

ELEC 405

Error Control Coding and Sequences

Introduction to Groups, Rings
and Fields

ISBN Codes

ERROR CONTROL SYSTEMS for Digital Communication and Storage

Stephen B. Wicker

Both students and practicing engineers will benefit from the information in this self-contained survey of error control. Current and complete with biographical references, it can serve as a starting point for those conducting graduate-level work in error control coding. As an applications-oriented text, it provides the background necessary to design and implement error control subsystems for digital communication systems. Finally, it includes a tutorial on trellis coded modulation and an up-to-date treatment of ARQ protocols.

Containing four basic parts (finite field theory, block codes, convolutional/trellis codes, and system design), **Error Control Systems for Digital Communication and Storage:**

- Provides an introduction to Galois fields and polynomials with coefficients over Galois fields (Chapters 2-3).
- Covers the various types of block error control codes that are currently being used or show promise of use in the future, including BCH and Reed-Solomon (Chapters 4-9).
- Treats convolutional codes and their trellis coded progeny; presents the design and performance of the Viterbi and sequential decoding algorithms; discusses the design and use of rate compatible punctured convolutional codes; and offers chapter-length treatment of trellis codes (Chapters 11-14).
- Discusses the various means for analyzing the performance of block codes over a variety of channels, particularly the slowly fading channel; examines retransmission request systems that make use of the various block, convolutional, and trellis codes; and explores some specific design applications, including the Compact Disc™ player and the magnetic recording channel (Chapters 1, 10, 15-16).

PRENTICE HALL
Englewood Cliffs, NJ 07632

ISBN 0-13-200809-2



The ISBN 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	=	$c_1 \dots c_{10}$
language	publisher	number	weighted check sum		
0	13	200809	2		

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

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

ISBN Errors

- Single Error Detection

- Let $\mathbf{c} = c_1 \dots c_{10}$ be the correct codeword and let

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

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

- Transposition Error Detection

- Let c_j and c_k be exchanged

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

Erasure Example

- Received ISBN codeword:

0-13-200e09-2

- Compute the parity equation:

$$1x0+2x1+3x3+4x2+5x0+6x0+7xe+8x0+9x9+10x2 = 0 \text{ mod } 11$$

$$7e+120 = 0 \text{ mod } 11$$

$$7e+10 = 0 \text{ mod } 11$$

$$e = -10/7 \text{ mod } 11$$

$$-10 = 1 \text{ mod } 11 \quad 1/7 = 8 \text{ mod } 11$$

$$e = 1 \times 8 = 8$$

Inverses Modulo 11

- Additive inverses

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

- Every element has an additive inverse

- Multiplicative inverses

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

$$1 \times 1 = 1, 2 \times 6 = 1, 3 \times 4 = 1, 5 \times 9 = 1, 7 \times 8 = 1, 10 \times 10 = 1$$

- Every nonzero element has a multiplicative inverse

Groups

Definition 2.1 A **group** (G, \cdot) is a set of objects G on which a binary operation \cdot is defined: $a \cdot b \in G$ for all $a, b \in G$

The operation must satisfy the following requirements:

- (i) Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (ii) Identity: there exists $e \in G$ such that for all $a \in G$,
 $a \cdot e = e \cdot a = a$ e : identity element of G
- (iii) Inverse: for all $a \in G$, there exists a unique element, $a^{-1} \in G$
such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ a^{-1} : inverse of a

A group is said to be **commutative** or **abelian** if it also satisfies

- (iv) for all $a, b \in G$, $a \cdot b = b \cdot a$

Niels Henrik Abel (1802-1829)





Examples

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

+	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 (\mathbb{R}, \cdot) ?

Integers Modulo p and Multiplication

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

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Linear Block Codes

- Linear Block Codes are also called
Group Codes
- Operation is codeword addition
- Identity is all-zero codeword
- The inverse of a codeword c is ?

