International Mathematical Forum, Vol. 14, 2019, no. 4, 189 - 203
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/imf.2019.9732

On the Generators of Codes of Ideals of the Polynomial Ring $F_2^N[X]/\langle X^N - 1\rangle$ for Error Control

Olege Fanuel

Department of Mathematics
Masinde Muliro University of Science and Technology
P.O. Box 190-50100, Kakamega, Kenya

Abstract

Shannon introduced error detection and correction codes to address the growing need of efficiency and reliability of code vectors. One of the structures that can generate these codes is a set of ideals of the candidate polynomial ring. Generators of codes of ideals of polynomial rings have not been fully characterized. In this research the generators of codes of the candidate polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ have been investigated and characterized using lattices, simplex Hamming codes and isometries.

Mathematics Subject Classification: Primary 20K30; Secondary 16P10

Keywords: Polynomial Ring, Ideals, generators of codes, Error Control

1 Introduction

1.1 Background information

Definition 1.1. *[5] Let A be a finite set. A code is a non-empty subset of the set A^n of n-tuples of elements from A. Let C be a code constructed by elements of A. If C is a code of length n and size $|C|$, then C is an $(n, |C|)$ code.*

Members of the code space are words, those belonging to C being codewords. If A has m elements, then C is said to be an m-ary code. If $|A| = 2$*, then C is a binary code and the set* $A = \{0, 1\}$.

1.2 Types of Computer Errors

According to Williams [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 (random) errors and burst (compound) errors. A single bit error is an isolated error condition that alters one bit but does not affect nearby bits. A burst error of length b is a continuous sequence of b - bits in which the first and the last bits and any number of intermediate bits are received in error.

1.3 Error detection, correction and control

Definition 1.2. *[4] Error detection is the ability to identify presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.*

Error correction is the ability to reconstruct the original, error free data.

Error control is the ability to detect and correct errors using a given code.

The tools we have used to characterize our results include kissing numbers, lattices and isometries.

Definition 1.3. *Wheeler [8] Kissing number is the number of n− spheres which can be arranged so that they all touch another central sphere of the same size. It is given by:*
$T(\Lambda) = \mid \{x \in \Lambda : \|x\| = d_{min}(\Lambda)\} \mid$.

A kissing number determines the maximum number of nearest neighbors a given code is likely to have. In error control coding a higher kissing number means a code has very many useful neighbors and can be easily decoded using minimum distance decoding.

According to Wheeler [8] the hyper volume and hyper surface area of sphere packing reduces significantly as n increases. Thus for the candidate polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$, we have $lim._{n\to\infty}$hyper surface area $\to 0$ and $lim._{n\to\infty}$hyper volume $\to 0$. In such a case the kissing numbers become very large. Hence too much kissing goes on as n approaches infinity. Therefore as $n \to \infty$, we are bound to get better codes for the purpose of error control.

1.4 Ideals in a commutative ring

Definition 1.4. *[6]*

A non-empty subset I of a ring $F_2^n[x]/\langle x^n-1\rangle$ is an ideal of $F_2^n[x]/\langle x^n-1\rangle$ if and only if:

(i) $0 \in I$

(ii) $\forall a, b \in I$, $a \pm b \in I$

(iii) $\forall a \in I$ *and* $r \in F_2^n[x]/\langle x^n-1\rangle$, $ra \in I$.

The ring $F_2^n[x]/\langle x^n-1\rangle$ itself and the subset consisting of 0 alone, denoted by $\{0\}$, are ideals in this ring called *trivial* or *improper ideals*. An ideal $I \neq F_2^n[x]/\langle x^n-1\rangle$ is a *proper* ideal (see Olege, *etal* [2]).

Since $F_2^n[x]/\langle x^n-1\rangle$ is commutative then $ar = ra$. An ideal I has closure if $a \pm b \in I$, for all $a, b \in I$. An ideal I absorbs elements from $F_2^n[x]/\langle x^n-1\rangle$, if $ra, ar \in I$ for all $a \in I$ and for all $r \in F_2^n[x]/\langle x^n-1\rangle$.

The left principal ideal of a ring R is a subset of R of the form RI=$\{aI$: a∈$R\}$. The right principal ideal of a ring R is a subset of the form IR=$\{Ia$: a∈$R\}$. A two-sided principal ideal is a subset of the form $RIR = \{aIa : a \in R\}$. In a commutative ring, these three types of ideals coincide.

2 Results

Theorem 2.1. *Let $g(x) \in F_2^n[x]/\langle x^n-1\rangle$ be an irreducible and monic factor of x^n-1. The following statements are equivalent:*

(i) $g(x)$ is a generator polynomial of $F_2^n[x]/\langle x^n-1\rangle$.

