Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

ON THE APPLICATION OF ALGEBRAIC CODING THEORY TO THE IDEALS OF THE POLYNOMIAL RING $F_2^N[X]/\langle X^N-1\rangle$

Olege Fanuel [1]

[1] Department of Mathematics
Masinde Muliro University of Science and Technology
P.O Box 190-50100, Kakamega (Kenya)
e-mail: olegefanuel@yahoo.com

Abstract

The polynomial ring $F_2^n[x]/\langle x^n-1\rangle$ has generated a lot of research in recent times especially because it is a generator of binary codes used in computer application. In this paper, properties of this ring are outlined and application of algebraic coding theory to its ideals discussed.

Mathematics Subject Classification: [2010] Primary 20K30; Secondary 16P10. **Keywords:** Polynomial Ring, Ideals, generator, irreducible, prime, code.

1 Introduction

1.1 Background information

Definition 1.1. *[6]*

Let $F_2^n[x]/\langle x^n-1\rangle$ be a commutative ring with unity and let $g\in F_2^n[x]/\langle x^n-1\rangle$. The set $\langle g\rangle=\{rg|\ r\in F_2^n[x]/\langle x^n-1\rangle\}$ is an ideal of $F_2^n[x]/\langle x^n-1\rangle$ called the principal ideal generated by g. The element g is the generator of the principal ideal.

So, I is a principal ideal of a commutative ring $F_2^n[x]/\langle x^n - 1\rangle$ with unity if there exists $g \in I$ such that for all $g \in I$ we have $rg \in F_2^n[x]/\langle x^n - 1\rangle$ for some $r \in F_2^n[x]/\langle x^n - 1\rangle$.

In a Principal Ideal Domain every ideal is principal. If $\mathbb{F}$ is a field then every ideal I in $\mathbb{F}$ is a principal ideal. If a polynomial ring $F[x]/\langle x^n - 1\rangle$ is irreducible over $\mathbb{F}$ then $F[x]/\langle x^n - 1\rangle$ becomes a field. According to Ronald, *etal* [5], given some $\mathbb{Z}$-basis of an ideal we should be able to find a sufficiently shorter generator g which is not necessarily g itself.

2 Results

Proposition 2.1. *Let I be a maximal ideal over the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$. The following statements are equivalent:*

(i) I is Noetherian.

(ii) Every chain of subsets $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I_n)$ stabilizes at some I_n.

(iii) Every non-empty collection of subsets of I has a maximal ideal.

Proof

(i) $\Rightarrow$ (ii). Let I be Noetherian. Then we have the chain $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I_n)$. We can write $I' = \bigcup I_i \subset I$ which is finitely generated since I is Noetherian. Let the generator elements be $I_1, I_2, ..., I_n$. Each of these elements is contained in the union of I_n. Therefore $I' \subset I_n$ hence $I_n = I'$

(ii)$\Rightarrow$ (i). Assume that the ascending chain condition exists. Let $I' \subset I_n$ be any subset of I. Define a chain of subsets $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I')$ as follows; $I_0 = \{0\}$. Let $I_{n+1} = I_n + x(F_2^n[x]/\langle x^n - 1\rangle)$ for some $x \in (I' - I_n)$ if such an x exists. Suppose such an x does not exist take $I_{n+1} = I_n$. Clearly $I_0 = \{0\}, I_1$ is generated by some non-zero element of I', I_2 is I_1 with some element of I' not in I_1 until the chain stabilizes. By construction we have an ascending chain which stabilizes at some finite point by ascending chain condition. Hence I' is generated by n elements since $I' = I_n$.

(i) $\Rightarrow$ (iii). If I is Noetherian then it has a maximal ideal. To see this let P be a set of all the proper ideals in the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ containing I_p where I_P is any proper ideal in this ring. Already we know that $P \neq \emptyset$ since $I_P \in P$. Since $F_2^n[x]/\langle x^n - 1\rangle$ is Noetherian the maximum condition gives a maximal element $I \in P$. We should show that I is a maximal ideal in $F_2^n[x]/\langle x^n - 1\rangle$. Suppose there is a proper ideal J with $I \subseteq J$. Then

$I_P \subseteq J$ and hence $J \in P$. Therefore maximality of I gives $I = J$ and so I is a maximal ideal in $F_2^n[x]/\langle x^n - 1\rangle$.

