MATH 342

Kevin L

Winter Term 1 2024

Contents

1 Linear Codes

Definition 1.1. A **linear code** C is a subspace of $V(n,q)$ for some positive n. Thus, C is linear iff

1. $u, v \in C \implies u+v \in C$
2. $u \in C, a \in GF(q) \implies au \in C$

If C is a k-dimensional subspace of $V(n,q)$ then C is called an $[n,k]$ or $[n,k,d]$ code.

Remark. A q-ary $[n,k,d]$ code is also a q-ary (n,q^k,d) code but converse is not true.
0 must be in C.

Definition 1.2. The **weight** of a vector x is defined to be the number of non-zero entries of x.

Lemma 1.3. If $x, y \in V(n,q)$ then $d(x,y) = w(x-y)$.

Proof. The vector $x-y$ has non-zero entries in those places where x, y differ. □

Theorem 1.4. Let C be linear. Then

$$d(C) = \min_{x \in C} w(x)$$

Proof. There are codewords x, y such that $d(x,y) = c = d(C)$. (As otherwise the distance of the codeword could never be c).
Then, $d(C) = w(x-y) \geq \min_{x \in C} w(x)$ since $x-y$ is a codeword of C. However, for some $x \in C$ $\min_{x \in C} w(x) = w(x) = d(x,0) \geq d(C)$. Thus have both inequalities. □

Definition 1.5. A $k \times n$ matrix whose rows form a basis of a linear $[n,k]$ code is called a **generator matrix** of the code.

Theorem 1.6. Let G be a generator matrix of an $[n,k]$ code. Using EROs, G can be transformed into **standard form**

$$[I_k \mid A]$$

where I_k is the $k \times k$ identity and A is $k \times (n-k)$

1.1 Encoding with a Linear Code

Definition 1.7. Let C be $[n,k]$-code over $GF(q)$ with generator G. C contains q^k codewords, so that is the max possible number of distinct messages.
A message is a k-tuple of $V(k,q)$. Encode a message vector $u = u_1 u_2 \dots u_k$ by multiplying as uG.
Note that this is a map $V(k,q) \to C \subset V(n,q)$

Corollary 1.8. If G is in standard form, then the encoding $x = uG = (x_1, x_2, x_3, \dots, x_k, x_{k+1}, \dots, x_n)$ has $x_i = u_i$ for $1 \leq i \leq k$ (called **message digits**) and $x_{k+i} = \sum_{j=1}^{k} a_{ji} u_j$ for $1 \leq i \leq n-k$ (called **check digits**).

Example. Let C be binary $[7,4]$ code. Let

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

be its generator matrix.

A message vector u_1, u_2, u_3, u_4 is encoded as

$$(u_1, u_2, u_3, u_4, u_1 + u_2 + u_3, u_2 + u_3 + u_4, u_1 + u_2 + u_4)$$

For instance 1000 is encoded as 1000101.

1.2 Decoding with a Linear Code

Definition 1.9. Suppose the codeword x is sent and the codeword y is recieved. Define the **error vector** e as $e = y - x$.

Remark. Decoder must decide from y which codeword x was recieved, or equivalently which error vector e has occurred.

Definition 1.10. Suppose C is $[n, k]$ code over $GF(q)$ and a is a vector in $V(n, q)$. Then the set $a + C$ defined by

$$a + C = \{a + x \mid x \in C\}$$

is called a **coset** of C.

Lemma 1.11. Suppose $a + C$ is a coset of C and that $b \in a + C$. Then $b + C = a + C$.

Theorem 1.12. Suppose C is $[n, k]$ code over $GF(q)$. Then

1. Every vector of $V(n, q)$ is in some coset of C.
2. Every coset contains q^k vectors.
3. Two cosets either are disjoint or the same.

Proof.