(ii) $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n[x]/\langle x^n-1\rangle$.

Proof

(i) ⇒ (ii). Suppose $g(x)$ is a generator polynomial of $F_2^n[x]/\langle x^n-1\rangle$ and is a factor of x^n-1. Then $p(x)g(x) = x^n-1$ for some $p(x) \in F_2^n[x]/\langle x^n-1\rangle$. Hence $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n[x]/\langle x^n-1\rangle$.

(ii) ⇒ (i). Suppose that $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n[x]/\langle x^n-1\rangle$. Then any element of $I(C)$ would be given by $p(x)g(x)$ for some $p(x) \in F_2^n[x]/\langle x^n-1\rangle$. Hence there exists some $h(x) \in F_2^n[x]/\langle x^n-1\rangle$ such that any element of $I(C)$ is given by $p(x)h(x) = x^n-1$. Hence $g(x)$ is the generator polynomial of $F_2^n[x]/\langle x^n-1\rangle$. □

Proposition 2.1. *For a given polynomial code $P_c \in F_2^n[x]/\langle x^n-1\rangle$ the generator polynomial $g(x)$ is unique.*

Proof

Assume the polynomial code $P_c \in F_2^n[x]/\langle x^n-1\rangle$ has two generator polynomials $g(x)$ and $g(x)'$. Since $g(x)'$ is the other generator polynomial then

$g(x)$ is a multiple of $g(x)'$. This means $g(x)' = h(x)g(x)'$ is a multiple of $g(x)$, for some $h(x) \in F_2^n[x]/\langle x^n - 1\rangle$. We can also write $g(x)' = r(x)g(x)$ for some $r(x) \in F_2^n[x]/\langle x^n - 1\rangle$. Hence $h(x)r(x) = 1 \Rightarrow h(x) = r(x) = 1$ (since $r(x)$ and $h(x)$ are monic). Equivalently $g(x) = g(x)'$. □

Theorem 2.2. *Let a polynomial $\sigma(x) \in F_2^n[x]$ be irreducible. Then the polynomial ring $F_2^n[x]/\langle\sigma(x)\rangle$ is a field.*

Proof

Let $r(x)$ be a non-zero element of $F_2^n[x]/\langle\sigma(x)\rangle$. If $r(x)$ is co-prime to $\sigma(x)$ then we can find polynomials $\alpha(x)$ and $\beta(x)$ such that $r(x)\alpha(x)+\sigma(x)\beta(x) = 1$. But $r(x)\alpha(x) \equiv 1 \bmod \sigma(x)$ implies that $r(x)$ has a multiplicative inverse $\alpha(x)/\sigma(x)$. □

Proposition 2.2. *A polynomial code $P_c \in F_2^n[x]/\langle x^n - 1\rangle$ can control up to e errors if and only if $d_{max} \geq 2e + 1$.*

Proof

Suppose P_c cannot control up to e errors. Then there exists a pattern of at most e errors which changes the code vector u into a code vector v for all $u, v \in P_c$. Since we can change u into v using a maximum of e errors, we have $d_{max}(u, v) \leq e$. Suppose it was not possible to change v then we have a code vector $w \neq u$ with $d_{max}(w, v) \leq d_{max}(u, v)$ for some $w \in P_c$. Hence $d_{max}(w, v) \leq e$. By triangle inequality $d_{max}(u, v) + d_{max}(v, w) \leq e + e = 2e$ which contradicts $d_{max} \geq 2e + 1$. □

Proposition 2.3. *A polynomial ring $F_2^n[x]/\langle x^n-1\rangle$ generates an error control code for $n \geq 3$.*

Proof

Assume the contrary that the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ does not generate error control codes. Then $F_2^n[x]/\langle x^n - 1\rangle$ has a maximum Hamming distance $d_{max} < 3$ for all the codewords it generates. But the most optimal codeword generated by $F_2^n[x]/\langle x^n-1\rangle$ has $d_{max} = n \geq 3$. This contradicts the original assumption. Hence $F_2^n[x]/\langle x^n - 1\rangle$ generates an error control code. □

Suppose we want to show the maximum number of errors the code generated by $F_2^{11}[x]/\langle x^{11} - 1\rangle$ can control. Then;

$2e + 1 = d_{max}$ (where e is the maximum number of errors this code can control)

$\Rightarrow 2e + 1 = 11$

$\Rightarrow e = 5$

Table 1: Generator Polynomials of $F_2^{11}[x]/\langle x^{11} - 1\rangle$

Generator Polynomial	**Corresponding Codeword,** C
0	00000000000
1	00000000001
$x+1$	00000000011
$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4$ $+x^3+x^2+x+1$	11111111111

From Table 1 the codewords in C are ideals of the polynomial ring $F_2^{11}[x]/\langle x^{11}-1\rangle$. Here $m=4, n=11$ (which is a safe prime), $W_{max}=11$, $d_{max}=11, (n,m,d_{max})=(11,4,11)$.

