Linear additive codes over $Z_2 \times Z_2$

S. Azab , M. Zayed, M.Atrash, M. Ashker

Abstract: In this paper we prove that the additive greedy and the additive self-orthogonal greedy codes with Hamming distance are linear when they are generated by using the additive B-ordering of vectors for any basis B of $(Z_2 \times Z_2)^n$ over Z_2.

AMS: Subject classification 2000:11H71

Key words:Greedy codes, $Z_2 \times Z_2$ -linear codes

1 Introduction

Greedy codes over Z_2 are studied by Levenstein [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^{2^a}, where a is a positive integer. Pless and Brualdi [2], Laura Monroe [9], [10] and El-Atrash [4] showed that the binary greedy codes are linear, when they are generated by using a B-ordering and Hamming distance. In [5] El-Atrash showed that greedy and self-orthogonal greedy codes over a field Z_p where p is prime integer using B* -ordering (a modification of B -ordering) and Hamming distance are linear. In [6], [7] El-Atrash and Al-Ashker showed that the codes over the rings Z_4 and over the $F_2 + uF_2$ when they are generated by B-ordering of any ordered basis using an algorithm that is "almost" greedy and Lee 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 are linear when they are generated by using the additive B-ordering of vectors for any basis $\mathbb{B}$ of $\mathbb{Z}_2 \times \mathbb{Z}_2$ over $\mathbb{Z}_2$.

2 Definitions and preliminaries

The set $R = \mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$; for convenience we can write these elements in the form 0, 1, 2 and 3. R is a ring under componentwise addition and multiplication; these operations are given in the following tables:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	0	1
2	0	0	2	2
3	0	1	2	3

We define a code C over the ring R as a subset of elements $\in (R)^n$ generated in an arbitrary manner.
Additive codes over the group R are introduced in [1], the additive codes means 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 groups of order 4, the cyclic group $\mathbb{Z}_4$ and $R = \mathbb{Z}_2 \times \mathbb{Z}_2$. The later one gives the best results a bout additive linear codes. **The Hamming weight** of a codeword x denoted by $wt(x)$ is the number of nonzero coordinates of x. **The Hamming distance** between two codewords x and y denoted by $d(x,y)$ is the number of locations in which they are differ and $d(x,y) = wt(x - y)$. **The minimum distance** d of the code C is the smallest Hamming distance $d(x,y)$ where $x, y \in C$, and $x \neq y$.

3 Greedy Codes

Greedy codes are defined 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 case there is a " natural " way of ordering the vectors called the lexicographic ordering [8] in which $0 < 1$ and a vector $(a_1, a_2, ..., a_n) < (b_1, b_2, ..., b_n)$ iff $\exists\, i$ such that $a_k = b_k$ for all $1 \leq k < i$ and $a_i = 0$, $b_i = 1$.

Pless and Brauldi [2] have generalized this and defined what they called B-ordering of vectors over Z_2 as in the following definition.

3.2 Definition [2]

A B-ordering is an ordering of vectors of length n over the binary field obtained recursively from an ordered basis $B = \{b_1, b_2, ..., b_n\}$, 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_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 $\{b_1, b_2, ..., b_{i-1}\}$, then the next 2^{i-1} vectors are generated by adding b_i to those vectors already produced in order.

3.3 Definition [1]

Lexicographic codes of length n and Hamming distance d are obtained by considering all q-array vectors in lexicographic order, and adding to the code if they are at a distance greater than or equal to d from the codewords that were added earlier. If we start with one or several codewords in the code; such codes are called lexicographic codes with seeds. Many codes can be obtained in this way see [1].

4 Main Results

Here we define the additive B-ordering of $(Z_2 \times Z_2)^n$ in the following way:

4.1 Definition

Let $B = \{b_1, b_2, ..., b_n\}$ be a basis for $(Z_2 \times Z_2)^n$ over 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^{i-1} vectors of the ordering have been generated using the basis elements $\{b_1, b_2, ..., b_{i-1}\}$, then the next 2^{i-1} vectors are generated by adding b_i to those vectors already produced in order.

