal{R}^n \). A linear code over \( \mathcal{R} \) is a left \( \mathcal{R} \)-submodule of \( \mathcal{R}^n \). We show the set of all \( k \times n \) matrices over \( \mathcal{R} \) as

2000 Mathematics Subject Classification: Primary: 94B65, 94B60; Secondary: 16P10.

Key words and phrases: Linear codes over rings, Gilbert-Varshamov bound, asymptotic bounds.
\( \mathcal{R}^{k\times n} \). Moreover \( w(\cdot) \) will be a suitable weight function on \( \mathcal{R}^n \). For a finite set \( S \), \( \#S \) will denote the cardinality of \( S \).

2. A Finite Gilbert-Varshamov Type Bound

In this section we obtain a finite Gilbert-Varshamov type bound for linear codes over arbitrary finite chain rings. We begin with a simple lemma.

**Lemma 1.** For \( \alpha \in \mathcal{R}^k \setminus (a\mathcal{R})^k \) and \( u \in \mathcal{R}^n \), we have

\[
\# \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \# \{ G \in \mathcal{R}^{k\times n} : \alpha G = 0 \}.
\]

**Proof.** The matrix equation \( \alpha G = u \) defines a linear system over \( \mathcal{R} \) with \( kn \) unknowns. Its number of solutions is the same as the number of solutions of the corresponding homogeneous system \( \alpha G = 0 \) provided that there exists at least one \( G \in \mathcal{R}^{k\times n} \) satisfying \( \alpha G = u \). As \( \alpha \not\in (a\mathcal{R})^k \), there exists \( i \in \{1, \ldots, k\} \) such that the \( i \)-th component \( \alpha_i \) of the vector \( \alpha \) is invertible in \( \mathcal{R} \). Let \( G \) be the \( k \times n \) matrix obtained from the \( k \times n \) zero matrix by putting the row vector \( \alpha_i^{-1}u \) into the place of its \( i \)-th row. Then \( \alpha G = u \), which completes the proof. \( \square \)

Now we generalize the previous lemma.

**Corollary 1.** For each \( 0 \leq i \leq t - 1 \), if \( \alpha \in \langle a^i \rangle \setminus \langle a^i \rangle^{k} \setminus \langle a^{i+1} \rangle^{k} \) and \( u \in \langle a^{i} \rangle^{n} \), then we have

\[
\# \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \# \{ G \in \mathcal{R}^{k\times n} : \alpha G = 0 \}.
\]

**Proof.** As in the proof of Lemma 1 it is enough to show the existence of \( G \in \mathcal{R}^{k\times n} \) such that \( \alpha G = u \) holds. Let \( \alpha = a^i\alpha_1 \) and \( u = a^iu_1 \). We have \( \alpha_1 \in \mathcal{R}^k \setminus (a\mathcal{R})^k \) and \( u_1 \in \mathcal{R}^n \). From the proof of Lemma 1 we obtain \( G \in \mathcal{R}^{k\times n} \) such that \( \alpha_1 G = u_1 \), which implies that \( \alpha G = u \). \( \square \)

The next lemma is useful.

**Lemma 2.** For \( \alpha \in \mathcal{R}^k \setminus (a\mathcal{R})^k \), we have that

\[
\bigcup_{u \in \mathcal{R}^n} \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \mathcal{R}^{k\times n}
\]

is a disjoint partition of \( \mathcal{R}^{k\times n} \), and for each \( u \in \mathcal{R}^n \) we have

\[
\# \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \frac{\# \mathcal{R}^{k\times n}}{\# \mathcal{R}^n}.
\]

**Proof.** The disjoint partition is clear. Using Lemma 1 we complete the proof. \( \square \)

Using Corollary 1 now we give a generalization.

