Linearity of Greedy Codes over Z_p

Mohammed S. EL-Atrash*
Amany J. El-Massry**

الملخص

أثبتنا في هذا البحث الخطية لترميز جريدي فوق الحقل Z_p حيث p عـدد أولي باستخدام الترتيب B-ordering من خلال تحويل الأساس المرتـب B_1 إلي الأساس المرتب B_2 بالمصفوفة المثلثية السفلية P حيث $B_2 = PB_1$. إضافـة إلي ذلك أثبتنا نفس النتيجة السابقة لترميز جريدي المتعامد ذاتياً.

ABSTRACT

In this paper we prove that for any ordered basis B_1 of a vector space there is a basis B_2 for which the greedy code generated using the B-ordering is linear with respect to B_2, where B_2 is derived from B_1 by a lower triangular matrix P; $B_2 = PB_1$. In Addition we prove a similar result for self-orthogonal greedy codes.

Key words: Linear codes, Greedy codes, Self-orthogonal codes.

AMS Subject Classification 2000: Primary 94B27; Secondary 94B05.

* ***Assoc. Prof. of Mathematics, department of mathematics, Islamic University-Gaza, Email: matrash@mail.iugaza.edu.***

** ***Lecturer Asst. of mathematics, department of mathematics, Al-Aqsa University-Gaza, P.O. Box 4051, Gaza, Palestine.***

the alphabet, and let α^n be the set of all strings of length n over α. Any nonempty subset C of α^n is called *q-ary block code*. Each string in C is called a *codeword*. If $C \subset \alpha^n$ contains M codewords then C has length n and size M or is an (n, M)-code. A code whose $\alpha = \{0, 1\}$ is called *binary code*. Let F be a field and n be a positive integer. Let $u = \{x_1, x_2, \ldots, x_n\}$. The ***Hamming weight*** function is defined as

$w_h(u)$ = The cardinality of $\{i \in \{1, 2, \ldots., n\}: x_i \neq 0\}$

= The number of non-zero coordinates x_i $(1, 2, \ldots., n)$.

Let x and y be two words of the same length. The ***Hamming distance*** or simply the ***distance*** between x and y differ. We denote distance between x and y by $d_h(x, y)$.

A code C is said to have minimum distance d if d = minimum $\{d_h(x, y) \mid x, y \in C, x \neq y\}$, and it is denoted by $d(C)$.

3. Orderings

Lexicographic ordering. If the order of the list is in the "natural" order, then these codes are called *lexicode*, where the "natural" order means that 0<1, and two binary vectors

$$(c_1, c_2\ldots\ldots, c_n) < (b_1, b_2\ldots\ldots, b_n)$$

if there is anon-negative integer k such that $c_i = b_i$ for all $i = k = 1$ and $c_{k+1} = 0$, $b_{k+1} = 1$.

For example (1, 0, 1) < (1, 1, 0).

Lexicodes are proved to be linear codes (c.f. [2]).

4. B-Orderings

Let V be a finite vector space of a dimension n over a field Z_p of prime order. A ***B-Orderings*** is generated recursively using an ordered basis $B = \{b_1, b_2 \ldots\ldots, b_n\}$ as follows:

The first p vectors are $0, b_1, 2b_1, \ldots., (p\text{-}1)b$. The B-orderings is then generated recursively, where if p^k vectors of the ordering have been generated using the basis elements $b_1, b_2, \ldots, b_k$ then the $(p\text{-}1)p^k$ vectors are generated by adding b_{k+1} to those vectors already produced, in order, $i = 1, 2, \ldots, p\text{-}1$.

Let d be an integer greater than or equal to one. The greedy code is the set C of vectors that are selected using the following ***greedy algorithm***.

1. Set up some ordering of vectors of a vector space V.
2. The first vector in the ordering is selected and placed in C.
3. We follow the ordering and if we find a vector u with $d_h(u, c) \geq d$ for all vectors $c \in$ C, then u is selected and placed in C.
4. Continue until the end of the ordering.

Example

Let $B = \{100, 010, 001\}$ be a basis over the field Z_3. If $d = 2$; then greedy codes generated by the B-ordering as follows:

The B-ordering	Seria
000	1
100	2
200	3
010	4
110	5
210	6
020	7
120	8
220	9

The B-ordering	Serial
001	10
101	11
201	12
011	13
111	14
211	15
021	16
121	17
221	18

The B-ordering	Serial
002	19
102	20
202	21
012	22
112	23
212	24
022	25
122	26
222	27

The greedy code for $d = 2$ is C = {000, 110, 220, 101, 011, 202, 022}. This example shows that greedy code generated by B-ordering over Z_3 is not always linear.

