4.0 Cyclic Codes

4.1 Informal Definition

Definition 1 *A code C is a* **cyclic code** *if every cyclic shift of* $\mathbf{c}$ *also belongs to* $\mathcal{C}$.

$\square$

That is, if $\mathcal{C}$ is cyclic,

- $(a, b, c) \in \mathcal{C} \Rightarrow (b, c, a) \in \mathcal{C}$;
- recursively so.

We will study linear cyclic codes. **Why?**

- Cyclic code words are easily generated?
  - They are, but *that's not the reason.*
- Cyclic codes have a **rich, complex structure** which permits the coding theorist and the engineer to:
  1. understand precisely the *performance* and *limitations* of the code, and
  2. study classes and families of cyclic codes that have properties specific to an application.

Definition 2 *For a cyclic code $\mathcal{C}$,*

$$(c_0, c_1, \ldots c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \ldots c_{n-2}) \in \mathcal{C}.$$

$\square$

- Let us represent a cyclic code word of length n by a polynomial of degree $n-1$:

$$\begin{aligned} \mathbf{c} &= (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \\ c(x) &= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathcal{C} \end{aligned}$$

- or 2 *equivalent* notations for the same concept.
- So, in addition to $c(x)$,

$$\begin{aligned} & c_{n-1} + c_0 x + c_1 x^2 \cdots + c_{n-2} x^{n-1} \in \mathcal{C} \\ & c_{n-2} + c_{n-1} x + c_0 x^2 \cdots + c_{n-3} x^{n-1} \in \mathcal{C} \\ & c_1 + c_2 x + \cdots + c_{n-1} x^{n-2} + c_0 x^{n-1} \in \mathcal{C} \end{aligned}$$

Write

$$\begin{aligned} c(x) &= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}. \\ xc(x) &= c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1} x^n. \end{aligned}$$

But, the cyclic shift of $c(x)$ is

$$c_{n-1} + c_0 x + c_1 x^2 \cdots + c_{n-2} x^{n-1}.$$

Is there a way to derive the cyclic shift of $c(x)$ *from the polynomial* $xc(x)$?

Yes!

- Divide $xc(x)$ by $x^n - 1$.
- The remainder is the cyclic shift of codeword $c(x)$.

Proof: Straightforward algebra (**Exercise**). $\square$

Temporarily, we write this remainder as $< xc(x) >$. Then,

$$\begin{aligned} c(x) &= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathcal{C} \\ < xc(x) > &= c_{n-1} + c_0 x + c_1 x^2 \cdots + c_{n-2} x^{n-1}. \\ < x^2 c(x) > &= c_{n-2} + c_{n-1} x + c_0 x^2 \cdots + c_{n-3} x^{n-1}. \\ &\vdots \end{aligned}$$

Theorem 1 *The set of polynomials of degree $n-1$ is* **closed** *under addition, subtraction, and multiplication* **modulo** $x^n - 1$.

Proof: By construction. Work it out. $\square$

- Such an algebraic structure is called a **ring.**
- To study the rich algebraic structures of cyclic codes, we need some **modern** or **abstract** algebra.

4.2 The Algebra of Cyclic Codes
4.2.1 Rings

Definition 3 *A* **commutative ring** *is a set* $\mathbf{R}$ *with two operations* $\oplus$ *and* $\star$ *such that:*

- $\mathbf{R}$ *is a commutative group under* $\oplus$ *;*
- $\mathbf{R}$ *is closed under* $\star$ *;*
- $\star$ *is commutative and associative: For* $a, b \in \mathbf{R}$*,* $(a \star b) \star c = a \star (b \star c)$*;*
- $\star$ *distributes over* $\oplus$*:*

$$\begin{aligned} a \star (b \oplus c) &= a \star b \ \oplus \ a \star c \\ (d \oplus e) \star f &= d \star f \ \oplus \ e \star f; \end{aligned}$$

- *If there is an identity e under* $\star$*, it is unique.*

$\square$

Ring Properties:

- Let $\mathcal{O} =$ the identity under $\oplus$ and $\mathcal{E} =$ the identity under $\star$ (*e.g.*, like 0 and 1.)

$$\begin{aligned} \mathcal{O} \star a &= a \star \mathcal{O} = 0. \\ a \star (-b) &= (-a) \star b = -(a \star b). \end{aligned}$$

- The (multiplicitive) identity $\mathcal{E}$ in $\mathbf{R}$ is unique.
- The (multiplicitive) inverse $(a^{-1})^{-1}$ of a^{-1} is a.

Exercise: Prove these.

Important Example:
The set $\mathbb{R}[x]$ of univariate polynomials with real coefficients is a commutative ring with identity 1.

Definition 4 *An* **integral domain** *is a ring with a* **cancellation property***.*

$\square$

e.g., $\mathbb{Z}$ is an integral domain, and:

$$ac = ad \Rightarrow c = d, \ \forall a \neq 0, \quad c, d \in \mathbb{Z}.$$

However, a^{-1} does *not* exist in $\mathbb{Z}$.

4.2.2 Fields

Definition 5 *A* **field** *is a commutative ring in which every element also has an inverse under the second operation* $\star$*.*

$\square$

Note: In most cases, you can think of $\oplus$ and $\star$ as "addition" and "multiplication."

Examples:

- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are examples of *infinite* fields. (**Exercise:** find the multiplicative inverse of $a + jb$ in $\mathcal{C}$.
- $GF(q)$ is the finite field of $q \in \mathbb{Z}$ elements. (There are restrictions on q as we shall see later.)
  - $GF(2)$ (**Exercise:** construct the tables.)
  - $GF(3) = \{0, 1, 2\}$. (**Exercise:** construct the tables.)

GF(4)

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

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Exercise: Is this modulo 4 arithmetic?

Later: How to construct $GF(q)$ for any *allowed* $q = p^m$.

4.2.1 Subfields

Definition 6 *A* **subfield** *is a subset of a field which itself is a field under the "inherited" operations.*

□

The original field is said to be an **extension** of the subfield.

Examples:

- $\mathbb{Q}$ (rationals) is a subfield of $\mathbb{R}$ (reals)
- $\mathbb{R}$ is a extension of $\mathbb{Q}$.
- $\mathbb{R}$ is a subfield of $\mathbb{C}$ (complex).
- $\mathbb{C}$ is a extension of $\mathbb{R}$.