1. If $a \in V(n, q)$, then $a = a + 0 \in C$ since the zero vector is always a codeword.
2. The mapping from C to $a + C$ defined by $x \to a + x$ is bijective. Thus $|a + C| = |C| = q^k$
3. Suppose $a+C, b+C$ overlap. Then for some vector v, have $v \in (a+C) \cap (b+C)$, thus for $x, y \in C$, $v = a+x = b+y$. Thus $b = a + (x - y) \in a + C$, by previous lemma $b + C = a + C$.

□

Example. Let C be binary $[4, 2]$ code with generator $G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$. That is, $C = \{0000, 1011, 0101, 1110\}$. Then the cosets are

$$\begin{aligned} 0000 + C &= C \\ 1000 + C &= \{1000, 0011, 1101, 0110\} \\ 0100 + C &= \{0100, 1111, 0001, 1010\} \\ 0010 + C &= \{0010, 1001, 0111, 1100\} \end{aligned}$$

All other cosets are the same as one of these. For instance, $0001 + C = 0100 + C$. This is because $0001 \in 0100 + C$ so lemma applies. Note that these cosets contain all 16 possible binary strings of length 4.

Definition 1.13. The vector having mininum weight in a coset is called the coset leader. Choose arbitrary ones if multiple have the same weight.
Above theorem shows $V(n, q)$ is partitioned into disjoint cosets of C:

$$V(n, q) = (0 + C) \cup (a_1 + C) \cup \cdots \cup (a_s + C)$$

where $s = q^{n-k} - 1$, and then take $0, a_1, \ldots, a_s$ to be the coset leaders.
A **standard array** for an $[n, k]$ code C is a $q^{n-k} \times q^k$ array of all the vectors in $V(n, q)$ in which the first row consists

of the code C with 0 on the extreme left, and the other rows are the cosets $a_i + C$, each arranged in order with the coset leader on the left.

Proposition 1.14. Creation of a standard array:

1. List the codewords of C starting with 0 as the first row.
2. Choose any vector a_1 not in the first row of min weight. List the coset $a_1 + C$ as the second row by putting a_1 under 0 and $a_1 + x$ under each $x \in C$.
3. Repeat until all cosets are listed and every vector appears exactly once.

Proposition 1.15. When a word is recieved, find its position in the array. Find the coset leader in that row, and subtract it from the word. The resulting codeword is the decoded word.
Briefly, take the codeword in the first row and same column as the recieved word.

2 Dual Codes and Syndrome Decoding

Definition 2.1. Let C be an $[n-k]$-code. The **dual code** of C, denoted by $C^\perp$ is defined to be the set of vectors of $V(n,q)$ which are orthogonal to every codeword of C, i.e.,

$$C^\perp = \{v \in V(n,q) \mid v \cdot u = 0 \; \forall u \in C\}$$

Lemma 2.2. Suppose C is an $[n-k]$-code having a generator matrix G. Then a vector $v \in V(n,q)$ is in $C^\perp$ iff v orthogonal to every row of G. That is, $v \in C^\perp \Leftrightarrow vG^T = 0$, where G^T is the transpose of G.

Theorem 2.3. Suppose C is an $[n,k]$-code over GF(q). Then the dual code $C^\perp$ is linear $[n, n-k]$ code.

Example. If $C = \{000, 110, 011, 101\}$ then $C^\perp = \{000, 111\}$.

Theorem 2.4. $(C^\perp)^\perp = C$.

Definition 2.5. A **parity-check** matrix H for an $[n,k]$ code C is a generator matrix for $C^\perp$.

Theorem 2.6. If $G = [I_k \mid A]$ is the standard form generator matrix of an $[n,k]$-code C, then a parity check matrix for C is $H = [-A^T \mid I_{n-k}]$.

Example. If

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

then

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

Definition 2.7. A parity check matrix H is said to be in **standard form** if $H = [B \mid I_{n-k}]$.

2.1 Syndrome Decoding

Definition 2.8. Suppose H is a parity-check matrix of $[n,k]$-code C. Then for any vector $y \in V(n,q)$, the $1 \times (n-k)$ row vector

$$S(y) = yH^T$$

is called the **syndrome** of y.

