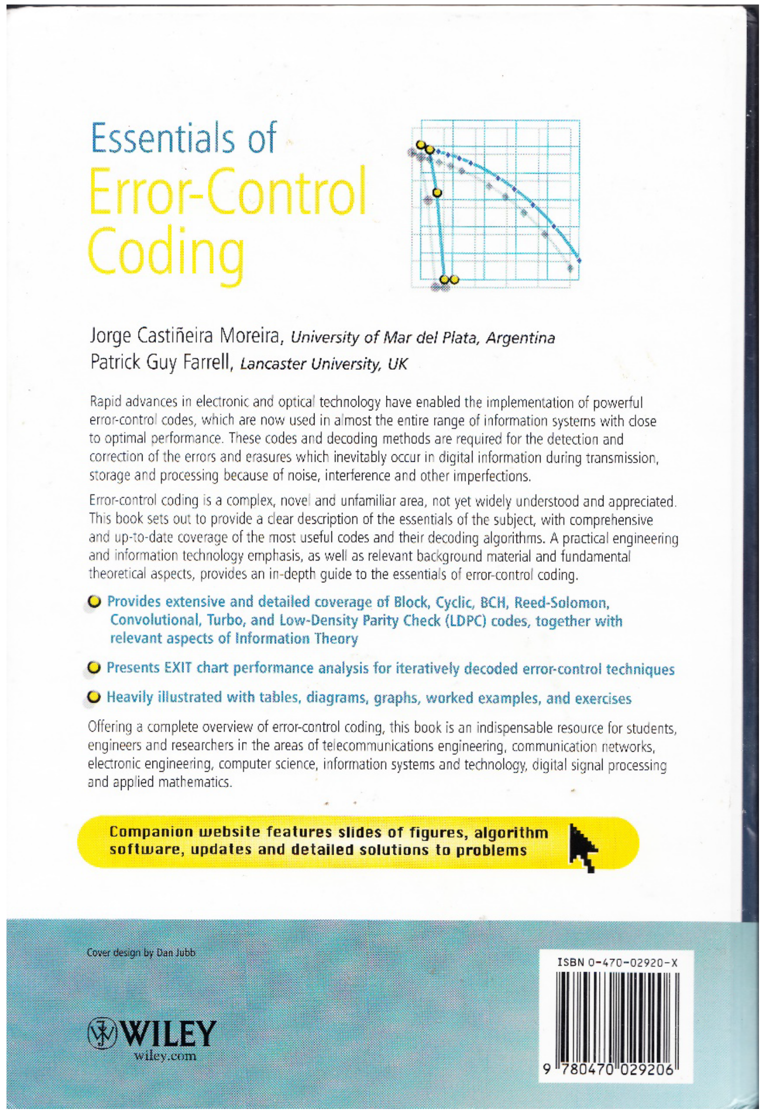
ECE 405/511
Error Control Coding

Introduction to Groups, Rings and Fields

ISBN Codes



Essentials of Error-Control Coding

Jorge Castiñeira Moreira, *University of Mar del Plata, Argentina*
Patrick Guy Farrell, *Lancaster University, UK*

Rapid advances in electronic and optical technology have enabled the implementation of powerful error-control codes, which are now used in almost the entire range of information systems with close to optimal performance. These codes and decoding methods are required for the detection and correction of the errors and erasures which inevitably occur in digital information during transmission, storage and processing because of noise, interference and other imperfections.

Error-control coding is a complex, novel and unfamiliar area, not yet widely understood and appreciated. This book sets out to provide a clear description of the essentials of the subject, with comprehensive and up-to-date coverage of the most useful codes and their decoding algorithms. A practical engineering and information technology emphasis, as well as relevant background material and fundamental theoretical aspects, provides an in-depth guide to the essentials of error-control coding.

- Provides extensive and detailed coverage of Block, Cyclic, BCH, Reed-Solomon, Convolutional, Turbo, and Low-Density Parity Check (LDPC) codes, together with relevant aspects of Information Theory
- Presents EXIT chart performance analysis for iteratively decoded error-control techniques
- Heavily illustrated with tables, diagrams, graphs, worked examples, and exercises

Offering a complete overview of error-control coding, this book is an indispensable resource for students, engineers and researchers in the areas of telecommunications engineering, communication networks, electronic engineering, computer science, information systems and technology, digital signal processing and applied mathematics.