4.2.3 Polynomial Algebra and Galois Fields

4.2.3.1 The Integer Ring, $\mathbb{Z}$

Since cyclic codewords are polynomials, an algebra *of* polynomials *will be helpful.*

Definition 7 *Let $a, b \in \mathbb{Z}$.*

- $(a, b) \triangleq \mathrm{GCD}(a, b) \triangleq$ *largest* $d \in \mathbb{Z}$ *s.t.:* $d|a$ *and* $d|b$.
- $\mathrm{LCM}(a, b) \triangleq$ *smallest* $m \in \mathbb{Z}$ *s.t.:* $a|m$ *and* $b|m$.
- a, b *are said to be relatively prime if* $\mathrm{GCD}(a, b) = 1$
- a *is said to be* **prime** *if divisible by* 1 *and* a *only.*

$\square$

The Division Algorithm of Algebra: For any $a, b \neq 0, \in \mathbb{Z}$, there exist a quotient q and a remainder r, both in $\mathbb{Z}$ *such that*:

$$a = bq + r.$$

Lemma *q and r are unique.*

Proof:

- Suppose not. Then there are two quotients and remainders:

$$\begin{aligned} a &= bq_1 + r_1 \\ a &= bq_2 + r_2 \\ 0 &= b(q_1 - q_2) + (r_1 - r_2) \end{aligned}$$

- *Therefore*, $(r_1 - r_2)$ is an integer multiple of b.
- But $r_1 < b$ and $r_2 < b \Rightarrow$ *contradiction*.

$\square$

Definition 8 *When $a = bq + r$, we write:*

$$R_b[a] \triangleq r.$$

□

Definition 9 *We say that*

$$\begin{aligned} a &\equiv r\ (b) \\ a &= r \mod b \end{aligned}$$

□

Theorem 2 *For $a, b, t \in \mathbb{Z}$,*

$$\begin{aligned} R_t[a+b] &= R_t[R_t[a] + R_t[b]] \\ R_t[ab] &= R_t\{R_t[a] \cdot R_t[b]\}. \end{aligned}$$

Proof: based upon the uniqueness of the remainder. □

The division algorithm is used to find the GCD:

Theorem 3 *(The Euclidean Algorithm) Let $a < b \in \mathbb{Z}$. Then $d = GCD(a, b)$ can be computed by the iterative algorithm:*

$$
\begin{aligned}
b &= q_1 a + r_1,\ 0 \leq r_1 < a \\
a &= q_2 r_1 + r_2,\ 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3,\ 0 \leq r_3 < r_2 \\
\ldots & \\
r_{n-2} &= q_n r_{n-1} + r_n,\ 0 \leq r_n < r_{n-1} \qquad (1) \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
$$

- *Now,* $d|a,\ d|b \Rightarrow d|r_1 \Rightarrow d|r_2 \cdots d|r_n$
- *Also,* $r_n|r_{n-1} \Rightarrow r_n|r_{n-2} \cdots r_n|a \Rightarrow r_n|b$.
- *Hence,* $r_n|d$ *and* $d|r_n$ *so* $d = r_n$. $\square$

Corollary: *let $a, b \in \mathbb{Z}$. Then there exist integers c and d such that*

$$GCD(a, b) = ac + bd. \tag{2}$$

Proof:

- From proof of Euclidean Algorithm, $GCD(a, b) = r_n$
- Solve the linear equations (in the proof) for r_n as a linear function of a and b. $\square$

4.2.3.2 Constructing finite fields from $\mathbb{Z}$

- Let q be a positive integer.
- Let $\mathbb{Z}/(q) = \{0, 1, \ldots, q-1\}$, the integers modulo q.
  - $\mathbb{Z}/(q)$ maps every integer in $\mathbb{Z}$ into an integer between 0 and $q-1$.
  - Hence, it decomposes the ring $\mathbb{Z}$ of integers into q semi-infinite cosets!
- For $a, b \in \mathbb{Z}/(q)$, define:

$$a + b \triangleq R_q[a + b] \quad (3)$$

$$a \cdot b \triangleq R_q[ab] \quad (4)$$

Theorem 4 *$\mathbb{Z}/(q)$ is a ring under the addition and multiplication operations defined above.*

Proof: Work through the axioms. $\square$

Definition 10 $\mathbb{Z}/(q)$ *is called the ring of integers modulo* q*.*

$\square$

Theorem 5 $\mathbb{Z}/(q)$ *is a field if and only if* q *is a prime integer.*

Proof: See, *e.g.*, Blahut, Sect 4.2. $\square$

- Hence, to construct a finite field $GF(p)$ for any prime integer p, form $\mathbb{Z}/(p)$.
- For certain nonprime values of q, a finite field $GF(q)$ can also be constructed.
- This requires the study of *rings of polynomials*.

4.2.3.3 The Polynomial Ring

Definition 11 *A* **polynomial** *over* $GF(q)$ *is an expression*

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{n-1} x^{n-1},$$

where $f_i \in GF(q),\ i = 0, 1, 2, \ldots, n-1.$

$\square$

- **degree:** $\deg[f(x)] = n - 1.$
- $\deg[0] = -\infty$ by convention.
- $f(x)$ is said to be **monic** whenever $f_{n-1} = 1.$
- **equality:**

$$f(x) = g(x) \Leftrightarrow f_i = g_i,\ i = 0, 1, \cdots, n-1.$$

Residues in $GF(q)[x]$:

- *Notice the analogies with residue theory in* $\mathbb{Z}$.