5. B*(d)-Ordering

Let d be an integer $1 = d = n$, we define the ***B*(d)-ordering*** using the distance d inductively consider the B-ordering using the basis vector $\{b_1, b_2, \ldots\ldots, b_n\}$. Set $C_0 = \{0\}$. Assume that we have defined the B*(d)-ordering and C_k for the basis vector $\{b_1, b_2, \ldots, b_k\}$ for p^k vectors. Now to define the B*(d)-ordering for the vectors in the range $[p^k+1, p^{k+1}]$ we find the first vector b in the B-ordering that satisfies $d_h(b, c) \geq d$ in the range $[p^k+1, p^{k+1}]$ for all $c \in C_k$. Then we list all linear combinations of b and all vectors c in C_k in the $p^k + (p-1).|C_k|$ places. If no such b exist, then the B*(d)-ordering is the same as the B-ordering.

The following two theorems are the main results of this paper. They both guarantee that for every basis B_1 there is another basis B_2 for which the greedy code using the B-ordering is a linear code, where B_2 is obtained from B_1. Both Theorems are considered as generalizations of the previously proved results in [1], [2], [5], [6],[7]. Proofs of both theorems are considered as constructive proofs from which we can derive the second basis for which the code is linear. In fact both theorems can be used to adjust a given basis to the other. We know how important to get a linear code. Theorems 1, 2 may be considered as a source of getting linear codes over any finite fields.

Theorem 1. *Let $B_1 = \{b_1, b_2, .., b_n\}$ be an ordered basis for the vector space V over Z_p. Then there exist a basis $B_2 = \{u_1, u_2, .., u_n\}$ for which the greedy code using the B-ordering is linear over Z_p with respect to B_2. Furthermore there exists an $n \times n$ lower triangular non-singular matrix P such that $u_i = Pb_i$, $i = 1, 2, \ldots, n$.*

Proof.

Let $W_k = \{b_1, b_2, \ldots b_k\}$, let C be the greedy code for V, C_k be the greedy code for W_k. We use induction on k.

For $k = 0$, it is clear that $W_0 = \{(0, 0, .., 0)\}$ and $C_0 = \{(0, 0, \ldots, 0)\}$, which implies that C_0 is linear.

Now, let $k \geq 1$, let C_k be the greedy code generated by $\{b_1, b_2, \ldots, b_k\}$. Also assume that C_k is linear and there exists

$\{u_1, u_2, \ldots, u_k\}$ basis for which the B-ordering using $\{u_1, u_2, \ldots, u_k\}$gives C_k, where $u_i = \sum_{j=1}^{i} \alpha_j b_j$.

Let j be the smallest integer, and let C_{k+j} be the greedy code of the vector space W_{k+j} that is not equal to C_k. Now, let b be the first vector in the B-ordering not in C_k that fits the greedy algorithm,

i.e., $d_h(b, c) \geq d$ for all $c \in C_k$. (1)

It follows that $b \in W_{k+j}$.

Put $u_{k+1} = b_{k+1}, u_{k+2} = b_{k+2}, \ldots, u_{k+j-1} = b_{k+j-1}, u_{k+j} = b$. (2)

Notice that for $i = 1, 2, \ldots, k$, $u_i = \sum_{j=1}^{i} \alpha_j b_j$ by mathematical induction, and, by (2), for $i = k + 1, k + 2, \ldots, k + j - 1$, $u_i = \sum_{j=1}^{i} \alpha_j b_j$ .Finally, for $i = k + j$, we have set $u_{k+j} = b \in W_{k+j}$, it follows that $u_{k+j} = b = \sum_{j=1}^{k+j} \alpha_j b_j$. Thus for all i, $i = 1, 2, \ldots, k+j$, we have $u_i = \sum_{j=1}^{i} \alpha_j b_j$. All we need to show now is the linearity of C_{k+j}.

Now we need to prove the following claim:

For $\alpha \in F$, $\alpha u_{k+j} + v \in C_{k+j}$ if and only if $v \in C_k$.