Remark.
1. If the rows of H are $h_1, h_2, \ldots, h_{n-k}$, then $S(y) = (y \cdot h_1, y \cdot h_2, \ldots, y \cdot h_{n-k})$.
2. $S(y) = 0 \Leftrightarrow y \in C$

Lemma 2.9. Two vectors u, v are in the same coset of C iff they have the same syndrome.

Proof. u, v in the same coset

$$\begin{aligned}
&\Leftrightarrow u + C = v + C \\
&\Leftrightarrow u - v \in C \\
&\Leftrightarrow (u-v)H^T = 0 \\
&\Leftrightarrow uH^T = vH^T \\
&\Leftrightarrow S(u) = S(v)
\end{aligned}$$

□

Corollary 2.10. There is a 1-1 correspondence between cosets and syndromes.

Proposition 2.11. Can simplify decoding by adding a syndromes column to the standard array, so when a word is recieved can calculate $S(y)$ to match the row in the standard array.

Proposition 2.12. Only need to keep track of two columns, the coset leader and the syndrome z.
1. For a recieved vector y calculate $S(y) = yH^T$.
2. Let $z = S(y)$ and locate the syndrome in the lookup table.
3. Let f map syndromes to their coset leaders. Then decode y as $y - f(z)$.

3 Hamming Codes

Definition 3.1. Let r be in $\mathbb{Z}^+$ and let H be an $r \times (2^r - 1)$ matrix whose columns are distinct non-zero vectors of $V(r,2)$. Then the code having H as its parity check matrix is called a **binary Hamming code** and is denoted by $\mathrm{Ham}(r,2)$.
That is, the parity check matrix contains all codewords of length r that are non-zero.

Example. For $r = 2$, $H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

Example. For $r = 3$,

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

and

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

Theorem 3.2. The binary Hamming code $\text{Ham}(r, 2)$ for $r \geq 2$,

1. is a $[2^r - 1, 2^r - 1 - r]$-code
2. has min distance 3
3. is perfect

3.1 Non-Binary Hamming Codes

Proposition 3.3. Constructing H for non-binary Hamming codes:
Consider all lines through zero. Pick one non-zero point on each line as the columns of H.

Example. $p = 3, r = 2$.

$$H = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Example. $p = 3, r = 3$

$$H = \begin{bmatrix} 0 & 1 & 2 & 0 & \dots & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & \dots & 2 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proposition 3.4. n in $\text{Ham}(r, p)$ is the number of lines in Z_p^r.

$$n = \frac{p^r - 1}{p - 1}$$

Proposition 3.5. A non-binary hamming code is a $[\frac{p^r-1}{p-1}, \frac{p^r-1}{p-1} - r]$ linear code.

4 Cyclic Codes

Definition 4.1. A code C is cyclic if

1. C is linear.
2. C is closed under shift S, i.e., $w \in C \implies S(w) \in C$.

Example. The code $C = \{000, 101, 011, 110\}$ is cyclic.

Remark. Note that a shift is a right shift, but left shifts can be simulated by shifting right $n - 1$ times where n is the length of the codeword.

Remark. Can view a cyclic code as a polynominal, where the digits of the codeword are coefficients for a polynominal of degree $n - 1$, $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$.

Definition 4.2. In a cyclic code, declare $x^n \equiv 1 \Leftrightarrow x^n - 1 = 0$.
Then a cyclic code C is a subspace of $Z_p[x]/(x^n - 1)$ such that C is closed under multiplication with x.

4.1 The Ring of Polynomials

Definition 4.3. Let F be a field. Then $F[x]$ is the set of polynominals with coefficients in F. Let $\deg f = d$, and f is **monic** if the term with highest degree has coefficient one.

Definition 4.4. Define division as

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

where $\deg r < \deg g$.

Definition 4.5. g divides f if $\frac{f(x)}{g(x)}$ has $r(x) = 0$.

Definition 4.6. Let $f(x)$ be a fixed polynominal in $F[x]$. Two polynominals g, h are said to be **congruent** modulo f symbolized by $g(x) = h(x) \pmod{f(x)}$ if $g(x) - h(x)$ is divisible by $f(x)$.