Definition 12 $r(x)$ **divides** $s(x)$, $r(x)|s(x)$ $\Leftrightarrow$ *there exists polynomial* $a(x)$ *such that*

$$a(x)r(x) = s(x)$$

$\square$

Definition 13 *An* **irreducible** *polynomial* $p(x)$ *is divisible only by scalar* α *and by* $\alpha p(x)$

$\square$

Definition 14 *A* **prime** *polynomial is a* **monic**, **irreducible** *polynomial of degree at least* 1. □

Definition 15 *The* **greatest common divisor** $GCD[r(x), s(x)]$ *is the monic polynomial of* **largest** *degree that divides each.* □

Notation: The following notation is also used.

$$GCD[r(x), s(x)] = (r(x), s(x))$$

Definition 16 *The* **least common multiple** $LCM[r(x), s(x)]$ *is the monic polynomial of* **smallest** *degree that is divisible by each.* □

Definition 17 *$r(x)$ and $s(x)$ are said to be* **relatively prime** *or* **coprime** *if*

$$GCD[r(x), s(x)] = 1.$$

$\square$

Definition 18 *The* **formal derivative** *of $f(x)$ is:*

$$((n-1))f_{n-1}x^{n-2} + ((n-2))f_{n-2}x^{n-2} + \cdots + f_1$$

where $((i)) = \overbrace{1 + 1 + \cdots + 1}^{i}$ *is called an* **integer of the field.**[a] $\square$

Lemma: If $r(x)|s(x)$ and if $s(x)|r(x)$ then $r(x) = \pm s(x)$. $\square$

[a] When there is no confusion, we will write i for $((i))$.

The Division Algorithm for Polynomials.

Theorem 6 *For every pair of polynomials, $b(x) \neq 0$, and $a(x)$, there exist a unique pair of polynomials, $Q(x)$ (quotient) and $r(x)$ (remainder) such that:*

$$a(x) = Q(x)b(x) + r(x)$$

where $\deg[r(x)] < \deg[b(x)]$.

Proof: Similar to of the Division Algorithm for Integers; replace the integer value with the degree of the polynomial (Blahut, p. 74). $\square$

Recall:

$$a(x) = Q(x)b(x) + r(x)$$

Definition 19 *We call* $R_{b(x)}[a(x)] = r(x)$ *the* **remainder** *or* **residue** *of* $a(x)$ *modulo* $b(x)$ *and write*

$$r(x) \equiv a(x) \bmod b(x),$$

where $\deg[r(x)] < \deg[b(x)]$.

$\square$

Theorem 7 *Let* $d(x) = g(x) \cdot h(x)$. *Then, for any polynomial* $a(x)$,

$$R_{g(x)}[a(x)] = R_{g(x)}\{R_{d(x)}[a(x)]\}$$

Proof: Divide $a(x)$ by $d(x)$:

$$\begin{aligned} a(x) &= Q_1(x)d(x) + R_{d(x)}[a(x)] \\ &= Q_1(x)g(x)h(x) + R_{d(x)}[a(x)] \end{aligned}$$

and

$$R_{g(x)}[a(x)] = R_{g(x)}\{R_{d(x)}[a(x)]\}$$

$\square$

Theorem 8

$$
\begin{aligned}
R_{d(x)}[a(x) + b(x)] &= R_{d(x)}[a(x)] + R_{d(x)}[b(x)] \\
R_{d(x)}[a(x) \cdot b(x)] &= R_{d(x)}\{R_{d(x)}[a(x)] \cdot R_{d(x)}[b(x)]\}
\end{aligned}
$$

Proof: As with the residues, use the division algorithm and equate the remainders. (Blahut, p. 74) $\square$

The Unique Factorization Theorem for Polynomials

Theorem 9 *Any monic polynomial over a field can be uniquely factored into monic irreducible polynomials over that field.*

Proof: Blahut, p.75. This generalizes the well-known UFT for integers:

$$a \in \mathbb{Z} \Rightarrow a = p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}$$

for some finite n. □

Theorem 10 *(**The Euclidean Algorithm for Polynomials.**) Let* $a(x), b(x) \subset GF(q)[x]$ *and* $\deg[a(x)] < \deg[b(x)]$. *Then* $GCD[a(x), b(x)]$ *can be found by the iterative algorithm:*

$$
\begin{aligned}
b(x) &= Q_1(x)a(x) + r_1(x) \\
a(x) &= Q_2(x)r_1(x) + r_2(x) \\
r_1(x) &= Q_3(x)r_2(x) + r_3(x) \\
\ldots & \\
r_{n-2}(x) &= Q_n(x)r_{n-1}(x) + r_n(x) \\
r_n(x) &= Q_{n+1}(x)r_n(x)
\end{aligned}
$$

and $\alpha \cdot GCD[a(x), b(x)] = r_n(x)$, *where* $\alpha \in GF(q)$.

Proof: of Euclidean Theorem for Polynomials parallels that for the integers (Blahut, p.76). $\square$

Theorem 11 *(The Fundamental Theorem of Algebra) Let* $\deg[f(x)] = n$*. Then,* $f(x)$ *has at most* n *zeros and* $f(\alpha) = 0$ *if and only if* $(x - \alpha)|f(x)$*.*

Proof: See text. $\square$

4.2.3.4 Finite Fields from Polynomial Rings

- By analogy with $\mathbb{Z}/(q)$, we use quotients in $GF(q)[x]$ to construct finite fields.
- This permits construction of fields not possible using integer residues.
- For notational simplicity, let $\mathbb{F}_q \triangleq GF(q)$. be any finite field having q elements.

Now, consider $p(x) \in \mathbb{F}_q[x]$ with $\deg[p(x)] > 0$.

Definition 20 *The* **polynomials modulo** $p(x)$ *over* $\mathbb{F}_q$*:*

$$\mathbb{F}_q[x]/(p(x)) \triangleq \{f(x) : \ s.t.\ deg[f(x)] < deg[p(x)]\}$$

□

Now divide:

$$\begin{aligned} g(x) &= Q_g(x) \cdot p(x) + r_g(x) \\ h(x) &= Q_h(x) \cdot p(x) + r_h(x) \end{aligned}$$

Then

- $r_g(x), \ r_h(x) \in \mathbb{F}_q[x]/(p(x))$.
- If $r_g(x) = r_h(x)$, then we write

$$g(x) \equiv h(x) \ (mod\ p(x))$$

even if $g(x) \neq h(x)$.

Theorem 12 *$\mathbb{F}_q[x]/(p(x))$ is a ring.*

Proof: Test the addition and multiplication axioms mod $p(x)$. $\square$

Theorem 13 *$\mathbb{F}_q[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible.*

Proof: Many texts. $\square$

- Clearly $\mathbb{F}_q[x]$ contains q^m elements where $m = deg[p(x)]$.
- We call this field, $GF(q^m)$ or F_{q^m}.
- So any *prime polynomial* $p(x)$ can generate a field.