Companion website features slides of figures, algorithm software, updates and detailed solutions to problems

Cover design by Dan Jubb

WILEY
wiley.com

ISBN 0-470-02920-X

9 780470 029206

The ISBN-10 Code

Most books have an International Standard Book Number which is a 10 digit codeword produced by the publisher with the following structure

l	p	m	w	=	$c_1 \ldots c_{10}$
language	publisher	number	weighted check sum		
0	470	02920	X		

such that $$\sum_{i=1}^{10} i c_i \equiv 0 \pmod{11} \qquad c_{10} = \sum_{i=1}^{9} i c_i \pmod{11}$$

An X is placed in the 10th position if $c_{10} = 10$

Example

- Essentials of Error Control Coding

  ISBN 0-470-02920-X

  0 - English

  470 - Wiley

$$c_{10} = \sum_{i=1}^{9} i c_i \pmod{11} = 120 \pmod{11} = 10$$

ISBN Errors

- Single Error Detection
  - Let **c** = $c_1 \ldots c_{10}$ be the correct codeword and let

    r = $c_1 \ldots c_{j-1}\, r_j\, c_{j+1} \ldots c_{10}$ with $r_j = c_j + x$, $x \neq 0$

$$\sum_{i=1}^{10} i r_i = \sum_{i=1}^{10} i c_i + jx \neq 0 \pmod{11}$$

- Transposition Error Detection
  - Let c_j and c_k be exchanged

$$\sum_{i=1}^{10} i r_i = \sum_{i=1}^{10} i c_i + (k-j)c_j + (j-k)c_k$$
$$= (k-j)(c_j - c_k) \neq 0 \pmod{11} \quad \text{if } k \neq j \text{ and } c_j \neq c_k$$

Erasure Example

- Received ISBN codeword:

  0-470-02e20-X

- Compute the parity equation:

$1\times0+2\times4+3\times7+4\times0+5\times0+6\times2+7\times e+8\times2+9\times0+10\times10 = 0 \bmod 11$

$7e+157 = 0 \bmod 11$

$7e+3 = 0 \bmod 11$

$7e = -3 \bmod 11$

$-3 = 8 \bmod 11 \rightarrow \; e = 8/7 \bmod 11 = 8\times8 \bmod 11$

$e = 64 \bmod 11 = 9$

Inverses Modulo 11

- Additive inverses

  $0+0 = 0, 1+10 = 0, 2+9 = 0, 3+8 = 0, 4+7 = 0, 5+6 = 0$

  – Every element has an additive inverse

- Multiplicative inverses

  $1 = 1^{-1}, 2 = 6^{-1}, 3 = 4^{-1}, 5 = 9^{-1}, 7 = 8^{-1}, 10 = 10^{-1}$

  $1\times1 = 1, 2\times6 = 1, 3\times4 = 1, 5\times9 = 1, 7\times8 = 1, 10\times10 = 1$

  – Every nonzero element has a multiplicative inverse

Groups

Definition A **group** $(G,\bullet)$ is a set of objects G on which a binary operation $\bullet$ is defined: $a\bullet b \in G$ for all $a,b \in G$

The operation must satisfy the following requirements:

(i) Associativity: $a\bullet(b\bullet c) = (a\bullet b)\bullet c$

(ii) Identity: there exists $e \in G$ such that for all $a \in G$,
$a\bullet e = e\bullet a = a$ e: identity element of G

(iii) Inverse: for all $a \in G$, there exists a unique element, $a^{-1} \in G$ such that $a\bullet a^{-1} = a^{-1}\bullet a = e$ a^{-1} : inverse of a

A group is said to be **commutative** or **abelian** if it also satisfies
(iv) for all $a,b \in G$, $a\bullet b = b\bullet a$

Niels Henrik Abel (1802-1829)

Examples

- (Z,+) integers with addition
  - identity 0, $a^{-1} = -a$
- (Z_n,+) integers modulo n with addition
  - identity 0, $a^{-1} = n-a$ ($0^{-1} = 0$)
  - (Z_4,+)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- What about (R,•)? Multiplication with R the real numbers

  No, 0 has no inverse

Integers Modulo p and Multiplication

- The set S = {1,2, …, *p*-1} and multiplication modulo *p* is a commutative group if and only if *p* is prime
- Example: *p* = 5

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Order of Group Elements

The cardinality of the group is called the **order**

Definition Let g be an element in $(G,\bullet)$.
Let $g^1 = g$, $g^2 = g\bullet g$, $g^3 = g\bullet g\bullet g$, …
The order of g is the smallest positive integer

$$\mathrm{ord}(g)$$

such that $g^{\mathrm{ord}(g)}$ is the identity element.

