ISSN 2347-1921
Volume 12 Number 5
Journal of Advances in Mathematics

CHARACTERIZATION OF CODES OF IDEALS OF THE POLYNOMIAL RING $F_2^{30}[x]mod(x^{30}-1)$ FOR ERROR CONTROL IN COMPUTER APPLICATONS

Olege Fanuel [1], Owino M. Oduor [2], Aywa Shem [3] and Okaka A. Colleta [4]

[1,4] Department of Mathematics, Masinde Muliro University of Science and Technology
P.O. Box 190-50100, Kakamega (Kenya)
olegefanuel@yahoo.com

[2] Department of Mathematics and Computer Science, University of Kabianga
P.O. Box 2030-20200, Kericho (Kenya)
morricearaka@yahoo.com

[3] Department of Mathematics Kibabii University
P.O. Box 1699-50200, Bungoma (Kenya)
shemaywa2014@gmail.com

[4] letticol@yahoo.com

ABSTRACT

The study of ideals in algebraic number system has contributed immensely in preserving the notion of unique factorization in rings of algebraic integers and in proving Fermat's last Theorem. Recent research has revealed that ideals in Noetherian rings are closed in polynomial addition and multiplication.This property has been used to characterize the polynomial ring $F_2^n[x]mod(x^n-1)$ for error control. In this research we generate ideals of the polynomial ring using GAP software and characterize the polycodewords using Shannon's Code region and Manin's bound.

Mathematics Subject Classification: Primary 20K30; Secondary 16P10.

Key Words and Phrases: Polynomial ring; Error detection; Error correction; Code region.

1 Introduction

1.1 Error control Coding

The modern approach to error control coding in digital communication systems was started by Shannon [1], Golay [2] and Hamming [3]. By mathematically defining entropy of an information source and the capacity of a communication channel Shannon [1] showed that it was possible to achieve reliable communication over a noisy channel provided that the source's entropy is lower than the channel's capacity. He did not explicitly state how channel capacity could be practically reached, only that it was attainable. Hamming [3] and Golay [2] developed the first practical error control schemes. According to Wicker [4] this Hamming code had some undesirable properties; first, it was not efficient, requiring three check bits for every four data bits and second, it could only correct a single error within the block.

Golay code [2] addressed these shortcomings by generalizing the construction of the Hamming code. In the process he discovered two codes; The first is the binary Golay code which groups data into blocks of twelve bits and then calculates eleven check bits. The associated decoding algorithm is capable of correcting up to three errors in the 23 bit code word. The second is the ternary Golay code, which operates on ternary, rather than binary, numbers. This code protects blocks of six ternary symbols with five ternary check symbols and has the ability to correct two errors in the resulting eleven symbol code word. The general techniques for developing Hamming and Golay codes were the same. They involved grouping q-ary symbols into blocks of k and then adding $n-k$ check symbols to produce an n symbol code word. The resulting code has the ability to correct t errors, and has a code rate $\frac{k}{n}$. A code of this type is called a block code, and is referred to as a (q,n,k,t) block code. Hamming and Golay codes are linear since the modulo-q sum of any two code words is itself a code word. According to Wicker [4] it is the binary Golay code which provided error control during the Jupiter fly-by of Voyager I launched in 1979 .

The next main class of linear block codes to be discovered were the Reed-Muller codes, which were first described by Muller [5] in the context of Boolean logic design. These codes were more superior to the Golay Codes since they allowed more flexibility in the size of the code word and the number of correctable errors per code word. According to Wicker [4], these codes had an extensive application between 1969 and 1977 in the Mariner Missions to Mars, which used a $(q=2;n=32;k=6;t=7)$

RM - code.

Next came the discovery of cyclic codes by Prange [6]. These are linear block codes that possess the additional property that any cyclic shift of a code word is also a code word. This property suggests that cyclic codes can be compactly specified by a polynomial of degree $n-k$, denoted by $g(x)$ (the generator polynomial).

Castagnoli *etal* [7] developed another class of Cyclic Codes called Cyclic Redundancy Check (CRC) codes. These have a desirable ability of increasing the number of correctable errors and are basically used to detect single and double bit errors. For this reason, CRC codes are primarily used today for error detection applications rather than for error correction.