Compare:

- $p(x) \in \mathbb{F}_q[x]$.
- $\mathbb{F}_q[x]/(p(x))$ **is** $\mathbb{F}_{q^m} \equiv GF(q^m)$ for prime $p(x)$.
- $\mathbb{F}_{q^m}$ is an **extension field** of $\mathbb{F}_q$.
- $\mathbb{F}_q \equiv GF(q)$ is a **subfield** of $\mathbb{F}_{q^m} \equiv GF(q^m)$.

Example: Let $p(x) = x^2 + x + 1$

- $p(x)$ is prime over $\mathbb{F}_2$ (verify). So,
- $\mathbb{F}_2(x)/(p(x))$ is a field with $2^2 = 4$ elements and
  - "$+$" and "$\times$" mod $p(x)$
  - Members (polynomials of degree < 2):

$$\begin{array}{ll} 0 & 0 \\ 1 & x \\ x & x^1 \\ x+1 & x^2 \end{array}$$

Important note: Although elements of nonprime fields are *polynomials*, now that we can write down the $+$ and $\times$ tables, we can use any convenient notation. For example, in $GF(8)$ we can use the symbols 0,1,...,7 *so long as we don't confuse the field with* $\mathbb{Z}_8$.

Lemma: The nonzero elements of $GF(q)$ form a *multiplicative group*.
Proof: Obvious $\square$.

- Suppose $1, \beta, \beta^2, \cdots \in GF(q)$ where $order$ of $\beta = m$.
- Then, $m \mid q-1$ (from coset decomposition).

Definition 21 *An element of $GF(q)$ of order $q-1$ is a* **primitive** *element of $GF(q)$* $\square$

Lemma: If α is primitive in $GF(q)$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ are all the nonzero elements of $GF(q)$.

Proof: From definition of primitive. $\square$

Theorem 14 *Let* $\{\beta_1, \beta_2, \cdots, \beta_{q-1}\}$ *be the non-zero elements of* $GF(q)$*. Then*

$$x^{q-1} - 1 = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_{q-1})$$

Proof:

- For $1 \leq j \leq (q-1)$ and $\beta_j \in GF(q)$

$$m_j \mid q - 1.$$

Therefore

$$\beta_j^{q-1} = (\beta_j^{m_j})^{\frac{q-1}{m_j}} = (1)^{\frac{q-1}{m_j}} = 1$$

so that β_j is a zero of $x^{q-1} - 1$. $\square$

Theorem 15 *$GF(q)$ always contains a primitive element.*

Proof:

- The non-zero elements form a cyclic group.
- Therefore, there is an element of order $q - 1$.

$\square$

Definition 22 *A* **primitive polynomial** *is an irreducible polynomial $p(x)$ of degree m over $GF(q)$ having a primitive element of $GF(q^m)$ as a root.*

$\square$

This definition means that, if:

1. $p(x)$ is irreducible over $GF(q)$,
2. α is primitive in $GF(q^m)$, and
3. $p(\alpha) = 0$,

then,

- $p(x)$ is a primitive polynomial and

$$\alpha^{q^m-1} = 1.$$

Example of generating a nonprime field

Let

- $p(x) = x^4 + x + 1 \in GF(2)$ be primitive (can verify – How?).
- α be primitive in $GF(2^4)$ and $p(\alpha) = 0$. Then,

$$\alpha^4 + \alpha + 1 = 0 \tag{5}$$

From (5) we can write:

$$\begin{aligned} \alpha^4 &= 1 + \alpha \\ \alpha^5 &= \alpha + \alpha^2 \end{aligned}$$

etc. The complete set of powers of α follows.

$$
\begin{aligned}
\alpha^0 &= 1 \\
\alpha^1 &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha^3 \\
\alpha^4 &= 1 + \alpha \\
\alpha^5 &= \alpha + \alpha^2 \\
\alpha^6 &= \alpha^2 + \alpha^3 \\
\alpha^7 &= 1 + \alpha + \alpha^3 \\
\alpha^8 &= 1 + \alpha^2 \\
\alpha^9 &= \alpha + \alpha^3 \\
\alpha^{10} &= 1 + \alpha + \alpha^2 \\
\alpha^{11} &= \alpha + \alpha^2 + \alpha^3 \\
\alpha^{12} &= 1 + \alpha + \alpha^2 + \alpha^3
\end{aligned}
$$

$$\begin{aligned}
\alpha^{13} &= 1 \quad\quad + \alpha^2 + \alpha^3 \\
\alpha^{14} &= 1 \quad\quad\quad\quad + \alpha^3 \\
\alpha^{15} &= 1
\end{aligned}$$

Exercise: Generate $GF(2^4)$ using a different primitive polynomial. Do you get the same field?

4.2.3.5 The Structure of $GF(q)$

- We seek to do "arithmetic" in $GF(q)$.

Definition 23 *The* **characteristic** *of $GF(q)$ is the number of elements in its smallest subfield.* $\square$

Example: The characteristic of $GF(16)$ is 2.

Theorem 16 *Every finite field $GF(q)$ contains a unique, smallest subfield that contains a prime number of elements.*

Proof:

- Every $GF(q)$ contains 0 and 1.
- Let $G \triangleq \{0,\ 1,\ 2, \ldots,\ r-1\}$, where $i = \underbrace{1+1+\cdots+1}_{i\ times}$,
  - So G is a cyclic additive, finite subgroup of $GF(q)$ of order r.
  - Hence, addition in G is modulo r.
  - For $i, j \in G$,

$$\begin{aligned} i \cdot j &= (1+1+\cdots+1) \cdot j \\ &= (j+j+\cdots+j). \end{aligned}$$

  - Therefore "$\times$" is modulo r as well.

- Since G is
  - cyclic,
  - of order r
  - having modulo r operations "$+$" and "$\times$",
- then it is by an earlier proof, a prime field of size r.
- Since it is prime, it has no subfield, and the theorem is proved.

$\square$

Corollary: *The characteristic of any Galois field is prime.*

Proof: Follows immediately from the previous construction

.