(ii) $\Rightarrow$ (iii). If (iii) is false there is a non-empty subset S of $F_2^n[x]/\langle x^n - 1\rangle$ with no maximal element and inductively we can construct a non -terminating strictly increasing chain in S. (iii)$\Rightarrow$(ii). The set $\{x_{(m)} : m \geq 1\}$ has a maximal element which is I. □

Proposition 2.2. *$F_2^n[x]/\langle x^n - 1\rangle$ is a Unique Factorization Domain.*

Proof

Let $t \in F_2^n[x]/\langle x^n - 1\rangle$. Then t is irreducible if and only if t is prime. We have to show the following two claims:

(i) if t is prime then t is irreducible.

(ii) if t is irreducible then t is prime.

For claim (i) suppose that t is prime and $t = uv$, for all $t, u, v, \in F_2^n[x]/\langle x^n - 1\rangle$. We should prove that either u or v is a unit. Using the definition of prime, t divides either u or v. Suppose t divides u then we have $u = tw \Rightarrow u = uvw \Rightarrow u(1 - vw) = 0 \Rightarrow vw = 1$, for all $t, u, v \in F_2^n[x]/\langle x^n - 1\rangle$ and some $w \in F_2^n[x]/\langle x^n - 1\rangle$. Since $F_2^n[x]/\langle x^n - 1\rangle$ is an integral domain v is a unit. This same argument holds if we assume t divides v, thus t is irreducible. For claim (ii) let t be irreducible and t divides uv. Then $uv = tw$ for some $w \in F_2^n[x]/\langle x^n - 1\rangle$. By property of unique factorization domain, we decompose t, u, v into products of irreducible elements, say (t_i, u_i, v_i) upto the units (a, b, c). Hence $a \cdot t_1 ... a \cdot t_n = b \cdot u_i ... u_n = c \cdot v_i ... v_n$. This factorization is unique and therefore t must be associated to some u_i or v_i implying that t divides u or v. □

Example 2.1. *Consider the ideals corresponding to the polynomial ring $F_2^7[x]/\langle x^7 - 1\rangle$. We have:*

$I_1 = 0$
$I_2 = 1$
$I_3 = x + 1$
$I_4 = x^3 + x + 1$
$I_5 = x^3 + x^2 + 1$
$I_6 = x^4 + x^3 + x^2 + 1$
$I_7 = x^4 + x^2 + x + 1$
$I_8 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

where each of the I_i's $(i = 1, 2, 3, ..., 8)$ is a principal ideal of this ring. We then have the chain:

ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

$(I_1) \subseteq (I_2) \subseteq (I_3) \subseteq (I_4) \subseteq (I_5) \subseteq (I_6) \subseteq (I_7) \subseteq (I_8)$

Generally, for any polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ *we can develop the chain* $(I_1) \subseteq (I_2) \subseteq (I_3) \subseteq ... \subseteq (I_j)$ *where* j *is the total number of principal ideals in the candidate polynomial ring hence* $I_{i+1} \mid I_i$, *for all* $I_i \in F_2^n[x]/\langle x^n - 1\rangle$. *The prime factors of* I_{i+1} *contain prime factors of* I_j. *Already* I_j *has a unique factorization into many finite prime factors which end up being the same and so the chain stabilizes or terminates.*

By Proposition 2.1 and 2.2 the ring $F_2^n[x]/\langle x^n - 1\rangle$ is Noetherian. It is also a Unique Factorization Domain.

The polynomial I_j is the maximal ideal of the candidate ring.

Proposition 2.3. $F_2^n[x]/\langle x^n - 1\rangle$ *satisfies the descending chain condition on principal ideals.*

Proof

Using Example 2.1 and rearranging the ideals from maximal to the least we have:

$(I_j) \supseteq (I_{j-1}) \supseteq (I_{j-2}) \supseteq ... \supseteq (I_1)$ which also terminates or stabilizes. □

By Proposition 2.3 the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ is Artinian.

