"Science Stays True Here"
Journal of Mathematics and Statistical Science, Volume 2016, 579-605 | Science Signpost Publishing

Perfect Repetition Codes of Ideals of the Polynomial Ring $F_2^n[x] mod(x^n - 1)$ for Error Control In Computer Applicatons

Olege Fanuel, Okaka Akinyi Colleta

Department of Mathematics, Masinde Muliro University of Science and Technology,

P.O Box 190-50100, Kakamega (Kenya).

Owino Maurice Oduor

Department of Mathematics and Computer Science, University of Kabianga,

P.O Box 2030-20200, Kericho (Kenya).

Aywa Shem

Department of Mathematics, Kibabii University,

P.O Box 1699-50200, Bungoma (Kenya).

Abstract

The study of perfect codes has attracted a lot of interest among researchers in coding theory in view of the fact that many authors have indicated that this type of codes is rare. These codes are considered the best for theoretical and practical reasons. In this paper we demonstrate the determination of perfect codes from ideals of polynomial rings and characterize them for error control in computer applications. GAP software has been used to generate these codes and to confirm that they are indeed perfect. The Mathematical Structure of the generating polynomial ring has been fully discussed and the corresponding perfect codes have been characterized.

Keywords: Polynomial Ring, Ideals, Perfect codes, Error Control.

Corresponding author: Owino Maurice Oduor, Department of Mathematics and Computer Science, University of Kabianga, P.O Box 2030-20200, Kericho (Kenya). E-mail: morricearaka@yahoo.com.

1. Introduction

1.1. Background Information

Error control coding started in the late 1940s, by Shannon [1], Hamming [2] and Golay [3]. Shannon introduced the basic theory on bounds for communication. He showed that it is possible to get arbitrarily low error probability using coding on any channel, provided that the bit-rate is below a channel-specific parameter called the capacity of the channel. He did not, however, show how that could be accomplished. His paper gave rise to at least two research fields, namely Information Theory which mainly deals with bounds on performance, and Coding Theory which deals with methods to achieve good communication using codes. Hamming published his construction of a class of single-error-correcting binary codes in 1950. Golay published a generalization of the construction to any alphabet of prime size. Both Hamming's original binary codes and Golay's generalizations are called Hamming codes.

The discoveries made by Hamming and Golay initiated research activities among mathematicians who were interested in investigating the algebraic and combinatorial aspects of codes. Coding Theory consists of two parts; code construction and development of decoding methods.

The history of error control coding can be broadly divided into two; pre-turbo code and post-turbo code. Turbo codes and their respective decoders were invented by Claude and Alain [4]. Prior to this invention, no one really knew how to get close to the theoretical performance limits promised by Shannon. Algebraic codes such as Reed-Solomon [5] and BCH codes [6] build algebraic structure into the code such that the code can be decoded using computationally efficient algorithms for solving systems of equations. All error control codes are based on one basic principle: that is redundancy is added to information in order to detect and correct any errors. MacKay and Neal [7] were able to show that Low Density Parity Codes can get as close to Shannon limit as turbo codes. Richardson *et al*. [8] showed that irregular LDPC codes can outperform turbo codes of approximately the same length and rate when the block length is large.

Today the theory of error control codes is well developed. A number of efficient codes have been constructed. Although most of the applications of our work are classical as obseved by Huffman and Pless [9], some of the real life applications of error control codes include and not limited to modern communication, such as digital radio and television, cellphone communication, computer networks, mobile money transfer (M-Pesa), M-Banking and deep space communication. According to Hall [10] most newer constructions are not readily adapted to instruments like discs, computer memories and others. A lot

of research in computer software and hardware is ongoing in order to make use of newer results. That is why computer size is reducing with time while its data processing capacity is increasing.

Huffman and Pless [9] studied cyclic codes and polynomials in indeterminate x over a field F. They realised that every cyclic code consists of polynomials as well as code words. Hall [10] showed that every codeword $a=(a_0, a_1, ..., a_i, a_{n-1}) \in F^n$. Since $c \in C$, $c=(c_0, c_1, ..., c_{n-2}, c_{n-1}) \in C$ and c=($c_{n-1}, c_0, c_1, ..., c_{n-3}, c_{n-2}$) $\in$ C, where c is a shifted codeword. Hence $c(x) = x\,c(x) - c_{n-1}$ $(x^n-1) \Rightarrow c(x)$ has degree $< n$ and is equal to remainder when $xc(x)$ is divided by (x^n-1). That is $c(x) = xc(x) \bmod (x^n-1) \Rightarrow c(x)$ and $xc(x)$ are equal in the ring of polynomials $F[x]$mod (x^n-1) where arithmetic is done modulo the polynomial x^n-1. Prange [11] showed that for each polynomial $f(x) \in F[x]$, $f(x) \in C \bmod (x^n-1)$. By linearity $\forall\, a_i \in F$, $a_i x^i\, c(x) \in C \bmod (x^n-1)$), and $\Sigma\, a_i\, x^i\, c(x) \in C \bmod (x^n-1) \in F[x] mod\ (x^n-1)$ According to Prange [11] these results point to the fact that the polynomial rendering of a cyclic code is an ideal of the polynomial ring $F[x] Mod(x^n-12)$. Peterson and Weldon [12] examined the concept of codes within a binary field and realised that for a code to be used for computer applications it must be binary or easily convertible into the binary alphabet.