Corollary: *In a field of characteristic* p, $(a+b)^p = a^p + b^p$.

Proof:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

But

$$\binom{p}{j} = 0 \mod p \ \forall j,$$

and the lemma is proved. $\square$

Example (continued)

Arithmetic in $GF(2^4)$ is performed in this manner:

- $(\times)$: $\alpha^j \times \alpha^k = \alpha^{j+k \pmod{2^4-1}}$.
- $(+)$: From the table,

$$\begin{aligned} \alpha^5 + \alpha^9 &= \alpha + \alpha^2 + \alpha + \alpha^3 \\ &= \alpha^2 + \alpha^3 \\ &= \alpha^6. \end{aligned}$$

More on **Extension Fields**

- Let $GF(q)$ be a subfield of $GF(Q)$ and $\beta \in GF(Q)$. Then,

Definition 24 *The* **minimal polynomial** $m_\beta(x)$ *of* β *over* $GF(q)$ *is the prime polynomial of smallest degree over* $GF(q)$ *for which* $m_\beta(\beta) = 0$. □

Theorem 17 *Two-part theorem:*

- *I: Every* $\beta \in GF(Q)$ *has a unique minimal polynomial over* $GF(q)$.
- *II: If* $m(x)$ *is the minimal polynomial of* β *and if* $g(\beta) = 0$, *then* $m(x)|g(x)$.

Proof: See text. □

Corollary: *If* $m_1(x), \cdots, m_k(x)$ *are the minimal polynomials over* $GF(q)$ *for all the elements of* $GF(Q)$*, then*

$$x^Q - x = \prod_{i=1}^{k} m_i(x).$$

Proof: β is always a zero of $x^Q - x$, so this is true by UFT. $\square$

Theorem 18 *For any* $g(x)$ *over* $GF(q)$*, there exists an extension field* $GF(Q)$ *in which* $g(x) = \prod(x - \beta_i)$*.*

Proof: See text. $\square$

Definition 25 *A* **splitting field** *of* $g(x) \in \mathbb{F}_q[x]$ *is any extension* $GF(Q)$ *of* $GF(q)$ *in which* $g(x)$ *factors into linear and constant terms only.*

$\square$

Theorem 19 *Let* α *be primtive in* $GF(Q)$*, an extension of* $GF(q)$ *and let* $\deg[m_\alpha(x)] = m$*. Then*

- $Q = q^m$*, and*
- *Any* $\beta \in GF(Q)$ *can be written as*

$$\beta = b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0, \; b_i \in GF(q).$$

Note: Therefore, $GF(Q)$ is a *vector space* over $GF(q)$.

Proof: See text. □

The following follow directly from the theorem and are computationally useful.

- For every prime number p and positive integer m, there exists a finite field of size p^m.
- In $GF(q),\ q = p^m$, $(a + b)^q = a^q + b^q$.
- The smallest splitting field of the polynomial $x^{p^m} - x$ has exactly p^m elements.

4.3 Viewing Cyclic codes from Extension Fields - An Example

- For α primitive in $GF(2^3)$, let

$$\begin{aligned} p(x) &= x^3 + x + 1 \\ p(\alpha) &= 0 \\ H &= \left[\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\right]. \end{aligned}$$

- Expanding powers of α, write H in binary form:

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

i.e., $\alpha^3 = 1 + \alpha$, etc.

- Let $\mathbf{H}$ be check matrix of some binary code $\mathcal{C}$.
- For $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} \cdot \mathbf{H}^T = 0.$$

$$\begin{aligned} \sum_{i=0}^{n-1} c_i \alpha^i &= 0 \\ c(\alpha) &= 0 \end{aligned}$$

  which defines a polynomial $c(x)$ having α as a root.

- Thus we establish the correspondence between *codewords* and *polynomials*
- **Note:** H is the check matrix of the binary, Hamming $(7, 4)$ code.

In general,

- Let $\mathbf{H}$ be $(n-k) \times n$ q-ary matrix *s.t.* $m|(n-k)$.
- Represent the first m rows of $\mathbf{H}$ as a single row of symbols from $GF(q^m)$, $(\beta_{11}, \ldots, \beta_{1n})$. Repeat for every set of m rows.

$$\mathbf{H} = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{11} & \beta_{12} & \cdots & \beta_{2n} \\ \vdots & & & \\ \beta_{\rho 1} & \beta_{\rho 2} & \cdots & \beta_{\rho n} \end{bmatrix}$$

where

$$\rho = \frac{n-k}{m}$$

This is not new, merely more *compact*. However,...

- Consider the special case where $B_{ij} = \gamma_i^{j-1}$.
- Then the i^{th} row of $\mathbf{H}$ can be written: $\gamma_i^0, \gamma_i^1, \ldots, \gamma_i^{n-1}$, for
  - $i = 1, \ldots, \rho$ and
  - $n = q^m - 1$.

$$\mathbf{H} = \begin{bmatrix} \gamma_1^0 & \gamma_1^1 & \cdots & \gamma_1^{n-1} \\ \gamma_2^0 & & & \\ \vdots & & & \\ \gamma_\rho^0 & & & \gamma_\rho^{n-1} \end{bmatrix}$$

- For some $\mathbf{c} \in \mathcal{C}$

$$\begin{aligned} \mathbf{c}H^T &= 0 \\ \sum_{i=1}^{n-1} c_i \gamma_j^i &= 0, \ j = 1, \cdots, \rho \end{aligned}$$

- So $\mathcal{C}$ is all $c(x)$ of degree $\leq n - 1$ *s.t.* $c(\gamma_i) = 0, i = 1, \ldots, \rho$

- and $\mathbf{H}$ is the check matrix of the code $\mathcal{C}$, where

$$\mathcal{C} = \{c(x) \ s.t., \ \deg[c(x)] \leq n, \ c(\gamma_j) = 0, \ j = 1, \ldots, \rho.$$

- $\Rightarrow$ But we have not shown that $\mathcal{C}$ is **cyclic.** $\Leftarrow$

4.4 Cyclic Codes, Formally

4.4.1 Algebraic Description of Cyclic Codes

Definition 26 $\mathbb{F}_q[x] \triangleq$ *the* **ring of polynomials** *over* $GF(q)$.