**Corollary 2.** For each \( 0 \leq i \leq t - 1 \) and \( \alpha \in \langle a^{i} \rangle \setminus \langle a^{i}\rangle^{k} \setminus \langle a^{i+1} \rangle^{k} \), we have that

\[
\bigcup_{u \in \langle a^{i} \rangle^{n}} \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \mathcal{R}^{k\times n}
\]

is a disjoint partition of \( \mathcal{R}^{k\times n} \), and for each \( u \in \langle a^{i} \rangle^{n} \) we have

\[
\# \{ G \in \mathcal{R}^{k\times n} : \alpha G = u \} = \frac{\# \mathcal{R}^{k\times n}}{\# \langle a^{i} \rangle^{n}}.
\]

Now we introduce a notation.
Notation 1. For \( d \geq 0 \) and each \( 0 \leq i \leq t - 1 \), let
\[
V_i(n, d) = \#\{u < a^i \geq n: w(u) \leq d\}.
\]

Corollary \( \Box \) implies the following result.

Proposition 1. For \( d \geq 1 \) we have that
\[
\#\{G \in \mathcal{R}^{k \times n} : \text{there exists } \alpha \in \mathcal{R}^k \setminus \{0\} \text{and } u \in \mathcal{R}^n \text{with } \alpha G = u \text{ and } w(u) \leq d - 1\} = \#\mathcal{R}^{k \times n} \sum_{i=0}^{t-1} V_i(n, d) \cdot \#\{<a^i >^k \geq a^{i+1} >^k\} \#<a^i >^n.
\]

Proof. For each \( \alpha \in \mathcal{R}^k \setminus \{0\} \), there exists a uniquely determined \( 0 \leq i \leq t - 1 \) such that \( \alpha < a^i >^k \geq a^{i+1} >^k \). For \( \alpha < a^i >^k \geq a^{i+1} >^k \), using Corollary \( \Box \) we obtain that the number of \( G \in \mathcal{R}^{k \times n} \) satisfying \( w(\alpha G) \leq d - 1 \) is exactly
\[
\#\mathcal{R}^{k \times n} \frac{V_i(n, d)}{\#<a^i >^n}.
\]
Summing over all \( 0 \leq i \leq t - 1 \) we complete the proof. \( \Box \)

Now we give our finite Gilbert-Varshamov type bound.

Theorem 2. For \( d \geq 1 \), if the inequality
\[
\sum_{i=0}^{t-1} \frac{p^{k(t-i)} - p^{k(t-i-1)}}{p^l(t-i)} V_i(n, d-1) < 1
\]
holds, then there exists a \( k \times n \) matrix \( G \) over \( \mathcal{R} \) such that the \( \mathcal{R} \)-linear code \( C := \{\alpha G : \alpha \in \mathcal{R}^k\} \) has minimum distance at least \( d \) and \#\( C = p^{kt} \).

Proof. Using Proposition \( \Box \) we obtain the existence of a \( k \times n \) matrix \( G \) over \( \mathcal{R} \) such that there is no \( \alpha \in \mathcal{R}^k \setminus \{0\} \) with \( w(\alpha G) \leq d - 1 \). It remains to prove that the size of the code \( C \) obtained using such a generator matrix \( G \) is exactly \( p^{kt} \). Assume that \( \alpha_1, \alpha_2 \in \mathcal{R}^k \) and \( \alpha_1 \neq \alpha_2 \). Then \( w(\alpha_1 G - \alpha_2 G) \geq d \geq 1 \), and hence \( \alpha_1 G \neq \alpha_2 G \). This completes the proof. \( \Box \)

3. A Special Weight

In this section we consider a special weight for finite chain rings. This weight has some applications to convolutional codes \( \Box \).

Let \( t \geq 1 \) and \( \mathcal{R} = \mathbb{F}_q[x]/(x^t) \) be the chain ring with the maximal ideal \( <x> \). We have that the nilpotency of \( x \) is \( t \) and let \( q = p^t \), where \( p \) is the characteristic of the finite field \( \mathbb{F}_q \). Let \( w(\cdot) \) be the weight function defined on \( \mathcal{R}^n \) as follows: For \( \alpha \in \mathcal{R} \) with \( \alpha = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \), let \( w(\alpha) = w_H(a_0, a_1, \ldots, a_{t-1}) \), where \( w_H(a_0, a_1, \ldots, a_{t-1}) \) is the Hamming weight of the vector \( (a_0, a_1, \cdots, a_{t-1}) \) in \( \mathbb{F}_q^t \). For \( \alpha = (a_1, \ldots, a_n) \in \mathcal{R}^n \), let
\[
w(\alpha) = \sum_{j=1}^{n} w(\alpha_j).
\]
For \( d \geq 1 \) and \( 0 \leq i \leq t - 1 \) we have
\[
V_i(n, d-1) = \sum_{j=0}^{d-1} \binom{(t-i)n}{j} (q-1)^j
\]
For $0 < y < 1$, recall that the $q$-ary entropy function $H_q(\cdot)$ is given by

$$H_q(y) = -y \log_q y - (1 - y) \log_q (1 - y) + y \log_q (q - 1).$$

As an application of Theorem 2 we obtain the following theorem.