2. The Results

Proposition 2.1 [13]

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

Proof

The condition $d_{(c)} \geq t+1$ 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. That is C can detect t errors. For the second part of the Proposition, assume first that $d_{(c)} \geq 2t+1$. Let $x \in F_2^n[x] \bmod (x^n-1)$ and let $c_1, c_2 \in C$

satisfy $d(x_1,c_1)\le t$ and $d(x_2,c_2)\le t$ then by triangle inequality $d(c_1,c_2)\le q2t\le d_{(c)}$. Therefore $c_1=c_2$.

Conversely assume $d_{(c)}\le 2t$: there is a no zero element $\underline{c}\in C$ with $w(\underline{c})\le 2t$, hence $\underline{c}$ has at most $2t$ non-zero components. Split the set of indices of the the non-zero components of $\underline{c}$ into two disjoint subsets I_1 and I_2 having at most t elements. Define $x\in F_2^n[x]\bmod(x^n-1)$ as the point having the same components x_i as $\underline{c}$ for $i\in I_1$ and 0 for $i\notin I_1$. Then x is in the Hamming ball of centre $\underline{c}$ and radius t.

2.1. Selection of Candidate Polynomial

This paper identifies the polynomial ring $F_2^n[x] mod(x^n-1)$ as one capable of providing polycodewords of any length n. The choice of n depends on the desired application. To demonstrate this we consider the polynomial ring $F_2^n[x] mod(x^n-1)$ in which $1\le n\le 31$. The results obtained are generalised to all polycodewords of length n generated by the polynomial ring $F_2^n[x] mod(x^n-1)\forall n\in\mathbb{N}$. A code is suitable for error control if and only if it can correct at least one error.

Table 2.1.1. Factorization of $x^n-1, 1\le n\le 31$ over $\mathbb{F}_2$

n	(x^n+1)	Irreducible Polynomial Factors (over $\mathbb{F}_2$)
1	$(x+1)$	$x+1$
2	(x^2+1)	$(x+1)^2$
3	(x^3+1)	$(x+1)(x^2+x+1)$
4	(x^4+1)	$(x+1)^4$
5	(x^5+1)	$(x+1)(x^4+x^3+x^2+x+1)$

6	(x^6+1)	$(x+1)^2(x^2+x+1)^2$
7	(x^7+1)	$(x+1)(x^3+x+1)(x^3+x^2+1)$
8	(x^8+1)	$(x+1)^8$
9	(x^9+1)	$(x+1)(x^2+x+1)(x^6+x^3+1)$
10	$(x^{10}+1)$	$(x+1)^2(x^4+x^3+x^2+x+1)$
11	$(x^{11}+1)$	$(x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
12	$(x^{12}+1)$	$(x+1)^4(x^2+x+1)^4$
13	$(x^{13}+1)$	$(x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
14	$(x^{14}+1)$	$(x+1)^2(x^3+x+1)^2(x^3+x^2+1)^2$
15	$(x^{15}+1)$	$(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$
16	$(x^{16}+1)$	$(x+1)^{16}$
17	$(x^{17}+1)$	$(x+1)(x^8+x^7+x^6+x^4+x^2+x+1)(x^8+x^5+x^4+x^3+1)$
18	$(x^{18}+1)$	$(x+1)^2(x^2+x+1)^2(x^6+x^3+1)^2$
19	$(x^{19}+1)$	$(x+1)(x^{18}+x^{17}x^{16}+\ldots+x+1)$
20	$(x^{20}+1)$	$(x+1)^4(x^4+x^3+x^2+x+1)^4$
21	$(x^{21}+1)$	$(x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)$ $(x^6+x^5+x^4+x^2-1)(x^6+x^4+x^2+x+1)$
22	$(x^{22}+1)$	$(x+1)^2(x^{10}+x^9+\ldots+x+1)^2$
23	$(x^{23}+1)$	$(x+1)(x^{11}+x^9+x^7+x^6+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$
24	$(x^{24}+1)$	$(x+1)^8(x^2+x+1)^8$

25	$(x^{25}+1)$	$(x+1)(x^{20}+x^{15}+x^{10}+x^5+1)(x^4+x^3+x^2+x+1)$
26	$(x^{26}+1)$	$(x+1)^2(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7$ $+x^6+x^5+x^4+x^3+x^2+x+1)^2$
27	$(x^{27}+1)$	$(x+1)(x^{18}+x^9+1)(x^6+x^3+1)(x^2+x+1)$
28	$(x^{28}+1)$	$(x+1)^4(x^3+x+1)^4(x^3+x^2+1)^4$
29	$(x^{29}+1)$	$(x+1)(x^{28}+x^{27}+...+x+1)$
30	$(x^{30}+1)$	$(x+1)^2(x^2+x+1)^2(x^4+x+1)^2(x^4+x^3+1)^2(x^4+x^3+x^2+x+1)^2$
31	$(x^{31}+1)$	$(x+1)(x^5+x^2-1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)$ $(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$

Table 2.1.1 was prepared using an online tool, www.quickmath.com. Each of the factors is irreducible. These factors are the generator polynomials and principal ideals of the corresponding polynomial ring.

Hamming Bound (Sphere Packing Bound 2.1.1) [10]

If C is an m-ary e-error-correcting code of length n, then

$$|C| \le \frac{m^n}{\sum_{i=0}^{e}\binom{n}{i}(m-n)^i}$$

A code which satisfies this bound with equality is called a perfect code.