$\square$

Definition 27 $\mathbb{F}_q[x]/(x^n - 1) \triangleq$ *the* **ring of polynomials** *over* $GF(q)$ $\bmod (x^n - 1)$.

$\square$

Definition 28 *A subset* I *of any ring* $\mathbf{R}$ *is an* **ideal** *if*

- *it is a subgroup of the additive group of* $\mathbf{R}$, *and*
- $r \in \mathbf{R}$ *and* $a \in I \Rightarrow ar \in I$.

$\square$

Clearly $c(x) \in \mathbb{F}_q[x]/(x^n - 1) \Rightarrow \deg[c(x)] \leq n - 1$

and,

Lemma: $xc(x) \in \mathbb{F}_q[x]/(x^n - 1)$.

Proof: See text. $\square$

So,

- Associate n-tuple $\mathbf{c} \in sC$ with $c(x) \in \mathbb{F}_q[x]/(x^n - 1)$.
- All such codewords $\mathbf{c}$, then, are **cyclic.**
- $xc(x)$ is the cyclic shift of $c(x)$.

Notation: $\mathcal{C}$ represents both the codewords $\{\mathbf{c}\}$ and the polynomials $\{c(x)\}$.

Theorem 20 *$\mathcal{C}$ is a q-ary linear cyclic code of length n if and only if the $\{c(x)\} \in \mathcal{C}$ form an ideal in $\mathbb{F}_q[x]/(x^n - 1)$.*

Simply put, *a cyclic code of block length n is an ideal in the ring of polynomials modulo $x^n - 1$.*

Proof:

Case i (if): Assume 1 and 2 are true. Then $\mathcal{C}$ is:

- closed under $+$.
- closed under mult by any scalar (where $a(x)$ is a "scalar.")
- therefore, is a subspace, therefore a code.
- If $a(x) = x$, $\mathcal{C}$ is cyclic.

Case ii (only if): Assume $\mathcal{C}$ is a cyclic code. Then it is

- a subspace;
- closed under
  - $+$
  - multiplication by a scalar, specifically -
  - multiplication by x.
- and, therefore, under multiplication by arbitrary polynomial $a(x)$.

$\square$

4.4.2 Generating Cyclic Codes

Lemma: *Given an ideal $\mathcal{I}$ of $\mathbb{F}_q[x]/(x^n - 1)$. The non-zero monic polynomial $g(x)$ of smallest degree in $\mathcal{I}$ is unique.*
Proof:

- Let $\deg[g(x)] = r$.
- Select $\alpha \in \mathbb{F}_q$ so that $\alpha g(x)$ is monic. Note that $\alpha g(x) \in \mathcal{I}$.
- Suppose another monic $f(x) \in \mathcal{I}$ with $\deg[f(x)] = r$.
- Then $f(x) - g(x) \in \mathcal{I}$.
- But $\deg[f(x) - g(x)] \leq \deg[g(x)]$.
  - This contradicts our choice of $g(x)$.
- Therefore $g(x)$ is as claimed. $\square$

Definition 29 : *The non-zero polynomial $g(x)$ of smallest degree in ideal $\mathcal{I}$ is called the* **generator polynomial** *of the ideal.*

$\square$

Theorem 21 *A cyclic code consists of all multiples of its generator polynomial $g(x)$ by polynomials $a(x)$ of degree $\leq k-1$.*

Proof:

- If $g(x) \in \mathcal{C}$, then $a(x)g(x) \in \mathcal{C}\ \forall a(x)$.
- Suppose $c(x) \in \mathcal{C}$, and suppose:

$$c(x) = Q(x)g(x) + s(x).$$

- But $c(x) \in \mathcal{C}$, and $Q(x)g(x) \in \mathcal{C} \Rightarrow s(x) \in \mathcal{C}$. But

$$\deg[s(x)] < \deg[q(x)]$$

  Yet $g(x)$ is the polynomial of smallest degree in $\mathcal{C}$. Hence, $s(x) \equiv 0$ $\square$

Theorem 22 : *A cyclic code $\mathcal{C}$ of length n and generator polynomial $g(x)$ exists if and only if $g(x)|(x^n - 1)$.*

Proof:

- Suppose $\mathcal{C} =< g(x) >$ but

$$\begin{aligned} x^n - 1 &= Q(x)g(x) + s(x), \;\; \deg[s(x) < \deg[g(x)] \\ R_{x^n-1}(x^n - 1) = 0 &= R_{x^n-1}[Q(x)g(x)] + R_{x^n-1}[s(x)] \\ &= R_{x^n-1}[Q(x)g(x)] + s(x) \end{aligned}$$

- Since $R_{x^n-1}[Q(x)g(x)] \in \mathcal{C}$, then $s(x) \in \mathcal{C}$.
- But: $\deg[s(x)] < \deg[g(x)]$, so $s(x) \equiv 0$ and $g(x)|(x^n - 1)$.
- Conversely, every $g(x)|(x^n - 1)$ can generate a code.

$\square$

4.4.3 Parity Check Polynomial

Definition 30 : *Let $x^n - 1 = g(x)h(x)$. If $g(x)$ generates a code, then we call $h(x)$ the* **parity check polynomial** *of the code.*

$\square$

Lemma: *For every $c(x) \in \mathcal{C}$*

$$R_{x^n-1}[h(x)c(x)] = 0$$

Proof:

- For some $a(x)$

$$h(x)c(x) = h(x)g(x)a(x) = (x^n - 1)a(x)$$

$\square$

4.4.4 Error Polynomial

- Transmit q-ary codeword $c(x) \in \mathcal{C}$ over noisy channel.
- Receive vector $v(x)$
- Both are in $\mathbb{F}_q[x]/(x^n - 1)$.

Definition 31 : *The* **error polynomial** *is the difference* $v(x) - c(x)$ *between received and transmitted polynomials.*

□

i.e.,

$$v(x) = c(x) + e(x)$$

This is a model for the class of **additive noise** channels.

Definition 32 : *The* **information** *encoded by* $\mathcal{C}$ *is represented by a polynomial* $a(x), \ \deg[a(x)] \leq k-1$.

□

- $c(x) = a(x)g(x) \mod x^n - 1$
- $\mathcal{C} = \{c(x) = a(x)g(x)\}$ is **not** systematic in (try it!).