By Proposition 2.2 this code can control up to five errors.

Definition 2.1. *[7]*

A lattice $\bigwedge$ *is a discrete additive subgroup of* $\mathbb{R}^n$*. That is* $\bigwedge \subseteq \mathbb{R}$ *satisfying the following properties:*

(i) $\bigwedge$ *is closed under addition and subtraction.*

(ii) There exists an $\epsilon > 0$ *such that any two distinct lattice points* $x \neq y$ *are at a distance at least* $\mid x-y \mid \geq \epsilon$*.*

In order to study their lattice properties we shall treat polynomial codes as spheres. Let a packing $P \subset \mathbb{R}^n$ contain spheres centered at u and v. Suppose this is true, then there is also a sphere centered at either $u+v$ or $u-v$.

Claim 2.1. *We claim that the minimum Hamming distance* d_c *induces a metric in the code space.*

Proposition 2.4. *Suppose* $1 \leq c < \infty$ *and* d_c *is the minimum Hamming distance of polynomial codes* $u, v \in F_2^n[x]/\langle x^n-1\rangle$ *given by* $d_c(u,v) = (\sum_{i=1}^n \mid u_i - v_i \mid^c)^{\frac{1}{c}}$ *for* $u=(u_1,u_2,...,u_n)$ *and* $v=(v_1,v_2,...,v_n)$*. Then, the induced metric in the code space is given by* $d_c(u,v) = (\sum_{i=1}^n d(u_i,v_i)^c)^{\frac{1}{c}}$*.*

Proof

Suppose $u=(u_1,u_2,...,u_n)$ and $v=(v_1,v_2,...,v_n)$ for all $u,v \in F_2^n[x]/\langle x^n-1\rangle$. The metric induced by d_c is given by $d_c(u,v)$= inf.$d(u',v')$; where $u' = u+qe, v' = v+qz$ for all $e,z \in F_2^n[x]/\langle x^n-1\rangle$ =(inf $\{\sum_{i=1}^n \mid u_i-v_i-q(z_i-e_i) \mid^c$ $, e,z \in F_2^n[x]/\langle x^n-1\rangle\})^{\frac{1}{c}} = (\sum_{i=1}^n \mid u_i-v_i-q(\frac{u_i-v_i}{q}) \mid^c)^{\frac{1}{c}}$.....(i)

Equation (i) is minimum when $= (\sum_{i=1}^n \mid u_i-v_i-qA_i \mid^c)^{\frac{1}{c}}$, for $A_i = \mid \frac{u_i-v_i}{q} \mid$.

Suppose $\alpha_i = (\frac{u_i - v_i}{q})$ for $i = 1, 2, 3, ..., n$. Since $0 \leq \mid u_i - v_i \mid \leq q$, it follows that $-1 \leq \frac{u_i - v_i}{q}$ and $\alpha_i \in \{-1, 0, 1\}$. If $\alpha^i = 0$ for some i then $\frac{-q}{2} \leq u_i - v_i \leq \frac{q}{2}$. In such a case $\min \{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = \mid u_i - v_i \mid$.

If $\alpha_i = 1$ for some i then $\frac{-q}{2} \leq u_i - v_i \leq q$ and $\min \{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = q- \mid u_i - v_i \mid$ and $\mid u_i - v_i \mid = u_i - v_i$. If $\alpha_i = -1$ for some i then $-q \leq u_i - v_i \leq \frac{-q}{2}$ and $\min \{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = q- \mid u_i - v_i \mid$ and $\mid u_i - v_i \mid = u_i - v_i$ and hence
$d_c(u, v) = (\sum_{i=1}^{n} d(u_i, v_i)^c)^{\frac{1}{c}}$. □

Proposition 2.5. *Suppose $\bigwedge_C$ is a $q-$ array lattice and $v = (v_1, v_2, ..., v_n)^e \in \mathbb{R}^n$ is the received vector. Let $v \in \mathbb{R}^n$, $C \in F_2^n[x]/\langle x^n - 1\rangle$ and $c \in C, c = (c_1, c_2, ..., c_n)^e$, $0 \leq c_i < q$, a neighbor codeword to u. Considering the induced metric $d_c \in F_2^n[x]/\langle x^n - 1\rangle$ another neighbor $z \in \bigwedge_C$ is given by $(z_1, z_2, ..., z_n)^e$ where $z_i = c_i + qA_i$ for $A_i = \mid \frac{v_i - u_i}{q} \mid$ for $i = 1, 2, 3, ..., n$.*