Proposition 2.1.2 [14]

A binary repetition code of length n with n odd is perfect.

Proof

Let $C=\{\alpha_0=000...00,\alpha_1=111...11\}$ be of length n. Any vector $x\in\mathbb{F}_2^n$ has t coordinates 1, and $n-t$ coordinates 0. So $d(x,\alpha_0)=t$ and $d(x,\alpha_1)=n-t$. Hence if $t<\frac{n}{2}$ then x is uniquely decoded as α_0, where as, if $t>\frac{n}{2}$, then x is uniquely decoded as α_1. Hence C is perfect.

C detects $n-1$ errors and corrects $\frac{n-1}{2}$ errors.

From proposition 2.1.2 rather than analyze all the repetition codes of length n for $1\le n\le 31$ we

can concentrate on those with odd n.

Table 2.1.2. Generator Polynomials of $F_2[x] mod(x-1)$

Generator Polynomial	Corresponding Codeword
0	0
1	1

The codes in C are ideals of the polynomial ring

$F_2[x] mod(x-1)$ $m=2, n=1, W_c=1, d_c=1, (n,m,d)=(1,2,1), C=[0,1]$

By proposition 2.1 this code can neither detect nor correct any errors. It is not suitable for error control.

Table 2.1.3. Generator Polynomials of $F_2^3[x] mod(x^3-1)$

Generator Polynomial	Corresponding Codeword
0	000
1	001
x	010
x^2	100
$1+x$	110
$x+x^2$	011
$1+x^2$	101
x^2+x+1	111

The codes in C are ideals of the polynomial ring $F_2^3[x] mod(x^3-1)$ $m=8, n=3, W_c=3, d_c=3,$ $(n,m,d)=(3,8,3)$, $C=[000,001,010,100,110,011,101,111]$.

By proposition 2.1 this code can detect two errors. It can correct only one error. It is suitable for error control.

Table 2.1.4. Generator Polynomials of $F_2^5[x] mod(x^5-1)$

Generator Polynomial	Corresponding Codeword
0	00000
$1+x$	00011
$1+x^2$	00101
$x+x^2$	00110
x^2+x^3	01100
$x+x^3$	01010
x^3+x^4	11000
$1+x+x^2+x^3+x^4$	11111

The codes in C are ideals of the polynomial ring $F_2^5[x] mod(x^5-1)$ $m=8,\ n=5,\ W_c=5,$ $d_c=5,\ (n,m,d)=(5,8,5),\ C=[00000,00011,00101,00110,01100,01010,11000,11111].$

By proposition 2.1 this code can detect four errors. It can correct two errors. It is therefore suitable for error control.

Table 2.1.5. Generator Polynomials of $F_2^7[x] mod(x^7-1)$

Generator Polynomial	Corresponding Codeword
0	0000000
1	0000001
$x+1$	0000011
x^3+x+1	0001011
x^3+x^2+1	0001101
$x^4+x^3+x^2+1$	0011101

x^4+x^2+x+1	0010111
$x^6+x^5+x^4+x^3+x^2+x+1$	1111111

The codes in C are ideals of the polynomial ring

$F_2^7[x] mod(x^7-1)$ $m=8, n=7, W_c=7, d_c=7, (n,m,d)=(7,8,7),$

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

By proposition 2.1 this code can detect six errors. It can correct three errors. It is therefore suitable for error control.

Table 2.1.6: Generator Polynomials of $F_2^9[x] mod(x^9-1)$

Generator Polynomial	**Corresponding Codeword**
0	000000000
1	000000001
$x+1$	000000011
x^2+x+1	000000111
x^6+x^3+1	001001001
x^3+1	000001001
$x^7+x^6+x^4+x^3+x+1$	011011011
$x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	111111111

The codes in C are ideals of the polynomial ring $F_2^9[x] mod(x^9-1)$ $m=8,$ $n=9,$ $W_c=9,$ $d_c=9,$ $(n,m,d)=(9,8,9),$ $C=[00000000, 000000001, 000000011, 000000111, 001001001, 000001001, 011011011, 111111111]$

By proposition 2.1 this code can detect eight errors. It can correct four errors. It is suitable for error control.

Table 2.1.7. Generator Polynomials of $F_2^{11}[x] mod(x^{11}-1)$

Generator Polynomial	Corresponding Codeword
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

The codes in C are ideals of the polynomial ring $F_2^{11}[x] mod(x^{11}-1)$ $m=4,\ n=11,\ W_c=11,$ $d_c=11,\ (n,m,d)=(11,4,11),\ C=[00000000000,00000000001,00000000011,11111111111]$

By proposition 2.1 this code can detect ten errors. It can correct five errors. It is suitable for error control.

Table 2.1.8. Generator Polynomials of $F_2^{13}[x] mod(x^{13}-1)$

Generator Polynomial	Corresponding Codeword
0	0000000000000
1	0000000000001
$x+1$	0000000000011
$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	1111111111111

The codes in C are ideals of the polynomial ring $F_2^{13}[x] mod(x^{13}-1)$ $m=4,\ n=12,\ W_c=13,$ $d_c=13,\ (n,m,d)=(13,4,13),\ C=[0000000000000,0000000000001,0000000000011,1111111111111]$

By proposition 2.1 this code can detect twelve errors. It can correct six errors. It is suitable for error control.