**Theorem 3.** For $0 < \delta < 1$, there exists a sequence of $R$-linear codes of length $n$, minimum distance $d$ and size $q^k$ such that $n \to \infty$, $d/n \to \delta$, $k/n \to R$ satisfying

$$R \geq 1 - H_q(\delta).$$

**Proof.** Using Theorem 2, it is enough to prove that

$$\lim_{n \to \infty} \frac{1}{n} \log \left\{ \frac{q^{Rn} - q^{(t-1)Rn}}{q^{tn}} \sum_{j=0}^{\lceil \delta n - 1 \rceil} \binom{tn}{j} (q - 1)^j \right\} + \frac{q^{(t-1)Rn} - q^{(t-2)Rn}}{q^{(t-1)n}} \sum_{j=0}^{\lceil \delta n - 1 \rceil} \binom{(t-1)n}{j} (q - 1)^j$$

$$+ \cdots$$

$$+ \frac{q^{Rn} - 1}{q^n} \sum_{j=0}^{\lceil \delta n - 1 \rceil} \binom{n}{j} (q - 1)^j \right\} \leq 0.$$
where the last equality follows from the fact that $1 - H_q(y)$ is a decreasing function on the interval $y \in (0, 1)$.

**Remark 1.** We have the following generalization of Theorem 3. Let $R$ be the arbitrary finite chain ring of Section 1 whose maximal ideal is $<a>$. Let $t$ be the nilpotency of $a$. Let $\Gamma$ be a subset of $t$ elements of $R$ such that $0 \in \Gamma$ and no two distinct elements of $\Gamma$ are equal modulo $<a>$. Each element $\alpha \in R$ is represented uniquely in the form $\alpha = a_0 + a_1a + \cdots + a_{t-1}a^{t-1}$ with $a_i \in \Gamma$. For $\alpha = a_0 + a_1a + \cdots + a_{t-1}a^{t-1} \in R$ with $a_i \in \Gamma$, let $w(\alpha) = \# \{0 \leq i \leq t-1 : a_i \neq 0\}$. Then Theorem 3 holds for the arbitrary finite chain ring $R$ under the weight given in (3). We have used a suggestion by one of the anonymous referees in the revision of this remark.

4. **Homogeneous weights**

In this section we study arbitrary homogenous weights for linear codes over finite chain rings.

We recall the definition of homogenous weights on finite chain rings ([1], [2], [3], [6], [7]).

**Definition 1.** For positive real number $\gamma$, the real valued function $w(\cdot)$ on $R$ defined as

$$w(y) = \begin{cases} 0 & \text{if } y = 0, \\ \gamma q/(q-1) & \text{if } y \in a^{t-1} \setminus \{0\}, \\ \gamma & \text{if } y \in R \setminus a^{t-1} \end{cases}$$

is called the homogenous weight on $R$ with the average value $\gamma$.

Note that the weight of Section 3 is not an homogenous weight on $R$.

We give a basic but useful lemma.

**Lemma 3.** Assume that $u, v, w, C$ and $D$ are positive real numbers such that $w > v$ and $C + \frac{w}{v}D > \frac{u}{v}$. Let $G(z)$ be the real valued function defined on the interval $z \in (0, 1]$ by

$$G(z) = z^{-u} + Cz^v + Dz^w.$$  

Then the function assumes its minimum at the point $z_0 \in (0, 1)$, which is the only solution of the equation

$$G'(z) = 0,$$

where $G'(z)$ is the derivative of $G(z)$.