Order of Group Elements

- (Z_4,+) integers modulo 4 with addition
  - identity 0
  - 0 = 0 order of 0 is 1
  - 1+1+1+1 = 0 order of 1 is 4
  - 2+2 = 0 order of 2 is 2
  - 3+3+3+3=0 order of 3 is 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Order of the group elements divides the group order

Binary Linear Block Codes

- Binary linear block codes are also called

  Group Codes
- Operation is codeword addition
- Identity is the all-zero codeword
- The inverse of a codeword **c** is?

  c as **c** + **c** = **0**

Rings

Definition A **ring** (R,+,•) is a set of objects R on which **two** binary operations + and • are defined. The following three properties hold:

1. (R,+) is a commutative group under + with identity \`0´
2. The operation • is associative
   $$a \bullet (b \bullet c) = (a \bullet b) \bullet c \quad \text{for all } a, b, c \in R$$
3. The operation • distributes over +
   $$a \bullet (b + c) = (a \bullet b) + (a \bullet c)$$

Rings

A ring is said to be a **commutative ring** if

4. The operation • commutes $a \bullet b = b \bullet a$

A ring is said to be a **ring with identity** if

5. The operation • has an identity element `1′

A ring that satisfies both properties 4 and 5 is said to be a **commutative ring with identity** or a **commutative, unitary ring**

Commutative, Unitary Ring Z_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Additive identity is 0

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Multiplicative identity is 1

Ring Examples

- $(Z_n,+,\bullet)$
  - additive identity is 0
  - multiplicative identity is 1
- $F_2[x]$ – polynomials with binary coefficients under polynomial addition and multiplication
  - additive identity is 0
  - multiplicative identity is 1
- $n \times n$ square matrices with integer elements
  - additive identity is the all-zero matrix 0_n
  - multiplicative identity is the identity matrix I_n

Rings

- Let R* = R - {0}
- If in addition to property 5

  (R*,•) is a **group,** the ring is said to be a **division ring**
- If (R*,•) is a **commutative group,** the ring is said to be a **field**

Fields

Definition A **field** (F,+,•) is a set of objects F on which two binary operations + and • are defined. F is said to be a field if and only if:

1. (F,+) is a commutative group under + with additive identity `0´
2. (F*,•) is a commutative group under • with multiplicative identity `1´
3. The operation • distributes over +

$$a \bullet (b+c) = (a \bullet b) + (a \bullet c)$$

Field Examples

- Rational numbers (Q,+,•)
- Real numbers (R,+,•)
- Complex numbers (C,+,•)

- These are infinite fields

Smallest Possible Field

$(Z_2, +, \bullet)$

$+$	0	1
0	0	1
1	1	0

$\bullet$	0	1
0	0	0
1	0	1

Finite Fields

- Finite fields were discovered by Evariste Galois and thus are also known as **Galois fields**
- The cardinality of the field is called the **order**
- A finite field of order *q* is denoted GF(*q*) or F_q
- Example: GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Evariste Galois (1811-1832)

Finite Fields

- Theorem The integers S = {0,1,2, ..., p-1} where p is a prime form the field GF(p) under modulo p addition and multiplication
- (Z_n,+,•) n prime

- Are there any other finite fields?

Properties of Finite Fields

- Let β be a nonzero element of GF(q) and let 1 be the multiplicative identity
- Definition The order of β is the smallest positive integer m such that $\beta^m = 1$
- Theorem If t = ord(β) then $t \mid (q-1)$
- Definition In any finite field, there are one or more elements of order q-1 called primitive elements

- Example: GF(5)

  S = {0,1,2,3,4} with modulo 5 addition and multiplication

- Order of the elements of the multiplicative group

$$1^1 = 1$$

$$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3 \quad \boxed{2^4 = 1}$$

$$3^1 = 3 \quad 3^2 = 4 \quad 3^3 = 2 \quad \boxed{3^4 = 1}$$

$$4^1 = 4 \quad 4^2 = 1$$

2 and 3 are primitive elements

- The number of elements of order t is given by Euler's totient function $\phi(t)$

Euler's Totient Function $\phi(t)$

- Consider the number of positive integers less than t which are relatively prime to t
  - Example: $t = 10$
  - complete set of values {1,2,3,4,5,6,7,8,9}
  - Relatively prime values {1,3,7,9}
- The number of elements in the set that are relatively prime to t is given by Euler's totient function $\phi(t)$
  - $\phi(10) = 4$

