Ideals of the Polynomial Ring $F_2^n[x] \bmod (x^n - 1)$ for Error Control In Computer Applications

Fanuel olege[1], Shem Aywa[2] Rao R. D. K[3], Aldrin W. Wanambisi' [4]

1. Dept of Mathematics, Masinde Muliro University of Science and Technology, P.O Box 150-50100, Kakamega, Kenya.
2. Dept of Mathematics, Masinde Muliro University of Science and Technology, P.O Box 150-50100, Kakamega, Kenya.
3. Dept. of Mathematics, Maseno University, Private Bag, Maseno-Kenya.
4. School of Pure and Applied Science, Mount Kenya University, P.O box 342-00100, Thika, Kenya

* E-mail of the corresponding author: olegefanuel@yahoo.com

Keywords: Ideals, cyclic codes, polynomial ring $F_2^n[x] \bmod (x^n - 1)$, error detection/correction/Control

ABSTRACT

This research provides ideals of the polynomial ring $F_2^n[x] \bmod (x^n - 1)$associated with the code words of a cyclic code C. If the set of polynomials corresponding to codeword is given by *me(c)*, an ideal of $F_2^n[x]$ $\bmod (x^n - 1)$, it can be shown that C is a cyclic code**.** Principal ideals of cyclic codes are defined from a new view point involving polynomials. The potentialities of these codes for error control in computer applications are described in detail. Error coding and decoding use mathematical formulas to encode data at the source into longer words for transmission. Performance of different types of error control codes has been investigated for application in computerized systems. Algebraic geometry over principal ideals of cyclic codes and their applications to error control are also discussed. A code region for optimal codes obtained has been constructed as predicted by Shannon's Theorem.

1.1 INTRODUCTION

A nonempty subset *B* of a ring *A* is called an ideal of *A* if *B* is closed with respect to addition and negatives and *B* absorbs products in *A*. The various types of ideals include maximal ideals, prime ideals, radical ideals, primary ideals, principal ideals, primitive ideals and irreducible ideals. In this research a lot of attention has been given to principal ideals. These are ideals generated by a single element.

A left principal ideal of a ring A is a subset of A of the form *Ax*=$\{ax : a \in A\}$. A right principal ideal of a ring A is a subset of the form *xA* =$\{xa : a \in A\}$, A two-sided principal ideal is a subset of the form *AxA*= $\{x_1 as_1 + ... + x_n as_n : x_1 s_1 ... x_n s_n \in A\}$. In a commutative ring the three types of ideals are the same. In this research, ring A is the polynomial $F_2^n[x] \bmod (x^n - 1)$. Principal ideals of this ring can be used in error control (detection and correction) in computerized systems. One of the ways of identifying these ideals would be to develop a code region for cyclic codes of the ring polynomial $F_2^n[x] \bmod (x^n - 1)$**.**By use of algebraic and projective geometry and Shannon's Theorem it should be possible to develop and improve on ideals for optimal error control in computerized systems [7].

Right ideals are stable under right-multiplication *($IR\in I$)* and left ideals are stable under left-multiplication *($RI\in I$).* *I* is a proper ideal if it is a proper subset of *R*, that is, *I* does not equal *R*. The ideal *R* is called the unit ideal [1].

Suppose we have a subset of elements *Z* of a ring *R* and that we would like to obtain a ring with same structure as *R,* except that the elements of *Z* should be zero. But if $z_1= 0$ and $z_2 =0$ in the new ring, then z_1+z_2 should be zero too, and rz_1 as well as z_1r should be zero for *any* element *r.*

The definition of an ideal is such that the ideal *I* generated by *Z* is exactly the set of elements that are forced to become zero if *Z* becomes zero and the quotient ring *R/I* is the desired ring where *Z* is zero and only elements that are forced by *Z* to be zero. The requirement that *R* and *R/I* should have the same structure is formalized by the condition that the projection from *R* to *R/I* is a ring homomorphism [2].
Any intersection of left ideals of *R* is again a left ideal of *R* containing *X.* If *x* is any subset of *R*, the intersection of all left ideals of *R* containing *x* is a left ideal *I* of *R* said to be generated by *X. I* is the smallest left ideal of *R* containing *X.*

