§ 9 Algebraic Codes

Polynomials

Let F be a field.

$F[x]$ = set of all polynomials with coefficients in F.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ and $a_n \neq 0$, we say that degree of $f(x)$ is n and it is denoted by $\deg(f(x)) = n$.

Proposition 9.1 (Division Algorithm)

Let $f(x), g(x) \in F[x]$ such that $\deg(g(x)) > 0$.

There exist unique $q(x), r(x) \in F[x]$ with $\deg(r(x)) < \deg(g(x))$ such that $f(x) = g(x)q(x) + r(x)$.

Example 9.1

Let $f(x) = x^4 + 2x^3 + 3x^2 + 4x + 4$, $g(x) = x^2 + 4x + 1 \in \mathbb{Z}_5[x]$.

$$
\begin{array}{r}
x^2 + 3x \\
x^2+4x+1 \;\overline{)\; x^4 + 2x^3 + 3x^2 + 4x + 4} \\
\underline{x^4 + 4x^3 + x^2} \\
3x^3 + 2x^2 + 4x \\
\underline{3x^3 + 2x^2 + 3x} \\
x + 4
\end{array}
$$

$q(x) = x^2 + 3x$, $r(x) = x + 4$

Proposition 9.2 (Factor Theorem)

Let $a \in F$ and $f(x) \in F[x]$.

$f(a) = 0$ if and only if $x - a$ is a factor of $f(x)$.

proof.

By division algorithm, $f(x) = (x-a)q(x) + r$ for some $q(x) \in F[x]$ and $r \in F$.

Then $f(a) = r$ and so $f(a) = 0 \Leftrightarrow x - a$ is a factor of $f(x)$.

Corollary 9.1

A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in F.

Corollary 9.2

If G is a finite subgroup of the multiplicative group $(F^*, \cdot)$ of a field F, then G is cyclic. In particular, if F is a finite field, $(F^*, \cdot)$ is a cyclic group.

proof:

Note that G is a finite abelian group and hence isomophic to $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z}$ for some primes p_i and $k_i \in \mathbb{Z}^+$

Let $m = \operatorname{lcm}(p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r})$, then $m \le p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

On the other hand, since $p_i^{k_i} \mid m$ for all $i = 1, 2, \cdots, r$, so if $(x_1, x_2, \ldots, x_r) \in \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z}$ we have $m(x_1, x_2, \ldots, x_r) = (0, 0, \ldots, 0)$. For the corresponding element $\alpha \in G$ of $(x_1, x_2, \ldots, x_r)$, we have $\alpha^m = 1$, and hence α is a zero of $x^m - 1 = 0$

Therefore $x^m - 1$ has at least $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ distinct zeros, which implies $m \ge p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

We have $m = \operatorname{lcm}(p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, and so those p_i's are distinct primes, and $G \cong \mathbb{Z}/m\mathbb{Z}$ which is a cyclic group.

Example 9.2

If p is a prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$ which is a cyclic group.

Definition 9.1

A noncontant polynomial $f(x) \in F[x]$ is irreducible over F or is an irreducible polynomial in $F[x]$ if $f(x)$ cannot be expressed as $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$ with $\deg(g(x)), \deg(h(x)) < \deg(f(x))$

Example 9.3

$x^2 - 2 \in \mathbb{Q}[x]$ is an irreducible polynomial.

$x^2 - 2 \in \mathbb{R}[x]$ is a reducible polynomial and $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Example 9.4

Let $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$. If $f(x)$ is reducible over $\mathbb{Z}_5$, then it must have a linear factor. However, $f(0) = 2$, $f(1) = 1$, $f(2) = 1$, $f(3) = 3$, $f(4) = 3$, all of them are nonzero which implies $f(x)$ has no linear factor. Therefore $f(x)$ is irreducible over $\mathbb{Z}_5[x]$.

Proposition 9.3

Let $f(x) \in F[x]$ such that $\deg(f(x)) = 2$ or 3.

Then $f(x)$ is reducible over F if and only if f has a zero in F.

Finite Fields

Proposition 9.4

If F is a field with $|F| = p$ where p is a prime, then F is isomorphic to $\mathbb{Z}_p$.

Proposition 9.5

For all primes p and positive integers k, there exists an irreducible polynomial $g(x) \in \mathbb{Z}_p[x]$ which is of degree k.

Note that the ideal $\langle g(x) \rangle$ in $\mathbb{Z}_p[x]$ is a maximal ideal, so $\mathbb{Z}_p[x]/\langle g(x) \rangle$ is a field.

Furthermore, elements in $\mathbb{Z}_p[x]/\langle g(x) \rangle$ are of the form $r(x) + \langle g(x) \rangle$ where $r(x) \in \mathbb{Z}_p[x]$ with $\deg(r(x)) \leq k-1$. Therefore, $|\mathbb{Z}_p[x]/\langle g(x) \rangle| = p^k$.

However, what we have is not just the existence of a field of order p^k, but the following:

Theorem 9.1 (Characterization of Finite Fields)

Every finite field has order p^k where p is a prime and k is a positive integer.

Furthermore, all fields of order p^k are isomorphic to $\mathbb{Z}_p[x]/\langle g(x) \rangle$ for an arbitrary choice of degree k irreducible polynomial $g(x) \in \mathbb{Z}_p[x]$.

Therefore, we denote the unique (up to isomorphism) finite field of order p^k by $GF(p^k)$.

Example 9.5

Let $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Note that $f(0) = f(1) = 1 \neq 0$, so $f(x)$ has no linear factor and hence it is irreducible over $\mathbb{Z}_2$.

Therefore, $F = \mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$ is a field of order $2^2 = 4$.