Rings

Definition 2.4 A **ring** $(R, +, \cdot)$ is a set of objects R on which two binary operations $+$ and \cdot are defined. The following three properties hold:

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

Rings

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

4. The operation \cdot commutes $a \cdot b = b \cdot a$

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

5. The operation \cdot has an identity element '1'

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

Commutative, Unitary Ring \mathbb{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

- $(\mathbb{Z}_n, +, \cdot)$
- $F_2[x]$ – polynomials with binary coefficients under polynomial addition and multiplication
- $n \times n$ square matrices
 - additive identity is the all-zero matrix
 - multiplicative identity is the identity matrix

Rings

- Let $R^* = R - \{0\}$
- If in addition to properties 4 and 5, (R^*, \cdot) is a **group**, the ring is said to be a **division ring**
- If (R^*, \cdot) is a **commutative group**, the ring is said to be a **field**

Fields

Definition 2.5 A **field** $(F, +, \cdot)$ is a set of objects F on which two binary operations $+$ and \cdot 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^*, \cdot) is a commutative group over \cdot with multiplicative identity 1
3. The operation \cdot distributes over $+$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Field Examples

- The rational numbers $(\mathbb{Q}, +, \cdot)$
- The real numbers $(\mathbb{R}, +, \cdot)$
- The complex numbers $(\mathbb{C}, +, \cdot)$

- These are infinite fields

Smallest Possible Field

$$(\mathbb{Z}_2, +, \cdot)$$

$+$	0	1
0	0	1
1	1	0

\cdot	0	1
0	0	0
1	0	1

Evariste Galois (1811-1832)



Finite Fields

- Finite fields were discovered by Evariste Galois and thus are 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
- Ex: $GF(3)$

+	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

Finite Fields

- **Theorem 2.5** The integers $S = \{0, 1, 2, \dots, p-1\}$ where p is a prime, form the field $GF(p)$ under modulo p addition and multiplication
- $(\mathbb{Z}_n, +, \cdot)$ 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 2-12** The **order** of β is the smallest positive integer m such that $\beta^m = 1$
- **Theorem 2-10** If $t = \text{ord}(\beta)$ then $t \mid (q-1)$
- **Definition 2-14** 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

$$1^1 = 1$$

$$\begin{array}{llll}
 2^1 = 2 & 2^2 = 4 & 2^3 = 3 & 2^4 = 1 \\
 3^1 = 3 & 3^2 = 4 & 3^3 = 2 & 3^4 = 1 \\
 4^1 = 4 & 4^2 = 1 & &
 \end{array}$$

← 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 $\phi(t)$**

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

- to compute $\phi(t)$, count the number of elements to be excluded
- in general need prime factorization
 - for p prime $\phi(p) = p-1$
- examples
 - $\phi(37) = 36$
 - $\phi(31) = 30$
 - $\phi(1) = 1$

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

- **Definition 2-19**
$$\phi(t) = t \prod_{\substack{p|t \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

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

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 $\phi(t)$
- In $GF(q)$, there are exactly $\phi(q-1)$ primitive elements
- A primitive element α is an element of order $q-1$. This means that $\alpha^{q-1} = 1$
- Therefore, the $q-1$ elements

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

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

Example GF(5)

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

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

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

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

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

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

$$2 \cdot 3 = 2^1 \cdot 2^3 = 2^4 = 1$$

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

Non-Prime Finite Fields

- **Theorem 2-14** A finite field exists for all prime powers - $\text{GF}(p^m)$
- How to construct nonprime fields?
- Consider all m -tuples (vectors of length m) over $\text{GF}(p)$ $(a_0, a_1, \dots, a_{m-1})$
 - Number of m -tuples is p^m
 - Addition is just element by element addition modulo p
 - How to do multiplication?

- Consider the elements of $\text{GF}(p^m)$ as polynomials over $\text{GF}(p)$ of degree less than m

$$f(x) = a_0 + a_1x + \dots + a_{m-2}x^{m-2} + a_{m-1}x^{m-1}$$

- 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 $m=2$

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

Polynomial has degree greater than $m-1=1$

- If we choose $p(x) = x^2 + 1$

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

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

doesn't work

this is because $p(x) = x^2 + 1 = (x+1)(x+1)$ is not **irreducible** over GF(2)

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

\cdot	1	x	$x+1$
1	1	x	$x+1$
x	x	1	$x+1$
$x+1$	$x+1$	$x+1$	0

$+$	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

- Choose $p(x) = x^2 + x + 1$ irreducible in $\text{GF}(2)$

\cdot	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

$+$	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

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

$$x^0 = 1$$

$$x^1 = x$$

$$x^2 = x^2 \dots$$

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

- Thus 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 $p(x)$ is $p^m - 1$

A primitive element can be used to construct $GF(2^m)$

- Start with $0, 1 \Rightarrow GF(2)$ (two identities – elements of the ground field)
- take a new symbol α and its powers
- require 2^m elements

$$\{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$$

- How to find α ?