Proof

We should show that if $u \in C$ and $z = u + qA$, for $A_i = \mid \frac{v_i - u_i}{q} \mid$, then $d(v, z) = d_c(v, z)$. We know that $c \in C$ satisfies $d_c(v, c) = \min\{d_c(v, u), u \in C\}$. For $A_i = \mid \frac{v_i - u_i}{q} \mid$ it follows that $d(v, c + qA_i) = d_c(v, c) \leq \min\{d(v, u + qe), u \in C, e \in F_2^n[x]/\langle x^n - 1\rangle$. Hence $c + qA_i$ is the neighbor of $\bigwedge_C$ that minimizes the distance $d_c(v, u)$. □

Our next problem is the characterization of perfect codes generated by the candidate ring.

We already know that perfect codes satisfy the sphere packing bound with equality, (see Hall [5]).

Proposition 2.6. *Given the range $1 \leq n < \infty$ perfect codes exist in the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ induced by the metric d_c for $\kappa_c = 1$ and any $\ell = 2n + 1$.*

Proof

If $n = 1$ the result is clear. Suppose $1 < n < \infty$. The inequality $\mid u_1 \mid^n + \cdots + \mid u_n \mid^n \leq 1$ has $2n + 1$ integer solutions namely $u_i = \pm 1$ and $u_j = 0$ for all $j \neq i$ and $u_i = 0$ for all i. Define $\aleph_n(n, 1)$ to be the number of points in $F_2^n[x]/\langle x^n - 1\rangle$ inside a sphere centered at the origin. Then $\aleph_n(n, 1) = 2n + 1 = \aleph_1(n, 1)$. But there exists at least one perfect code $C \subseteq F_2^n[x]/\langle x^n - 1\rangle$ in the metric d_c satisfying the proposition. It follows that this code must also be perfect in the metric d_c for any $1 < n < \infty$, because $\mid C \mid \aleph_n(n, 1) = \mid C \mid \aleph_1(n, 1) = 2^n$. □

The perfect codes characterized by Proposition 2.6 are trivial. The next problem is to characterize non- trivial perfect codes of the candidate polynomial ring.

Proposition 2.7. *For an odd integer $\alpha > 1 \in F_2^n[x]/\langle x^n - 1\rangle$ and any integer $\beta > 1 \in F_2^n[x]/\langle x^n - 1\rangle$, there exists a non-trivial perfect code $C \subseteq F_2^n[x]/\langle x^n - 1\rangle$ in the metric $d_\infty(u, v)$ if and only if $q = \alpha\beta$.*

Proof

By the sphere packing bound [1] we know that a code $C \subseteq F_2^n[x]/\langle x^n - 1\rangle$ with minimum distance $2\kappa + 1$ is perfect if and only if:

$\mid C \mid (2\kappa + 1)^n = q^n$. This implies that $\mid C \mid = \frac{q^n}{(2\kappa+1)^n}$. This means q must have an odd factor and so $q \neq 2^n$. If q is prime then $2\kappa + 1 = q$ which gives a perfect trivial code. Thus there is no perfect code for prime q or composite q, a power of 2.

Suppose $q = \alpha\beta$. Let the code C be generated by the vectors $\{(\alpha, 0..., 0), (0, \alpha, 0, 0, ..., 0), ..., (0, ..., 0, \alpha)\} \in C \subseteq F_2^n[x]/\langle x^n - 1\rangle$. Therefore $\mid C \mid = \beta^n$. Suppose $e \in F_2^n[x]/\langle x^n - 1\rangle$. If $e = \beta n + v$, for $0 \leq v < \beta$ then $e(0, ..., \alpha, 0, ..., 0) = v(0, ..., \alpha, ...0)$. In this case the minimum distance d_c=min$\{d_\infty(u, v), u, v \in C, u \neq v\} = \alpha$. This implies that $\kappa_c = \frac{\alpha-1}{2}$. Since $\aleph_\infty(n, \kappa_c) = (2\kappa + 1)^n = \alpha^n$, it follows that $\mid C \mid \aleph_\infty(n, \kappa_c) = \alpha^n\beta^n = q^n$ for $1 <\mid C \mid < q^n$. This code is perfect and non-trivial. □

Remark 2.1. *There are no perfect codes of length $n \in \mathbb{N}$ and $\kappa_c > 1$.*

Let W_{11} denote a polynomial code generated by $b(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Its generator matrix is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

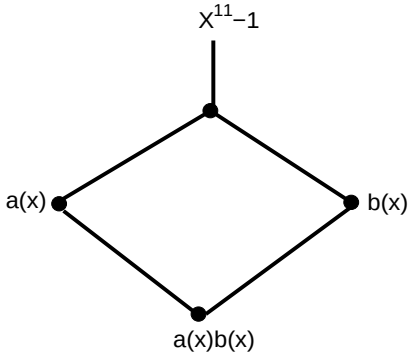
and hence (11, 1) is a repetition code.