$F = \{0, 1, x, x+1\}$ (For simplicity, we write $r(x)$ but not $r(x)+\langle x^2+x+1 \rangle$)

$x^2 + x + 1 \equiv 0 \pmod{x^2+x+1}$

$x^2 \equiv -x - 1 \equiv x + 1 \pmod{x^2+x+1}$

Therefore, $x \cdot (1+x) \equiv x + x^2 \equiv x + (x+1) \equiv 1 \pmod{x^2+x+1}$

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

·	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Let $\alpha = 1+x$, then $\alpha^2 = x$, $\alpha^3 = 1$.

We can see the multiplicative group $(F^*, \cdot)$ is cyclic with $\alpha = x+1$ as a generator.

(i.e. $(F^*, \cdot) \cong (\mathbb{Z}/3\mathbb{Z}, +)$)

Example 9.6

Exercise: Show that $g(x) = x^3+x+1 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$.

Therefore, $F = \mathbb{Z}_2[x]/\langle g(x) \rangle$ is a field of order $2^3 = 8$.

$F = \{ a_2x^2 + a_1x + a_0 : a_i \in \mathbb{Z}_2 \}$

Let $h(x) = x^2+x+1 \in F$. How to find the multiplicative inverse of $h(x)$?

Extended Euclidean Algorithm:

$g(x) = (x+1)\,h(x) + x$

$h(x) = (x+1)\,x + 1$

$$x^2+x+1 \;\overline{)\; x^3 \quad\quad\quad +1}\;\; x+1$$
$$x^3+x^2+x$$
$$x^2 \quad\quad +1$$
$$x^2+x+1$$
$$x$$

$1 = h(x) + (x+1)x$

$= h(x) + (x+1)[g(x) + (x+1)h(x)]$

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

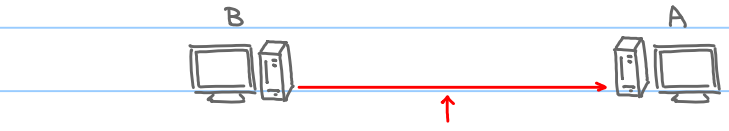
$\therefore x^2 h(x) \equiv 1 \pmod{g(x)}$ and multiplicative inverse of $h(x) = x^2+x+1$ is x^2

Note that $|F^*| = 2^3 - 1 = 7$, so the multiplicative group $(F^*, \cdot)$ is cyclic and isomorphic to $(\mathbb{Z}/7\mathbb{Z}, +)$. Since 7 is a prime, $\varphi(7) = 6$ which means all elements except 1 in F^* are generators.

Analogies between $\mathbb{Z}$ and $F[x]$:

The integer ring $\mathbb{Z}$	The polynomial ring $F[x]$
Integers	Polynomials
Primes	Irreducible polynomials
$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \cdots, m-1\}$	$F[x]/\langle f(x)\rangle = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in F\}$ $(\deg(f(x)) = n)$
$a+b \pmod m$	$g(x)+h(x) \pmod{f(x)}$
$a\,b \pmod m$	$g(x)\cdot h(x) \pmod{f(x)}$
$\mathbb{Z}/m\mathbb{Z}$ is a field $\Leftrightarrow$ m is a prime	$F[x]/\langle f(x)\rangle$ is a field $\Leftrightarrow$ $f(x)$ is irreducible

Error Correcting Codes



Error correction needed !

Example 9.7

Suppose we send a bit 0 or 1 across a noisy channel that has a probability $p = 0.1$ of error.

If $m = 1$ is the message to be sent, instead of send m directly, we send 111 (repeat 3 times).

If one receives 011, 101 or 110, he corrects it as 111;

but if he receives 001, 010, 100 or 000, he tends to think the original message is 000.

Then he has $0.9^3 + 3 \times 0.9^2 \times 0.1 = 0.972\ (> 0.9)$ chance to get the correct message.

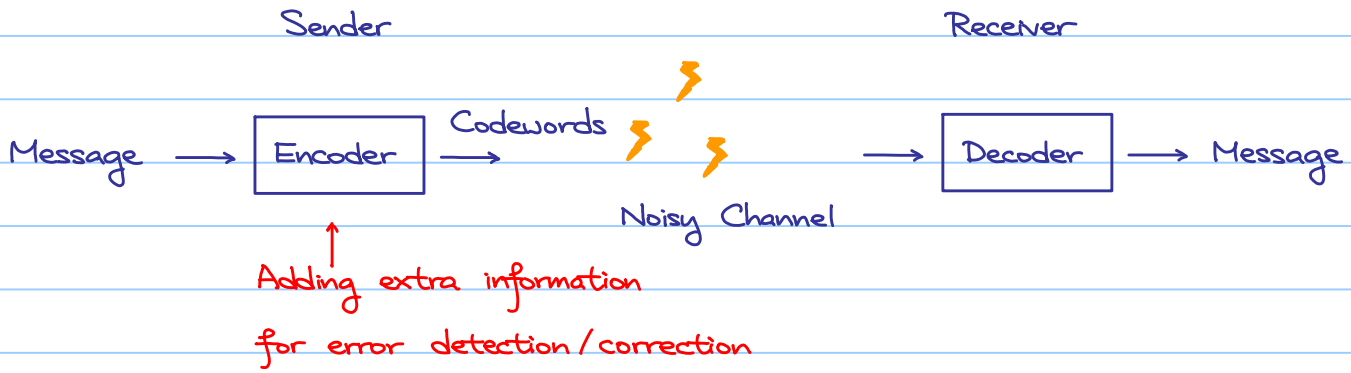
However, if 11 (repeat twice) is sent, 01 or 10 is received. The receiver is able to detect the error, but he does not know how to correct !