Table 2.1.9. Generator Polynomials of $F_2^{15}[x] mod(x^{15}-1)$

Generator Polynomial	Corresponding Codeword
0	000000000000000
1	000000000000001
$x+1$	000000000000011

$x^2 + x^x + 1$	000000000000111
$x^4 + x + 1$	000000000001011
$x^4 + x^3 + 1$	000000000011001
$x^4 + x^3 + x^2 + x + 1$	000000000011111
$x^3 + 1$	000000000001001
$x^5 + x^4 + x + 1$	000000000110011
$x^5 + x^3 + x + 1$	000000000101011
$x^5 + 1$	000000000100001
$x^6 + x^5 + x^4 + x^3 + 1$	000000001111001
$x^7 + x^3 + x + 1$	000000010001011
$x^6 + x^3 + ^2 + x + 1$	000000001001111
$x^{12} + x^9 + ^6 + x^3 + 1$	001001001001001
$x^7 + x^6 + x^4 + x + 1$	000000011010001
$x^6 + x^4 + x^3 + x^2 + 1$	000000001011101
$x^7 + 1$	000000011100111
$x^8 + x^2 + 1$	000000000000101
$x^9 + x^8 + x^3 + x^2 + x + 1$	000001100001111
$x^{10} + x^8 + x^5 + x^4 + x^3 + 1$	000010100110111
$x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3 + 1$	000110101011001

$x^8+x^4+x^2+x+1$	000000100010111
$x^9+x^8+x^5+x^4+x^3+1$	000001100111001
$x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7$ $+x^6+x^5+x^4+x^3+x^2+x+1$	111111111111111

The codes in C are ideals of the polynomial ring $F_2^{15}[x] mod(x^{15}-1)$ $m=25,\ \ n=15,\ \ W_c=15,$ $d_c=15,\ \ (n,m,d)=(15,25,15),$

$C=[000000000000000, 000000000000001, 000000000000011, 000000000000111,$
$000000000010011, 000000000011001, 000000000011111, 000000000001001, 000000000110011,$
$000000000101011, 000000000100001, 000000001111001, 000000010001011, 000000001001111,$
$000000011010001, 001000110100011, 000000001011101, 000000011100111, 000000100000101,$
$000001100001111, 000010100110111, 000110101011001, 000000100010111,$
$000001100111001].$

By proposition 2.1 this code can detect five errors. It can correct two errors. It is suitable for error control.

Table 2.1.10. Generator Polynomials of $F_2^{17}[x] mod(x^{17}-1)$

Generator Polynomial	**Corresponding Codeword**
0	00000000000000000
1	00000000000000001
$x+1$	00000000000000011
$x^8+x^7+x^6+x^4+x^2+x+1$	00000000111010111
$x^9+x^7+x^5+x^4+x^3+1$	00000001010111001
$x^8+x^5+x^4+x^3+1$	00000000100111001
$x^9+x^8+x^6+x^3+x+1$	00000001101001011
$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9$ $+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	11111111111111111

The codes in C are ideals of the polynomial ring $F_2^{17}[x] mod(x^{17}-1)$ $m=8,\ n=17,\ W_c=17,$ $d_c=17,\ (n,m,d)=(17,8,17),$

$C=[0000000000000000, 0000000000000001, 0000000000000011,$
$0000000111010111, 0000000101011001, 0000000100111001,$
$0000000110100 1011, 1111111111111111]$

By proposition 2.1 this code can detect sixteen errors. It can correct eight errors. It is suitable for error control.

Table 2.1.11. Generator Polynomials of $F_2^{19}[x] mod(x^{19}-1)$

Generator Polynomial	**Corresponding Codeword**
0	0000000000000000000
1	0000000000000000001
$x+1$	0000000000000000011
$x^{18}+x^{17}+x^{16}+...+x+1$	1111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{19}[x] mod(x^{19}-1)$ $m=4,\ n=19,\ W_c=17,$ $d_c=19,\ (n,m,d)=(19,4,19),$

$C=[0000000000000000000, 0000000000000000001, 0000000000000000011,$
$1111111111111111111]$

By proposition 2.1 this code can detect eighteen errors. It can correct nine errors. It is suitable for error control.

Table 2.1.12. Generator Polynomials of $F_2^{21}[x] mod(x^{21}-1)$

Generator Polynomial	**Corresponding Codeword**
0	00000000000000000000
1	00000000000000000001
$x+1$	00000000000000000011
x^2+x+1	00000000000000000111
x^3+x^2+1	00000000000000001101

x^3+x+1	00000000000000001011
$x^6+x^5+x^4+x^2+1$	00000000000000111011
$x^6+x^4+x^2+x+1$	00000000000001010111
x^3+1	00000000000000001001
x^4+x^2+x+1	00000000000000010111
$x^4+x^3+x^2+1$	00000000000000011111
$x^7+x^4+x^3+x^2+1$	00000000000010011111
$x^7+x^6+x^5+x^4+x^3+1$	00000000000011111001
x^5+x+1	00000000000000100011
x^5+x^4+1	00000000000000110001
$x^8+x^6+x^3+x+1$	00000000000101001011
$x^8+x^7+x^5+x^2+1$	00000000000110100101
$x^6+x^5+x^2+1$	00000000000001100101
x^6+x^4+x+1	00000000000001010011
$x^9+x^8+x^7+x^6+x^6+x^3+x^2+1$	00000000001111011101
$x^9+x^7+x^6+x^5+x^3+x^2+x+1$	00000000001011111111
$x^6+x^5+x^4+x^3+x^2+x+1$	00000000000001111111
x^9+x^3+1	00000000001000001001
x^9+x^3+1	00000000001000001001