The cyclic code C_{11} with generator polynomial $a(x) = x + 1$ is $(11, 10)$ code. From the generator polynomial we obtain a generator matrix which can be transformed into a systematic generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Hence C_{11} is isometric to a parity check code. It consists of all even weight vectors in $\mathbb{F}_2^{11}$.

Figure 1: Lattice diagram of the generators of $x^{11}-1$



Definition 2.2. *[7] A geometric lattice is a regular arrangement of points in an n-dimensional Euclidean space. A polyhedron is a solid in three dimensions whose surface is made up of a number of polygonal surfaces.*

Geometrically Figure 1 is a lattice diagram with 4 lattice points. In this research each lattice point is a codeword. The shape of this geometric lattice is a rhombus.

Let W_{15} denote a cyclic code which is generated by $d_1(x)d_2(x)d_3(x)d_4(x) = (x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) = x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$. Its generator matrix is $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ and hence W_{15} is a (15, 1) repetition code. The cyclic code S_4 with generator polynomial $a(x)d_1(x)d_2(x)d_4(x) = x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^3+1$ is a (15, 4) code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

which is the check matrix of the fourth order binary Hamming-code and so S_4 is a binary simplex code. The cyclic code S_4' with generator polynomial $a(x)d_1(x)d_3(x)d_4(x) = x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$ is also (15, 4) code which is isometric to S_4. The cyclic code C_{15} with generator polynomial $a(x) = x+1$ is (15, 14) code. From its generator polynomial we obtain a generator matrix that can be transformed using elementary row transformations into the systematic generator matrix

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{bmatrix}$$

Hence C_{15} is isometric to a parity check code. It consists of all even weight vectors in $\mathbb{F}_2^{15}$.

The cyclic code H_8 generated by $d_3(x)d_4(x) = x^8 + x^5 + x^3 + 1$ is (15, 7) code with generator matrix

$$\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}$$

Now $H_8^{\perp}$ has the generator polynomial $a(x)d_1(x)d_2(x) = x^7 + x^3 + x + 1$ so that $H_8^{\perp}$ is the simplex code S_8, hence H_8 is a Hamming code.

Generator matrix for $a(x)$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

Generator matrix for $d_1(x)$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $d_2(x)$

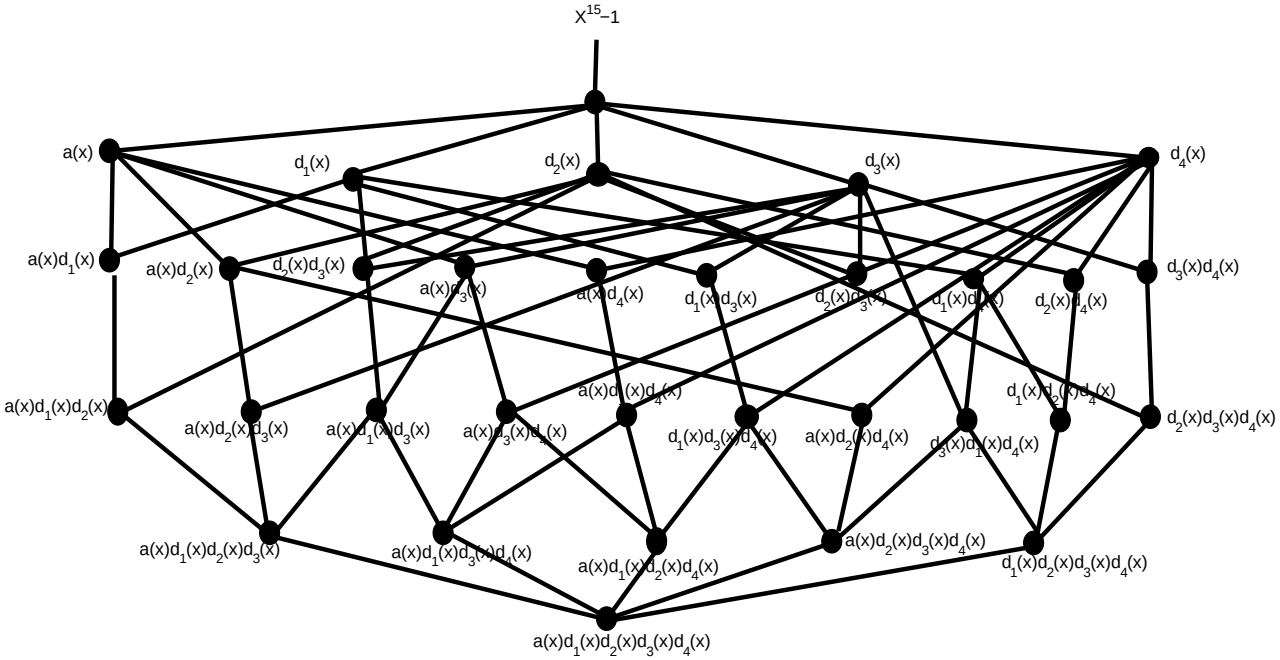
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $d_3(x)$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $d_4(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$