(Error Detection ≠ Error Correction)

Example 9.8 (Parity Check)

Suppose a message of 7 bit is sent. We add an eighth bit so that the number of nonzero bits is even. For example, the message 0110111 becomes 01101111.

If there is one error, it can be detected but not corrected



Definition 9.1

Let A be an alphabet (set of symbols). A code of length n is a nonempty subset $C \subseteq A^n$. Each element in C is called a codeword. If $|A| = q$, C is called a q-ary code.

In example 9.7 and 9.8, $A = \mathbb{Z}_2 = \{0, 1\}$.

In example 9.7, $C = \{(0,0,0), (1,1,1)\}$;

in example 9.8, $C = \{(a_1, a_2, \cdots, a_8) : a_i \in \mathbb{Z}_2 \text{ and } \sum_{i=1}^{8} a_i \equiv 0 \pmod 2\}$

Definition 9.2

Let $u, v \in A^n$, the Hamming distance $d(u,v)$ is the number of places where u and v differ.

Proposition 9.6

The Hamming distance is a metric on A^n, i.e.

1) $d(u,v) \geq 0$ for all $u, v \in A^n$ and $d(u,v) = 0$ if and only if $u = v$;

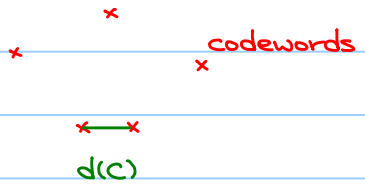
2) $d(u,v) = d(v,u)$ for all $u, v \in A^n$;

3) $d(u,v) \leq d(u,w) + d(w,v)$ for all $u, v, w \in A^n$ (called triangle inequality)

Definition 9.3

Let C be a code.

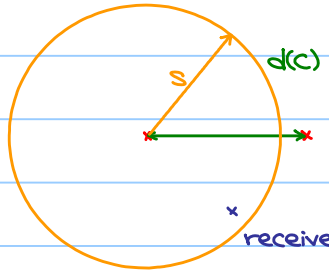
The minimum distance of C is defined as $d(C) = \min\{d(u,v) : u, v \in C, u \neq v\}$.



Notation: A code of length n, with $M = |C|$ codewords, and with minimum distance $d = d(C)$, is called an (n, M, d) code.

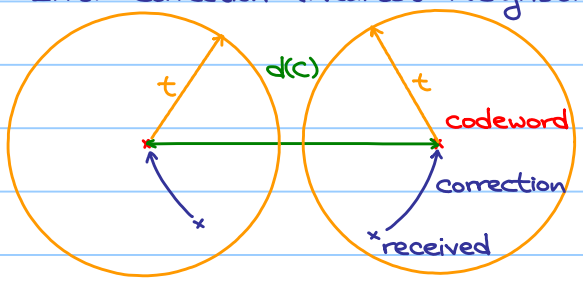
Idea:

Error Detection



error detected

Error Correction (Nearest Neighbor Decoding)



Proposition 9.7

A code C can detect up to s errors if $d(C) > s$, i.e. $d(C) \geq s+1$

A code C can correct up to t errors if $d(C) > 2t$, i.e. $d(C) \geq 2t+1$

Bounds on General Codes

Proposition 9.8 (Singleton Bound)

Let C be a q-ary code. Then $M \leq q^{n-d+1}$.

proof:

Let $c = (c_1, c_2, \cdots, c_n)$ and $c' = (c_d, c_{d+1}, \cdots, c_n)$.

If $b, c \in C$ with $b \neq c$, then $d(b, c) \geq d(C) = d$. Therefore, $d(b', c') \geq 1$.

$b = (b_1, b_2, \cdots, b_{d-1}, b_d, b_{d+1}, \cdots, b_n)$

$c = (c_1, c_2, \cdots, c_{d-1}, c_d, c_{d+1}, \cdots, c_n)$

$\vdots$

M

each pair of truncated codewords differ in at least one place

$\Rightarrow M \leq q^{n-d+1}$

Remark: A code satisfies the Singleton bound with equality is called an MDS code (Maximum Distance Separable)

(Maximize the number of possible codewords)

Definition 9.4

A Hamming sphere of radius r centered at a codeword c, $B(c,r)$ is defined as $B(c,t) = \{x \in A^n : d(x,c) \leq r\}$.

Remark: $B(c,r)$ contains elements $x \in A^n$ that differ from c in at most r places.

Lemma 9.1

$B(c,t)$ has $\sum_{k=0}^{r} C_k^n (q-1)^k = C_0^n + C_1^n(q-1) + C_2^n(q-1)^2 + \cdots + C_r^n(q-1)^r$ elements

Proposition 9.9 (Sphere Packing Bound)

Let C be a q-ary (n,M,d) code with $d \geq 2t+1$ (Correct up to t errors). Then,

$$M \leq \frac{q^n}{\sum_{k=0}^{t} C_k^n (q-1)^k}.$$

proof:

If $c_1, c_2 \in C$ with $c_1 \neq c_2$, $d(c_1,c_2) \geq d(C) = d \geq 2t+1$.

Therefore, $B(c_1,t) \cap B(c_2,t) = \phi$.

(number of codewords) $\times$ (number of elements per sphere) $\leq q^n$

$$M\left(\sum_{k=0}^{t} C_k^n (q-1)^k\right) \leq q^n$$

Remark: A code satisfies the sphere packing bound with equality is called a perfect code

In this case, we have $\coprod_{c \in C} B(c,t) = A^n$ and so every received $x \in A^n$ can be corrected to the unique $c \in C$ with $x \in B(c,t)$.