x^7+1	00000000000010000001
$x^{10}+x^9+x^4+x^3+x+1$	00000000011000011011
$x^{10}+x^7+x^6+x^4+x^2+1$	00000000100011010101
x^8+x^7+x+1	00000000000110000011
$x^9+x^8+x^5+x^4+x^2+x+1$	00000000001100110111
x^9+1	00000000001000000001
$x^{10}+x^8+x^6+x^4+x^3+1$	00000000010101011001
$x^{12}+x^{11}+x^9+x^8+x^6+x^5+x^3+x+1$	00000001101101101011
$x^{13}+x^{12}+x^{11}+x^8+x^7+x^5+x^4+x^3+x^2+1$	00000111001101111101
$x^{14}+x^9+x^8+x^4+1$	00000100001100010001
$x^{15}+x^{14}+x^{11}+x^{10}+x^8+x^7+x^4$ $+x^3+x^2+x+1$	00001100110110011111
$x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^7$ $+x^6+x^5+x^2+1$	00001111011011100101
$x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^8$ $+x^5+x^4+x^2+1$	00001111011100110101
$x^{18}+x^{15}+x^{12}+x^9+x^6+x^3+1$	00100100100100100001
$x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+$ $\ldots+x^2+x+1$	11111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{21}[x] mod(x^{21}-1)$ $m=36,\ n=21,\ W_c=21,$ $d_c=21,(n,m,d)=(21,39,21)$,

$C=[00000000000000000000, 00000000000000000001, 00000000000000000011,$
$00000000000000000111, 00000000000000001101, 00000000000000001011,$
$00000000000000111011, 00000000000001010111, 00000000000000001001,$
$00000000000000010111, 00000000000000001111, 00000000000000111001,$
$00000000000010011111, 00000000000011111001, 00000000000000100011,$
$00000000000000110001, 00000000000101001011, 00000000000110100101,$
$00000000000001100101, 00000000000001010011, 00000000001111011101,$
$00000000001011111111, 00000000000001111111, 00000000001000001001,$
$00000001110110110011, 00000000000010000001, 00000000011000011011,$
$00000000010011010101, 00000000000110000011, 00000000001100110111,$
$00000000001000000001, 00000000010101011001, 00000001101101101011,$
$00000011100110111101, 00001100110110011111, 00001111011011100101,$
$11111111111111111111]$

By proposition 2.1 this code can detect twenty errors. It can correct ten errors. It is suitable for error control.

Table 2.1.13. Generator Polynomials of $F_2^{23}[x]mod(x^{23}-1)$

Generator Polynomial	**Corresponding Codeword**
0	00000000000000000000000
1	00000000000000000000001
$x+1$	00000000000000000000011
$x^{11}+x^9+x^7+x^6+x^5+x+1$	00000000000010101110011
$x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$	00000000000110001110101
$x^{12}+x^{11}+x^{10}+x^9+x^8+x^5+x^2+1$	00000000001111100100101
$x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1$	00000000010100100111111
$x^{22}+x^{21}+x^{20}+...+x+1$	11111111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{23}[x]mod(x^{23}-1)$ $m=8,$ $n=23,$ $W_c=23,$ $d_c=23,(n,m,d)=(23,8,23),$

$C = [00000000000000000000000, 00000000000000000000001, 00000000000010101110011,$
$00000000001100011101 01, 00000000001111100100101, 00000001010010010011111,$
$11111111111111111111111]$

By proposition 2.1 this code can detect twenty two errors. It can correct eleven errors. It is suitable for error control.

Table 2.1.14. Generator Polynomials of $F_2^{25}[x] mod(x^{25}-1)$

Generator Polynomial	**Corresponding Codeword**
0	0000000000000000000000000
1	0000000000000000000000001
$x+1$	0000000000000000000000011
$x^4+x^3+x^2+x+1$	0000000000000000000011111
$x^{20}+x^{15}+x^{10}+x^5+1$	0000100001000010000100001
$x^{12}+x^{11}+x^{10}+x^9+x^8+x^5+x^2+1$	0000000000001111100100101
$x^{21}+x^{20}+x^{16}+x^{15}+x^{11}+x^{10}+x^6+x^5+x+1$	0000110001100011000110001
$x^{24}+x^{23}+x^{22}+...+x+1$	1111111111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{25}[x] mod(x^{25}-1)$ $m=8,$ $n=25,$

$W_c, d_c = 25, (n, m, d) = (25, 8, 25)$,

$C = [00000000000000000000000, 00000000000000000000001,$
$00000000000000000000011, 00000000000000000000011111,$
$00001000010000100001 00001, 00000000000011111100100101,$
$00001100011000110001 10001, 11111111111111111111111]$

By proposition 2.1 this code can detect tenty four errors. It can correct twelve errors. It is suitable for error control.