Bose, Ray-Chaudhuri and Hocquenghem [8] discovered BCH codes. They have length $n = q^m - 1$,where m is an integer valued design parameter. The number of errors that the binary $(q = 2)$ BCH code can correct is at least $t = (n-k) = m$ though for some BCH codes it could be more. BCH codes were extended to the nonbinary case $(q \neq 2)$ by Reed and Solomon [9]. Reed Solomon (RS) codes constituted a major advancement because their non binary nature allows for protection against bursts of errors. However, it was not until Berlekamp [10] introduced an efficient decoding algorithm that RS codes began to find practical applications. In his paper on the application of error control to communication, Berlekamp [10], realized that RS codes have found extensive applications in such systems as Compact Disk (CD) players, Digital Video Decoders (DVD) players, and the Cellular Digital Packet Data (CDPD).

Lin, *etal* [11] realized several fundamental drawbacks when block codes were in use. First, due to their frame oriented nature,the entire code word must be received before decoding can be completed. This introduces an intolerable lateness into the system, particularly for large block lengths. A second drawback was that block codes require precise frame synchronization. A third drawback was that most algebraic-based decoders for block codes work with hard-bit decisions, rather than with the unquantized, or â€œsoftâ€, outputs of the demodulator. With hard-decision decoding typical for block codes, the output of the channel is taken to be binary,while with soft-decision decoding the channel output is continuous-valued.

According to Lin, *etal* [11], in order to achieve the performance bounds predicted by Shannon [1] a continuous-valued channel output is required. While block codes can achieve impressive performance, they are typically not very power efficient, and therefore exhibit poor performance when the signal-to-noise ratio is low. The poor performance of block codes at low signal to -noise ratios is not a function of the code itself, but a function of the sub optimality of hard-decision decoding.

Elias [12] introduced convolution codes to solve the drawbacks of block codes. By segmenting data into distinct blocks, convolution codes add redundancy to a continuous stream of input data by using a linear shift register. Each set of n output bits is a linear combination of the current set of k input bits and the m bits stored in the shift register. The total number of bits that each output depends on is called the constraint length, and denoted by κ_c. The rate of the convolution encoder is the number of data bits κ taken in by the encoder in one coding interval, divided by the number of code bits n output during the same interval. Just as the data is continuously encoded,it can also be continuously decoded.

Convolution codes have been used by several deep space exploration such as Voyager and Pioneer. According to Odenwalder [13] a sub class of convolution codes has become a standard for commercial satellite communication applications. Berlekamp [10] noted that all of the second generation digital cellular standards incorporate convolution coding.

The major weakness of convolution codes is their susceptibility to burst errors. Convolution codes have properties that are complimentary to those of Reed-Solomon codes [9]. While convolution codes are susceptible to burst errors, RS codes handle burst errors quite well, Wicker [4]. Ungerboeck [14] discovered Trellis Coded Modulation (TCM) which use convolution codes and multidimensional signal constellations to achieve reliable communications over band limited channels. TCM have enabled telephone modems to break the 9600 bits per second (bps) barrier, and today all high speed modems use TCM. They are also used for satellite communication applications, Wicker [4]. TCM comes remarkably close to achieving Shannon's promise of reliable communications at channel capacity, and is now used for channels with high signal to noise ratio that require high bandwidth efficiency. Berrou and Glavieux [15] discovered Turbo codes. The performance of Turbo codes has helped in narrowing the gap between practical coding systems and Shannon's theoretical limit. A turbo code is the parallel concatenation of two or more component codes. In its original form, the constituent codes were from a subclass of convolution codes. Due to the presence of the inter leaver, optimal (maximal likelihood) decoding of turbo codes is complicated and therefore impractical. It is the decoding method that gives turbo codes their name, since the feedback action of the decoder resembles that of a turbo-charged engine. Turbo codes approach the capacity limit much more closely than any of the other codes.

