Linear additive codes over $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

S. Araz, M. Zaved, M. Atrash, M. Asker

Abstract: In this paper, we prove that the additive greedy and the additive self-orthogonal greedy codes with Hamming distance one are linear when they are generated by using the additive $B$-ordering of vectors for any basis $B$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ over $\mathbb{Z}_2$.

AMS Subject Classification 2000: 11T71
Key words: Greedy codes $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, Linear codes

II Introduction

Greedy codes over $\mathbb{Z}_2$ are studied by Levenson [8]. He proved that binary greedy codes are linear when using lexicographic ordering. In [3], Conway and Sloane proved that the greedy codes are linear when using lexicographic ordering over a field of order $2^q$, where $q$ is a positive integer. Pless and Brualdi [2], Ruma Monika [9], [10], and M. Atrash [4] showed that the binary greedy codes are linear when they are generated by using a B-ordering and Hamming distance in [5]. A. Atrash showed that greedy and self-orthogonal greedy codes over a field $\mathbb{Z}_2$, where $q$ is a prime integer using B-ordering in modification of B-ordering, and Hamming distance are linear in [6]. A. Atrash and A. Aashir showed that the codes over the rings $\mathbb{Z}_2$ and over the $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, when they are generated by B-ordering in any integral basis using algorithm that is almost greedy and Hamming distance are linear codes, respectively. In this paper, we will give an inductive proof that the additive greedy and the
additive self-orthogonal greedy codes with Hamming distance one linear when they are generated by using the additive $Z$-ordering of vectors for any basis $Z$ in $\mathbb{Z} \times \mathbb{Z}$ over $\mathbb{Z}$.

## Definitions and preliminaries

The set $\mathbb{Z} = \mathbb{Z} \times \mathbb{Z}$ has four elements $0, 0$, $1, 0$, $1, 1$, $1, 1$ for $0$-convention we can write these elements in the form $1, 0$ and $1, 1$ is a ring under componentwise addition and multiplication these operations are given in the following table:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

We define a word $Z$ over the ring $\mathbb{Z}$ as a subset of elements $\{0, 1\}$ generated in an arbitrary manner.

Additive codes over the group $\mathbb{Z}$ are introduced in [1] the additive codes mean the codes that are invariant under vector addition. A code that is additive over a cyclic group of prime order is linear and in particular binary and ternary additive codes are linear but in the quaternary case being linear is stronger than being additive. There are two nonisomorphic finite groups $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$. The later one gives the best results in both additive linear codes. The Hamming weight of a codeword $u$ is denoted by $w(u)$ is the number of nonzero coordinates $u$. The Hamming distance between two codewords $u$ and $v$ denoted by $D(u, v)$ is the number of locations in which they are different and $D(u, v) = \min\{d | d \neq 0\}$. The minimum distance $d$ of the code $C$ is the smallest Hamming distance $D(u, v)$ where $u \neq v$ and $d \neq 0$. 

\[d = \min\{D(u, v) | u \neq v \}
\]
3: Greedy Codes

Greedy codes are defined by Fox in [2,9]. For the purpose of this paper, we define the ordering and the greedy codes in the following general way:

3.1 Definition

In the binary ordering basis there is a "natural" way of ordering the vectors called the lexicographic ordering \( \mathcal{S} \) in which \( i = 1 \) and a vector \( (a_1, a_2, \ldots, a_n) \) is \( b_1, b_2, \ldots, b_n \) if \( i + 1 \) such that \( a_k = b_k \) for all \( 1 \leq k \leq n \) and \( a_n = 1 \).

Desse and Brasen [2] have generalized this and defined what they called \( B \)-ordering of vectors \( u_i \) as in the following definition:

3.2 Definition 2

A \( B \)-ordering is an ordering of vectors \( u \) such that the binary field \( \mathbb{F}_2 \) is obtained recursively from an ordered basis \( b = (b_1, b_2, \ldots, b_n) \), which can be any ordered basis of the binary vectors of length \( n \). The first vector in the \( B \)-ordering is the zero vector and the next is \( b_n^{-1} \). The \( B \)-ordering is then generated recursively, where if the first \( 2^{i-1} \) vectors of the ordering have been generated using the basis elements \( (b_1, b_2, \ldots, b_{i-1}) \), then the next \( 2^{i-1} \) vectors are generated by adding \( b \) to those vectors already produced in order.

3.3 Definition 1

Lexicographic codes of length \( n \) and Hamming distance 2 are obtained by considering all \( 2^n \) vectors in lexicographic order and adding to the word if they are at a distance greater than or equal to 2 from the word vectors that were added earlier. If we start with two in several code words in the code such words are called lexicographic codes with words. Many codes can be obtained in this way as.

