Properties Of Linear Codes Over Finite Strict Semidomain

Vidya Nikam
Research Student, School of Mathematical Sciences,

North Maharashtra University, Jalgaon 425001, Maharashtra-India

Abstract
In this paper we combine results of algebraic geometry and linear algebra and proved some results of linear codes over finite Strict Semidomain.

Keywords: *codewords, Hamming weight, Hamming distance, strict semidomain, genrator matrix.*

Introduction

Errors occur after transmission of data through a channel. Generally encoding of the data is in the form of 0`s and 1`s and it has some fixed length in the form of vector over finite field Fq. In other words C is the code which is a subset of Fq^n and its length is n. The main tools of coding theory are Group theory and Combinatorics. First Goppa defined algebraic geometric codes over finite fields [1, 2]. After Goppa, to construct a code Tsfasman and Vladut used modular curves [4].Recently linear codes and algebraic geometric codes over rings are defined by Judy Walker using new techniques in algebraic geometry [8]. We have introduced linear codes over finite strict semidomain and explore the relation with associated linear codes over finite fields [14].In semirings, additive inverse and multiplicative inverse is absent, so I feel that codes over semirings can be more convenient and useful.

The purpose of this paper is to prove some results of linear codes over finite strict semidomain. Section 2, gives the background to prove some results of linear codes over finite Strict Semidomain. In section 3 we prove some results of linear codes over finite strict semidomain.

2. Preliminaries

Definition2.1 [11]: Let S be the non empty set on which is defined two binary operations, addition '+' and multiplication '•' satisfying the following conditions.

1) (S, +, 0) is commutative monoid.
2) (S, •, 1) is monoid.
3) (a + b) • c = a•c + b•c and
4) a • (b + c) = (a•b) + (a•c), ∀a, b, c ∈ S

that is multiplication '•' distributes over the operation addition '+' . (S , + , •) is a semiring.

Definition2.2 [11, 12]: Let S be a semiring. S is a Strict Semiring if (a + b) = 0 $\Rightarrow$ a = 0 and b = 0

Example 2.1.: Z_0^+ (set of positive integers with zero) is a Strict Semiring.

Strict Semidomain:-

Definition2.3 [12]: Let S be a non empty set. S is said to be a Strict Semidomain

if

1) S is a Commulative Semiring with 1.

2) S is a Strict Semiring. That is for a, b ∈ S, if a + b = 0 then a = 0 and b = 0

3) If in S, a • b = 0 then either a = 0 or b = 0.

Example 2.2:1) Let Z_0^+ (set of positive integers with zero) be the semiring, Z_0^+ is strict Semidomain.

3) Every Chain lattice is a Strict Semidomain.

Note that for strict semidomain 'SSD' abbrivation is used throughout. Also unless otherwise mentioned S will denote a SSD.

Semimodules over Strict Semidomain

Definition2.4[11]: Let S be a SSD. A S-Semimodule is commulative monoid (M, +) with additive identity 0_M for which we have a function S x M → M denoted by (s , m) → s m and called scalar multiplication Which satisfies the following conditions for all elements S, S'∈ S and all elements m, m' ∈ M

1) $(s\, s')\, m = s\, (s'\, m)$

2) $s(m + m') = s\, m + s\, m'$

3) $(s + s')m = s\, m + s'\, m$

4) $1_S\, m = m$

5) $s\, 0_M = 0_M = 0_s\, M$

Example 2.3: 1) Every Semiring S is an Z_0^+ -Semimodule.

2) Let V = Z_0^+ x Z_0^+ x …… x Z_0^+ (n times) then V is a Z_0^+ -Semimodule over Z_0^+.

Sub-Semimodule:-

Definition2.5[11]:A non-empty subset N of a S-Semimodule M is a subsemimodule of M if and only if N contains additive identity 0 and N is closed under addition and scalar multiplication.

Basis of S-Semimodule

Definition 2.6[9]: Let M be a semimodule over SSD S. The expression $a_1m_1 + a_2m_2 + \ldots + a_nm_n$, where $a_1, a_2, \ldots\ldots, a_n \in S$ are scalars is called a linear combination of elements $m_1, m_2, \ldots, m_n \in M$.

Definition 2.7[9]: In semimodule M over SSD S, a single element m is linearly independent.

If none elements $m_1, m_2, \ldots\ldots, m_n \in M$, $n \geq 2$ can be represented by a linear combination of the others then they are linearly independent. Otherwise, we say that $m_1, m_2, \ldots.., m_n$ are linearly dependent. An infinite set of elements is linearly independent if any finite subset of it is linearly independent.

A nonempty subset of semimodule M over SSD S is called a set of generators if every element of the semimodule M over SSD S is a linear combination of its elements.

Definition 2.8[9]: A linearly independent set of generators of semimodule M over SSD S is called a basis of M.

Note [9, 11, 12] In semimodule M over SSD S**, t**he number of elements in each basis may not be same.

Additive Irreducible Element:-

Definition2.9 [9]: Let s∈ S is called an additive irreducible element of SSD S if for all a, b ∈ S, $s = a + b \Rightarrow s = a$ or $s = b$.