Shannon's model [1] was developed using error coding techniques based on algebraic coding theory. According to his Theorem "Given a code with a code rate that is less than the communication channel capacity , a code exists for a block length of n bits, with code rate that can be transmitted over the channel with an arbitrarily small probability of error". Theoretically, we should be able to devise a coding scheme for a particular communication channel for any error rate, but no one has been able to develop a block code that satisfies Shannon's Theorem. While many previous results for polynomial effectiveness have been published, no previous work has attempted to achieve complete screening of all possible polynomials for error control. According to Castagnoli

etal [7] polynomial's effectiveness is evaluated by computing weights for that polynomial. A critical measurement of polynomial effectiveness for general purpose computing is the HD. Each undetectable error pattern is itself a codeword. This also means that determining the minimum HD for a polynomial is equivalent to determining the lowest non-zero weight for that polynomial. Furthermore, the weights of a polynomial give the number of undetectable errors for corresponding numbers of bit errors.

The candidate polynomials considered in this paper are ideals of the polynomial ring $F_2^n[x] mod(x^n - 1)$ with $1 \le n \le 31$. Castagnoli *etal* [7] utilized Fujiwara's [16] techniques to evaluate the weights of polynomials that had been carefully selected based on prime factorization characteristics. Lin and Costello [17] conjectured that there must be techniques for error control coding that could provide the best code. Alderson [18] introduced one of the techniques of using Geometric construction on optimal optical orthogonal codes.

Koopman [19] provided a standard for describing previous work and expected results. He recommended the following shorthand notation to represent factorization of a polynomial: $\{d_1,..,d_k\}$, where each $"d"$ represents the degree of a factor. Thus $"\{1,5,29\}"$ represents the set of all polynomials whose irreducible factorization is: $\hat{a}$ (i.e., has irreducible factors of degrees 1, 5, and 29).

Prange [6] showed that under polynomial addition, the polynomial rendering of a cyclic code is an ideal of some ring. This correspondence opened the way for the application of algebra to cyclic code. Fujiwara *etal* [16] developed cyclic codes based upon polynomials over finite fields.

Projective geometry and Shannon's Theorem have been used to determine and characterize the required types of ideals. Geometrical constructions of the code region has also been used to define a region which can provide these codes. Principal ideals which form the generator element in the polynomial ring were found very useful in this study. This research was primarily a determination and characterization of principal ideals of the polynomial ring which provide codes that satisfy Shannon Theorem.

Charles [20] improved on Prange's [6] work to show that polynomial addition and multiplication of cyclic codes were closed in polynomial rings. His work could also be used to confirm that the polynomial rendering of a cyclic code is an ideal of the polynomial ring .

According to Peterson and Weldon [21] a code can only be useful for computer application if and only if it is expressed in binary form or easily convertible into binary symbols. To be used for error detection a given polynomial code must have both a generator polynomial and a check polynomial.

Over the years the desire to reconcile efficiency and reliability of various code vectors has motivated researchers into this area of study. An exhaustive search for codes of ideals of polynomial rings has not been done. According to Castagnoli *etal* [7] there might be other forms of polynomials not explored which provide other similarly useful error detection and error correction capabilities. Internet Engineering Task Force (IETF) [22] filtered cyclic redundancy codes within the code region of 32-bit for greater HD. It singled out a class of polynomials of {1,3,28} with HD=6 as the best polynomial for the purpose of preserving message length while detecting errors at the same time. This was however a CRC Code and could not be used for error correction.

To date it is regrettable that no block code has been developed that precisely meets the promise of Shannon [1] of reconciling efficiency and reliability.

2 The Results

Definition 2.1

A nonempty subset I of a ring $F_2^n[x] mod(x^n - 1)$ shall be called an ideal of $F_2^n[x] mod(x^n - 1)$ 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 $r \in F_2^n[x] mod(x^n - 1)$, $ra \in I$.

The ring $F_2^n[x] mod(x^n - 1)$ itself and the subset consisting of 0 alone, which we denote by $\{0\}$, are ideals in this ring called trivial or improper ideals. An ideal $I \neq F_2^n[x] mod(x^n - 1)$ shall be called a proper ideal.

Since $F_2^n[x] mod(x^n - 1)$ is commutative, $ar = ra$, hence we need only check that $ra \in I$.