Remark. Any polynominal $a(x)$ is congruent modulo $f(x)$ to a unique polynominal $r(x)$, which is the principal remainder when $a(x)$ is divided by $f(x)$.

Definition 4.7. The GCD of f, g is the monic polynominal of highest degree that divides them.

Definition 4.8. $\alpha \in F$ is a **root** of f if $f(\alpha) = 0$

Theorem 4.9. α is a root of f if and only if $x - \alpha$ divides f.

Corollary 4.10. If $\deg f = n$, then f can have at most n roots.

Definition 4.11. $f(x) \in F[x]$ is **irreducible** if $f(x) \neq g(x)h(x)$ where $\deg g, \deg h < \deg f$. Usually take irreducibles monic.

Theorem 4.12. Every f can be factored as the product of irreducibles.

Corollary 4.13. Irreducible degree 3 or less polynominals must have no roots.

Remark. To find all monic irreducibles, helpful to list all polynominals (There are p^n of them, where p is the modulus, and n the degree), then count the reducible ones and subtract. Use stars and bars formula.

Definition 4.14. $Z_p[x]/f(x) = \{\text{all principal remainders divided by } f\} = \{\text{all } r(x) \text{ such that } \deg r < \deg f\}$ which is the set $\{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}\}$.

Example. The ring $Z_2[x]/(x^3 + x + 1)$ has the elements $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

4.1.1 Inverses

Definition 4.15. g^{-1} is the element such that $gg^{-1} = 1$ in $Z_p[x]/f(x)$. Note that the inverse may not always exist.

Theorem 4.16. g^{-1} exists if and only $\gcd(f, g) = 1$ in a ring mod f.

Theorem 4.17. $Z_p[x]/f(x)$ is a field if and only if $f(x)$ is irreducible in $Z_p[x]$

Example. $Z_2[x]/(x^2 + x + 1)$ is a field with four elements, also called $\mathbb{F}_4$.
$Z_2[x]/(x^3 + x + 1)$ is a field with eight elements, also called $\mathbb{F}_8$.

Proposition 4.18. Every field with finite number of elements has form $\mathbb{F}_q$ where $q = p^n$ for some prime p.

Remark. If two fields have the same modulus p and the same degree modular polynominal, then they are isomorphic.

Proposition 4.19. Every $\mathbb{F}_{p^n}$ has a primitive element g such that the powers $g, g^2, \ldots, g^{p^n-1} = 1$ are distinct.

4.2 Ideals

Definition 4.20. Let $R_n = F[x]/(x^n - 1)$ where $F = F_q$ be implicit.

Definition 4.21. A simpler definition for a cyclic code $C \subset R_n$ is

1. $0 \in C$
2. $g(x), h(x) \in C \implies g(x) + h(x) \in C$
3. $g(x) \in C, r(x) \in \mathbb{R}_n \implies r(x)g(x) \in C$

C is called an **ideal** in the ring R_n.

Proof. Suppose C is cyclic in R_n. C is thus linear and so the additive closure condition holds.
Let $a(x) \in C$ and $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} \in R_n$. Since multiplication by x corresponds to a cyclic shift, we have $xa(x) \in C$ and $x^2a(x) \in C$ and so on. Hence $r(x)a(x) = r_0a(x) + r_1xa(x) + \cdots + r_{n-1}x^{n-1}a(x)$ is also in C since each term is in C. This the multiplicative closure condition holds.
Taking $r(x) = 0$ satifies the zero condition. □

Remark. Note that taking $r(x) = c$ in the above proof implies C is linear and $r(x) = x$ implies C is cyclic.

Definition 4.22. Let R be a ring. I is **principal** if $I = \langle g \rangle = R \cdot g$.

Example. $R = \mathbb{Z}, I = \langle 12, 18 \rangle$, $I = \{a \cdot 12 + b \cdot 18 \mid a, b \in \mathbb{Z}\}$. Claim $6 \in I$, since 6 is the gcd. Claim $I = \langle 6 \rangle$ because $12a + 18b = \mathbb{Z} \cdot 6$

Proposition 4.23. Every ideal in $\mathbb{Z}$ is principal. $\langle g_1, g_2, \ldots, g_n \rangle = \langle d \rangle$ where $d = \gcd(g_i)$.