Example 9.9

Suppose $C = \{(0,0,0), (1,1,1), (2,2,2)\} \leq A^3$ where $A = \mathbb{Z}_3$. Then $n=3$, $q=3$, $M=3$.

Clearly $d = d(C) = 3 \geq 2t+1$ where $t=1$

We see that $M = 3 < \frac{27}{7} = \frac{q^n}{\sum_{k=0}^{t} C_k^n (q-1)^k}$.

In particular, we have six elements $(0,1,2), (0,2,1), (1,0,2), (1,2,0), (2,0,1), (2,1,0)$ which do not lie in any $B(c,1)$ with $c \in C$.

Linear Codes

Definition 9.5

If $A = F$ which is a finite field, the code $C \subseteq F^n$ is a vector subspace, then C is called a linear code.

In this case, if $|F| = q$ and $\dim(C) = k \leq n$, then there exists a basis $\{v_1, v_2, \cdots, v_k\} \subseteq C$ such that for all $v \in C$, there exist unique $a_1, a_2, \cdots, a_k \in F$ such that $v = a_1v_1 + a_2v_2 + \cdots + a_kv_k$.
Hence, $M = |C| = q^k$

Notation: A linear code of dimension k and length n is called a $[n,k]$ code.
Furthermore, if the minimum distance of the code is d, it is called a $[n,k,d]$ code.
(Therefore a $[n,k,d]$ code is a (n, q^k, d) code, where $|F| = q$.)

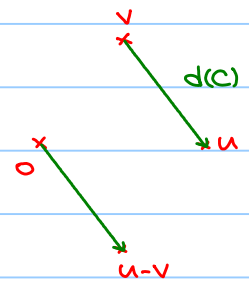
For a general code C, it may be hard to compute $d(C)$, but we have the following proposition if C is a linear code:

Proposition 9.10

If $u \in F^n$, the Hamming weight $wt(u)$ of u is defined as the number of nonzero places.
Then $d(C) = \min\{wt(u) : u \in C \text{ and } u \neq 0\}$.

proof:
Note that $0 \in C$, so $d(C) \leq d(u,0) = wt(u)$ for all $u \in C$ with $u \neq 0$.
Therefore, $d(C) \leq \min\{wt(u) : u \in C \text{ and } u \neq 0\}$.
On the other hand, $d(C) = d(u,v)$ for some $u, v \in C$.
Since $u, v \in C$, we have $u - v \in C$ Therefore,

$$d(u,v) = d(u-v, 0) = wt(u-v) \geq \min\{wt(u) \cdot u \in C \text{ and } u \neq 0\}.$$



One way to construct a $[n,k]$ code is the following.

Let $I_k \in M_k(F)$ be the identity matrix, $P \in M_{k,n-k}(F)$.

Then $G = [I_k \; P] \in M_{k\times n}(F)$

Note that the k row vectors $v_1, v_2, \cdots, v_k \in F^n$ form a linearly independent set,

so $C = \text{span}(\{v_1, v_2, \cdots, v_k\}) = \{v = a_1v_1 + a_2v_2 + \cdots + a_kv_k : a_i \in F\}$ is a k-dimensional subspace of F^n.

In this case, G is called a generating matrix. Also, $C = \{xG \in F^n : x \in F^k\}$.

Suppose that $x \in F^k$ is the message, then $xG \in F^n$ is the encoded message.

Question: Given $v \in F^n$, how do we determine whether v is a codeword, i.e. $v \in C$?

Definition 9.6

A matrix H is called a parity check matrix for C if H has the property that $v \in C$ if and only if $vH^T = 0$ (It means v is perpendicular to each row vector of H)

Proposition 9.11

If $G = [I_k \; P] \in M_{k\times n}(F)$ is the generating matrix for a code C, then $H = [-P^T, I_{n-k}] \in M_{(n-k)\times n}(F)$ is a parity check matrix for C.

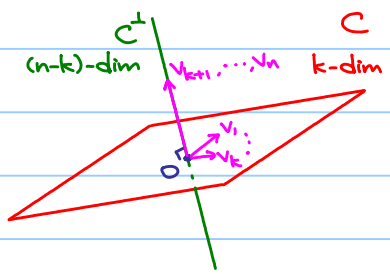
proof:

$$\begin{bmatrix} v_1H^T \\ v_2H^T \\ \vdots \\ v_kH^T \end{bmatrix} = GH^T = [I_k \; P] \cdot \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} = -P + P = 0 \; (\in M_{k\times(n-k)}(F)) \quad \text{where } v_i\text{'s are row vectors of } G.$$

$\therefore v_iH^T = 0$ for $i = 1, 2, \cdots, k$.

If $v \in C$, $v = \sum_{i=1}^{k} a_iv_i$ for some $a_i \in F$, then $vH^T = (\sum_{i=1}^{k} a_iv_i)H^T = \sum_{i=1}^{k} a_iv_iH^T = 0 \quad (\in M_{1\times(n-k)}(F))$

Idea. $G = \begin{bmatrix} v_1 \\ \vdots \\ v_k \end{bmatrix} \in M_{k\times n}(F)$, $H = \begin{bmatrix} v_{k+1} \\ \vdots \\ v_n \end{bmatrix} \in M_{(n-k)\times n}(F)$ i.e. $v_i \in F^n$ for $i = 1, 2, \cdots, n$.



Therefore, another way to construct a linear code is giving $H \in M_{(n-k)\times n}(F)$ such that the row vectors form a linearly independent set and define $C = \{v \in F^n : vH^T = 0\}$ (Null space of H).