The left ideal of *R* generated by a subset *X* of *R* is the set of all finite sums of elements of *R* of the form *ra* where $r \in R$ and $a \in X$ .That is, the left ideal generated by *X* is the set of all elements of the form $r_1a_1+\ldots+r_na_n$ with each r_i in *R* and each a_i in *X* [7].

By convention, 0 is viewed as the sum of zero such terms, agreeing with the fact that the ideal of *R* generated by Ø is {0}.

If $a\in R$, then the left ideal of *R* generated by {a} is denoted by *Ra*. *Ra* is the set of elements of *R* of the form *ra* for $r\in R$. An analogous statement holds for *aR,* but not for *RaR.*

If an ideal *I* of *R* is such that there exists a finite subset *X* of *R* generating it, then the ideal *I* is said to be finitely generated.

In the ring **Z** of integers, every ideal can generated by a single number and the ideal determines the number up to its sign. The concepts of "ideal" and "number" are therefore almost identical in **Z.** In an arbitrary principal ideal domain this is also true, except that instead of differing only by sign, the various generators of a given ideal may differ multiplicatively by any invertible element of the ring. This research investigates the capabilities of such principal ideals for optimal error control in computer applications [2].
According to William, S.[9], in digital transmission systems, an error occurs when a bit is altered between transmission and reception, that is a binary 1 is transmitted and a binary 0 is received or a binary 0 is transmitted and a binary 1 is received. Two general types of errors can occur: single bit errors and burst errors. A single bit error is an isolated error condition that alters one bit but doesn't affect nearby bits. A burst error of length *n* is a

continuous sequence of *n* bits in which the first and the last bits and any number of intermediate bits are received in error.

Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Error correction is the additional ability to reconstruct the original, error free data. Error control is the ability to detect and correct errors using a given code [5]

PRELIMINARIES

Definition [2]

A nonempty subset *I* of a ring *A* is called an ideal written I $\lhd$ A if

(i) $(\forall x, y \in \mathrm{I}) x + y, \in \mathrm{I}$

(ii) $(\forall x, y \in \mathrm{I}) x - y \ \in \mathrm{I}$

(iii) $(\forall x \in \mathrm{I})(\forall y \in \mathrm{A}) xy \in \mathrm{I}$

I is an additive subgroup of A, so we can form the quotient group

A/I = $\{\mathrm{I} + a \mid a \in A\}$ the group of cosets of I with addition defined by, for $a, b \in A$

$(\mathrm{I} + a) + (\mathrm{I} + b) = \mathrm{I} + (a + b)$. Further *A/I* forms a ring by defining for *a, b,* ∈ *A,*

(I+a) (I+b) = I+ (ab). A/I is the quotient ring.

The mapping

$\phi : \mathrm{A} \to \mathrm{A}/\mathrm{I}, x \mapsto \mathrm{I} + x$ is a surjective ring homomorphism, called the natural map whose Kernel is

$Ker \quad \phi = \{x \in \mathrm{A} | \mathrm{I} + x = \mathrm{I}\} = I$.

Thus all ideals are Kernels of ring homomorphism. Conversely if $\mathrm{I} + a = \mathrm{I} + a'$ and $\mathrm{I} + b = \mathrm{I} + b'$ then $a - a', b - b' \in \mathrm{I}$ so

$$ab - a'b' = ab - ab' + ab' - a'b'$$

$$= a(b - b') + (a - a')b' \in \mathrm{I}$$

$$\Rightarrow \mathrm{I} + ab = \mathrm{I} + a'b'$$

Kernels of ring homomorphism with domain *A* are ideals of *A*.