**Proof.** Using the change of variable $x = z^v$ we simplify $G(x)$ to the function

$$G_1(x) = x^{-\alpha} + Cx + Dx^\beta$$

defined over the interval $x \in (0, 1]$, where $\alpha = u/v$ and $\beta = w/v$. Note that $\alpha > 0$, $\beta > 1$ and $C + D\beta > \alpha$. The first and the second derivatives of $G_1(x)$ are

$$G_1'(x) = -\alpha x^{-\alpha-1} + C + D\beta x^{\beta-1}, \text{ and}$$

$$G_1''(x) = \alpha(\alpha+1)x^{-\alpha-2} + D\beta(\beta-1)x^{\beta-2}.$$  

(4)
As $\alpha > 0$, $\beta > 1$ and $C+D\beta > \alpha$, using (4) it is easy to observe that $\lim_{x \to 0^+} G'_1(x) = -\infty$, $\lim_{x \to 1^-} G'_1(x) = -\alpha + C + D\beta > 0$, and $G''_1(x) > 0$ for each $x \in (0, 1)$. This completes the proof.

Let
\[
 f_{t-1}(z) = 1 + (q - 1)z^{\gamma q/(q-1)},
\]
and for $0 \leq i \leq t - 2$ let
\[
 f_i(z) = 1 + (q^{t-i} - q)z^{\gamma} + (q - 1)z^{\gamma q/(q-1)}
\]
be real valued functions of $z$. For $0 < \delta < \gamma$ and $0 \leq i \leq t - 1$, let
\[
 F_i(\delta) = \min_{z \in (0, 1]} \log_q \frac{f_i(z)}{z^\delta}.
\]
For $0 \leq i \leq t - 1$, we prove the existence of $F_i(\delta)$ and determine it in the next proposition.

**Proposition 2.** Assume that $0 < \delta < \gamma$. We have
\[
 F_{t-1}(\delta) = \log_q \left\{ \frac{\gamma q}{\delta \frac{1}{q-1}} \left( \frac{\gamma q - \delta(q - 1)}{\gamma q} \right)^{\frac{\gamma q - \delta(q - 1)}{\gamma q}} \right\}.
\]
For $0 \leq i \leq t - 2$ we have
\[
 F_i(\delta) = \log_q \left\{ z_{i-1}^{\delta} + (q^{t-i} - q)z_i^{\gamma - \delta} + (q - 1)z_i^{\gamma q/(q-1)} \right\},
\]
where $z_0 \in (0, 1)$ is the unique solution of (5).

**Proof.** Let $G_{t-1}(z)$ be the real valued function on the interval $z \in (0, 1]$ given by
\[
 G_{t-1}(z) = \frac{f_{t-1}(z)}{z^\delta} = z^{-\delta} + (q - 1)z^{\gamma q/(q-1)}.
\]
Let $G'_{t-1}(z)$ be its derivative. Let $z_{t-1} \in (0, 1)$ be the unique solution of
\[
 G'_{t-1}(z) = 0.
\]
We have $-\delta z_{t-1}^{\delta-1} + (q - 1) \left( \frac{\gamma q}{\gamma q - \delta} \right) z_{t-1}^{\gamma q/(q-1)} = 0$ and hence
\[
 z_{t-1}^{\frac{\gamma q}{\gamma q - \delta}} = \frac{\delta}{\gamma q - \delta(q - 1)}.
\]
Using (4) we determine $F_{t-1}(\delta)$ explicitly as
\[
 F_{t-1}(\delta) = \log_q \frac{f_{t-1}(z_{t-1})}{z_{t-1}^{\delta}} = \log_q \frac{1 + (q - 1)z_{t-1}^{\gamma q/(q-1)}}{\delta \frac{1}{q-1} \left( \frac{\gamma q - \delta(q - 1)}{\gamma q} \right)^{\frac{\gamma q - \delta(q - 1)}{\gamma q}}}.
\]
\[
 = \log_q \frac{\gamma q}{\delta \frac{1}{q-1} \left[ \gamma q - \delta(q - 1) \right]^{\frac{\gamma q - \delta(q - 1)}{\gamma q}}}. \]
For $0 \leq i \leq t - 2$ we complete the proof using Lemma 3.