Example 9.10 (Revisit of example 9.8)

Let $G = \left(\boxed{I_7} \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} \right) \in M_{7\times 8}(\mathbb{Z}_2)$

If $x = (a_1, a_2 \cdots a_7) \in \mathbb{Z}_2^7$, then $xG = (a_1, a_2 \cdots a_7\ a_8)$ where $a_8 \equiv \sum_{i=1}^{7} a_i \pmod 2$

There $C = \{(a_1, a_2 \cdots a_8) \in \mathbb{Z}_2^8 : a_8 \equiv \sum_{i=1}^{7} a_i \pmod 2\} \leq \mathbb{Z}_2^8$

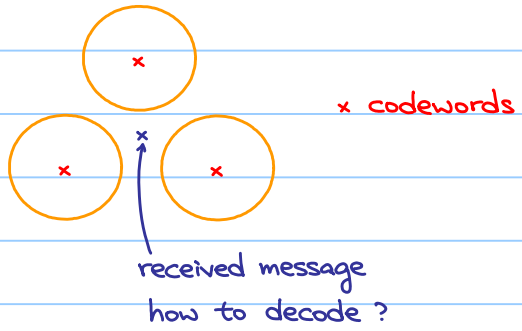
Note that $\sum_{i=1}^{8} a_i \equiv 2\sum_{i=1}^{7} a_i \equiv 0 \pmod 2$, i.e. we add the eighth place to a message $x \in \mathbb{Z}_2^7$ so that the number of nonzero places of the encoded message $xG \in \mathbb{Z}_2^8$ is even.

Also, $H = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \in M_{1\times 8}(\mathbb{Z}_2)$. If one receives $v = (a_1, a_2 \cdots a_8) \in \mathbb{Z}_2^8$, we compute vH^T which is exactly $\sum_{i=1}^{8} a_i \pmod 2$ (1×1 matrix, to be precise) which is 0 if and only if $v \in C$.

Decoding

Nearest neighbor decoding.

Problems: If C is not a perfect code,



In general, the problem of finding the nearest neighbor in a general linear code is an NP-complete problem

Syndrome decoding:

If a codeword $c \in C \subseteq F^n$ is sent and $v \in F^n$ is received, then $r = v - c \in F^n$ is the error.

Idea: Construct a table:

$r_1 = 0$	$c_1 = 0$	c_2	$\cdots$	c_M	codewords
r_2	r_2	$c_2 + r_2$	$\cdots$	$c_M + r_2$	
r_3	r_3	$c_2 + r_3$	$\cdots$	$c_M + r_3$	
$\vdots$					
r_N	r_N	$c_2 + r_N$	$\cdots$	$c_M + r_N$	

decode

complete lists of elements of F^n

How to choose r_i's?

Among the vectors which are not in the first row, choose one of the smallest weight to be r_2 (probably more than one choices).

Among the vectors which are not in the first two rows, choose one of the smallest weight to be r_3.

$\vdots$

Until getting a complete list of elements of F^n.

Exercise 9.1

Let $u + C = \{u + c \mid c \in C\}$ (called a coset of C)

Show that $(r_i + C) \cap (r_j + C) = \phi$ if $i \neq j$.

Example 9.11

Let C be a linear code with generating matrix $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in M_{2\times 4}(\mathbb{Z}_2)$.

Then, $C = \{(0,0,0,0), (1,0,1,1), (0,1,1,0), (1,1,0,1)\}$.

c_1 =	c_2 =	c_3 =	c_4 =
$(0,0,0,0)$	$(1,0,1,1)$	$(0,1,1,0)$	$(1,1,0,1)$
$(1,0,0,0)$	$(0,0,1,1)$	$(1,1,1,0)$	$(0,1,0,1)$
$(0,1,0,0)$	$(1,1,1,1)$	$(0,0,1,0)$	$(1,0,0,1)$
$(0,0,0,1)$	$(1,0,1,0)$	$(0,1,1,1)$	$(1,1,0,0)$

decode

It may be slow, since we have to search among the whole table!

Parity check matrix H helps!

Note that if $v \in F^n$, $v = c_i + r_j$ for some $c_i \in C$ and r_j

Then, $vH^T = (c_i + r_j)H^T = c_iH^T + r_jH = r_jH$ (depends on r_j only)

Construct a table: Coset Leader — Syndrome

Coset Leader	Syndrome
$r_1 = 0$	$r_1H^T = 0$
r_2	r_2H^T
$\vdots$	$\vdots$
r_N	r_NH^T

Once v is received, compute vH^T and it equals r_jH^T from some j.

Then, we decode v as $c = v - r_j$.

Back to the example, $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, then $H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$.

Coset Leader	Syndrome
$r_1 = (0,0,0,0)$	$r_1H^T = (0,0)$
$r_2 = (1,0,0,0)$	$r_2H^T = (1,1)$
$r_3 = (0,1,0,0)$	$r_3H^T = (1,0)$
$r_4 = (0,0,0,1)$	$r_4H^T = (0,1)$

If $v = (1,1,1,1)$ is received, $vH^T = (1\ 1\ 1\ 1)\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (1\ 0) = r_3H^T$

↑ Only need to search the table of syndromes!

then we decode it as $c = v - r_3 = (1,0,1,1)$.

Discussion:

Every received vector $v \in F^n$ can be decoded.

However, it may not be the nearest neighbor decoding.

Note that $d(v, c_2) = d(v, c_4) = 1$, but we decode v as c_2 but not v_4.

In fact $d(C) = 2$, so we cannot correct one error.

Exercise 9.2

Replace $r_3 = (0,1,0,0)$ by $(0,0,1,0)$ in the above example and decode $v = (1,1,1,1)$ again.

Ans: $c_4 = (1,1,0,1)$ will be obtained. Therefore, the result depends on choices of r_i's.