$X^{15}-1$
a(x)
$d_1(x)$
$d_2(x)$
$d_3(x)$
$d_4(x)$
$a(x)d_1(x)$
$a(x)d_2(x)$
$d_2(x)d_3(x)$
$a(x)d_3(x)$
$a(x)d_4(x)$
$d_1(x)d_3(x)$
$d_2(x)d_3(x)$
$d_1(x)d_4(x)$
$d_2(x)d_4(x)$
$d_3(x)d_4(x)$
$a(x)d_1(x)d_2(x)$
$a(x)d_2(x)d_3(x)$
$a(x)d_1(x)d_3(x)$
$a(x)d_3(x)d_4(x)$
$a(x)d_1(x)d_4(x)$
$d_1(x)d_3(x)d_4(x)$
$a(x)d_2(x)d_4(x)$
$d_3(x)d_1(x)d_4(x)$
$d_1(x)d_2(x)d_4(x)$
$d_2(x)d_3(x)d_4(x)$
$a(x)d_1(x)d_2(x)d_3(x)$
$a(x)d_1(x)d_3(x)d_4(x)$
$a(x)d_1(x)d_2(x)d_4(x)$
$a(x)d_2(x)d_3(x)d_4(x)$
$d_1(x)d_2(x)d_3(x)d_4(x)$
$a(x)d_1(x)d_2(x)d_3(x)d_4(x)$

Geometrically this is a closed lattice diagram with 57 lattice points. It is a polyhedron with 57 vertices.

Theorem 2.3. *Let W_n denote a code with generator polynomial $g(x) = g_0(x) + g_1(x) + g_2(x^2) + ... + g_{n-k}(x^{n-k})$, the generator matrix is given by*

$$G = \begin{bmatrix} g_0 & g_1 & . & . & . & g_{n-k} & 0 & 0...0 \\ 0 & g_0 & g_1 & . & . & . & g_{n-k} & 0...0 \\ 0 & . & . & . & . & & . & . \\ . & & . & . & . & . & . & . \\ . & & & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & . & g_{n-k} \end{bmatrix}$$

Proof

We should show that:

(i) $g_0(x) + g_1(x) + g_2(x^2) + ... + g_{n-k}(x^{n-k})$ forms a basis of W_n.

(ii)$dim.(W_n) = k$.

For part (i) the vectors $g_0(x), g_1(x), g_2(x^2), ..., g_{n-k}(x^{n-k})$ are linearly independent. If not we must have a set of coefficients $\{\alpha_i\}$ such that $\alpha_o g_0(x) + \alpha_1 g_1(x) + \alpha_2 g_2(x^2) + ... + \alpha_k g_{n-k}(x^{n-k}) = 0$. But this product has degree $k - 1 + n - k = n - 1 < n$, which cannot be $= 0 \bmod(x^n - 1)$ unless all the $\alpha_i = 0$. Suppose we have $w(x)$ in W_n, then $w(x) = \alpha(x)g(x)$. Assume $\alpha(x)$ has degree $< k - 1$. Then $w(x)$ can be written as a linear combination of $x^i g(x)$ for $0 < i < k - 1$. The set of all the linear combinations $\{x^i g(x)\}$ is a basis for W_n.

For part (ii) suppose we have two polynomials $p_1(x) \neq p_2(x)$ with degree $p_i(x) \leq k-1$ (for $i = 1, 2$) and $g(x)p_1(x) \neq g(x)p_2(x)$. The set $\tau = \{g(x)p(x) : p(x) \in F_q^n[x]/\langle x^n - 1\rangle,$ degree $p(x) \leq k - 1\}$ has q^k elements and is a subset of the ideal $\langle g(x)\rangle$.