Recall that for $0 \leq i \leq t - 1$, $V_i(n, d)$ denotes the size of the corresponding discrete ball in $\mathbb{R}^n$, which depends on the weight function (cf. Notation 1).

**Proposition 3.** For $0 < \delta < \gamma$ and $0 \leq i \leq t - 1$, we have
\[
\lim_{n \to \infty} \frac{1}{n} \log_q \{V_i(n, \lfloor \delta n \rfloor - 1)\} = (t - i) F_i(\delta).
\]

**Proof.** Note that $\# < a_i > = q^{(t - i)}$ and hence using [7, Theorem 4.1] we obtain
\[
\lim_{n \to \infty} \frac{1}{n} \log_q \{V_i(n, \lfloor \delta n \rfloor - 1)\} = F_i(\delta),
\]
which completes the proof.

Now we give our main theorem in this section.

**Theorem 4.** For $0 < \delta < \gamma$, there exists a sequence of $R$-linear codes of length $n$, minimum distance $d$ and size $q^k$ such that $n \to \infty$, $d/n \to \delta$, $k/n \to R$ satisfying
\[
R \geq 1 - \max \left\{ \frac{F_0(\delta)}{t}, \frac{F_1(\delta)}{t - 1}, \ldots, \frac{F_{t - 1}(\delta)}{t} \right\}.
\]

Moreover if
\[
F_{t - 1}(\delta) = \max \{F_0(\delta)/t, F_1(\delta)/(t - 1), \ldots, F_{t - 1}(\delta)\},
\]
holds, then
\[
R \geq 1 - \log_q \left( \frac{\gamma q^{\gamma}}{\delta^{\frac{\gamma(q - 1)}{\gamma - 1}} \cdot (\gamma q - \delta(q - 1))^{\frac{\gamma - 1}{\gamma}}} \right).
\]

**Proof.** Using the methods of the proof of Theorem 3, the proof follows from Theorem 2, Proposition 2 and Proposition 3.

**Remark 2.** Although we could not give a proof, we observe that the condition (7) in Theorem 4 holds in all of our numerical examples.

5. Lee, Euclidean and PSK weights

In this section we study further non homogenous weights over $\mathbb{Z}_8$. Similar results also hold other finite chain rings.

5.1. Lee weight over $\mathbb{Z}_8$. For $0 \leq \alpha \leq 7$, let $w_L(\alpha)$ be defined as
\[
w_L(\alpha) = \min \{\alpha, 8 - \alpha\}.
\]

Recall that for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_8^n$, its Lee weight $w_L(\alpha)$ is given by $w_L(\alpha) = \sum_{i=1}^{n} w_L(\alpha_i)$. Lee weight is not homogeneous on $\mathbb{Z}_8$. In this subsection we obtain an analogue of Theorem 4 for codes over $\mathbb{Z}_8$ with Lee weight.

$\mathbb{Z}_8$ is a chain ring and
\[
\mathbb{Z}_8 \supseteq 2\mathbb{Z}_8 \supseteq 4\mathbb{Z}_8 \supseteq \{0\}.
\]

We have $4\mathbb{Z}_8 = \{0, 4\}$ and $2 = \frac{1}{2}(w(0) + w(4))$. For $0 < \delta < 2$, let $G_2(z) = z^{-\delta} + z^{4-\delta}$ be the differentiable real valued function and for its derivative $G_2'(z)$,
let $z_2$ be the unique solution of the equation $G'(z) = 0$ in the interval $(0, 2)$. We observe that

$$z_2 = \left( \frac{\delta}{4 - \delta} \right)^{1/4}.$$  

Using [7, Theorem 4.1] we obtain that (cf. Notation 1)

$$F_2(\delta) := \lim_{n \to \infty} \frac{1}{n} \log_2 \{V_2(n, \lfloor \delta n \rfloor - 1)\} = \log_2 \frac{1 + \frac{\delta}{4 - \delta}}{(\frac{\delta}{4 - \delta})^{3/4}}.$$  