Binary Hamming Codes

Application of the (binary) Hamming codes:

Controlling errors in long-distance telephone calls.

code length: $n = 2^m - 1$

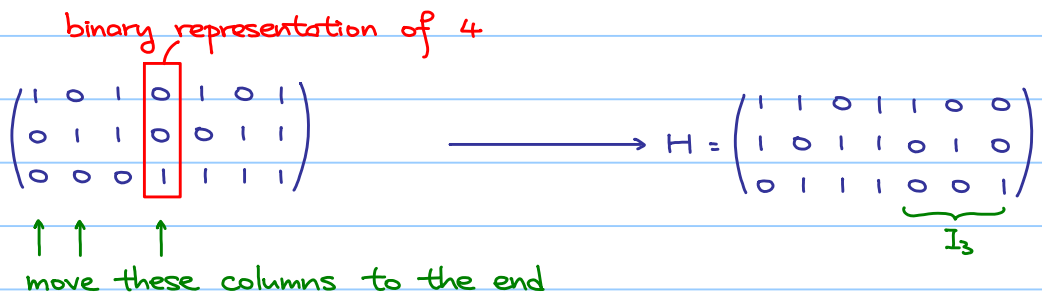
$\dim(C)$: $k = 2^m - m - 1$ (so $n - k = m$)

where $m \geq 2$

Construction of H:

Construct a $m \times n$ matrix such that the j-th column is the binary representation of j. Move the column representing $1, 2, 4, \cdots, 2^{m-1}$ to the end to obtain $H = (* \; I_m)$.

Example: $m = 3$, then $n = 7$, $k = 4$.



The linear code associated by the above H is called the Hamming code

Example 9.12 ([7,4] Hamming code)

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{and so} \quad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$-P^T$ $\qquad$ P

Let $v \in C$ with $v \neq 0$. Then $wt(v) > 0$.

Note that $vH^T = 0$, so

(i) $wt(v) \neq 1$, otherwise $v = e_i$ and $vH^T = e_i H^T =$ i-th row of $H^T \neq 0$

(ii) $wt(v) \neq 2$, otherwise $v = e_i + e_j$, $i \neq j$ and $0 = vH^T = e_i H^T + e_j H^T$ which implies the i-th and j-th row of H^T are the same (Contradiction).

$\therefore wt(v) \geq 3$

Also, note that if $v=(1\,1\,1\,0\,0\,0\,0)$, then $wt(v)=3$ and $vH^T=0$ implies $v\in C$.
Therefore, $d(C)\geq 3$ and we can correct at least one error.
Furthermore, $M=|C|=2^4=16=\frac{2^7}{1+7}=\frac{q^n}{\sum_{k=0}^{t} C_k^n (q-1)^k}$,

So [7,4] Hamming code is a perfect code.

Syndrome decoding:

Coset Leader	Syndrome
$r_1=(0,0,0,0,0,0,0)$	$r_1H^T=(0,0,0)$
$r_2=(1,0,0,0,0,0,0)$	$r_2H^T=(1,1,0)$
$r_3=(0,1,0,0,0,0,0)$	$r_3H^T=(1,0,1)$
$r_4=(0,0,1,0,0,0,0)$	$r_4H^T=(0,1,1)$
$r_5=(0,0,0,1,0,0,0)$	$r_5H^T=(1,1,1)$
$r_6=(0,0,0,0,1,0,0)$	$r_6H^T=(1,0,0)$
$r_7=(0,0,0,0,0,1,0)$	$r_7H^T=(0,1,0)$
$r_8=(0,0,0,0,0,0,1)$	$r_8H^T=(0,0,1)$

The syndromes except $(0,0,0)$ are exactly the rows of H^T.

Remark: $\coprod_{i=1}^{8}(r_i+C)=\mathbb{Z}_2^8$

Since we can correct up to 1 error, the syndrome decoding above is exactly the nearest neighbor decoding.

Suppose that $v=(0,1,0,1,0,1,1)$ is received, $vH^T=(0,0,1)=r_8H$,
then we decode it as $c=v-r_8=(0,1,0,1,0,1,0)$
If $x=(x_1,x_2,x_3,x_4)\in\mathbb{Z}_2^4$ is the original message, then

$$c=xG=x[I\ P]=[x\ xP]$$

$$\therefore x=(0,1,0,1)$$

Exercise 9.3
Write down the parity check matrix of the [3,1] Hamming code, and observe that the associated code is the repetition code in example 9.7.

Example 9.13 / Exercise 9.4 ([15,11] Hamming code)

The [15,11] Hamming code has parity check matrix

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

Show that $d(C) = 3$.

Correct the received vector $v = (0,0,0,0,1,0,0,0,0,0,0,1,1,0,0,1)$.

Ans: $c = (0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1)$

↑ changed

Example 9.14 / Exercise 9.5

Let $F_4 = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{0, 1, x, x+1\}$.

Let $H = \begin{pmatrix} 1 & x & 1 & 1 & 0 \\ x & 1 & 1 & 0 & 1 \end{pmatrix} \in M_{2\times 5}(F_4)$ and so $G = \begin{pmatrix} 1 & 0 & 0 & 1 & x \\ 0 & 1 & 0 & x & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in M_{3\times 5}(F_4)$.

Show that the associated code C is a perfect code with $d(C) = 3$.

Suppose that $m = (1\ x\ 1+x)$ is intended to be sent.

Then, the encoded message is $mG = (1\ x\ 1+x\ 1\ 1+x)$

However, if $v = (1\ 1\ 1+x\ 1\ 1+x)$ is received, then $vH^T = (1\ 1+x) = (1+x)(x\ 1) = (1+x)(0\ 1\ 0\ 0\ 0)H^T$.

syndrome

coset leader r

Therefore, the original encoded message is $c = v - r = (1\ x\ 1+x\ 1\ 1+x)$.