We say that an ideal I has closure since $a \pm b \in I \quad \forall a, b \in I$. We say that an ideal I absorbs elements from $F_2^n[x] mod(x^n - 1)$, since $ra, ar \in I \quad \forall a \in I$ and $\forall r \in F_2^n[x] mod(x^n - 1)$.

Proposition 2.2

A linear code C of length n over $F_2^n[x] mod(x^n - 1)$ is cyclic if and only if C satisfies the following two conditions:

(i) If $a(x)$ and $b(x)$ are code polynomials in C, then $a(x) \pm b(x) \in C$

(ii) If $a(x)$ is a code polynomial in C and $r(x)$ is any polynomial $\in F_2^n[x] mod(x^n - 1)$ of degree less than n, then $r(x)a(x) \in C$

Proof

Suppose C is a cyclic code of length n over $F_2^n[x] mod(x^n - 1)$, then C is linear, so Condition (i) holds.

Let $a(x) \in C$ and $r(x) = r_0 + r_1 x + \ldots r_{n-1} x^n - 1$, where $r_i \in F_2^n[x] mod(x^n - 1)$. Multiplication of a code polynomial by x corresponds to a right cyclic shift of the corresponding codeword. Since C is a cyclic code, it contains the cyclic shifts of all codewords, so $xa(x) \in C$. Similarly, $x^i c(x)$, (for $0 < i < n$), is the i^{th} cyclic shift of $c(x)$, so $x^i \ c(x) \in C$. Now, by the linearity of C, $r(x)a(x) = r_0 \ a(x) + r_1 xa(x) + \ldots + r_{n-1} x^{n-1} \ a(x) \in C$ since each summand is in C.

Therefore, condition (ii) also holds. So if C is a cyclic code, then conditions (i) and (ii) hold.

Conversely, suppose that conditions (i) and (ii) hold. Take $r(x)$ to be a scalar $\in F_2^n[x] mod(x^n - 1)$. The conditions imply that C is a linear code. Then, if we take $r(x) = x$, condition (ii) implies that C is a cyclic code. Hence, if conditions (i) and (ii) hold, then C is a cyclic code.

Proposition 2.3

Polynomial codes of length n over $F_2^n[x]$ correspond to ideals in the ring $F_2^n[x] mod(x^n - 1)$

Proof

Suppose C is a polynomial code of length n over $F_2^n[x]$. Then, the corresponding set of code polynomials $I(C)$ is contained in $F_2^n[x] mod(x^n - 1)$ since the polynomials are of degree less than n over $F_2^n[x]$. By Definition 2.1, to show that $I(C)$ forms an ideal in $F_2^n[x] mod(x^n - 1)$, we must show that:

(i) $0 \in I(C)$

(ii) $c(x) \pm d(x) \in I(C)$ for any code polynomials $c(x)$ and $d(x)$ in $I(C)$; and

(iii) $r(x)c(x) \in I(C)$ for any polynomial $r(x) \in F_2^n[x] \ /(x^n - 1)$ and $c(x) \in I(C)$.

By definition, the ring $F_2^n[x] mod(x^n - 1)$ itself and the subset consisting of 0 alone, which we

denote by $\{0\}$, are ideals in this ring called trivial or improper ideals. By Proposition 2.2 every cyclic code C does indeed satisfy conditions (ii) and (iii).

On the other hand, suppose that I is an ideal in $F_2^n[x] mod(x^n-1)$. Then its elements are polynomials of degree less than n, and by Definition, its elements satisfy (ii) $a(x) \pm b(x) \in$ I $\forall$ $a(x), b(x) \in$ I ; and (iii) $r(x)a(x) \in$ I $\forall$ $r(x) \in F_2^n[x] mod(x^n-1)$ and $\forall$ $a(x) \in$ I . Proposition 2.2 then shows that the set of polynomials $I(C)$ represent code polynomials of a cyclic code. Therefore, polynonial codes of length n over $F_2^n[x]$ are ideals in the ring $F_2^n[x] mode(x^n-1)$.

Proposition 2.4 [23]

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 $d_{(c)} \geq 2t+1$.