A principal ideal *P* of *A* is an ideal generated by a single element that is for some $x \in A$

$P = \mathrm{A}x = x\mathrm{A} = \{ax \mid a \in \mathrm{A}\}$.

Polynomials are associated with the codeword of a cyclic code C [5]. Let $(a_1,...a_n)\in C$. Then the corresponding polynomial is $a_1 + a_2x + ...a_nx^{n-1}$. we denote the set of polynomials corresponding to codewords by $\mathrm{I}(C)$.

If $f(x)\in \mathrm{I}(C)$ represents a member of C, then $x^{\kappa} f(x)\in \mathrm{I}(C)$. But C is linear. Therefore if $f(x), g(x)\in \mathrm{I}(C)$ so is $f(x)+g(x)$ and hence $f(x)h(x)$ for any $h(x)\in F[x](\mathrm{mod}\, x^n - 1)$.

Theorem 1

Let C be a set of vectors in $F_2^n[x]\ \mathrm{mod}(x^n - 1)$. Then C is a cyclic code if and only if *I(C)* is an ideal of $F_2^n[x]\ \mathrm{mod}(x^n - 1)$.

Proof

Assume that *I(C)* is an ideal of $F_2^n[x]\ \mathrm{mod}(x^n - 1)$. We need to prove that *C* is a cyclic code. We start by proving that is C is a linear code. To do this we need to know that *C* is non-empty, is closed under addition and is closed under scalar multiplication. The first two facts follow from the fact that ideals are closed under addition and contain 0.

Scalars correspond to polynomials of degree 0 and these polynomials belong to our ring. If *S* is scalar, and $a_1 + a_2x + ...a_nx^{n-1}\in \mathrm{I}(C)$, then by definition, $Sa_1 + Sa_2x + ...Sa_nx^{n-1} \in \mathrm{I}(C)$ so that $(Sa_1Sa_2,..., Sa_n)\in C$. Therefore C is linear.

We also know that a cyclic shift of $(a_1, a_2,...a_n)$ corresponds in *I(C)* to multiplication by *x*. By definition *x* $(a_1 + a_2x + ...a_nx^{n-1})\in \mathrm{I}(C)$. Hence *C* is cyclic code.

Conversely, assume that *C* is a cyclic code. Then as *C* is a linear code it contains the zero vectors and is closed under addition. Hence *I(C)* is closed under addition and contains the zero polynomial.

Say *p(x)* is in *I(C)*. Let *h(x)* be a polynomial in $F_2^n[x]\ \mathrm{mod}(x^n - 1)$. We need to show that $h(x)p(x)\in \mathrm{I}(C)$ .Let $h(x) = h_1 + h_2x + ... + h_ix^{i-1} + ...h_nx,^{n-1}$ so that $h(x)p(x) = h_1p(x) + h_2xp(x) + ... + h_ix^{i-1}p(x) + ... + h_nx^{n-1}p(x)$.

Consider $h_ix_i\,p(x)$. As multiplication by x^{i-1} corresponds to a sequence of cyclic shifts and *C* is a cyclic code we see that $x^{i-1}p(x)\in \mathrm{I}(C)$.

As *C* is closed under scalar multiplication it follows that $h_i\left(x^{i-1}p(x)\right)\in \mathrm{I}(C)$. But *C* is closed under addition. Therefore $h(x)p(x)\in \mathrm{I}(C)$ **[5]**

Theorem 2

Every ideal of $F_2^n[x]\bmod(x^n-1)$ is principal.

Proof.

Let *I* be any ideal of $F_2^n[x]\bmod(x^n-1)$. If *I* contains nothing but the zero polynomial, *I* is the principal ideal generated by 0. If there are non-zero polynomials in *I*, Let *b(x)* be any polynomials of lowest degree in *I*. We will show that $\mathrm{I}=\langle b(x)\rangle$, which is to say that every element of *I* is a polynomial multiple $b(x)q(x)$ of $b(x)$.