Conversely for any codeword $g(x)r(x)$ (for some $r(x) \in F_q^n[x]/\langle x^n - 1\rangle$), we have $g(x)r(x) = y(x)(x^n - 1) + z(x)$ (for some $z(x) \in F_q^n[x]/\langle x^n - 1\rangle$). This means
$z(x) = g(x)r(x) - y(x)(x^n - 1)$. Therefore $g(x)$ divides $z(x)$. Let $z(x) = g(x)t(x)$ for some polynomial $t(x) \in F_q^n[x]/\langle x^n - 1\rangle$. This implies that degree $t(x) < k$ and hence $z(x) \in \tau$. Equivalently, $\tau = \langle g(x)\rangle$. Hence the dimension of the code is given by $\log_q|\tau| = k$.

Proposition 2.8. *Let $S_k(q)$ be a simplex code. Then $S_k(q)$ is a constant weight code with parameters $[(q^k - 1)/q - 1, k, q^{k-1}]$.*

Proof

Let $H_k^{\perp}(q)$ be a Hamming code. We know that the simplex code $S_k(q)$ and the Hamming code $H_k^{\perp}(q)$ are dual codes. $H_k(q)$ is a parity check matrix of $H_k^{\perp}(q)$ and the generator matrix of $S_k(q)$.

Consider a parity check matrix $H_k(q)$ with redundancy k. The rank of this matrix = dimension =k. Let u be a non zero codeword of the simplex code $S_k(q)$. We have $u - mH_k(q)$ for some non-zero $m \in F_q^n[x]/\langle x^n - 1\rangle$. Let $h_i^{\perp}(q)$ be the i^{th} column of $H_k(q)$ (for $i = 1, 2, 3, ...$). Then $\Sigma u_i = 0$ if and only if $mh_i = 0$. Let $mv = 0$ for some $v \in F_q^n[x]/\langle x^n - 1\rangle$ be a non-trivial homogeneous linear equation. This equation has q^{k-1} solutions. The solutions $(q^{k-1})/q - 1$ such that v^T is a column of $H_k(q)$ is a non-zero multiple of v^T. Hence the number of zeros of u is $(q^{k-1} - 1)/q - 1$. Therefore the weight of u is the number of non-zeros which is q^{k-1}. □

Proposition 2.9. *For a polynomial code $P_c \in F_2^n[x]/\langle x^n - 1\rangle$ the the following statements are equivalent*

(i) Hamming weight of P_c is isomorphic to the homogeneous weight.

(ii) Homogeneous weight of P_c is isomorphic to the Hamming weight .

Proof

(i)⇒ (ii) Let $f^n(u) = f(x_1) + ... + f(x_n)$ for all $f^n(u) \in I$ where I is an ideal in $F_2^n[x]/\langle x^n - 1\rangle$. Then;

$$\begin{aligned}
(\Sigma f^n)u &= \frac{1}{R_n u}\Sigma_{v\in R_n} f^n v \text{ for all } f^n(v) \in R_n \text{ and } R_n = F_2^n[x]\langle x^n - 1\rangle \\
&= \frac{1}{R_n u}\Sigma_{v\in R_n}\Sigma_{i=1}^n f^n(v_i) \\
&= \Sigma_{i=1}^n \frac{1}{R_n u_i}\Sigma_{v\in R_n} f^n(u_i) \\
&= \Sigma_{i=1}^n (\Sigma f)(u_i) \\
&= (\Sigma f)^n(u)
\end{aligned}$$

(ii)⇒ (i) Let $f^n(v) = f(x_1) + ... + f(x_n)$ for all $f^n(v) \in I$ where I is an ideal in $F_2^n[x]/\langle x^n - 1\rangle$. Then;

$$\begin{aligned}
(\Sigma f^n)v &= \frac{1}{R_n v}\Sigma_{v\in R_n} f^n u \text{ for all } f^n(u) \in R_n \text{ and } R_n = F_2^n[x]/\langle x^n - 1\rangle \\
&= \frac{1}{R_n v}\Sigma_{u\in R_n}\Sigma_{i=1}^n f^n(u_i) \\
&= \Sigma_{i=1}^n \frac{1}{R_n v_i}\Sigma_{u\in R_n} f^n(v_i) \\
&= \Sigma_{i=1}^n (\Sigma f)(v_i) \\
&= (\Sigma f)^n(v)
\end{aligned}$$