Proposition 2.4. *Let* (I_n) *be a family of ideals such that* $(I_n) \geq (I_m)$ *for some fixed* $(I_m) \in (I)$, *if:*

(i) (I_m) *is true and (* (I_m) *true means its fixed in* (I_n), *false means its varying in* (I_n)*)*

(ii) (I_n) *is true* $\Rightarrow (I_{n+1})$ *is true, then* (I_n) *is true for all* $n \geq m$.

Proof

Let $I_c \in F_2^n[x]/\langle x^n - 1\rangle$ be a family of all principal ideals for which (I_n) is false. If (I_c) is empty there is nothing to prove. Otherwise there is the smallest ideal $(I_k) \subseteq (I_c)$. From (i) $(I_k) > (I_m)$ and so we have some (I_{k-1}). But $(I_{k-1}) < (I_k)$ implies that $(I_{k-1}) \notin (I_c)$ since (I_k) is the smallest ideal in (I_c). Hence (I_{k-1}) is true. From (ii) $(I_k) = (I_{([k-1]+1)})$ is true and this contradicts $(I_k) \in (I_c)$ which claims that (I_k) is false. □

ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

2.1 Application of Maximum Likelihood Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$

Definition 2.1. *[1]*

Let C be a linear code over $\mathbb{F}_q$ and u a vector in the code space $\mathbb{F}_q^n$. The Maximum Likelihood Decoding problem is to find a code $v \in C$ such that:

$d_c(v, u) = d_c(u, c) = min\{d_c(u, c)\}$ *for all* $c \in C$.

On an mSC (p), the probability of receiving v after the transmission of u is given by $P(\frac{v}{u}) = p^{d_c}q^{n-d_c}$, (where d_c is the Hamming Distance between u and v, p is transition parameter such that $p + q = 1$ and n is the length of the code).

Definition 2.2. *[2] A Fermat prime is a prime of the form $2^{2^n} + 1$ where n is itself prime. A Mersenne prime is one of the form $2^n - 1$ for some prime n. A safe prime is a prime number of the form $2p + 1$ where p is also prime.*

Consider the set of generators of the polynomial ring $F_2^6[x]/\langle x^6 - 1\rangle$. Here $n = 6$ which is a composite integer. The code generated is given by

$$C = [000000, 000001, 000011, 000101, 001001, 010101, 001001, 011011, 111111].$$

Suppose a codeword 010101 was transmitted on a BSC (0.02) and two codewords, 000001 and 111111 were received. Then we have $P(000001|010101)$ $=q^4p^2 \approx$ 0.000368947264, while $P(111111|010101) = q^3p^3 \approx 0.000007529536$; it would therefore be efficient to decode 010101 to 000001.

Suppose $n = 7$ which is a safe prime. This would give the polynomial ring $F_2^7[x]/\langle x^7 - 1\rangle$. The code generated is given by

$$C = [0000000, 0000001, 0000011, 0001011, 0001101, 0011101, 0010111, 1111111].$$

Consider a codeword 0000011 transmitted on a BSC (0.03) and the two codewords, 0001011 and 1111111 are received. We have $P(0001011|0000011) = q^6p^1 \approx$ 0.02498916, while $P(1111111|0000011) = q^2p^5 \approx 0.00000002286387$; it would be efficient to decode 0000011 to 0001011.

Hence principles of maximum likelihood decoding are applicable to the polynomial ring $F_2^n[x]\text{mod}(x^n - 1)$ for prime values of n and for composite values of n.

ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

2.2 Application of Minimum Distance Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$

Definition 2.3. *[8]*

A code vector v is said to have undergone minimum distance decoding if and only if, when v is received, it is decoded to a codeword u that minimizes the Hamming distance $d_c(u, v)$.

Consider the set of generators of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ in which $n = 5$ which is a safe prime. The code generated is represented by

$$C = [00000, 00011, 00101, 00110, 01100, 01010, 11000, 11111].$$

Suppose we want to decode 01100 to any of the other codewords in C we must compute minimum distance as follows:

$d_c(01100, 00000) = 2$
$d_c(01100, 00011) = 2$
$d_c(01100, 00101) = 2$
$d_c(01100, 00110) = 2$
$d_c(01100, 01010) = 2$
$d_c(01100, 11111) = 3$

Hence it would be more efficient to decode 01100 to any of the codewords in C except to 11111.