Indeed if *a(x)* is any element of *I*, we may use division algorithm to write $a(x)=b(x)q(x)+r(x)$, where *r(x)* = 0 or deg *r(x)* < deg *b(x)*. Now, *r(x)* = *a(x)* – *b(x)q(x)* but *a(x)* was chosen in *I*, and $b(x)\in \mathrm{I}$. Hence $b(x)q(x)\in \mathrm{I}$. It follows that $r(x)\in \mathrm{I}$.

If $r(x)\neq 0$ its degree is less than the degree of *b(x)*. But this is impossible because *b(x)* is a polynomial of lowest degree in *I*. Therefore *r(x)* = 0. Finally a*(x)* = *b(x) q(x)*. So every member of *I* is multiple of *b(x)* as claimed **[2]**

Its now clear that *I* is generated by any one of its members of lowest degree. Such a polynomial is called the generator polynomial *g(x)*.

Theorem 3

If *g(x)* is the generator polynomial of the cyclic code *C* of length *n* then *g(x)* divides $x^n-1\in F_2^n[x]$ $\bmod(x^n-1)$.

Proof

If not, we can write $x^n-1=g(x)q(x)+r(x)$ where *r(x)* is a nonzero polynomial with lower degree than *g(x)*. Since $q(x)g(x)\in C$ and $r(x)=-q(x)g(x)$ in this ring, the linearity of *C* implies $r(x)\in C$ and thus contradicts the definitions of *g*(*x*) as the polynomial of minimum degree in *C*.

Now given any $g(x) \in \mathrm{I}(C)$, we can form the ideal $\langle g(x) \rangle$ and hence get a corresponding code by taking all the products of $g(x)$ with members of $F_2^n[x] \bmod (x^n - 1)$. Such a code must be generated by a factor of $x^n - 1$ **[4]**

Theorem 4

If C is a cyclic code of length n and with a generator polynomial $g(x)$ of degree k, then a polynomial $p(x)$ of degree $< n$ is a codeword if and only if $p(x)\ h(x) = 0$, where $h(x)$ is the polynomial of degree *n-k* satisfying $g(x)\ h(x) = x^n - 1$.

Proof

If $C(x)$ is a codeword then we know that $C(x) = f(x)\ g(x)$ for some polynomial $f(x)$. Hence since $g(x)\ h(x) = 0$, we have *c(x) h(x) =0.* Conversely, suppose that $p(x)$ is a nonzero polynomial satisfying $p(x)\ h(x) = 0$ .Then $p(x)$must have degree $\geq \kappa$. Thus if $p(x)$ is not a codeword, we know that it is not divisible by $g(x)$ and so $\exists$ a polynomial $r(x)$ of degree < degree $g(x)$, with $p(x) = q(x)g(x) + r(x)$.

Since $p(x)\ h(x) = 0$ and $q(x)g(x)\ h(x) = 0$ we must have $r(x)\ h(x) = 0$. But since the degree of $r(x) <$ degree $g(x)$ the condition $r(x)\ h(x) = 0$ is impossible unless $r(x) = 0$ **[4]**

The polynomial $h(x)$ is called the parity check polynomial of the code C.

By Theorem 4 there is a one to one correspondence between cyclic codes of length *n* and monic divisiors of the polynomial ring $F_2^n[x] \bmod (x^n - 1)$.

Richard Hamming in 1950 developed important codes called Hamming codes [6]. Certain forms of these codes can detect and correct some errors .We now discuss Hamming distance and Hamming weight in the context of cyclic binary Hamming codes suitable for computer architecture.\

Definition

The Hamming distance on the set $F_2^n[x] \bmod (x^n - 1)$ is $d_H(\underline{x}, \underline{y}) = \{i : 1 \leq i \leq n, x_i \neq y_i\}$ for $\underline{x} = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$.