□

Proposition 2.10. *Let W_n be a cyclic code with a check polynomial $h(x) = h_0 + h_1(x) + ... + h_k x^k$. Then W_n has dimension k with the parity check matrix*

given by:

$$H = \begin{bmatrix} h_k & h_{k-1} & . & . & .h_0 & .0 & 0 & . & . & . & 0 \\ 0 & h_k & h_{k-1} & . & . & h_0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & .h_0 & . & . & & . \\ . & & . & . & . & . & . & h_0 & . & . & . \\ . & & & . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 0 & h_k & h_{k-1} & . & . & .h_0 \end{bmatrix}$$

Proof

Let the degree of the generator matrix $= n-k$. The dimension of this code is k. Let $u = c_0 + c_1(x) + c_2(x^2) + ... + c_n(x^{n-1})$ for some $u \in F_q^n[x]/\langle x^n - 1\rangle$. Then $u(x)h(x) = 0$. For $d = k, k+1, ..., n-1$ we have $\Sigma c_i h_j = 0$ (for $i+j = d$). These code-vectors are orthogonal to the linear combinations of the rows of H. Hence $C^{\perp}$ contains the span of the rows of H. Since $hk = 1$, the rank of $h = n - k$. This generates a linear subspace of $C^{\perp}$, implying that H is the parity check matrix for the check polynomial $h(x)$. □

2.1 Syndromes of the simplex codes in the candidate ring

Definition 2.3. *[1] Let C be an (n, κ, d) code over $F_2^n[x]/\langle x^n - 1\rangle$ and let H be a parity check matrix for C. For any $w \in F_2^n[x]/\langle x^n - 1\rangle$ the syndrome of w is the codeword $S(w) = wH^T \in F_2^{n-k}[x]/\langle x^n - 1\rangle$.*

Proposition 2.11. *[1] Let $u, v \in C$, where C is a codeword generated by $F_2^n[x]/\langle x^n - 1\rangle$. The following statements are equivalent.*

(i) u and v are in the same coset.

(ii) u and v have the same syndrome

Proof

(i)$\Longrightarrow$(ii). Suppose u and v belong to the same coset. Then $u = z_1 + e$ and $v = z_2 + e$ for $z_1, z_2 \in C$ and $e \in F_2^n[x]/\langle x^n - 1\rangle$. The syndrome corresponding to u is given by $Hu^T = H(z_1 + e)^T = He^T$.

The syndrome corresponding to v is given by $Hv^T = H(z_2 + e)^T = He^T$. Hence the syndrome of u and v are the same.

(ii)$\Longrightarrow$(i). Suppose u and v have the same syndrome. Then $Hu^T = Hv^T = H(u-v)^T = 0 \Longrightarrow (u-v) \in C$. Since $u-v$ is a codeword then u and v must belong to the same coset. □

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] C. Xing and S. Ling, *Coding Theory: A first course*, New York, Cambridge University Press, 2004. https://doi.org/10.1017/cbo9780511755279

[2] F. Olege, M. O. Oduor, S. Aywa and A.C. Okaka, Characterization of codes of ideals the polynomial ring $F_2^{30}[x]$ mod $(x^{30}-1)$ for error control in computer applications, *Journal of Advances in Mathematics*, **12** (2016), 6238-6247.

[3] F. Olege,M. O. Oduor, S. Aywa,and A. C. Okaka (2016), Perfect repetition codes of ideals the polynomial ring $F_2^n[x]$ mod (x^n-1) for error control in computer applications, *Journal of Mathematics and Statistical Sciences*, **10** (2016), 579-605.

[4] F.Olege, S. Aywa,G. K. R. Rao and A. W. Wanambisi , Ideals of the polynomial ring $F_2^n[x]$ mod (x^n-1) for error control in computer applications, *Journal of Mathematical Theory and Modelling*, **3** (2013), 55-63.

[5] J. Hall, *Algebraic Coding Theory*, Michigan State University USA, 2003.

[6] J. Rotman, *Advanced Mordern Algebra*, (2nd ed.), Prentice Hall, 2003. https://doi.org/10.1090/gsm/180

[7] M. Daniele and U. Feige, The inapproximability of lattice and coding problems with preprocessing, *Journal of Computer and System Sciences*, **69** (2004), 45-69. https://doi.org/10.1016/j.jcss.2004.01.002

[8] N. Wheeler, Upper bound on the number $N-$ spheres that can simultaneously kiss a central sphere, *Journal of Science News*, **166** (2004).

[9] S. Williams, *Data and Computer Communication*, (8th ed.), Prentice Hall USA, 2007.

Received: August 14, 2019; Published: September 3, 2019