Cyclic Codes

Definition 9.7

A linear $[n,k]$ code C over a finite field F is called cyclic if

$(a_1, a_2, \cdots, a_n) \in C$ implies $(a_n, a_1, \cdots, a_{n-1}) \in C$.

Main questions:

1) How to construct a cyclic code?

2) Why do we need cyclic codes?

Think: $F[x]/\langle x^n-1\rangle$ is a ring as well as a vector space over F.

$$\begin{array}{ccc} F^n & \xrightarrow{\varphi} & F[x]/\langle x^n-1\rangle \\ \wr & \text{vector space isomorphism} & \wr \\ (a_0, a_1, \cdots, a_{n-1}) & & g(x) = a_0 + a_1 x + a_2 x + \cdots + a_{n-1}x^{n-1} \quad -(*) \end{array}$$

C : cyclic code $\longrightarrow$ $\varphi(C)$: subspace of $F[x]/\langle x^n-1\rangle$

subspace — but what special it is ?

Remark: Elements in $F[x]/\langle x^n-1\rangle$ are of the form $g(x)+\langle x^n-1\rangle$ where $g(x)\in F[x]$, we can choose a representative $g(x)$ so that $\deg(g(x))<n$.

Also, sometimes we simply write $g(x)\in F[x]/\langle x^n-1\rangle$ instead of $g(x)+\langle x^n-1\rangle$

Proposition 9.12

C is cyclic if and only if $\varphi(C)$ is an ideal of $F[x]/\langle x^n-1\rangle$.

proof:

"$\Rightarrow$" 1) $\varphi(C)$ is an additive subgroup of $F[x]/\langle x^n-1\rangle$ as $\varphi(C)$ is a vector subspace

2) $g(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in\varphi(C)$ $\qquad$ $xg(x)\in\varphi(C)$

$\Rightarrow \varphi^{-1}(g(x)) = (a_0, a_1, \cdots, a_{n-1})\in C$

$\Rightarrow (a_{n-1}, a_0, a_1, \cdots, a_{n-2})\in C$ $\quad(\because C \text{ is cyclic})$

$\Rightarrow \varphi(a_{n-1}, a_0, a_1, \cdots, a_{n-2}) = a_{n-1}+a_0x+a_1x^2+\cdots+a_{n-2}x^{n-1} = xg(x)\in\varphi(C)$.

By the same argument $xg(x), x^2g(x), \cdots$ are all in $\varphi(C)$

and so $a(x)g(x)\in\varphi(C)$ for all $a(x)\in F[x]/\langle x^n-1\rangle$

Therefore, $\varphi(C)$ is an ideal.

"$\Leftarrow$" Trivial.

Proposition 9.13

Every ideal of $F[x]/\langle x^n-1\rangle$ is an ideal generated by a monic polynomial $g(x)\in F[x]$ which is a factor of x^n-1.

proof:

Let I be an ideal of $F[x]/\langle x^n-1\rangle$ and let $g(x)$ be the monic polynomial in I with the lowest degree. Then, claim I is the ideal generated by $g(x)$.

Also, by division algorithm, there exist $q(x), r(x)\in F[x]$ with $\deg(r(x))<\deg(g(x))$ such that $x^n-1 = q(x)g(x)+r(x)$ and so $r(x)\equiv -q(x)g(x) \pmod{x^n-1}$ which implies $r(x)$ is contained in the ideal generated by $g(x)$ Therefore, $r(x)=0$, i.e. $g(x)$ is a factor of x^n-1.

In conclusion, take a monic polynomial $g(x) \in F[x]$ which is a factor of x^n-1, then $\langle g(x) \rangle = \{a(x)g(x) \in F[x]/\langle x^n-1 \rangle : a(x) \in F[x]/\langle x^n-1 \rangle\}$ is an ideal of $F[x]/\langle x^n-1 \rangle$.
Furthermore, $\langle g(x) \rangle$ is also a vector subspace of $F[x]/\langle x^n-1 \rangle$.
Under the isomorphism between F^n and $F[x]/\langle x^n-1 \rangle$, the corresponding subspace is a cyclic code.
In fact, every cyclic group is constructed by the above.

Example 9.15

Let $x^7-1 \in \mathbb{Z}_2[x]$.

x^7-1 can be factorized as $(x+1)(x^3+x+1)(x^3+x^2+1)$ where every factor is irreducible over $\mathbb{Z}_2$.

Take $g(x) = (x+1)(x^3+x+1) = x^4+x^3+x^2+1$, then

Elements in $\langle g(x) \rangle$	$\longrightarrow$	Elements in C
$0 \cdot g(x) = 0$		$(0,0,0,0,0,0,0)$
$1 \cdot g(x) = 1+x^2+x^3+x^4$		$(1,0,1,1,1,0,0)$
$x \cdot g(x) = x+x^3+x^4+x^5$		$(0,1,0,1,1,1,0)$
$(1+x) \cdot g(x) = 1+x+x^2+x^5$		$(1,1,1,0,0,1,0)$
$x^2 \cdot g(x) = x^2+x^4+x^5+x^6$		$(0,0,1,0,1,1,1)$
$(x+x^2) \cdot g(x) = x+x^2+x^3+x^6$		$(0,1,1,1,0,0,1)$
$(1+x^2) \cdot g(x) = 1+x^3+x^5+x^6$		$(1,0,0,1,0,1,1)$
$(1+x+x^2) \cdot g(x) = 1+x+x^4+x^6$		$(1,1,0,0,1,0,1)$

Exercise 9.6

List all elements of C associated by $g(x) = x^3+x+1$.

