International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume 2 Issue 4, pp : 295-297 1 April 2013

Application of Module Structure of Algebra in Coding Theory in Different Branches of Engineering

Arvind Kumar Sinha
Department of Mathematics, National Institute of Technology, Raipur, (C. G.) India.
dr_arvindsinha2003@rediffmail.com

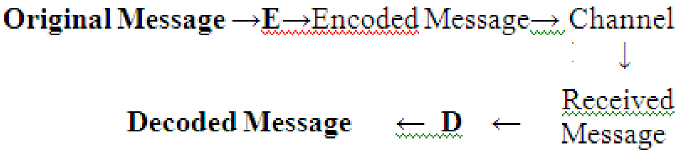
Abstract

In this paper we see how the module structure of Algebra plays a vital role in coding theory in different branches of Engineering mainly in Information Technology, Electronics and Telecommunications Engineering, Computer Science etc. The basic result was given by S. K. Sarkar [1] for group code. Here I generalize this concept for module theory in algebra and I introduce the concept module code. I give some results on module code and also give conclusion that why the module code is useful in coding theory.

Introduction

Coding theory deals essentially with the transmission of a message through a medium such that whatever errors the medium may introduce, could be detected and if possible corrected, in an efficient manner, at the receiver's end.

The following diagram represents the various aspect of transmission of information:


Original Message →E→Encoded Message→ Channel
↓
Decoded Message ← D ← Received Message

where **E** means encoding function and **D** means decoding function.

The message to be send is encoded into a code word using an encoding rule. Then the coded version is transmitted over a channel. The physical medium through which the messages are transmitted is called a channel e.g. a telephone line, a wireless channel used for mobile communications, a satellite link etc. When the coded word passes through the channel, errors may occur due to weather interference, electrical problems and so on and it becomes distorted. The decoder corrects the error in the distorted message and decodes the corrected version using decoding rule into the original message.

However the role of decoder is very important to find the correct original message but if we apply module structure in coding theory then the original message will be less distorted, comparative to word coding rule. This is due to that the coded version is in a form of module structure which is more general than word coding and being a mass and structural coding , it is always beneficial than word coding.

Preliminary

Message: The basic unit of information, called a message is a finite sequence of characters form a finite alphabet.

Word: A sequence of letters from an alphabet is often referred to as word.

Code: A code is a collection of words that are to be used to represent distinct messages.

Codeword: A word in a code is called a codeword.

Through-out this papers the sign + denotes component wise addition (mod2).

We assume that the alphabet is the binary alphabet {0, 1} There are 2^n binary words of length n. For n (any integers) ≥ 1 , let

$B^n = Z_2 Z_2 Z_2 Z_2 \ldots\ldots\ldots Z_2$ (n times) where Z_2 represents binary number.

For Example, $B^2 = \{00, 01, 10, 11\}$

$B^3 = \{000, 011,010, 111, 100, 110, 101, 001 \}$

$B^4 = \{0000, ,0001, 0011, 0111, 1111, 1001, 1011, 0111, 1010, 0101, 0110, 1110, 1000, 0100, 0011, 0010\}$ and so on.

It is easy to show that $(B^m, +)$ and $(B^n, +)$ are commutative group under the component wise addition (mod2) of words where m, n are integers $\geq$ 1. Note that every element in B^m

and B^n has its own inverse and zero word is the identity element.

Definition of left R-module [2]: Let R be a ring, M an additive abelian group and $(r, m) \mapsto r\,m$, a mapping of $R \times M$ into M such that

(1) $r(m_1 + m_2) = rm_1 + rm_2$
(2) $(r_1 + r_2)\,m = r_1m + r_2m$
(3) $(r_1 r_2)\,m = r_1(r_2 m)$

for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$. Then M is called **left R-module**

Definition of R-submodule[2] : A non empty subset N of an R-module M is called an **R-submodule** (or simply **submodule**) of M if

(i) $a + b \in N$ for all $a, b \in N$ (or N is an additive subgroup of M)

(ii) $ra \in N$ for all $a \in N$, $r \in R$

Main Results

Here I give the definition of **module code**:

Let $E : B^m \mapsto B^n$ be an encoding function. The code $C = E(B^m)$ is called a **module code** if C is a submodule of B^n.

From the definition of submodule, C the subset of B^n consisting of all code words is a submodule of B^n if

(1) If $x, y \in C$ then $x + y \in C$ (or C is additive subgroup of B^n)

(2) $ra \in C$ for all $a \in C$, $r \in B$

Now using above definition I give the following results:

Results 1: B^2 is a **left B-module** under the composition component wise addition (mod 2) where $B = \{0, 1\}$

Proof: Here $B^2 = \{00, 01, 10, 11\}$ and B is a ring (obvious)

First of all we have to show that B^2 is an additive abelian group. For this we see:

(G1) Closure Property: It holds closure property.