Proof of the claim:

Let $v \in C_k$, for $\alpha u_{k+j} + v$ to be in C_{k+j} it has to satisfy the following:

$d_h(\alpha u_{k+j} + v, u) \geq d$, for all previously chosen vectors $u \in C_{k+j}$.
Now vectors in C_{k+j} have the form $\gamma u_{k+j} + c$ for $c \in C_k$. It follows that $d_h(\alpha u_{k+j} + v, \gamma u_{k+j} + c) = wt_h(\alpha u_{k+j} + v - \gamma u_{k+j} - c)$

$$= wt_h((\alpha - \gamma)u_{k+j} - (c - v))$$

$$= wt_h(\delta u_{k+j} - \omega),$$

where $\delta = (\alpha - \gamma) \in F$, $\omega = (c - v)$ is in C_k by linearity of C_k. Since $wt_h(\delta u_{k+j} - \omega) = wt_h(u_{k+j} - \delta^{-1}\omega) \geq d$, by (1), it follows that $d_h(\alpha u_{k+j} + v, u) \geq d$, for all previously chosen vectors in C_{k+j}.

Conversely, assume that $\alpha u_{k+j} + v \in C_{k+j}$, then we have the following:

$d_h(\alpha u_{k+j} + v, u) \geq d$, for all previously chosen vectors in C_{k+j}.

In particular $d_h(\alpha u_{k+j} + v, \alpha u_{k+j} + c) \geq d$, for all previously chosen vectors $c \in C_k$. It follows that $d_h(v, c) \geq d$, for all previously chosen vectors $c \in C_k$, and so $v \in C_k$. This proves our claim.

Our claim showed that $\alpha u_{k+j} + v \in C_{k+j}$ if and only if $v \in C_k$.

This means that C_{k+j} = the linear span of b and vectors in C_k i.e., $C_{k+j} = \langle b, C_k \rangle$. This finishes the proof.

Example

Let $B_1 = \{100, 010, 001\}$ be a basis over Z_3, then there is a basis $B_2 = \{u_1, u_2, u_3\} = \{b_1, b_1+b_2, b_1+b_2+b_3\} = \{100, 110, 111\}$

1. INTRODUCTION

In [4], Conway and Sloane proved that greedy codes are linear when using lexicographic ordering and a field of order 2^{2^α}, where α is a positive integer. In [5], Pless and Brauldi generalized these results to general ordering than the lexicographic ordering called the B-ordering over the binary field. In [3], El-Atrash proved that the greedy codes are linear when using the B-ordering over any field of order 2^n for all $n \geq 1$. In [6], Monroe simplified the proof that binary greedy codes are linear. In [2], El-Atrash introduced a much shorter proof that: binary greedy codes and self-orthogonal greedy codes are linear when using B-ordering. In [1], El-Atrash defined what is called the B^*-ordering, for which that author proved the greedy code generated when using B^*-ordering is linear, in addition to a similar result for self-orthogonal greedy codes.

In this paper, we prove that for any ordered basis of a vector space over a field Z_p there is another basis for which the greedy codes when using a B-ordering are linear. The second basis can be obtained from the first using a lower triangular matrix.

2. Basic Definitions in Coding Theory

A *word* is a sequence of digits. *The length* of a word is the number of digits in the word. Let $\alpha = \{a_1, \ldots\ldots, a_q\}$ be a finite set called

over Z_3. The greedy code using the B-ordering is linear over Z_3 with respect to B_2.

The B-ordering	Seria
000	1
100	2
200	3
110	4
210	5
010	6
220	7
020	8
120	9

The B-ordering	Serial
111	10
211	11
011	12
221	13
021	14
121	15
001	16
101	17
201	18

The B-ordering	Serial
222	19
022	20
122	21
002	22
102	23
202	24
112	25
212	26
012	27

If $d = 2$, then the greedy code {000, 110, 220, 211, 021, 101, 122, 202, 012} is a linear code over Z_3.

Clearly, the transformation matrix $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

Theorem 2. *Let $B = \{b_1, b_2, .., b_n\}$ be an ordered basis for the vector space V over Z_p. Then there exists a basis $B_2 = \{u_1, u_2, .., u_n\}$ for which the self-orthogonal greedy code using the B-ordering is a linear code over Z_p with respect to the basis B_2. Furthermore there exists an $n \times n$ lower triangular non-singular matrix P such that $u_i = Pb_i$, $i = 1, 2, ..., n$.*

Proof.