---

[Note: The page continues with more definitions and further explanations related to the topic of greedy codes. The content is not fully transcribed here.]
4. Main Results

Here we define the additive B-ordering of $\mathbb{Z}_2 \oplus \mathbb{Z}_2^F$ in the following way.

4.1 Definition

Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis for $(\mathbb{Z}_2 \oplus \mathbb{Z}_2^F) \times \mathbb{Z}_2$. We define the additive B-ordering as follows. The first vector in the additive B-ordering is the zero vector and the next is $b_1$. The additive B-ordering is then generated recursively, where if the first $2^k$ vectors of the ordering have been generated using the basis elements $\{b_1, b_2, \ldots, b_{n-1}\}$, then the next $2^k$ vectors are generated by adding $b_n$ to those vectors already produced in order.

4.2 Definition

Additive greedy code of vectors of length $n$ listed in some ordering even in group $B = \mathbb{Z}_2 \oplus \mathbb{Z}_2^F$ and designed Hamming distance $d$ is generated as follows. The first vector in the ordering is selected for the code. Then proceeding once through the ordering, a vector is selected if its distance from all previously chosen vectors is at least $d$.

4.3 Example

Let $B = \{b_1, b_2, b_3\}$ be a basis of $(\mathbb{Z}_2 \oplus \mathbb{Z}_2^F) \times \mathbb{Z}_2$. Then the additive B-ordering is

$0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1.$

4.4 Example

Let $B = \{011, 012, 210, 211\}$ be a basis of $(\mathbb{Z}_2 \oplus \mathbb{Z}_2^F) \times \mathbb{Z}_2$. Then the additive B-ordering and the additive greedy code is as in the following table.
The example shows that the additive greedy codes for \( n = 2 \) in column \( 2 \) and for \( n = 3 \) are linear. It follows that the greedy code when generated by additive B-ordering even if \( k \) is linear.

Here we state and prove the first of the two theorems of the paper.

### Theorem

Let \( n \) be an integer \( \geq 2 \). Let \( \mathcal{B} = \{b_1, b_2, \ldots, b_m\} \) be any ordered basis of \( \mathbb{R}^n \). Then the additive greedy code generated by the additive B-ordering is linear code.

**Proof:** Let \( \mathcal{C} \) be the additive greedy code generated by using the additive B-ordering. Let \( \mathcal{C} \subseteq \mathbb{R} \) be a set of vectors that have been chosen for the additive greedy code for the subbase \( \mathcal{B} = \{b_1, b_2, \ldots, b_m\} \). We will use induction on \( n \) to show that \( \mathcal{C} \) is a linear code. This is obviously true for \( n = 1 \). Assume that it is true for \( n = k - 1 \).

To prove linearity of \( \mathcal{C} \), let \( \mathcal{C} \) be the first vector chosen for the code.
If \( x = 2 \) and \( x \not\in c_1 \) then \( a \) satisfies
\[
\delta_H(x,c) = \delta_H(a,c) \quad 2 \leq n \quad 1
\]
for all \( x \in c_1 \).

If \( a \in c_1 \) then either \( a - y = n - a = 2y \) for some \( y \in c_1 \).

We will show that
\[
\delta_H(x,c) = 2 \quad \text{and} \quad \delta_H(v,c) = 2 \quad \text{for arbitrary} \quad x \in c_1.
\]

For the first case \( a - y = n - a = 2y \) we have
\[
\delta_H(x,c) = 2 \quad \text{and} \quad \delta_H(v,c) = 2 \quad \text{by inductive hypothesis}
\]
for the second case we have
\[
\delta_H(x,c) = \delta_H(a - 2a) = \delta_H(a, c_0) \leq 2 \quad \text{by} \quad 1
\]
and
\[
\delta_H(x,c) = \delta_H(x - c) = \delta_H(x + c_c - c) = \delta_H(x - (c - c)) \leq 2 \quad \text{by} \quad 1
\]
Since \( c_1 \quad 1 \leq \quad 2 \)

It remains to show that \( \delta_H(x - c) = 2 \) then \( a \in c_1 \).

So assume that \( a \in c_1 \) for some \( a \in c_1 \).

If \( a \in c_1 \) there must be some codeword \( a \) in preceding \( s \) such that
\[
\delta_H(a,c) = 2
\]
then
\[
\delta_H(v,v) - \delta_H(2a,2a) = 2
\]
which is a contradiction because \( v \in c_1 \) and \( 2a = c_1 \) we have \( v = 2a \) and only \( v = c_1 \) this completes the proof.