(G2) Associative Property: It holds Associative Property.

(G3) Existence of identity element: there exist $00 \in B^2$ such that $00 + a = a$ for all $a \in B^2$.

(G4) Existence of inverse element: It is obvious here every element in B^2 is its own inverse.

(G5) Commutative Property: It holds commutative property.

Now we see it holds all the three conditions under the component wise addition (mod 2)

(1) $r(m_1 + m_2) = rm_1 + rm_2$
(2) $(r_1 + r_2)\,m = r_1m + r_2m$
(3) $(r_1 r_2)\,m = r_1(r_2 m)$

Therefore $(B^2, +)$ is **left B-module** where $B = \{0, 1\}$.

Similarly we can show that $(B^3, +)$, $(B^4, +)$, $(B^5, +)$ etc are **left B-module** where $B = \{0, 1\}$.

Result 2: The (2, 5) encoding function $E: B^2 \mapsto B^5$ defined by

$E(00) = 00000$

$E(01) = 01110$

$E(10) = 10101$

$E(11) = 11011$

is a **B-module code**.

Proof: Let C be the set of all given code words, so

$C = \{00000, 01110, 01110, 10101, 11011\}$

To prove that the encoding function E is a module code we have to show that C is a **submodule** of B^5.

(1) C is clearly **a additive subgroup** of B^5 with operation component wise addition (mod2) because:

(I) The identity element in B^5 is 00000 which is also in C.

(II) Now $01110 + 10101 = 11011$

$01110 + 11011 = 10101$

$10101 + 11011 = 01110$

$00000 + 01110 = 01110$ etc

so all the elements in the right side belong to C.

(III) It is obvious that every element in B^5 is its own inverse

As 10101 + 10101 = 00000 (identity element)

Hence C is a subgroup of B^5 under the operation component wise addition (mod2)

(2) Now we only check that $ra \in C$ for all $a \in C$, $r \in B$

As $0(01110) = 00000 \in C$

$1(10101) = 10101 \in C$ etc

So $ra \in C$ for all $a \in C$, $r \in B$

Therefore C is a **sub module code** of B^5. Thus the encoding function E is **module code** over B (or **B-module code)** where B = {0, 1}.

Result 3: In a module code, the minimum distance between distinct code words is the minimum of the weights of the non-zero elements of the code.

Proof: Let (B^m , B^n, E, D) be module code. Let d be the minimum distance between two distinct code words.

Then their exists two distinct code words p and q in B^m such that d (p, q) = d (which is minimum distance) .

Let f be a non zero code word such that $w(f) \leq w(g)$ for all non zero code words g , where w denotes the weight of the code word.

Since $d \leq d(f, 0)$ (f and 0 being distinct code words) $= w(f)$

that is $d \leq w(f)$ ……………………(1)

Again $d = d(p, q) = w(p + q) \geq w(f)$

that is $d \geq w(f)$ ………………(2)

Therefore from (1) and (2) we get,

$$d = w(f)$$

Thus in a module code, the minimum distance between distinct code words is the minimum of the weights of the non-zero elements of the code. This proves the proposition.

Conclusion

If C be the set of code word and suppose $|C|$ (the number of code words in the set) = 128 then we have to compute ${}^{128}C_2 = 8128$ distances between every pair of code words. But if C possesses a **module code**, we need only compute **the weights** of 127 non -zero elements of C and they are in more general structured form due to scalar multiplication property which is inbuilt in these feathers which save our time and the original message will be less distorted.

Acknowledgement

I am very thank full to S. K. Sarkar [1] who has presented the basic concept in very nice and easy form so that I could do this work in very short span of time.

References

1. A text book of Discrete Mathematics – S. K. Sarkar , S Chad and Comp Ltd fourth edition 2006.
2. Basic Abstract Algebra – P. B. Bhattacharya, S K Jain, S R Nagpaul, Cambridge University Press, Second Edition 2012.
3. Introduction to coding theory, J. H. Van lint, Springer- Verlag, New York, 1982.
4. Coding Theory, The Essentials, K. G. Hoffman, et al, Marcel Dekker, New York, 1991.
5. Wood, J. A., Duality for modules over finite ring and applications to coding theory, American Journal of Mathematics, Vol. 121, No. 3 (1999) pp. 555-575.
6. Wood, J. A., Foundations of Linear codes defined over finite modules, codes over rings, Series on coding theory, Vol. 6, (2009) Singapore, World Scientific, pp. 124-190
7. Wood, J. A., Anti-isomorphism, character modules and self dual code over non-commutative rings, Int. J. Information and coding theory, Vol. I, No. 4(2010), pp. 429-444.