Table 2.1.15. Generator Polynomials of $F_2^{27}[x] mod\left(x^{27}-1\right)$

Generator Polynomial	**Corresponding Codeword**
0	000000000000000000000000000
1	000000000000000000000000001
$x+1$	000000000000000000000000011
x^2+x+1	000000000000000000000001011
x^6+x^3+1	000000000000000000001001001
$x^{18}+x^9+1$	000000001000000001000000001
x^3+1	000000000000000000000001001
$x^7+x^6+x^4+x^3+x+1$	000000000000000000011011011
$x^{19}+x^{18}+x^{10}+x^2+x$	000000011000000010000000110
$x^8+\ldots+x+1$	000000000000000000111111111
x^9+1	000000000000000001000000001
$x^{20}+x^{19}+x^{18}+x^{11}+x^{10}+x^9+x^2+x+1$	000000111000000111000000111
$x^{21}+x^{18}+x^{17}+x^9+x^3+1$	000001001000001001000001001
$x^{26}+x^{25}+x^{23}+\ldots+x+1$	111111111111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{27}[x] mod\left(x^{27}-1\right)$ $m=14,\ \ n=27,\ \ W_c=27,$

$d_c=27,\ \ (n,m,d)=(27,14,27),$

$C=[00000000000000000000000000, 00000000000000000000000001,$
$00000000000000000000000011, 00000000000000000000001011,$
$00000000000000000001001001, 00000000100000001000000001,$
$00000000000000000000001001, 00000000000000000011011011,$
$00000001100000001000000110, 00000000000000000111111111,$
$00000000000000001000000001, 00000011100000111000000111,$
$00000100100000100100000100111111111111111111111111111111]$

By proposition 2.1 this code can detect tenty six errors. It can correct thirteen errors. It is suitable for error control.

Table 2.1.16. Generator Polynomials of $F_2^{29}[x] mod(x^{29}-1)$

Generator Polynomial	**Corresponding Codeword**
0	00000000000000000000000000000
1	00000000000000000000000000001
$x+1$	00000000000000000000000000011
$x^{28}+x^{27}+x^{26}+...+x+1$	11111111111111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{29}[x] mod(x^{29}-1)$ $m=4,$ $n=29,$ $W_c=29,$ $d_c=29,$ $(n,m,d)=(29,4,29),$

$C=[00000000000000000000000000000, 00000000000000000000000000001,$
$00000000000000000000000000011, 11111111111111111111111111111]$

By proposition 2.1 this code can detect twenty eight errors. It can correct fourteen errors. It is suitable for error control.

Table 2.1.17. Generator Polynomials of $F_2^{31}[x] mod(x^{31}-1)$

Generator Polynomial	**Corresponding Codeword**
0	0000000000000000000000000000000
1	0000000000000000000000000000001
$x+1$	0000000000000000000000000000011
x^5+x^2+1	0000000000000000000000000100101
x^5+x^3+1	0000000000000000000000000101001

$x^5+x^3+x^2+x+1$	00000000000000000000000000101111
$x^5+x^4+x^2+x+1$	00000000000000000000000000110111
$x^5+x^4+x^3+x+1$	00000000000000000000000000111011
$x^5+x^4+x^3+x^2+x+1$	00000000000000000000000000111111
$x^6+x^5+x^3+x^2+x+1$	00000000000000000000000001101111
$x^5+x^4+x^3+x^2+x+1$	00000000000000000000000000111111
$x^6+x^5+x^3+x^2+x+1$	00000000000000000000000001101111
$x^6+x^5+x^4+x^3+x+1$	00000000000000000000000000111111
$x^6+x^5+x^4+1$	00000000000000000000000001110001
$x^6+x^4+x^3+1$	00000000000000000000000001011001
x^6+1	00000000000000000000000001000001
$x^{10}+x^8+x^7+x^5+x^3+x^2+1$	00000000000000000000010110101101
$x^{11}+x^{10}+x^9+x^7+x^5+x^4+x^2+x+1$	00000000000000000000111010110111
$x^{10}+x^8+x^6+x^5+x^4+x+1$	00000000000000000000010101110011
$x^{11}+x^{10}+x^9+x^8+x^7+x^4+x^2+1$	00000000000000000000001111100101
$x^{10}+x^9+x^3+x+1$	00000000000000000000011000001011
$x^{11}+x^9+x^4+x^3+x^2+1$	00000000000000000000101000011101
$x^{10}+x^9+x^8+x^7+x^5+x^4+x^2+x+1$	00000000000000000000011110110111
$x^{11}+x^7+x^6+x^4+x^3+1$	00000000000000000000100011011001

$x^{10}+x^9+x^8+x^5+x+1$	00000000000000000000011100100011
$x^{11}+x^8+x^6+x^5+x^2+1$	00000000000000000000100101100101
$x^{10}+x^7+x^5+x^4+x^2+x+1$	00000000000000000000010010110111
$x^{11}+x^{10}+x^8+x^7+x^6+x^4+x^3+1$	00000000000000000000110111011001
$x^{10}+x^9+x^8+x^6+x^5+x^3+x^2+x+1$	00000000000000000000011101101111
$x^{11}+x^8+x^7+x^5+x^4+1$	00000000000000000000010110110001
$x^{10}+x^9+x^7+x+1$	00000000000000000010011010000011
$x^{11}+x^9+x^8+x^7+x^2+1$	00000000000000000000101110000101
$x^{10}+x^9+x^5+x^2+x+1$	00000000000000010101011000100111
$x^{11}+x^9+x^6+x^5+x^3+1$	00000000000000000000101001101001
$x^{15}+x^7+x^3+x+1$	00000000000000010000000010001011
$x^{16}+x^{15}+x^8+x^7+x^4+x^3+x^2+1$	00000000000001100000000111011101
$x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^9$ $+x^8+x^5+x^4+1$	00000000000011111011011100110011
$x^{16}+x^{12}+x^{11}+x^8+x^6+x^4+x^2+1$	00000000000000100011001010101010
$x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x^2+1$	00000000000000000000001111011101
$x^{11}+x^6+x^5+x^2+x+1$	00000000000000000001000001100111
$x^{15}+x^{14}+x^{13}+x^9+x^8+x^3+1$	00000000000000001110001100001001
$x^{16}+x^{13}+x^8+x^4+x^3+x+1$	00000000000000010010000100011011
$x^{15}+x^{14}+x^9+x^7+x^4+x^2+1$	00000000000000000110000010010101