Lemma: $c(x)$ *belongs to a systematic, cyclic code if*

$$c(x) = x^{n-k}a(x) + t(x)$$

where $t(x)$ *is chosen so that* $c(x) \equiv 0 \ mod \ x^n - 1$.

Proof: Exercise □

4.5 Explicit Constructions of Cyclic Codes

- **Objective:** *To find an explicit construction of $g(x)$ for cyclic code of length n.*

  Consider the *prime factorization*:

$$\begin{aligned} x^n - 1 &= f_1(x) f_2(x) \cdots f_s(x) \\ &= \prod_{i=1}^{s} f_i(x). \end{aligned}$$

- Select some factors of $x^n - 1$:

$$g(x) = f_{i_1}(x) \cdot f_{i_2}(x) \cdots f_{i_j}(x), \ j = 1, 2, \cdots, s.$$

- How many such $g(x)$ can we form?
  - 2^s possibilities;
  - Eliminate choosing no factors.
  - Eliminate choosing all factors.
  - $\Rightarrow\ 2^s - 2$ possiblities.

4.5.1 Finding a Generator Polynomial $g(x)$

We consider two ways to specify $g(x)$, by its *factors* and by its roots.

$$x^{q^m-1} - 1 = \prod f_i(x) \tag{6}$$

- This **prime factorization** is unique.
- $\beta_j \neq 0 \in GF(q^m)$ is a root of (6).
- And we can *factor* each $f_i(x)$ in $GF(q^m)$:

$$x^{q^m-1} - 1 = \prod_{i=1}^{s} f_i(x) = \prod_{j=1}^{q^m-1} (x - \beta_j)$$

- Each β_ρ will be a zero of exactly one such polynomial.
- Each $f_i(x)$ is the polynomial of *smallest degree* such that $f_i(\beta_j) = 0$.

Theorem 23 : *A polynomial $c(x)$ is a codeword in a primitive code if and only if all the roots of $g(x)$ are also roots of $c(x)$.*

Proof:

Let $\{\beta_j\}$ be the set of roots of $g(x)$.

- Every codeword $c(x) = a(x)g(x)$. Therefore

$$c(\beta_j) = a(\beta_j)g(\beta_j) = 0.$$

- **Conversely** let $c(\beta_j) = 0$. Divide by $m_{\beta_j}(x)$:

$$\begin{aligned} c(x) &= Q(x)m_{\beta_j}(x) + r(x) \\ c(\beta_j) &= 0 = Q(\beta_j)m_{\beta_j}(\beta_j) + s(\beta_j) \\ s(x) &= 0 \end{aligned}$$

because $\deg[s(x)] < \deg[m_{\beta_j}(x)]$. □

Example: *Find all binary cyclic codes of length* $n = 15$.

$$\begin{aligned} x^{15} - 1 &= (x+1)(x^2+x+1)(x^4+x+1) \\ &\quad \cdot (x^4+x^3+1)(x^4+x^3+x^2+x+1) \\ &= f_1(x) f_2(x) f_3(x) f_4(x) f_5(x) \end{aligned}$$

- There are 5 factors, so $2^5 - 2$ nontrivial binary cyclic codes.

- **Example:**(continued) Let $g(x) = f_4(x)f_5(x)$:

$$g(x) = x^8 + x^4 + x^2 + x + 1$$

  – $f_4(x)$ is primitive (verify), so one of its roots α is primitive in $GF(2^4)$.
  – Also α^3 is a root of $f_5(x)$ (verify).
  – Therefore the roots of $g(x)$ include α, α^3.
  – $\deg[g(x)] = 8 = n - k$, so $k = 7$.
  – $w_H[g(x)] = 5$ (see above) so $d_{min} \leq 5$.

- Generally, if we want $g(\beta_i) = 0,\ i = 1, \cdots, r$:
  - we must find $m_{\beta_1}(x), \cdots, m_{\beta_r}(x)$.
  - Set

$$g(x) = LCM[m_{\beta_1}(x), \cdots, m_{\beta_r}(x)]$$

    and $g(x)$ is as desired.

- How do we find m_{β_j}? (See next Theorem.)

Exercise: *If* $\deg[m_\beta(x)] = h$ *and* $m_\beta(\beta) = 0$ *what are the other* $h - 1$ *other zeros of* $m_\beta(x)$*?*

Theorem 24 : *If β is an element of $GF(q^m)$ with minimal polynomial $m_\beta(x)$ over $GF(q)$, then $m_\beta(x)$ is also the minimal polynomial of β^q.*

Proof: Text. $\square$

Definition 33 : *Two elements of $GF(q^m)$ having the same minimal polynomial over $GF(q)$ are said to be* **conjugates** *with respect to $GF(q)$.*

$\square$

- So β and β^q are conjugates by the theorem.
- So are $\beta^{q^2}, \cdots, \beta^{q^{r-1}}$ where r is the smallest integer such that $\beta^{q^r} = \beta$.
- This leads directly to ...

Theorem 25 $m_\beta(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{q^{r-1}})$.

Proof:

- All the conjugates of β are roots.
- Must show that the coefficients of $m_\beta(x)$ lie in $GF(q)$.

$$\begin{aligned}
[m_\beta(x)]^q &= (x-\beta)^q \cdots (x-\beta^{q^{r-1}})^q \\
&= (x^q-\beta^q)\cdots(x^q-\beta^{q^r}) \\
&= (x^q-\beta^q)\cdots(x^q-\beta) \\
&= m_\beta(x^q) \\
&= \sum m_{i\beta} x^{iq}
\end{aligned}$$

But also, by the theorem:

$$[m_\beta(x)]^q = \sum m_{i\beta}^q x^{iq}$$

Therefore $m_{i\beta}^q = m_{i\beta}$. $\square$

Summary of foregoing:

- Given a field $GF(q)$, select blocklength n.
- Using primitive element, find minimal polynomial and conjugate roots.
- Add additional roots if needed to obtain desired k.
- Write down $g(x)$.