Theorem2.1 [9]: In S-Semimodule, each basis has the same number of elements if and only if 1 is an additive irreducible element.

Definition2.10 [9]: Let S be a SSD. If for a ∈ S there exists an element b ∈ S such that ab = ba = 1 then a is called an invetible element in S and element b is said to be an inverse of a, denoted by a^{-1}.

Note: U(S) denote the set of all invertible elements in SSD S.

Note [9]: If 1 is an additive irreducible element and U(S) = 1, then in n-dimensional S-Semimodule S^n ,{e_1, e_2,……, e_n} is the unique basis.

Definition2.11 [9]: If each basis has the same number of elements then we call the number of elements in each basis a dimension of S-Semimodule M. In symbols dim(M). In this case number of elements in basis is called rank of M.

Free S-Semimodule

Definition2.12 [11]: A S-Semimodule having a basis over S is called a free S-Semimodule. Not every semimodule over a SSD is free.

Linear Codes over finite Strict Semidomain.

Definition2.12 [14]: Let S be finite Strict Semidomain. A linear code C of length n over S is a subsemimodule of the free semimodule S^n. If C is a free subsemimodule then we define dimension of C to be dimC = rank(C). Elements of C are called codewords.

Example 2.4: Let C_3 be a Chain lattice which is a finite strict semidomain. Linear code over C_3.

Definition2.13 [14]: If $C \subseteq S^n$ is a code of dimension K then a generator matrix of C is a K x N matrix whose rows form an S-base of C.

Definition2.14 [14]: If $C \subseteq S^n$ is a code then $C^{\perp}$ is the dual code of C and it is defined as

$C^{\perp} = \{ x \in S^n / \ < x, y > = 0, \forall\ y \in C\}$

Where $x = (x_1, x_2, \ldots . x_n)$, $y = (y_1, y_2, \ldots . y_n)$,

$< x, y > = \sum_{i=1}^{n} x_i y_i$ is the usual bilinear form on $S^n \times S^n$.

Proposition 2.1[14]: If $C \subseteq S^n$ is a code then the dual code $C^{\perp}$ of code C is a linear code.

Lemma 2.1[14]: If $C \subseteq S^n$ is a linear code of dimension K and M a generator matrix of C.

Then $C^{\perp} = \{ x \in S^n / Mx^t = 0\}$

Lemma 2.2[14]: Let $f : S^n \to S^n$ be a linear map Such that, $f(x) = Mx^t$ then $C^{\perp}$ is the Kernel of f.

If $C \subseteq S^n$ is a linear code of dimension K and M a generator matrix of C then dimension of $C^{\perp}$ is $n - k$.

Corollary 2.1[14]: If C is a linear code and H a generator matrix of $C^{\perp}$ then $(C^{\perp})^{\perp} = C$.

Corollary 2.2[14]: If C is a linear code and H a generator matrix of $C^{\perp}$ then $C = \{ x \in S^n / H x^t = 0\}$.

3. Some results of Linear Codes over finite Strict Semidomain.

Definition3.1: The Hamming distance d on $S^n \times S^n$ is given by

$$d(x, y) = \#\{ i : x_i \neq y_i\}$$

Where $x = (x_1, x_2, \ldots . x_n)$ and $y = (y_1, y_2, \ldots . y_n)$

Definition3.2: The minimum distance of a code C $\subseteq S^n$ is given by

d (C) = min{ d(x, y) / $x, y \in C, x \neq y$}

Definition3.3: The weight of x is defined by

W (x) = d (x, 0)

Where 0 = (0, 0,…., 0)

Remark 3.1: The function d is a metric on $S^n \times S^n$.

Proof: 1) d$(x, y) \geq 0$.

ii) d(x, y) = 0 if and only if $x = y$

iii) d(x, y) = d(y, x)

iv) d$(x, y) \leq$ d(x, z)+ d(z, y)

Where$x = (x_1, x_2, \ldots . x_n)$, $y = (y_1, y_2, \ldots . y_n)$and $z = (z_1, z_2, \ldots . z_n)$

(i), (ii) and (iii) are obvious from the definition of the Hamming distance.

It is enough to prove (iv), when *n* = 1, then it is true.

If $x = y$, then (iv) is obviously true since $d(x,y) = 0$.

If $x \neq y$, then either $z \neq x$ or $z \neq y$, so (iv) is again true.

Remark 3.2: For a linear code C $\subseteq S^n$, d(C) = min {W (x): $x \in C \setminus \{0\}$}.

Definition3.4: In S^n , the redundancy is $n - k$ of a k-dimensional linear code .

Definition3.5: Parity check matrix of linear code is generator matrix of its dual.

Lemma3.1:

If C is a linear code and H a parity check matrix of C then

1) There exists $x \in$ C of weight W if and only if there exists W columns of H which are S – linearly dependent.
2) We have

d (C) = min {W $\in Z^+$ / $\exists$ W Columns S- linearly dependent in H}

Proof: 1) If C is a linear code and H a parity check matrix of C.