### 1.6 Definition

The inner product of two codewords \( x = (x_1, x_2, \ldots, x_n) \) and \( y = (y_1, y_2, \ldots, y_n) \) on \( [R]^n \) is defined by
\[
\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n
\]

The dual code \( C^\perp \) of \( C \) is defined as
\[
C^\perp = \{ g = R^\perp : g \cdot x = 0 \quad \text{for all} \quad y \in C \}
\]

\( C \) is called self-orthogonal if \( C \subseteq C^\perp \) and \( C \) is called self-dual if \( C = C^\perp \).
4.7 Definition

A self-orthogonal additive greedy code over \( \mathbb{F} \) of length \( n \) and designed Hamming distance \( n \) when it is generated by the additive B-ordering is a code with additional restrain that the vectors must be orthogonal to themselves and each other.

The following is the second main theorem in this paper.

4.8 Theorem

Additive self-orthogonal codes over \( \mathbb{F} \) are linear when generated from additive B-ordering in any basis for \( R^n \).

Proof: The proof is almost same as the proof of Theorem 4.5, however we have to make sure that the code is self-orthogonal.

We prove by induction that the self-orthogonal code \( \mathcal{C} \) is linear. Let \( \mathcal{C} \) be the additive self-orthogonal greedy code generated by using the additive B-ordering. Let \( \mathcal{C}_1 = \mathcal{C} \) be a set of vectors that have been chosen for the additive greedy code for the subbase \( \mathbf{v}^1 = (b_1, b_2, \ldots, b_k) \).

We will use induction on \( k \) to show that \( \mathcal{C}_1 \) is a linear code. This is obviously true for \( k = 1 \). Assume that it is true for \( k - 1 \).

To prove linearity of \( \mathcal{C}_1 \), let \( \mathbf{v} \) be the first vector chosen for the code \( \mathcal{C}_1 \) and let \( x \) be a set of vectors that satisfy

\[ d_H(x, c) = wt_H(x) \geq n \quad (1) \]

and

\[ d_H(x, c) = 1 \quad \text{for all vectors } \mathbf{c} \neq \mathbf{c}. \quad (2) \]

For \( b \geq \mathbf{c}_k \), then either \( a = \mathbf{c}_k \) or \( a \) is \( \geq \mathbf{c}_k \) for some \( b = \mathbf{c}_k \).

We will show that

\[ wt_H(v) \geq 1 \text{ and } d_H(v, c) \geq 1 \text{ for arbitrary } \mathbf{c} \neq \mathbf{c}. \]

and

\[ wt_H(v) = 1 \quad \text{for all vectors } \mathbf{c} \neq \mathbf{c}. \]

For our first case \( a = \mathbf{c}_k \), we have

\[ wt_H(v) = 1 \quad \text{and } d_H(v, c) = 1 \quad \text{by (1)}. \]
and also
\[ w_d - 1 \leq w_a - 1 \text{ for all } x \neq 0 \text{ by inductive hypothesis 2.} \]

For the second case we have
\[ w_H(a) - w_H(x + c_0 - a) \leq 7 \text{ if } a \neq 0 \]
and
\[ d_H(v, c) - w_H(v) - w_H(x + c_0 - a) - w_H(x + c_0 - c) \leq 7 \text{ if } a \neq 0 \]

Since \( c_0 \neq 0 \), and also
\[ \text{Lemma } - (a = 0). (x = c_0) \]
and
\[ w_d - (a = 0), d - c_0 = x - c_0 - 1 \text{ for all } x \neq 0 \text{ by inductive hypothesis 2.} \]
\[ \text{So we get } a = c_0. \]

It remains to show that \( w_d - a = 0 \) if \( c_0 \neq 0 \) then \( a = c_0 \).

So assume that \( a = c_0 \) for some \( a = c_0 \).

Thus, \( a = c_0 \). Hence, there must be some word \( \alpha \) preceding \( a \) such that
\[ w_H(\alpha, c_0) = 7. \]

Then
\[ w_H(\alpha, c_0) - w_H(\alpha, c_0) = 0 \]
Which is a contradiction because both of the words \( \alpha = 0 \) and \( c_0 = 0 \) are not \( c_0 \) and only \( 7 = 0 \) that completes the proof.

5 References

1. J. Levenstine "A class of systematic codes" Dokl Akad Nauk (1960),368-371


3. K. Fummk and V.Pless "Greedy codes" JCT(A)64(1993),10-30


7 | M. El-Atrash, "Greedy codes over \( \mathbb{Z}_2^r \) conference on "Information Technology and its future role" Musul Iraq Mar. 11-13 2000.

8 | M. El-Atrash and M. Al-Ashker, "Linear codes over \( \mathbb{Z}_2^r \) using almost-greedy algorithm" The Islamic University Journal, Vol. 11, No 2, Natural Sciences Series pp 32 to 38, January 2003.

9 | M. El-Atrash and M. Al-Ashker, "Linear codes over \( \mathbb{Z}_2 \) using \( \mathbb{Z}_2^r \)". The Islamic University Journal, Vol. 11, No 2, Natural Sciences Series pp 32 to 38, January 2003.