4.2 Definition

Additive greedy code of vectors of length n listed in some ordering over a group $R = Z_2 \times Z_2$ 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 $(R)^3$ over Z_2. Then the additive B-ordering is:
0, b_1, b_2, $b_2 + b_1$, b_3, $b_3 + b_1$, $b_3 + b_2$, $b_3 + b_2 + b_1$.

4.4 Example

Let $B = \{0131, 2103, 2231, 1012\}$ be a basis of $(R)^3$ over Z_2, then the additive B-ordering and the additive greedy are as in the following table:

Additive B-ordering	Additive Greedy codes	
0000	$d = 3$	$d = 4$
0131	0000	0000u
2103	0131	0000
2032	2103	2231
2231	2032	1123
2300	3223	3312
0332	3312	
0203	1320	
1012	1211	
1123		
3111		
3020		
3223		
3312		
1320		
1211		

This example shows that the additive greedy codes for $d = 3$ in column 2 and for $d = 4$ are linear. It follows that the greedy code when generated by additive B-ordering over R is linear.

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

4.5 Theorem

Let d be an integer ≥ 1. Let $B = \{b_1, b_2, ...b_n\}$ be any ordered basis of $(R)^n$. Then the additive greedy code generated by the additive B-ordering is linear code.

Proof: Let C be the additive greedy code generated by using the additive B-ordering. Let $C_i \subset C$ be a set of vectors that have been chosen for the additive greedy code for the subbase $W_i = \{b_1, b_2, ...b_i\}$. We will use induction on i to show that C_i is a linear code. This is obviously true for $i = 0$. Assume that it is true for $i = k$.

To prove linearity of C_{k+1}, let u be the first vector chosen for the code

$C_{k+1} \subset C$ that is not in C_k. Then x satisfies,

$$d_H(x,c) = wt_H(x - c) \geq d \qquad (1)$$

for all $c \in C_k$.

Let $v \in C_{k+1}$. Then either $v = c_0$ or $v = x + c_0$ for some $c_0 \in C_k$.
We will show that

$$wt_H(v) \geq d, \text{ and } d_H(v,c) \geq d, \text{ for arbitrary } c \in C_k.$$

For the first case $v = c_0$, we have

$$wt_H(v) \geq d \text{ and } d_H(v,c) \geq d, \text{ by inductive hypothesis.}$$

For the second case we have:

$$wt_H(v) = wt_H(x + c_0) = wt_H(x - c_0) \geq d \text{ by } (1)$$

and

$$d_H(v,c) = wt_H(v - c) = wt_H(x + c_0 - c) = wt_H(x - (c_0 - c)) \geq d, \text{ by } (1),$$

since $(c_0 - c) \in C_k$. So we get $v \in C$.

It remains to show that if $v = x + s$ with $s \notin C_k$, then $v \notin C$.
So, assume that $x + s \in C$ for some $s \notin C_k$.
For $s \notin C_k$, there must be some codeword c_1 preceding s such that $wt_H(s - c_1) < d$.
Then

$$wt_H(s - c_1) = wt_H((x + s) - (x + c_1)) < d.$$

Which is a contradiction because both of the codewords $x + s$ and $x + c_1 \in C$, so we have $x + c \in C$ if and only if $c \in C_k$. This completes the proof.

4.6 Definition

The inner product of a codewords $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ on $(R)^n$ is defined by

$$x.y = x_1y_1 + x_2y_2 + ... + x_ny_n.$$

The dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in (R)^n : x.y = 0 \text{ for all } y \in C\}.$$

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 R of length n and designed Hamming distance d when it is generated by the additive B-ordering is a code with additional restraint that the vectors must be orthogonal to themselves and each other.

The following is the second main theorem in this paper.

4.8 Theorem.

Additives self-orthogonal codes over R are linear, when generated from additive B-ordering of any basis for $(R)^n$.

Proof: The proof is almost same as the proof at Theorem (4.5), however, We have to make sure that our codewords are self orthogonal.