Consider the set of codes generated by the polynomial ring $F_2^6[x]/\langle x^6 - 1\rangle$ in which $n = 6$ which is composite. The code is represented by

$$C = [000000, 000001, 000011, 000101, 010101, 001001, 011011, 111111].$$

Suppose we want to decode 111111 to any of the other codewords in C we must compute minimum distance d_c as follows:

$d_c(111111, 000000) = 6$
$d_c(111111, 000001) = 5$
$d_c(111111, 000011) = 4$
$d_c(111111, 000101) = 4$
$d_c(111111, 010101) = 3$
$d_c(111111, 001001) = 4$
$d_c(111111, 011011) = 2$

Therefore it would be more efficient to decode 111111 to 011011.

ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

Hence principles of Minimum Distance Decoding are applicable to the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ for prime values of n as well as for composite values of n.

Proposition 2.5. *Let $p < \frac{1}{2}$ where $p + q = 1$. Then maximum likelihood decoding and minimum distance decoding are equivalent.*

Proof

Let the the probability of receiving v after the transmission of u be given by
$P(\frac{v}{u}) = p^{d_c} q^{n-d_c}$, (where d_c is the Hamming Distance between u and v, p is transition parameter such that $p+q = 1$ and n is the length of the code). Minimizing the quantity $P(\frac{v}{u}) = p^{d_c} q^{n-d_c}$ is equivalent to minimizing d_c.

2.3 Application of Incomplete Minimum Distance Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$

Definition 2.4. *[8]*

Incomplete Minimum Distance Decoding for a received codeword v, occurs when it is decoded to a codeword u that minimizes the Hamming distance or when decoded to the error detected symbol η.

Consider a set of generators of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ in which $n = 5$, which is a safe prime. It was observed for instance in Section 2.2 that 01100 could be decoded to any of the codewords in C except to 11111. By Incomplete Minimum Distance Decoding, 01100 could also be decoded to the error detected symbol η. In this case the minimum distance cannot be determined.

Hence principles of Incomplete Minimum Distance Decoding are applicable to the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ for prime values of n as well as for composite values of n.

2.4 Application of Features of an optimal code to codewords of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$

According to Huffman and Pless [3], an (n, m, d_c) - code is a code of length n containing m words and having minimum distance d_c. Thus for instance, in the polynomial ring $F_2^7[x]/\langle x^7-1\rangle$, $n=7, m=8, d_c=7$, hence it is a $(7,8,7)$ - code, while for the polynomial ring $F_2^{30}[x]/\langle x^{30}-1\rangle$, $n=30, m=31, d_c=30$, hence it is a $(30,31,30)$- code. A good code is one with small n for fast transmission of messages, large m to enable transmission of wide variety of messages and large d_c to detect and correct a large number of errors. Generally good codes are those whose value of m and d_c are large relative to values of n.

Define $A_q(n,1)$ as the maximum m such that (n,m,d_{max})-code exists. Determining the values of $A_q(n,1)$ is the main coding problem.

Theorem 2.1. *[4] For any set of codewords C of a q-ary of length n over a finite set A the following statements hold:*
(a)$A_q(n,1)=q^n$
(b)$A_q(n,n)=q$

Proof

(a) Suppose C is the set of all codewords of length n. Then $C=A^n$. Any two distinct codewords must differ in at least one position. The minimum distance between two such words is at least 1. A q-ary code of length n cannot be bigger than this.

(b) Suppose C is a q-ary code with parameters (n,m,n). The minimum distance between two such words is n if any two distinct codewords of C differ in all n positions. Therefore the entries in fixed positions of m codewords must be different. This implies that $A_q(n,n)\le q$
(i)

But the q-ary repetition code has parameters (n,q,n). This yields
$A_q(n,n)\ge q$ (ii)
Combining (i) and (ii) we have $A_q(n,n)=q$. □

2.5 Measurement of Efficiency and Reliability of codewords of the polynomial ring $F_2^n[x]/\langle x^n-1\rangle$

Definition 2.5. *[9]*

Efficiency of a code is a function of its information rate κ. The dimension of a code k is the number of symbols which carry information as opposed to redundancy. Normalized dimension or rate κ of an m-ary code C of length n is the ratio $\frac{k}{n}$ of message symbols to coded symbols. A code is said to be reliable when its minimum distance $d_c\ge 2$.

ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online) DOI: 10.7176/MTM
Vol.9, No.9, 2019

Table 1: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^6[x]/\langle x^6-1\rangle$

Code vector	δ	$\delta_C=\frac{\delta}{n}$	Reliability %	$\kappa_C=\frac{\kappa}{n}$	Efficiency %
000000	0	0	0	1.000	100
000001	1	0.1667	16.67	0.8333	83.33
000011	2	0.3333	33.33	0.6667	66.67
000101	2	0.3333	33.33	0.6667	66.67
001001	2	0.3333	33.33	0.6667	66.67
010101	3	0.5000	50.00	0.5000	50.00
011011	4	0.6667	66.67	0.3333	33.33
111111	6	1.00	100	0.00	0.00

Table 2: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^7[x]/\langle x^7-1\rangle$

Code vector	δ	$\delta_C=\frac{\delta}{n}$	Reliability %	$\kappa_C=\frac{\kappa}{n}$	Efficiency %
0000000	0	0	0.00	1.0000	100
0000001	1	0.1429	14.29	0.8571	85.71
0000011	2	0.2857	28.57	0.7142	71.42
0001011	3	0.4286	42.86	0.5714	57.14
0001101	3	0.4286	42.86	0.5714	57.14
0011101	4	0.5714	57.14	0.4286	42.86
0010111	4	0.5714	57.14	0.4286	42.86
1111111	7	1.0000	100	0.00	0.00

From Tables 1 and 2, its clear that as efficiency increases the code becomes more unreliable.

According to Shannon [7] we need to evaluate information content and error performance of any given codeword. High rate codewords are desirable since they employ a more efficient use of redundancy than lower rate codewords. Error correcting capabilities must also be considered when choosing a code for a particular application. A rate 1 code has the optimal rate but has no redundancy and hence not suitable for error control. Generally given a q-ary (n,m,d)-code C we define the rate of C to be $\frac{\log_q m}{n}$. We can then deduce that; $\lim_{n\to\infty}\frac{\log_q m}{n}=0$

This trend of efficiency and reliability is applicable to the polynomial ring $F_2^n[x]/\langle x^n-1\rangle$ for any values of $n\geq 2$ for all $n\in\mathbb{N}$.

ACKNOWLEDGEMENTS I acknowledge the invaluable academic support I have received from my supervisors: Prof. Shem Aywa, Prof. Maurice Owino Oduor and Dr. Okaka Akinyi Colleta. I thank the Government of Kenya through the National Commission for Science Technology and Innovation for funding this research.

References

[1] Cesar, F. C., Nestor R. B., and Araceli N. P. (2007), Maximum Likelihood Decoding on a Communication Channel, *Journal of Information Control*, Vol. 16, No. **18**, 55-57.

[2] Dubner, H. and Gallot, Y. (2002), Distribution of generalized Fermat prime numbers, *Math. Comp.* Vol.71, No.**238**, 825-832.

[3] Huffman, W. C. and Pless, V. (2003), *Fundamentals of Error-Control Coding*, Cambridge University Press, New York, USA.

[4] Macwilliams, F. J. and Sloane, N. J. A. (1981), *Theory of error correcting codes,* North Holland publishing company.

[5] Ronald, C., Ducas, L., Chris, P. and Oded, R. (2016), Recovering short generators of principal ideals in cyclotomic rings, a paper presented at the annual international conference on the theory and application of cryptographic techniques.

[6] Rotman, J. (2003), *Advanced Mordern Algebra,* (2nd ed.), Prentice Hall.

[7] Shannon, C. E. (1948), A mathematical theory of communication Bell Syst. *Tech. J.,* Vol. 27, 379-423, 623-656.

[8] Sidorenko, V., Chabaan, A., Senger, C. and Bossert, M. (2009), On extended Forney Kovalev generalised minimum distance decoding, *IEEE International symposium on information theory,* Seoul, Korea.

[9] Xing, C. and Ling, S. (2004), *Coding Theory: A first course*, New York, Cambridge University Press.