Therefore $d_H(\underline{x},\underline{y})=0 \Leftrightarrow \underline{x}=\underline{y}$ and $d_H(\underline{x},\underline{y})=\ d_H(\underline{x},\underline{y})\ \ \forall \underline{x},\underline{y}\in\ F_2^n[x]\ \mathrm{mod}(x^n-1)$ and $d_H(\underline{x},\underline{z})\le d_H(\underline{x},\underline{y})+d_H(y,z)\forall x,y,\underline{z}\in\ F_2^n[x]\,\mathrm{mod}(x^n-1)$. From this definition, Hamming distance d_H is a metric on the codespace.

We define the minimum distance *d(C)* of a code $C\ \subset F_2^n[x]\mathrm{mod}(x^n-1)$ by $d_{(C)}=\min\{d(\underline{x},\underline{y}):\underline{x},\underline{y}\in C\underline{x}\ne y\}$.

The Hamming weight $W(\underline{x})$ of an element of $F_2^n[x]\,\mathrm{mod}(x^n-1)$ is its Hamming distance with 0; for $\underline{x}=(x_1,\ldots x_n)$

$w(\underline{x})=\{i:1\le i\le n, x_i\ne 0\}$. Hence for $\underline{x},\underline{y}\in\ F_2^n[x]\,\mathrm{mod}(x^n-1)\ d_H(\underline{x},\underline{y})=w(\underline{x}-\underline{y})$

For a linear code, $d_{(C)}$ is the minimal weight of a non-zero element in C.

Lemma 1

A code *C* of length *n* over $F_2^n[x]\,\mathrm{mod}(x^n-1)$ can detect *t* errors if and only if $d_{(C)}\ge t+1$. The code *C can correct t* errors if and only if $d_{(C)}\ge 2t+1$.

Proof

The condition $d_{(C)}\ge t+1$ means that a message at Hamming distance at most *t* from an element $\underline{c}$ of *C* and distinct from $\underline{c}$ does not belong to *C*. This is equivalent to saying that *C* can detect *t* errors.

For the second part of the Lemma, assume first that $d_{(C)}\ge 2t+1$. Let $\underline{x}\in F_2^n[x]\mathrm{mod}(x^n-1)$ and let $\mathbf{c}_1 and \mathbf{c}_2\in C$ satisfy $d(\mathbf{x}_1,\mathbf{c}_1)\le t$ and $d(\mathbf{x}_2,\mathbf{c}_2)\le t$ then by triangle inequality

$d(\mathbf{c}_1,\mathbf{c}_2)\le 2t<d(c)$. Therefore $c_1=c_2$.

Conversely assume $d_{(C)}\le 2t$: there is a none zero element $\underline{c}\in C$ with $w(\underline{c})\le 2t$, hence $\underline{c}$ has atmost *2t* non-zero components. Split the set of indices of the non-zero components of $\underline{C}$ into two disjoint subsets I_1 and I_2 having atmost *t* elements. Next we define $\underline{x}\in F_2^n[x]\mathrm{mod}(x^n-1)$ as the point having the same components

x_i as $\underline{c}$ for $i \in \mathrm{I}_1$ and 0 for $i \notin \mathrm{I}_1$. Then in the Hamming ball of centre $\underline{x}$ and radius *t* there are atleast two points *c*, namely 0 and $\underline{c}$. Hence is not

t –error correcting **[8]**

This means that the ability of a code to correct errors is related to its ability to detect errors. Hence a code which can correct errors can effectively be used for the purpose of controlling errors.

Theorem 5

A cyclic code generated by a polynomial of degree *n-k* detects any burst- error of length *n-k* or less.