Example. Given an ideal $I \subset \mathbb{Z}$, know that $I = \langle d \rangle$. Find d by taking the smallest positive number in I.

Theorem 4.24. Every cyclic code (non-zero) is of the form $\langle g(x) \rangle \subset R_n$ where g divides $x^n - 1$. The generator g is unique if it is monic.

Corollary 4.25. Cyclic codes are 1-1 with monic g that divide $x^n - 1$

4.3 Generator Polynomials

Definition 4.26.

$$\langle f(x) \rangle = \{r(x)f(x) \mid r(x) \in R_n\}$$

Theorem 4.27. For any $f(x) \in R_n$, the set $\langle f(x) \rangle$ is a cyclic code, and it is called the code generated by $f(x)$.

Proof. Check the conditions of 4.21

1. Let $a(x)f(x), b(x)f(x) \in \langle f(x) \rangle$. then $a(x)f(x) + b(x)f(x) = (a(x) + b(x))f(x) \in \langle f(x) \rangle$
2. Let $a(x)f(x) \in \langle f(x) \rangle$, $r(x) \in R_n$, then

$$r(x)(a(x)f(x)) = (r(x)a(x)) \in \langle f(x) \rangle$$

□

Example. Consider the code $C = \langle 1 + x^2 \rangle$ in R_3 with $F = GF(2) = \mathbb{Z}_2$. Multiplying by each of the 8 elements of R_3, (i.e. $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$) and reducing modulo $x^3 - 1$ produces only 4 distinct codewords, namely $0, 1 + x, 1 + x^2, x + x^2$. Thus C is the code $\{000, 110, 101, 011\}$.

Theorem 4.28. Let C be a non-zero cyclic code in R_n. Then,

1. There exists a unique monic polynominal $g(x)$ of smallest degree in C.
2. $C = \langle g(x) \rangle$
3. $g(x)$ is a factor of $x^n - 1$

Definition 4.29. The polynominal given by the above is called the **generator polynominal** of C.

Example. We find all the binary cyclic codes of length $n = 3$. Factor $x^3 - 1$ as $(x-1)(x^2+x+1)$, both irreducible. By 4.28. Thus, a list of binary cyclic codes is:

1. Generator Polynomial: 1, Code in R_3: All of R_3, Corresponding Code in $V(3,2)$: all of $V(3,2)$
2. Generator Polynomial: $x+1$, Code in R_3: $\{0, 1+x, x+x^2, 1+x^2\}$, Corresponding Code in $V(3,2)$: $\{000, 110, 011, 101\}$.
3. Generator Polynomial: x^2+x+1, Code in R_3: $\{0, 1+x+x^2\}$, Corresponding Code in $V(3,2)$: $\{000, 111\}$.
4. Generator Polynomial: $x^3 - 1 (= 0)$, Code in R_3: $\{0\}$, Corresponding Code in $V(3,2)$: $\{000\}$.

Lemma 4.30. Let $g(x) = g_0 + g_1 x + \cdots + d_r x^r$ be generator polynominal of a cyclic code. Then $g_0 \neq 0$.

Example. Let $p = 2$, $n = 7$ (binary codes of length 7). Find all cyclic codes. Must find all $g(x) \mid x^n - 1$ since they will be generators (also multiplied togeher). Have $x^n - 1 = (x-1)(x^3+x+1)(x^3+x^2+1)$. Let $a(x), b(x), c(x)$ correspond to these three polynominals. Then,

$\deg g$	$g(x)$	$\dim C$
0	1	7
1	$a(x)$	6
2	–	5
3	$b(x), c(x)$	4
4	$a(x)b(x), a(x)c(x)$	3
5	–	2
6	$b(x)c(x)$	1
7	$a(x)b(x)c(x)$	0

Note that $\dim C = n - \deg g(x)$.
Confused here and next theorem.