4.5.2 Non-primitive Cyclic Codes.

Definition 34 *For a code over $GF(q)$, a blocklength of the form $n = q^m - 1$ is called a* **primitive blocklength**. □

A cyclic code of such length is called a **primitive cyclic code.**

Lemma: *n divides $q^m - 1$ for some m.* □

Theorem 26 : *Given $GF(q)$ and integer n relatively prime to q. Then there exists an integer m for which*

$$(x^n - 1) | (x^{q^m - 1} - 1)$$

□

Then $x^n - 1$ has m distinct roots in $GF(q^m)$.

4.5.3 Summary: How to Describe any Cyclic Code

- A cyclic code of (given) length n over $GF(q)$ is generated by $g(x)$ where

$$g(x)|(x^n - 1)$$

- To get $g(x)$, select primitive element $\alpha \in GF(q^m)$, where

$$\begin{aligned} q^m - 1 &= nb \\ \alpha^{nb} &= 1 \end{aligned}$$

- Determine the minimal polynomial $m_\alpha(x)$ over $GF(q)$.
- Then $m_\alpha(x) \mid g(x)$.
- For lower rate code, find another root, $\hat{\alpha}$ and write

$$g(x) = LCM\left(m_\alpha(x), m_{\hat{\alpha}}(x)\right).$$

Note: We can (and will) say more about how to design $\mathcal{C}$ to have given rate or minimum distance.

4.6 Matrix Description of Cyclic Codes
4.6.1 Formal Method

- Let $g(x) \in \mathbb{F}_q[x]$ have zeros $\gamma_i,\ i = 1, \ldots, r$ in $GF(q^m)$.
- If $c(x)$ is a codeword, $c(\gamma_i) = 0,\ i = 1, \ldots, r$, or

$$\sum_{j=0}^{n-1} c_j \gamma_i^j = 0,\ i = 1, \ldots, r.$$

- Since there is $\mathbf{H}$ for which $\mathbf{c}H^T = 0$, this suggests:

$$\mathbf{H}^T = \begin{bmatrix} \gamma_1^0 & \gamma_2^0 & \cdots & \gamma_r^0 \\ \gamma_1^1 & \gamma_2^1 & \cdots & \gamma_r^1 \\ \gamma_1^2 & \gamma_2^2 & \cdots & \gamma_r^2 \\ \cdots & & & \\ \gamma_1^{n-1} & \gamma_2^{n-1} & \cdots & \gamma_r^{n-1} \end{bmatrix}$$

over $GF(q^m)$.

- Can write $\gamma_i^j = (\gamma_{i0}, \gamma_{i1}, \ldots, \gamma_{i(n-1)}),\ \gamma_{i\sigma} \in GF(q)$.
- Then replace each element in $\mathbf{H}$ by a *column* $m-$tuple over $GF(q)$.
- This gives a matrix having dimensions $rm \times n$ over $GF(q)$.
- **Note:** Remove linearly dependent rows.
- This gives $\mathbf{H}$ matrix over $GF(q)$.

This is a cumbersome algorithm.

4.6.2 A Direct Method

- Use the generator $g(x)$:

$$c(x) = a(x)g(x)$$

where,

$$\begin{aligned} g(x) &= \sum_{j=0}^{n-k} g_j x^j \\ a(x) &= \sum_{i=0}^{k-1} a_i x^i \end{aligned}$$

- Consider coefficients of $\mathbf{c} = \mathbf{a}G$:

$$
\begin{aligned}
c(x) &= a(x)g(x) = \sum_{i=0}^{k-1}\sum_{j=0}^{n-k} a_i g_j x^{i+j} \\
&= a_0g_0 + (a_1g_0 + a_0g_1)x + \cdots \\
&\quad + (a_{k-2}g_{n-k} + a_{k-1}g_{n-k-1})x^{n-2} + a_{k-1}g_{n-k}x^{n-1}
\end{aligned}
$$

$$\mathbf{c} = (a_{k-1}g_{n-k}, (a_{k-2}g_{n-k} + a_{k-1}g_{n-k-1}), \cdots (a_1g_0 + a_0g_1), a_0g_0),$$

$$
(a_0, a_1, \cdots, a_{k-1})
\begin{bmatrix}
0 & 0 & \cdots & g_1 & g_0 \\
0 & 0 & \cdots & g_0 & 0 \\
\vdots & & & & \\
0 & g_{n-k} & \cdots & 0 & 0 \\
g_{n-k} & g_{n-k-1} & \cdots & 0 & 0
\end{bmatrix}
$$

Or,

$$\mathbf{G} = \begin{bmatrix} 0 & 0 & \cdots & g_1 & g_0 \\ 0 & 0 & \cdots & g_0 & 0 \\ \vdots & & & & \\ 0 & g_{n-k} & \cdots & 0 & 0 \\ g_{n-k} & g_{n-k-1} & \cdots & 0 & 0 \end{bmatrix}$$

- Recall $x^n - 1 = g(x)h(x)$
- For any codeword $c(x)$

$$R_{x^n-1}[c(x)h(x)] = 0$$

- As above, we can use $h(x)$ to write:

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & \cdots & h_0 & h_1 & \cdots & h_{k-1} & h_k \\ \cdots & & & & & & & & \cdots \\ 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k & 0 & \cdots & 0 \\ h_0 & h_1 & h_2 & \cdots & 0 & 0 & \cdots & 0 & \end{bmatrix}$$

- To show that $\mathbf{G}H^T = \mathbf{0}$:
  - The product of s^{th} row of $\mathbf{G}$ and t^{th} column of $\mathbf{H}^T$ has the form

$$u_r = \sum_{i=0}^{r} g_{r-i}h_i = 0,\ 1 \le r \le n-1,$$

  - and u_r is the coefficient of x^r in $g(x) \cdot h(x) = x^n - 1$.
- Hence, $u_r = 0$ unless $r = 0$ or n.

Hence, $\mathbf{G}H = 0$ and $\mathbf{H}$ is the parity check matrix.

4.6.3 The Dual Code

- The check matrix $\mathbf{H}$ of the code generated by $\mathbf{G}$ has the form of a generator matrix for a cyclic code.
- Therefore, the dual of a cyclic code is a cyclic code.
- Examining the order of coefficients in $\mathbf{H}$ shows that the dual code is generated by

$$\tilde{h}(x) = x^k h(x^{-1})$$

STOP