Proof

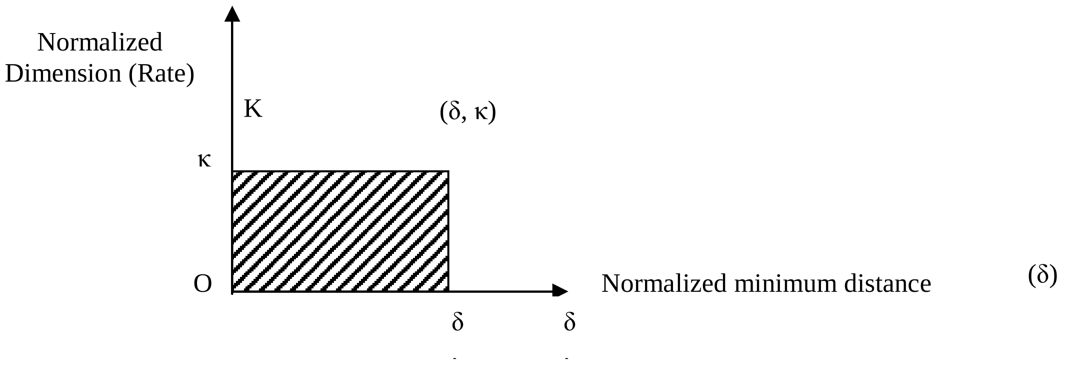
Any burst-error polynomial can be factored into the form $E(x) = x^i E_1(x)$ where $E_1(x)$ is of degree *b-1*, where *b* is the length of the burst. This burst can be detected if $p(x)$ does not evenly divide $E(x)$. Since $p(x)$ is assumed not to have *x* as a factor, it could divide *E(x)* only if it could divide $E_1(x)$. But if $b \leq n-k$, $p(x)$ is of higher degree than $E_1(x)$ and therefore, certainly could not divide $E_1(x)$ **[4]**

It is now clear that principal ideals of the polynomial ring $F_2^n[x] \bmod (x^n - 1)$ can detect the two general types of errors which may occur: Single bit errors and burst errors. We now need to look for optimal codes by use of Shannon's theorem and Geometrical construction [7].

If the point (δ, κ) is in the code region, then it seems reasonable that the code region should contain as well the points (δ', κ) , δ΄< δ, corresponding to codes with the same rate but smaller distance and also the points (δ, κ'), $\kappa' < \kappa$, corresponding to codes with the same distance but smaller rate. Thus for any point (δ, κ) of the code region, the rectangle with corners $(0,0), (\delta,0), (0,\kappa)$ and (δ, κ) should be entirely contained within the code region.

Any region with this property has its upper boundary function non increasing and continuous.

Graph 1 Code region



Conclusion

So far we have established that if $C \in F_2^n[x] \bmod (x^n - 1)$ then *C* is a cyclic code if and only if *I(C)* is an ideal of $F_2^n[x] \bmod (x^n - 1)$. Every ideal of $F_2^n[x] \bmod (x^n - 1)$ is principal.

Our search is for codes which are contained in the code region of graph 1. Before we make any generalizations we would analyse all the principal ideals in the polynomial ring $F_2^n[x] \bmod (x^n - 1)$ with $n \leq 20$. The objective is to characterize those ideals which satisfy Shannon's theorem, can be plotted in the code region and hence suitable for computer application. This is work in progress.

REFERENCE

[1] ATIYAH., M.F. (1966), Introduction to Commutative Algebra, Addison-Wesley

[2] CHARLES, C.P. (2000) *Abstract Algebra* 2nd Edition, McGraw Hill Publishing Company, New York, U.S.A

[3] ERNST, KUMAR. (1847), *Theory of Ideals*

[4] HALL, J. (2003) *Algebraic Coding Theory* Michigan State University, U.S.A.

[5] PRANGE, S. PETERSON, W. and KASAMI, T. (1960) *Cybernetics and Systems*, Cambridge University Press.

[6] RICHARD (1950) Hamming Codes

[7] SHANNON, C. (1948) *A Mathematical Theory of Communication*. Michigan State University. U.S.A

[8] SLEPIAN D. 1956. A class of binary signally alphabet Tech. J., Vol. 35 pp. 2003-234

[9] WILLIAM, S. (2007) *Data and computer Communication* eighth edition, Prentice Hall U.S.A.