We have $2\mathbb{Z}_8 = \{0, 2, 4, 6\}$ and $2 = \frac{1}{9} (w(0) + w(2) + w(4) + w(6))$. For $0 < \delta < 2$, let $G_1(z) = z^{-\delta} + 2z^{2-\delta} + z^{4-\delta}$ and for its derivative $G'_1(z)$ let $z_1$ be the unique solution of the equation $G'_1(z) = 0$ in the interval $(0, 2)$. The existence and the uniqueness of $z_1 \in (0, 2)$ is proved similarly as in Lemma 3. Using [7, Theorem 4.1] we obtain that

$$F_1(\delta) := \frac{1}{2} \lim_{n \to \infty} \frac{1}{n} \log_2 \{V_1(n, \lfloor \delta n \rfloor - 1)\} = \log_2 G_1(z_1).$$  

Finally for $\mathbb{Z}_8$ itself, we again have $2 = \frac{1}{9} (w(0) + w(1) + \cdots + w(7))$. For $0 < \delta < 2$, let $f_0(z) = 1 + 2z + 2z^2 + 2z^3 + z^4$ be the real valued function and

$$F_0(\delta) := \frac{1}{3} \min_{\alpha \in \{0, 2, \cdots, 7\}} \log_2 f_0(z)$$  

(cf. [7, Theorem 4.1]). Using the methods of Section 4 and the definitions of this subsection we obtain the following analogue of Theorem 4

**Theorem 5.** Assume the notation above. For $0 < \delta < 2$, there exists a sequence of $\mathbb{Z}_8$-linear codes of length $n$, minimum distance $d$ and size $2^k$ such that $n \to \infty$, $d/n \to \delta$, $k/n \to R$ satisfying

$$R \geq 1 - \max\{\frac{F_0(\delta)}{3}, \frac{F_1(\delta)}{2}, F_2(\delta)\}.$$  

Moreover if

$$F_2(\delta) = \max\{F_0(\delta)/3, F_1(\delta)/2, F_2(\delta)\},$$  

holds, then

$$R \geq 1 - \log_2 \frac{1 + \frac{\delta}{4 - \delta}}{(\frac{\delta}{4 - \delta})^{3/4}}.$$  

5.2. Euclidean weight over $\mathbb{Z}_8$. For $0 \leq \alpha \leq 7$, let

$$w_E(\alpha) = W_L(\alpha)^2,$$  

where $w_L$ is defined in [8]. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_8^n$, its Euclidean weight is given by $w_E(\alpha) = \sum_{i=1}^{n} w_E(\alpha_i)$. We have

$$8 = \frac{1}{2} \sum_{\alpha \in 2\mathbb{Z}_8} w_E(\alpha), \quad 6 = \frac{1}{4} \sum_{\alpha \in 2\mathbb{Z}_8} w_E(\alpha), \quad \frac{11}{2} = \frac{1}{8} \sum_{\alpha \in \mathbb{Z}_8} w_E(\alpha).$$  

Assume that $0 < \delta < \frac{11}{2}$. Let

$$F_2(\delta) = \log_2 \frac{1 + \frac{\delta}{4 - \delta}}{(\frac{\delta}{4 - \delta})^{3/4}}.$$  

**Advances in Mathematics of Communications**

Volume 1, No. 1 (2007), 99–109
be the real valued function. Moreover let $G_1(z) = z^{-\delta} + 2z^4 - \delta + z^{16} - \delta$ be the real valued and differentiable function and for its derivative $G'_1(z)$, let $z_1$ be the unique solution of the equation $G'_1(z) = 0$ in the interval $(0, \frac{11}{2})$ (cf. Lemma 3). Let $F_1(\delta) = \log_2 G_1(z_1)$. Let $\tilde{f}_0(z) = 1 + 2z + 2z^4 + 2z^9 + z^{16}$ be the real valued function and

$$F_0(\delta) = \frac{1}{3} \min_{z \in (0, \frac{11}{2})} \log_2 \frac{\tilde{f}_0(z)}{z^6}$$

Now we give an analogue of Theorem 4. Its proof is similar to the proof of Theorem 4.