Table 2.5: Generator Polynomials of $F_2^{30}[x] mod(x^{30}-1)$

Generator Polynomial	Corresponding Codeword
	000000000000000000000000000000
1	000000000000000000000000000001
$x+1$	000000000000000000000000000011
x^2+1	000000000000000000000000000101
Generator Polynomial	**Corresponding Codeword**
x^8+x^6+	000000000000000000000000000111 000000000000000000000000001101

x^3+1	000000 000000000000 000000001001
x^4+x+	000000 000000000000 000000011011
x^5+x^4	000000 000000000000 000000111111
x^6+1	000000 000000000000 000001000001
x^5+x^4	000000 000000000000 000000110101
x^6+x^4	000000 000000000000 000001011111
x^6+x^5	000000 000000000000 000001111001
x^7+x^3	000000 000000000000 000010001011
x^8+x^7	000000 000000000000 000110011101
x^8+x^6	000000 000000000000 000101101111
x^9+x^8	000000 000000000000 001110110001
x^7+x^6	000000 000000000000 010011010011
$x^{12}+x^{1}$	000000 000000000001

$x^{13}+x^{12}$	
$x^{14}+x^{6}$	
$x^{20}+x^{19}$	
$+x^{3}+x$	
$x^{24}+x^{2}$	
$x^{28}+x^{2}$	
$+x^{13}+x$	
$x^{29}+x^{2}$	
$+x^{7}+x$	
$x^{2}+x+$	
$x^{4}+x^{2}$	000000000000000000000000010101
$x^{4}+x+$	000000000000000000000000010011
$x^{8}+x^{2}$	000000

	000000000000 000100000101
$x^4 + x^3$	000000 000000000000 000000011001
$x^8 + x^6$	000000000000 000000000101 000001
$x^4 + x^3$	000000000000 000000000000 011111
$x^8 + x^6$	000000000000 000000000101 001101

The codes in C are ideals of the polynomial ring $F_2^{30}[x] mod\left(x^{30}-1\right)$, $m = 31, n = 30, W_c = 30, d_c = 30, (n, m, d) = (30,31,30),$

By proposition 2.4 this code can detect 29 errors. It can correct 14 errors. It is suitable suitable for error control.

Table 2.6a: Relationship between κ and δ for $F_2^{30}[x]$ mod $\left(x^{30}-1\right)$

Weight	d	δ_c	κ_c
	0	0.0000	1.0000
	1	0.0333	0.9677
	2	0.0667	0.9333
	3	0.1000	0.9000
	4	0.1333	0.8667
	5	0.1667	0.8333
	6	0.2000	0.8000
	7	0.2333	0.7667
	8	0.2667	0.7333

Table 2.6b: Relationship between κ and δ for $F_2^{30}[x]$ mod$\left(x^{30}-1\right)$

Weight	d	δ_c	κ_c
	10	0.3333	0.6667
	13	0.4333	0.5633
	17	0.5667	0.4333
	30	1.000	0.0000

Graph 1: Graph of the Code region of $F_2^{30}[x]$ mod$\left(x^{30}-1\right)$

We could graph in $[0,1]\times[0,1]$, all pairs (δ_c,κ_c) determined by some code $C\in F_2^n[x]mod\left(x^n-1\right)$, but some of these correspond to codes which are not practical. For instance, the length 1 binary code $C=[0,1]$ has (δ_c,κ_c) = (1, 1) but it can neither detect nor correct any error. In this paper a code of length n is suitable for error control if and only if $n\geq 3$. The results become more meaningful when the length n is large enough.

Therefore, rather than graph all attainable pairs (δ_c,κ_c), we adopt the other extreme and consider only those pairs that can be realized by codes of arbitrarily large n. The point $(\delta,\kappa)\in[0,1]\times[0,1]$ belongs to the code region if and only if there is a sequence (C_n) of codes C_n with unbounded length n for which $\delta=\lim_{n\to\infty}\delta(C_n)$ and $\kappa=\lim_{n\to\infty}\kappa(C_n)$. The code region is therefore the set of all accumulation points in $[0,1]\times[0,1]$ of the graph of determined pairs (δ_c,κ_c).