- Let α be a root of $p(x)$, a primitive polynomial over $\text{GF}(2)$ of degree m
- Then $\alpha^{2^m-1} - 1 = 0$
or $\alpha^{2^m-1} = 1$
- Thus, $\alpha, \alpha^2, \dots, \alpha^{2^m-2}$ are distinct and are closed under multiplication

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^{(2^m-1)+r} = \alpha^{(2^m-1)} \alpha^r = \alpha^r$$
- **Definition 2-15** The roots of a degree m primitive polynomial are primitive elements in $\text{GF}(p^m)$

Example $\text{GF}(4)=\text{GF}(2^2)$

- Take a primitive polynomial of degree 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 $0, 1, \alpha, \alpha^2= \alpha+1$

$$\text{GF}(4)=\text{GF}(2^2), p(x) = 1 + x + x^2 \quad p(\alpha) = 1 + \alpha + \alpha^2 = 0$$

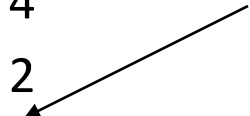
Power representation	Polynomial representation	2-tuple representation	Integer representation
0	0	(0 0)	0
1	1	(1 0)	2
α	α	(0 1)	1
α^2	$1 + \alpha$	(1 1)	3
α^3	1	(1 0)	2

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

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

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

Integer representation



More About GF(8)

- primitive polynomial $p(x) = x^3+x+1$
- Roots of $p(x)$ are $\alpha, \alpha^2, \alpha^4$
- $$\begin{aligned}(x+\alpha)(x+\alpha^2)(x+\alpha^4) &= (x^2+(\alpha+\alpha^2)x+\alpha^3)(x+\alpha^4) \\ &= (x^2+\alpha^4x+\alpha^3)(x+\alpha^4) \\ &= (x^3+(\alpha^4+\alpha^4)x^2+(\alpha^8+\alpha^3)x+\alpha^7) \\ &= x^3+x+1\end{aligned}$$

- The number of primitive elements in $GF(8)$ is $\phi(q-1) = \phi(7)=6$
- 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}
- $\alpha^{-1} = \alpha^{7-1} = \alpha^6$
- $\alpha^{-2} = \alpha^{7-2} = \alpha^5$
- $\alpha^{-4} = \alpha^{7-4} = \alpha^3$
- $$\begin{aligned} (x+\alpha^6)(x+\alpha^5)(x+\alpha^3) &= (x^2+(\alpha^6+\alpha^5)x+\alpha^4)(x+\alpha^3) \\ &= (x^2+\alpha x+\alpha^3)(x+\alpha^3) \\ &= (x^3+(\alpha+\alpha^3)x^2+(\alpha^4+\alpha^4)x+\alpha^7) \\ &= x^3+x^2+1 \end{aligned}$$
- If $p(x)$ is primitive, so is $p^*(x) = x^m p(x^{-1})$

Binary Primitive Polynomials

- Number of primitive polynomials of degree m is $\phi(q-1)/m$

$$x^2+x+1$$

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

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

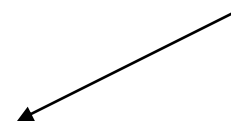
$$x^5+x^2+1, x^5+x^3+1, x^5+x^3+x^2+x+1, x^5+x^4+x^3+x^2+1, x^5+x^4+x^2+x+1, x^5+x^4+x^3+x+1$$

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

$$\text{GF}(2^4), p(x) = 1 + x + x^4 \quad (p(\alpha) = 1 + \alpha + \alpha^4 = 0)$$

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

Integer representation



$$\alpha^{15} = 1$$

Example: GF(5)

- There are four nonzero elements $\{1,2,3,4\}$
- $\phi(p-1) = \phi(4) = 2$
- $2 \mid 4$ and $\phi(2) = 1$
- $1 \mid 4$ and $\phi(1) = 1$

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1