**Theorem 6.** Assume the notation above. For $0 < \delta < \frac{11}{2}$, there exists a sequence of $\mathbb{Z}_8$-linear codes of length $n$, minimum distance $d$ and size $2^k$ such that $n \to \infty$, $d/n \to \delta$, $k/n \to R$ satisfying

$$R \geq 1 - \max \{ \frac{F_0(\delta)}{3}, \frac{F_1(\delta)}{2}, F_2(\delta) \}.$$ 

Moreover if

$$F_2(\delta) = \max \{ \frac{F_0(\delta)}{3}, \frac{F_1(\delta)}{2}, F_2(\delta) \}$$

holds, then

$$R \geq 1 - \log_2 1 + \delta - \frac{\delta^2 - \delta}{\left( \frac{\delta}{2} \right)^{\frac{2}{3}}}.$$ 

5.3. **PSK weight over $\mathbb{Z}_8$.** For $0 \leq \alpha \leq 7$, let

$$w_{PSK}(\alpha) = |e^{2\pi i \frac{\alpha}{8}} - 1| = \begin{cases} 0 & \text{if } \alpha = 0, \\ \sqrt{2} - \sqrt{2} & \text{if } \alpha \in \{1, 7\}, \\ \sqrt{2} & \text{if } \alpha \in \{2, 6\}, \\ \sqrt{2} + \sqrt{2} & \text{if } \alpha \in \{3, 5\}, \\ 2 & \text{if } \alpha = 4. \end{cases}$$

For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_8^n$, its **PSK weight** is given by $w_{PSK}(\alpha) = \sum_{i=1}^n w_{PSK}(\alpha_i)$. We have

$$1 = \frac{1}{2} \sum_{\alpha \in 4\mathbb{Z}_8} w_{PSK}(\alpha), \quad \frac{1 + \sqrt{2}}{2} = \frac{1}{4} \sum_{\alpha \in 2\mathbb{Z}_8} w_{PSK}(\alpha) = 1.20710 \ldots,$$

$$\sqrt{2} - \sqrt{2} + \sqrt{2} + \sqrt{2} + \sqrt{2} = \frac{1}{8} \sum_{\alpha \in \mathbb{Z}_8} w(\alpha) = 1.25683 \ldots.$$ 

Assume that $0 < \delta < 1$. Let

$$F_2(\delta) = \log_2 1 + \frac{\delta}{\left( \frac{\delta}{2} \right)^{\frac{2}{3}}}.$$

$G_1(z) = z^{-\delta} + 2z^{\sqrt{2}-\delta} + z^{2-\delta}$ be the differentiable real valued function with the derivative $G'_1(z)$, and let $z_1$ be the unique solution of the equation $G'_1(z) = 0$ in the
interval $(0, 1)$ (cf. Lemma 3). Let $F_1(\delta) = \log_2 G_1(z_1)$. Let $f_0(z) = 1 + 2z\sqrt{2} - \sqrt{2} + 2z\sqrt{2} + z^2$, and

\[ F_0(\delta) = \frac{1}{3} \min_{\delta \in [0, 1]} \log_2 \frac{f_0(z)}{z^3} \]

(cf. [7, Theorem 4.1]). We obtain the following theorem using the methods of Theorem 4.

**Theorem 7.** Assume the notation above. For $0 < \delta < 1$, there exists a sequence of $\mathbb{Z}_8$-linear codes of length $n$, minimum distance $d$ and size $2^k$ such that $n \to \infty$, $d/n \to \delta$, $k/n \to R$ satisfying

\[ R \geq 1 - \max\{\frac{F_0(\delta)}{3}, \frac{F_1(\delta)}{2}, F_2(\delta)\}. \]

Moreover if

\[ F_2(\delta) = \max\{F_0(\delta)/3, F_1(\delta)/2, F_2(\delta)\}, \]

holds, then

\[ R \geq 1 - \log_2 \frac{1 + \frac{\delta}{2}}{\left(\frac{2-\delta}{2}\right)^2}. \]

**Acknowledgments**

The authors would like to thank the anonymous referees for the useful suggestions.

The second author acknowledges the partial support from TÜBİTAK and is grateful to METU Department of Mathematics and METU Institute of Applied Mathematics, where he stayed while a part of this paper was written.

The first author acknowledges the partial support from the Turkish Academy of Sciences in the framework of the Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

**References**


Received June 2006; revised August 2006.

*E-mail address:* ozbudak@metu.edu.tr  
*E-mail address:* sole@essi.fr