Where C = { $x \in S^n$ / Hx^t= 0} by Corollary 2.2

Suppose $\exists\, x \in C$ of weight W.

Let $H'_1, H'_2, \ldots . H'_n$ be the columns of H.

$\Rightarrow$ H$x^t = \sum_{i=1}^{n} x_i H'_i$

Where $x = (x_1, x_2, \ldots . x_n)$

$\Rightarrow$Which are S-linearly dependent.

2) $\exists\, x \in C$ of weight W

By definition of d(C)

$\Rightarrow$ d(C) = min{ W (x) / $x \in C \setminus \{0\}$}

$\Rightarrow$d(C) = min {W $\in$ Z^+ / $\exists$ W Columns S- linearly dependent in H}

Corollary3.1: (Singleton Bound)

For a S-linear code of length n, dimension k and minimum distance d,

$$d - 1 \leq n - k$$

Proof: Let H being a parity check matrix of C.

$\Rightarrow d - 1$ Columns of H are S-linearly independent.

Since H has rank $n - k$.

(Because H is generator matrix of $C^{\perp}$ and dimension of C is k.)

$\Rightarrow d - 1 \leq n - k$.

OR

Proof:

Let E be the encoding of the code

$E: \{0,1\}^k \rightarrow \{0,1\}^n$

Consider a projection π of $k - 1$ bits of the encoded string. By projection, we mean consider only the first $k - 1$ bits and ignore the rest.

Since the original message is k bits, by Pigeon Hole principle, there exists at least

$\pi\,(E(C1)) = \pi\,(E(C2))$

These two codes can differ in maximum of $n - (k - 1)$ bits

$\Rightarrow d \leq n - k + 1$

Definition3.5:

If $d - 1 = n - k$ then a linear code of length n, dimension k and minimum distance d over finite SSD S is called maximum distance separable (MDS) .

Proposition3.1:

The dual code of a maximum distance separable code is maximum distance separable.

Proof: Let C be maximum distance separable code of length n and dimension k , H be a parity check matrix of C and $C^{\perp}$ is dual code of maximum distance separable code C.

$Here\ H'_1, H'_2, \ldots\ldots H'_n$ be the columns of H.

Then the usual element of $C^{\perp}$ can be written as,

yH = $\langle H'_1, y\rangle, \ldots\ldots\ldots, \langle H'_n, y\rangle$

Where y ranges over S^{n-k} and H'_i is the i^{th} column of H.

Since C is MDS, $n-k$ columns of H are linearly independent.

Hence, the maximum number of columns of H are $n-k-1$which are solutions of the linear equation $\langle x, y\rangle = 0$.

$\Rightarrow$The minimum distance of $C^{\perp}$ is at least $n-(n-k-1)-1$ and hence $C^{\perp}$ is maximum distance separable.

Conclusions:

In this paper we proved some results of linear codes over finite strict semidomain and explore the relation with associated linear codes over finite fields.

Acknowledgements:

I would like to thank my research guide Prin. Dr. K.B. Patil, Ex. Vice Chancellor of North Maharashtra University, Jalgaon for his support and encouragement.

References

[1] Goppa V.D., 'Algebraic Geometric Codes', Math. USSR-Izv. 21(1), 75-93, 1983.

[2] Goppa V.D., 'Geometry and codes', Kluwer Academic Publishers, (1988).

[3] Tsfasman M. and Vladut S., 'Algebraic-geometric codes', Kluwer Academic Publishers, Dordrecht-Boston-London, (1991).

[4] Tsfasman M., Vladut S. and Zink T.,On Goppa codes which are better than the Varshamov-Gilbert bound, Math. Nachr.109, 21–28, 1982.

[5] Calderbank A., McGuire G., P. Kumar, Helleseth T., Cyclic codes overZ4, locator polynomialsand Newton's identities, IEEE Transactions on Information Theory, 42, 217-226, (1996).

[6] San Ling and Chaoping Xing,Coding Theory, A First Course , Cambridge University Press, 2004 .

[7] Van Lint J.H., Van der Geer G., Introduction to Coding Theory and Algebraic Geometry, Birkhauser,Basel, 1988.

[8] Walker J.L., Algebraic geometric codes over rings, Journal of Pure and Applied Algebra 144, 91-110, 1999.
[9]Qian- Yu Shu, Xue- ping Wang, Bases in semilinear spaces over zerosumfreesemirings,
Linear Algebra and its applications, 435, 2681-2692, Elsevier, 2011,
[10] Qian- Yu Shu, Xue- ping Dimensions of L- semilinear spaces over zerosumfreesemirings,
IEEE, 978-1-4799-0348-1/13, (2013).
[11] Golan J.S., Semirings and TheirApplications, Kluwer Academic Publishers, Dordrecht/Boston/London, 1999.
[12] VasanthaKandasamy W.B., Smarandachesemirings, semifields and semivector spaces.
[13] Nikam Vidya, Rank-Nullity theorem over zerosumfreesemirings, International Journal of Applied Engineering Research, © Research India Publications,0973-4562 Vol. 13(5), (2018) 54-57.
[14] Nikam Vidya, Linear codes over finite strict semidomain communicated.