We prove by induction that the self- orthogonal code C is linear. Let C be the additive self-orthogonal greedy code generated by using the additive B-ordering. Let $C_i \subset C$ be a set of vectors that have been chosen for the additive greedy code for the subbase $W_i = \{b_1, b_2, ...b_i\}$. We will use induction on i to show that C_i is a linear code. This is obviously true for $i = 0$. Assume that it is true for $i = k$.

To prove linearity of C_{k+1}, let x be the first vector chosen for the code $C_{k+1} \subset C$ that is not in C_k. Then x satisfies,

$$d_H(x,c) = wt_H(x - c) \geq d \qquad (1),$$

and

$$x.x = 0, \; x.c = 0 \text{ for all codewords } c \in C_k \qquad (2)$$

Let $v \in C_{k+1}$. Then either $v = c_0$ or $v = x + c_0$ for some $c_0 \in C_k$.

We will show that

$$wt_H(v) \geq d, \text{ and } d_H(v,c) \geq d, \text{ for arbitrary } c \in C_k.$$

and

$$v.v = 0, \; v.c = 0 \text{ for all codewords } c \in C_k$$

For the first case $v = c_0$, we have

$$wt_H(v) \geq d \text{ and } d_H(v,c) \geq d, \qquad \text{By } (1)$$

and also

$$v.v = 0, \ v.c = 0 \text{ for all codewords } c \in C_k \text{ by inductive hypothesis (2)}$$

For the second case we have:

$$wt_H(v) = wt_H(x + c_0) = wt_H(x \quad c_0) \geq d \text{ by (1)}$$

and

$$d_H(v, c) = wt_H(v - c) = wt_H(x + c_0 - c) = wt_H(x - (c_0 - c)) \geq d, \text{ by (1),}$$

since $(c_0 \quad c) \in C_k$. And also

$$v.v = (x + c_0).(x + c_0) = x.x + x.c_0 + c_0.x + c_0.c_0 = 0,$$

and
$v.c = (x + c_0).c = x.c + c_0.c = 0$ for all codewords $c \in C_k$ by inductive hypothesis (2).So we get $v \in C$.
It remains to show that if $v = x + s$ with $s \notin C_k$, then $v \notin C$.
So, assume that $x + s \in C$ for some $s \notin C_k$.
For $s \notin C_k$, there must be some codeword c_1 preceding s such that $wt_H(s \quad c_1) < d$.
Then

$$wt_H(s \quad c_1) = wt_H((x + s) \quad (x + c_1)) < d.$$

Which is a contradiction because both of the codewords $x + s$ and $x + c_1 \in C$, so we have $x + c \in C$ if and only if $c \in C_k$. This completes the proof.

5 References

[1] V.Levenstine, "A class of systematic codes", Dokl.Akad 1 (1960),368-371.

[2] J.Conway and N.J.A.Sloane, "Lexicographic codes: Error correcting codes from game theory ", IEEE Trans.Inform.Theory IT-32(1986),337-348.

[3] R.Brualdi and V.Pless,"Greedy codes", JCT(A)64(1993),10-30.

[4] Laura,Monroe, "Binary greedy codes",to appear in congressus numeratium , vol. 100-104.

[5] Laura,Monroe, "Self orthogonal greedy codes", Designs,codes and cryptography ,9(1):79-83,August 1996.

[6] M.EL-Atrash," Linearity of binary greedy codes",The Islamic University Journal,Volume-8-NO.2 Part 2-June 2000.

[7] M.EL-atrash, "Greedy codes over Z_p", conference on " Information Technology and its future role", Musil, Iraq, Mar., 11-13, 2000.

[8] M. EL-Atrash and M. AL-Ashker "Linear codes over Z_4 using almost-greedy algorithm ", The Islamic University Journal, Vol. 11, No. 1, Natural Sciences Series pp. 20 − 34, January, 2003.

[9] M. EL-Atrash and M. AL-Ashker "Linear codes over $F_2 + uF_2$ ", The Islamic University Journal, Vol. 11, No. 2, Natural Sciences Series pp. 53 − 68, 2003.

[10] G.Bogdanova, A.Brouwer, S.Kapralov and P.Ostergard "Error-Correcting Codes Over An Alphabet of Four Elements", Des.codes Cryptography, (to appear).