$x^{16}+x^{14}+x^{10}+x^9+x^8$ $+x^7+x^5+x^4+x^3+x^2+x+1$	00000000000000010100011110111111
$x^{10}+x^6+x^5+x^4+1$	00000000000000000000010001110001
$x^{11}+x^{10}+x^7+x^4+x+1$	00000000000000000000110010010011
$x^{15}+x^{12}+x^{11}+x^9+x^8+x^7$ $+x^4+x^2+1$	00000000000000010011011100101010 1
$x^{16}+x^{15}+x^{13}+x^{11}+x^{10}$ $+x^7+x^5+x^4+x^3+x+1$	00000000000000011010110010111111
$x^{15}+x^{13}+x^{11}+x^8+x^7+x^6$ $+x^4+x^3+1$	00000000000000010101001110110011
$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}$ $+x^{11}+x^9+x^6+x^5+x^3+x+1$	00000000000000011111101001101011
$x^{15}+x^{13}+x^{12}+x^7+x^6+x^5+x^4$ $+x^3+x^2+x+1$	00000000000000010110000111111111
$x^{16}+x^{15}+x^{14}+x^{12}+x^8+1$	00000000000000011101000100000001
$x^{10}+x^8+x^7+x^5+x^3+1$	00000000000000000000010110101001
$x^{11}+x^{10}+x^9+x^7+x^6+x^5+x^4$ $+x^3+x+1$	00000000000000000000111011111011
$x^{15}+x^{13}+x^{10}+x^9+x^5+x^3+x^2+1$	00000000000000010100110001011 01
$x^{16}+x^{15}+x^{14}+x^{13}+x^{11}+x^9$ $+x^6+x^5+x^4+x^2+x+1$	00000000000000011110101001110111
$x^{15}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+1$	00000000000000010011101110000001
$x^{16}+x^{15}+x^{13}+x^{10}+x^9+x^6+x+1$	00000000000000011010011001000 11
$x^{15}+x^5+x^4+x^2+x+1$	00000000000000010000000000110111

$x^{20}+x^{19}+x^{17}+x^{16}+x^{15}+x^{12}$ $+x^{11}+x^9+x^3+x^2+x+1$	00001100100011111010000110001011
$x^{20}+x^{19}+x^{17}+x^{16}+x^{15}+x^{12}$ $+x^{11}+x^9+x^6+x^5+1$	00000000001101110001010011000001
$x^{25}+x^{23}+x^{21}+x^{20}+x^{19}+x^{17}+x^{15}+x^{13}$ $+x^{12}+x^{10}+x^9+x^8+x^7+x^4+x^3+x+1$	00000101011101010111011110011011
$x^{26}+x^{25}+x^{22}+x^{19}+x^{18}+x^{17}$ $+x^{16}+x^{15}+x^{13}+x^8+x^7+x^3+x+1$	00001100100011111010000110001011
$x^{30}+x^{24}+x^{22}+x^{21}+x^{20}+x^{14}+x^{12}+x^{11}$ $+x^{20}+x^{10}+x^9+x^8+x^7+x^6+x^5$ $+x^4+x^3+x^2+1$	00000010111000001011111111111111
$x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}$ $+x^{20}+x^{19}+x^{18}+x^{17}+x^8+x^7+x^6$ $+x^5+x^2+1$	11111111111111000000000111100101
$x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}$ $+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}$ $+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7$ $+x^6+x^5+x^4+x^3+x^2+x$	11111111111111111111111111111111

The codes in C are ideals of the polynomial ring $F_2^{31}[x] mod(x^{31}-1)$ $m=71,\ n=31,\ W_c=31,$ $d_c=31,\ (n,m,d)=(31,71,31),$