4.4 Generator and Parity Check Matrices

Theorem 4.31. Let $C = \langle g(x) \rangle$. Then every codeword in C can be written as $w(x) = a(x)g(x)$ where $\deg a(x) < n - \deg g(x)$. Moreover, such a is unique.

Example. Continued from previous example. Pick $g(x) = (x+1)(x^3+x+1)$. Note that $\deg g = 4$. Then any codeword $w(x) = (a_0 + a_1 x + a_2 x^2) g(x) = a_0 g + a_1 xg + a_2 x^2 g$. Thus $g, xg, x^2 g$ are a basis for C.

Theorem 4.32. Let $C = \langle g \rangle$. Let $\deg g = d$. Then $g, xg, x^2 g \ldots x^{n-d-1} g$ form a basis for C. There are $n-d$ elements.

Theorem 4.33. Let C be cyclic with generator

$$g(x) = g_0 + g_1 x + \cdots + g_r x^r$$

of degree r. Then $\dim C = n - r$ with generator matrix

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 \\ 0 & 0 & \vdots & \vdots & \vdots & \cdots & \cdots & \ddots & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r \end{bmatrix}$$

This matrix is $n - r \times n$.

Example. 12.13

Example. Let $n = 12$ and work in $GF(2)$. How many cyclic codes of dimension $k = 8$?
This is the same as saying how many $g(x)$ of degree 4 since $\dim C = n - \deg g$.
Factor $x^{12} - 1$ into $(x + 1)^4(x^2 + x + 1)^4$.
Thus there are 3 such codes comprised of the polynominals $(x + 1)^4, (x^2 + x + 1)^2, (x^2 + x + 1)(x + 1)^2$.

Definition 4.34. Let C be cyclic $[n, k]$-code with generator $g(x)$. By theorem, $g(x)$ is a factor of $x^n - 1$ and so

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

for some polynominal h. Note that h is monic since g is. $g(x)$ has degree $n - k$ from 4.33 so h has degree k. The polynominal h is called the **check polynominal** of C.

Theorem 4.35. Suppose C is cyclic in R_n with generator g and check polynominal h. Then an element $c(x)$ is a codeword of C iff $c(x)h(x) = 0$.

Example. Let $n = 7$ working in $GF(2)$, with $g(x) = (x - 1)(x^3 + x + 1)$. Then $h(x) = x^3 + x^2 + 1$. Want to know if $w(x) = x^6 + x^3 + x^2 + x \in C$. Multiplying with $h(x)$ yields 0 so it is a codeword.

Theorem 4.36. Suppose C is cyclic $[n, k]$-code with check polynominal $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Then,

1. a parity-check matrix for C is

$$H = \begin{bmatrix} h_k & k_{k-1} & \cdots & h_0 & 0 & 0 & 0 & 0 \\ 0 & h_k & k_{k-1} & \cdots & h_0 & 0 & 0 & 0 \\ 0 & 0 & h_k & k_{k-1} & \cdots & h_0 & 0 & 0 \\ 0 & 0 & 0 & h_k & k_{k-1} & \cdots & h_0 & 0 \\ 0 & 0 & 0 & 0 & h_k & k_{k-1} & \cdots & h_0 \end{bmatrix}$$

2. $C^\perp$ is a cyclic code generated by the polynominal $\overline{h}(x) = h_k + h_{k-1}x + \cdots + d_0x^k$

The size of H is $n - k \times n$ since $n - k = \dim C^\perp = \deg g$

Definition 4.37. The polynominal $\overline{h}(x) = x^k h(x - 1) = h_k + h_{k-1}x + \cdots + h_0x^k$ is called the **reciprocal polynominal** of h, its coefficients are those of h in reverse order.
We may regard $\overline{h}$ as the generator of $C^\perp$ though we should multiply by h_0^-1 to make it monic.

Remark. The polynominal $h(x - 1) = x^{n-k}\overline{h}(x)$ is a member of $C^\perp$