The proof is basically the same as the proof of theorem . However, we have to make sure that codewords are self-orthogonal.

We will use same notation as in the proof of theorem1. We need to shoe that if b is self-orthogonal and orthogonal to all vectors $c \in C_k$, the linear combination of u_i and members of C_k are self-orthogonal, i.e., we have

$$b \circ b = 0, \tag{1}$$

$$b \circ u = 0 = c \circ b, \text{ for all } u \in C_k. \tag{2}$$

And we need to prove the following

$(\alpha b + v) \circ (\alpha b + v) = 0$. For all $v \in C_k$, $\alpha \in F$. (3)

And $(\alpha b + v) \circ u = 0$, for all $u \in C_k$. (4)

To prove (3) we have

$(\alpha b + v) \circ (\alpha b + v) = \alpha^2 b \circ b + \alpha b \circ v + \alpha v \circ b + v \circ v = 0$, since, $b \circ b = 0$,

$b \circ v = 0 = v \circ b$, $v \circ v = 0$ by (1) and (2).

And to prove (4) we have

$(\alpha b + v) \circ u = (\alpha b + v) \circ (\gamma b + c) = 0$, for the same reasons by (2).

Conversely, assume that $\alpha b + v \in C_{k+j}$, then we have the following:

1. $d_h(\alpha b + v, u) \geq d$, for all previously chosen vectors in C_{k+j}.

2. $(\alpha b + v) \circ (\alpha b + v) = 0$ (4)

In particular $d_h(\alpha b + v, \alpha b + c) \geq d$, for vectors $c \in C_k$.

It follows that $d_h(v, c) \geq d$, for all vectors $c \in C_k$.

By (4) above $(\alpha b + v)\bullet(\alpha b + v) = 0$, then

$\alpha^2 b\bullet b + \alpha b\bullet v + \alpha v\bullet b + v\bullet v = 0$, and since $\alpha b + v$ comes after αb in the B-ordering, then by the choice of $\alpha b + v$, by (3).

$(\alpha b + v)\bullet \alpha b = 0$, therefore $b\bullet v = 0 = v\bullet b$. Thus $v\bullet v = 0$. It follows that $v \in C_k$. Our claim showed that $\alpha b + v \in C_{k+j}$ if and only if $v \in C_k$.

This means that $C_{k+j} = \langle b, C_k \rangle$. This finishes the proof.

Example

In the last example $B_1 = \{100, 010, 001\}$ is a basis over Z_3. There is a basis $B_2 = \{u_1, u_2, u_3\} = \{b_1, b_1+b_2, b_1+b_2+ b_3\} = \{100, 110, 111\}$ basis over Z_3. The self-orthogonal greedy code using B-ordering is linear over Z_3, where the self-orthogonal greedy code used $d = 3$ is $\{000, 111, 222\}$, which is a linear code.

Conclusion

We have showed that for any basis B_1 there is another basis B_2 for which the B-ordering always gives linear greedy and linear self-orthogonal greedy codes. This has been proved for vector spaces over fields of prime order, and in [2], [3], [5], [6], [7] for fields of characteristic 2. At the end of this paper, it is worthy to mention that we can generalize our results on arbitrary finite fields of order p^n, for p prime. We hope to publish this in a forthcoming paper.

References

[1] El-Atrash M., "*Greedy codes over Z_p*", Journal of Al-Hadbaa University College, (2000)

[2] El-Atrash M., "*Linearity of binary greedy codes*", Islamic University Journal, (2000) Vol.12 No. 2, part 2.

[3] El-Atrash M., " *Linearity of binary greedy codes over fields of Characteristic 2*", (Islamic University of Gaza, Palestine) preprint, (2000).

[4] J.H. Conway and N.J.A. Sloane, "*Lexicographic Codes: Error Correcting Codes from Game Theory*", IEEE Trans. Inform. Theory IT-32 (1986), (337-348).

[5] Richard, Brualdi and Verra Pless, "*Greedy Codes*", JCT (A) 64 (1993), (10-30).

[6] Monroe and Laura, "*Binary Greedy Codes*", to appear in Congressus Numerantium, vol.14 (100-104).

[7] Monroe, Laura, "*Self-orthogonal Greedy Codes*", Designs, Codes and Cryptography, 9(1) pp. 79-83, august 1996.