$C = [0000000000000000000000000000000, 0000000000000000000000000000001,$
$0000000000000000000000000000011, 0000000000000000000000000100101,$
$0000000000000000000000000101001, 0000000000000000000000000101111,$
$0000000000000000000000000110111, 0000000000000000000000000111011,$
$0000000000000000000000000111111, 0000000000000000000000001101111,$
$0000000000000000000000000111111, 0000000000000000000000001110001,$
$0000000000000000000000001011001, 0000000000000000000000001000001,$
$0000000000000000000010110101101, 0000000000000000000111010110111,$
$0000000000000000000010101110011, 0000000000000000000001111100101,$
$0000000000000000000011000001011, 0000000000000000000101000011101,$
$0000000000000000000011110110111, 0000000000000000000100011011001,$
$0000000000000000000011100100011, 0000000000000000000100101100101,$
$0000000000000000000010010110111, 0000000000000000000110111011001,$
$0000000000000000000011101101111, 0000000000000000000010110110001,$
$0000000000000000010011010000011, 0000000000000000000101110000101,$
$0000000000000010101011000100111, 0000000000000000000101001101001,$
$0000000000000010000000010001011, 0000000000000011000000011101101,$
$0000000000011110110111001100111, 0000000000000010001100101010101,$
$0000000000000000000001111011101, 0000000000000000001000001100111,$
$0000000000000011100011000010011, 0000000000000010010000100011011,$
$0000000000000000110000010010101, 0000000000000010100011110111111,$
$0000000000000000000010001110001, 0000000000000000000110010010011,$
$0000000000000010011011110010101, 0000000000000011010110010111111,$
$0000000000000010101001110110011, 0000000000000011111101001101011,$
$0000000000000010110000111111111, 0000000000000011101000100000001,$
$0000000000000000000010110101001, 0000000000000000000111011111011,$
$0000000000000010100110001011101, 0000000000000011110101001110111,$
$0000000000000010011101110000001, 0000000000000011010011001000011,$
$0000000000000010000000000110111, 0000110010001111010000110001011,$
$0000000000110111000101001100001, 0000110010001111010000110001011,$
$0000110010001111010000110001011, 0000001011100000101111111111111,$
$1111111111111100000000111100101]$

By proposition 2.1 this code can detect nineteen errors. It can correct nine errors. It is suitable for error control.

GAP Software has also been used to confirm that all our repetition codes of odd length are perfect codes. Thus we have generated perfect codes for odd n for $1 \le n \le 31$ from the polynomial ring $F_2^n[x] \mod (x^n-1)$.

The best perfect code obtained was generated by $F_2^{31}[x] mod(x^{31}-1)$. The worst perfect code was generated when $n=1$.

Theorem 2.3

Let I be a maximal ideal over the polynomial ring $F_2^n[x] mod(x^n-1)$. 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 nonempty 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 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 $I_{n+1} = I_n + x(F_2^n[x] mod(x^n-1))$ 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 nonzero 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 noetherian then it has a maximal ideal.To see this let P be a set of all the proper ideals in the polynomial ring $F_2^n[x] mod(x^n-1)$ containing I_p where I_P is any proper ideal in thisring. Already we know that $P \neq \varnothing$ since $I_P \in P$. Since $F_2^n[x] mod(x^n-1)$ is noetherian the maximum condition gives a maximal element $I \in P$. We should show that I is a maximal ideal in

$F_2^n[xght]mod(x^n-1)$. 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 $F_2^n[x]mod(x^n-1)$.

(ii) $\Rightarrow$ (iii). If (iii) is false there is a nonempty subset S of $F_2^n[x]mod(x^n-1)$ 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 2.4

$F_2^n[x]mod(x^n-1)$ is a Unique Factorization Domain

Proof

Let $t \in F_2^n[x]mod(x^n-1)$. 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 $t = uv, \forall t,u,v, \in F_2^n[x]mod(x^n-1)$. 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 $u = tw \Rightarrow u = uvw \Rightarrow u(1-vw) = 0 \Rightarrow vw = 1, \forall t,u,v,w \in F_2^n[x]mod(x^n-1)$. Since $F_2^n[x]mod(x^n-1)$ 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 $t \mid uv$. Then $uv = tw$ for some $w \in F_2^n[x]mod(x^n-1)$. BY some 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 $a \cdot t_1 ... t_n = b \cdot u_i ... u_n = c \cdot v_i ... v_n$. This factorization is unique and therefore t must be associated to some u_i or v_i implying that t divides u or v.

References

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

[2]. Hamming, R.W., Error detecting and error correcting codes, Bell Syst. Tech. J., Vol. 29, (1950), pp. 147-150.

[3]. Golay, M. J. E (1949), Notes on digital coding, Proc. IEEE, vol. 37, p. 657.

[4]. Berrou, C. Glavieux, A. (1996), Near optimum error correcting coding and decoding: Turbo-codes, IEEE Trans. Commun., vol. 44, pp. 1261-1271.

[5]. Reed, I. S. and Solomon, G. (1960), Polynomial codes over certain finite fields, SIAM Journal on Applied Mathematics, vol. 8, pp. 300-304.

[6]. Bose R. C. and Ray-Chaudhuri, D. K. (1960), On a class of error correcting binary group codes, Information and Control, vol. 3, pp. 68-79.

[7]. MacKay, D. J. C. and Neal, R. M. (1996, 1997), Near Shannon limit performance of low density parity check codes, Electron. Lett., vol. 32, no. 18, pp. 1645-1646, 1996, reprinted Electron. Lett, vol. 33(6), pp. 457- 458.

[8]. Richardson T. J. et al. (2001), The capacity of low-density parity check codes under message-passing decoding, IEEE Trans. Inform. Theory, vol. 47, no. 2, pp. 599-618.

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

[10]. Hall, J. (2003), Agebraic Coding Theory, Michigan State University U.S.A., pp 15-152.

[11]. Prange, E. (1957), Cyclic Error-Correcting Codes in Two Symbols, Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN-57-103.

[12]. Peterson, W. W. and Weldon, Jr. (1972), Error Correcting Codes, 2nd Edition MIT Press Cambridge Mass.

[13]. Adams, S. S. (2008), Introduction to Coding Theory, 3rd Edition, Cornel University Press, Berlin.

[14]. Aimo T. On the nonexistence of perfect codes over finite fields. SIAM Journal of Applied Mathematics, 24 (1): 88-96, January 1973.

Published: Volume 2016, Issue 10 / October 25, 2016