Euler's Totient Function ø(t)

- to compute ø(t), consider the number of elements to be excluded
- in general the prime factorization of t is needed
  - for a prime p ø(p) = p-1
- examples
  - ø(37) = 36
  - ø(31) = 30
  - ø(1) = 1

Euler's Totient Function ø(*t*)

Definition

$$\phi(t) = t \prod_{\substack{p|t \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

$$\phi(6) = \phi(2 \cdot 3) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 2$$

1,5 relatively prime to 6

$$\phi(15) = \phi(3 \cdot 5) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8$$

1,2,4,7,8,11,13,14 relatively prime to 15

$$\phi(63) = \phi(3 \cdot 3 \cdot 7) = 63\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 36$$

- The number of elements in GF(q) of order t is ø(t)
- In GF(q), there are exactly ø(q-1) elements of order q-1
- A primitive element α is an element of order q-1 and $\alpha^{q-1} = 1$
- Therefore, the q-1 elements

$$1, \alpha, \alpha^2, \cdots, \alpha^{q-2}$$

must be the non-zero elements of GF(q)

Example GF(5)

- q-1=4 nonzero elements {1,2,3,4}

$$1^1 = 1 \quad \text{order 1}$$

$$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3 \quad 2^4 = 1 \quad \text{order 4}$$

$$3^1 = 3 \quad 3^2 = 4 \quad 3^3 = 2 \quad 3^4 = 1 \quad \text{order 4}$$

$$4^1 = 4 \quad 4^2 = 1 \quad \text{order 2}$$

$$\phi(1) = 1 \quad \phi(2) = 1 \quad \phi(4) = 2$$

- All non-zero elements of GF(5) are given by 4 consecutive powers of 2 or 3.

ECE 405/511 Test

- Friday, February 17, 2023 10:30 AM
  - constitutes 20% of the final grade
- Test will cover material up to bounds on codes
- Shortening and extending are included but not the Hamming, Gilbert, and Gilbert-Varshamov bounds.
  - Moreira and Farrell Chapter 2 (not Section 2.11)
  - Assignments 1 and 2 (Problems 1-4)
- Aids allowed: 1 sheet of paper 8.5×11 in^2
calculator

Non-Prime Finite Fields

- Theorem A finite field exists for all prime powers - GF(p^m)
- How to construct non-prime fields?
- Consider all m-tuples (vectors of length m) over GF(p) $(a_0, a_1, \cdots, a_{m-1})$
  – Number of m-tuples is p^m
  – Addition is just element by element (vector) addition modulo p
  – How to do multiplication?

- Consider the elements of GF(p^m) as polynomials over GF(p) of degree less than m

$$f(x) = a_0 + a_1 x + \ldots + a_{m-2} x^{m-2} + a_{m-1} x^{m-1}$$

- Addition is still element by element addition modulo p (the polynomial exponents are only placeholders)
- But, multiplication can produce a result of degree greater than m-1

Solution

- Multiplication can be done modulo a polynomial p(x) of degree m, for example with m=2

$$x(x+1)=x^2+x$$

← Polynomial has degree greater than m-1=1

- If we choose $\mathrm{p}(x)=x^2+1$

$$x(x+1)=x^2+x \bmod (x^2+1)=x+1$$

$$(x+1)(x+1)=x^2+1 \bmod (x^2+1)=0$$

← doesn't work

this is because $\mathrm{p}(x)=x^2+1=(x+1)(x+1)$ is not irreducible over GF(2)

Irreducible Polynomials

- x^2+1 has no real roots (no roots in R)
- $x^2+1 = (x+\mathrm{j})(x-\mathrm{j})$ $\mathrm{j} = \sqrt{-1}$ (roots in C)

- x^2+x+1 has no roots in GF(2)[x]
- x^2+x+1 has roots in GF(3)[x]

  $x^2+x+1 = (x+2)(x+2)$
- x^2+1 has no roots in GF(3)[x]
- x^2+1 has roots in GF(2)[x]

  $x^2+1 = (x+1)(x+1)$

- With $p(x) = x^2 + 1$

+	1	x	x+1	0
1	0	x+1	x	1
x	x+1	0	1	x
x+1	x	1	0	x+1
0	1	x	x+1	0

•	1	x	x+1
1	1	x	x+1
x	x	1	x+1
x+1	x+1	x+1	0

- With $p(x) = x^2 + x + 1$ irreducible in GF(2)