By Manin's bound on the Code Region [24], there is a continuous non increasing function f_m on the interval [0, 1] such that the point (δ,κ) is in the code region if and only if $0\leq\kappa\leq f_m$.

If the point (δ,κ) is in the code region, then the code region should contain as well the points , (δ',κ) for $\delta'<\delta$, corresponding to codes with the same rate but smaller distance and also the points (δ,κ') for $\kappa'<\kappa$, corresponding to codes with the same distance but smaller rate. Thus for any point in the code region, the rectangle with corners $(0,0),(0,\kappa),(\delta,\kappa)$ and $(\delta,0)$ should be entirely contained within the code region. Any region with this property has its upper boundary function non increasing and continuous.

3 Acknowledgements

The first author acknowledges the co-authors for their meaningful and well done supervision. Their selflessness in giving scholarly comments and direction is invaluable. May God bless you. We thank The Government of Kenya through National Commission for Science Technology and Innovation for funding this research.

References

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

[2] Golay, M. J. E (1949) â€œNotes on digital coding,â€ Proc. IEEE, vol. 37, p. 657.

[3] Hamming, R.W.(1950) â€œError detecting and error correcting codes,â€ Bell Syst. Tech. J., vol. 29, pp. 147-150.

[4] Wicker,S.(1995), "Error Control Systems for Digital Communications and Storage",Englewood Cliffs, NJ: Prentice Hall, Inc.

[5] Muller, D. E.(1954), "Application of boolean algebra to switching circuit design," IEEE Trans. on Computers, vol. 3, pp. 6 - 12.

[6] Prange, E. (1957) â€œCyclic Error-Correcting Codes in Two Symbolsâ€, Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN-57-103.

[7] Castagnoli, G., Braeuer, S. and Herrman, M.(1993),"Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity

Bits", IEEE Trans. on Communications, Vol. 41, No. 6.

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

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

[10] Berlekamp,E.R.,Peile, R.E. and Pope,S. P.(1987) "The application of error control to communications,"IEEE Commun. Magazine, vol. 25, pp. 44 to 57.

[17] Lin,S. Kasami, T. Fujiwara,T and Fossorier,M (1998) Trellises and trellis based decoding algorithms for linear block codes. Kluwer Academic Publishers.

[12] Elias,P.(1955), "Coding for noisy channels," IRE Conv. Record, vol. 4, pp. 37 to 47

[13] Odenwalder,J. P.(1976), Error Control Coding Handbook. Linkabit Corporation.

[14] Ungerboeck,G. and Csajka,I(1976) "On improving data link performance by increasing the channel alphabet and introducing sequence coding," in Proc., IEEE Int. Symp. on Inform. Theory, (Ronneby, Sweeden).

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

[16] Fujiwara, T. Kasami, T. Kitai, A. and Lin, S. (1985), undetected error probability for Shortened hamming codes, IEEE Trans. On communications, Vol. 33, No.6, 1985, pp570-573.

[17] Lin, S. and Costello, (1983), Error Control Coding: Fundamentals and Applications. Prentice Hall.ISBN 0-13 283796-x,pp 19 - 201.

[18] Alderson, T.L. (2008), Geometric constructions of optimal Optical Orthogonal codes volume 2, No. 4, pp 451-467.

[19] Koopman, P. (2002), 32-Bit Cyclic Redundancy Codes for Internet Applications, Verification of Castagnoli's results by exhaustive search and some new good polynomials. The International Conference on Dependable Systems and Networks:459.Doi:1109/DSN.2002.1028931.

[20] Charles, C. (2000), Abstract Algebra second edition, McGraw Hill publishing Company, New York, USA,pp 25 - 292

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

[22] Internet Engineering Task Force,(2001) "IP Storage (ips)Charter," http://www.ietf.org/html.charters/ips-charter.htm,accessed Nov. 10, 2001.

[23] Salwach, C. J.(1988), Codes That Detect and Correct Errors, The College Mathematics Journal volume 19, No. 5, pp 402-416.

[24] Manin,Y.I.(1986),Cubic Forms 2nd Edition, North Holland Mathematical Library 4, North Holland Publishing Company.