+	1	x	x+1	0
1	0	x+1	x	1
x	x+1	0	1	x
x+1	x	1	0	x+1
0	1	x	x+1	0

•	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

- Requirement: an element of order $q-1=p^m-1$ to construct the multiplicative group of GF(q)
- Consider the powers of x modulo an irreducible polynomial p(x)

$$x^0=1$$

$$x^1=x$$

$$x^2=x^2$$

$$\vdots$$

$$x^{p^m-1} \bmod \mathrm{p}(x)=1 \quad \text{or} \quad \mathrm{p}(x) \mid x^{p^m-1}-1$$

which means that $\mathrm{p}(x)\mathrm{q}(x)=x^{p^m-1}-1$

- The smallest n such that $\mathrm{p}(x) \mid x^n - 1$ is called the order of p(x)
- We require an irreducible polynomial p(x) such that the smallest positive integer n for which p(x) divides x^n-1 is

$$n = p^m - 1$$

This is called a primitive polynomial

- The order of a primitive polynomial p(x) is

$$p^m - 1$$

- Definition The roots of a degree *m* primitive polynomial are primitive elements in GF(p^m)
- Let α be a root of p(*x*), a primitive polynomial over GF(2) of degree *m*
- Then $\alpha^{2^m-1} - 1 = 0$

  or $\alpha^{2^m-1} = 1$

- Thus $1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}$ are distinct and closed under multiplication

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^{(2^m-1)+r} = \alpha^{(2^m-1)}\alpha^r = \alpha^r$$

Example GF(4)=GF(2^2)

- Take a primitive polynomial of degree 2 over GF(2)

  $$p(x) = x^2+x+1$$

  Let α be a root of p(x), then

  $$\alpha^2+\alpha+1=0$$

  or

  $$\alpha^2= \alpha+1$$

- The field elements are 0, 1, α, $\alpha^2= \alpha+1$

GF(4)=GF(2^2), p(x) = 1 + x + x^2 (p(α) = 1 + α + α^2 = 0)

Power representation	Polynomial representation	2-tuple representation	Integer representation
$\alpha^{-\infty}=0$	0	(0 0)	0
$\alpha^0=1$	1	(1 0)	1
α	α	(0 1)	2
α^2	1 + α	(1 1)	3
α^3	1	(1 0)	1

Note: $\alpha^3 = \alpha^2 \cdot \alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$

GF(4) using the Integer Labels

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Additive identity is 0

$\bullet$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Multiplicative identity is 1

$0 = 0 \qquad 1 = 1$

$\alpha = 2 \qquad \alpha^2 = 3$

$GF(8) = GF(2^3)$, $p(x) = 1 + x + x^3$ ($p(\alpha) = 1 + \alpha + \alpha^3 = 0$)

Power representation	Polynomial representation	3-tuple representation	
0	0	(0 0 0)	0
1	1	(1 0 0)	1
α	α	(0 1 0)	2
α^2	α^2	(0 0 1)	4
α^3	$1 + \alpha$	(1 1 0)	3
α^4	$\alpha + \alpha^2$	(0 1 1)	6
α^5	$1 + \alpha + \alpha^2$	(1 1 1)	7
α^6	$1 + \alpha^2$	(1 0 1)	5
α^7	1	(1 0 0)	1

Integer representation

More About GF(8)

- primitive polynomial $p(x) = x^3+x+1$
- Roots of $p(x)$ are α, α^2, α^4
- $(x+\alpha)(x+\alpha^2)(x+\alpha^4) = (x^2+(\alpha+\alpha^2)x+\alpha^3)(x+\alpha^4)$

$$= (x^2+\alpha^4 x+\alpha^3)(x+\alpha^4)$$

$$= (x^3+(\alpha^4+\alpha^4)x^2+(\alpha^8+\alpha^3)x+\alpha^7$$

$$= x^3+x+1$$

- The number of primitive elements in GF(8) is $\phi(q\text{-}1) = \phi(7) = 6$
- The roots of a primitive polynomial are primitive elements
- Therefore the number of primitive polynomials of degree 3 is 6/3 = 2
- What is the other primitive polynomial?

- If α is a primitive element, so is α^{-1}
- $\alpha^{-1} = \alpha^{7-1} = \alpha^6$
- $\alpha^{-2} = \alpha^{7-2} = \alpha^5$
- $\alpha^{-4} = \alpha^{7-4} = \alpha^3$
- $(x+\alpha^6)(x+\alpha^5)(x+\alpha^3) = (x^2+(\alpha^6+\alpha^5)x+\alpha^4)(x+\alpha^3)$

$$= (x^2+\alpha x+\alpha^3)(x+\alpha^3)$$

$$= (x^3+(\alpha+\alpha^3)x^2+(\alpha^4+\alpha^4)x+\alpha^7$$

$$= x^3+x^2+1$$

- If p(x) is primitive, so is the reciprocal polynomial

$$p^*(x) = x^m p(x^{-1})$$

Binary Primitive Polynomials

- The number of binary primitive polynomials of degree m is $\phi(q-1)/m$ where $q = 2^m$

x^2+x+1

x^3+x+1, x^3+x^2+1

x^4+x+1, x^4+x^3+1

x^5+x^2+1, x^5+x^3+1, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$

x^6+x+1,x^6+x^5+1,$x^6+x^4+x^3+x+1$,$x^6+x^5+x^3+x^2+1$,$x^6+x^5+x^2+x+1$,$x^6+x^5+x^4+x+1$

GF(16)=GF(2^4), $p(x) = 1 + x + x^4$ ($p(\alpha) = 1 + \alpha + \alpha^4 = 0$)

Power representation	Polynomial representation	4-tuple representation	
0	0	(0 0 0 0)	0
1	1	(1 0 0 0)	1
α	α	(0 1 0 0)	2
α^2	α^2	(0 0 1 0)	4
α^3	α^3	(0 0 0 1)	8
α^4	$1+\alpha$	(1 1 0 0)	3
α^5	$\alpha+\alpha^2$	(0 1 1 0)	6
α^6	$\alpha^2+\alpha^3$	(0 0 1 1)	12
α^7	$1+\alpha+\alpha^3$	(1 1 0 1)	11
α^8	$1+\alpha^2$	(1 0 1 0)	5
α^9	$\alpha+\alpha^3$	(0 1 0 1)	10
α^{10}	$1+\alpha+\alpha^2$	(1 1 1 0)	7
α^{11}	$\alpha+\alpha^2+\alpha^3$	(0 1 1 1)	14
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	(1 1 1 1)	15
α^{13}	$1+\alpha^2+\alpha^3$	(1 0 1 1)	13
α^{14}	$1+\alpha^3$	(1 0 0 1)	9

Integer representation

$\alpha^{15} = 1$

Table F-1: Equivalence of Representations[4,5]

POWER	POLY IN ALPHA	$\ell_{01234567}$	POWER	POLY IN ALPHA	$\ell_{01234567}$
*	00000000	00000000	31	11001101	01111010
0	00000001	01111011	32	00011101	10011110
1	00000010	10101111	33	00111010	00111111
2	00000100	10011001	34	01110100	00011100
3	00001000	11111010	35	11101000	01110100
4	00010000	10000110	36	01010111	00100100
5	00100000	11101100	37	10101110	10101101
6	01000000	11101111	38	11011011	11001010
7	10000000	10001101	39	00110001	00010001
8	10000111	11000000	40	01100010	10101100
9	10001001	00001100	41	11000100	11111011
10	10010101	11101001	42	00001111	10110111
11	10101101	01111001	43	00011110	01001010
12	11011101	11111100	44	00111100	00001001
13	00111101	01110010	45	01111000	01111111
14	01111010	11010000	46	11110000	00001000
15	11110100	10010001	47	01100111	01001110
16	01101111	10110100	48	11001110	10101110
17	11011110	00101000	49	00011011	10101000
18	00111011	01000100	50	00110110	01011100
19	01110110	10110011	51	01101100	01100000
20	11101100	11101101	52	11011000	00011110
21	01011111	11011110	53	00110111	00100111
22	10111110	00101011	54	01101110	11001111
23	11111011	00100110	55	11011100	10000111
24	01110001	11111110	56	00111111	11011101
25	11100010	00100001	57	01111110	01001001
26	01000011	00111011	58	11111100	01101011
27	10000110	10111011	59	01111111	00110010
28	10001011	10100011	60	11111110	11000100
29	10010001	01110000	61	01111011	10101011
30	10100101	10000011	62	11110110	00111110

[4] From table 4 of reference [E4]. Note: Coefficients of the 'Polynomial in Alpha' column are listed in descending powers of α, starting with α^7.

[5] The underlined entries correspond to values with exactly one non-zero element and match a row in the matrix.