Proposition 9.14

If $g(x) = a_0+a_1x+\cdots+a_{\ell-1}x^{\ell-1} \in F[x]$ which is a factor of x^n-1, and C is the associated linear code, then (1) $\dim(C) = n-\ell$ (let $k = n-\ell$)

(2) $G = \begin{pmatrix} a_0 & a_1 & \cdots & a_{\ell-1} & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{\ell-1} & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & \cdots & & a_0 & a_1 & \cdots & & a_{\ell-1} \end{pmatrix} \in M_{k \times n}(F)$ is a generating matrix of C.

(3) If $h(x) = b_0+b_1x+\cdots+b_{k+1}x^{k+1} \in F[x]$ such that $g(x)h(x) = x^n-1$, then

$H = \begin{pmatrix} b_{k+1} & b_k & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_{k+1} & b_k & \cdots & b_0 & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & \cdots & & b_{k+1} & b_k & \cdots & & b_0 \end{pmatrix} \in M_{(n-k) \times n}(F)$ is a parity check matrix.

proof: (1) Every element of C is of the form $f(x)g(x)$ where $\deg(f(x)) \le (n-1) - \deg(g(x)) = n-\ell$

(2) Note that $\{g(x), xg(x), \cdots, x^{n-\ell-1}g(x)\}$ is a linearly independent set of vectors, it forms a basis of $\langle g(x) \rangle$.

(3) Check: $GH^T = 0$, but it is true because $g(x)h(x) \equiv 0 \pmod{x^n-1}$ and

$$[GH^T]_{ij} = \text{coeff. of } x^{k+1-i+j} \text{ of } g(x)h(x) = 0$$

entry at i-th row, j-th column of GH^T

BCH Codes

Application of BCH codes:

Satellite communications, CD, DVD, $\cdots$

Recall: If we take a factor $g(x)$ of $x^n-1 \in F[x]$, then the ideal generated by $g(x)$ gives a cyclic code C. However, what is the minimum distance $d(C)$?

It leads us to study more about x^n-1.

Let F be a finite field, then $|F| = p^m$ for some prime p and $m \in \mathbb{Z}^+$.

Assume $\gcd(n,p) = 1$, then $[p] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Consider $[p], [p]^2, [p]^3, \cdots$, since $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite group, there exist $i, j \in \mathbb{Z}^+$ with $i > j$ such that $[p]^i = [p]^j$, i.e. $p^i \equiv p^j \pmod n$. Let $d = i-j$.

Then, $p^d \equiv 1 \pmod n$ which implies $p^{md} \equiv 1 \pmod n$ and so $n \mid p^{md}-1$.

Therefore, we can construct a field F' which contains F with order p^{md}.

Let $(F')^\times = \{1, \beta, \beta^2, \cdots, \beta^{p^{md}-2}\}$ and $\alpha = \beta^{\frac{p^{md}-1}{n}}$.

Then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1} \in F'$ are zeros of $x^n-1 \in F'[x]$.

Summary: Let F be a finite field of order p^m.

If $\gcd(n,p) = 1$, then there exists a field F' contains F as a subfield and there exists $\alpha \in F'$ such that x^n-1 has exactly n zeros, namely $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$

In other words, $x^n-1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-1})$.

Example 9.16

Consider $x^3-1 \in \mathbb{Z}_2[x]$ $(n=3)$. $x^3-1=(x-1)(x^2+x+1)$ which cannot be further factorized over $\mathbb{Z}_2$.

However, we can consider $F=\mathbb{Z}_2[y]/\langle y^2+y+1\rangle=\{0,1,y,1+y\}\supseteq\mathbb{Z}_2$.
($y = \alpha$, $1+y = \alpha^2$)

If we consider $x^3-1\in F[x]$,

then $x^3-1=(x-1)(x-\alpha)(x-\alpha^2)$.

Example 9.17

Consider $x^7-1\in\mathbb{Z}_2[x]$ $(n=7)$.

$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$ which cannot be further factorized over $\mathbb{Z}_2$.

Let $F=\mathbb{Z}_2[y]/\langle y^3+y+1\rangle=\{a_0+a_1y+a_2y^2 : a_i\in\mathbb{Z}_2\}$.

Note that F^* is a cyclic group of order 7 which is a prime, so if we let $\alpha=y\neq 1$,

then α is a generator of F^*, i.e. $F^*=\{1,\alpha,\alpha^2,\cdots,\alpha^7\}$

We can check α,α^2,α^4 are zeros of x^3+x+1 and $\alpha^3,\alpha^5,\alpha^6$ are zeros of x^3+x^2+1.

$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6)=\prod_{i=0}^{6}(x-\alpha^i)$

Let $g(x)\in F[x]$ be a factor of $x^n-1=\prod_{i=0}^{n-1}(x-\alpha^i)$ for some $\alpha\in F'$.

Then $g(x)=(x-\alpha^{j_1})(x-\alpha^{j_2})\cdots(x-\alpha^{j_k})$ with $0\le j_1<j_2<\cdots<j_k\le n$

If some of j_i's form a set of consecutive integers, then we have a lower bound for $d(C)$:

Proposition 9.15

If there exist integers l and δ such that $g(\alpha^l)=g(\alpha^{l+1})=\cdots=g(\alpha^{l+\delta})=0$, then $d(C)\ge\delta+2$.

Example 9.17 (Cont.)

If $g(x)=(x-1)(x^3+x+1)=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^4)$, then we have $g(1)=g(\alpha)=g(\alpha^2)=0$.

Take $l=0$, $\delta=2$, we have $d(C)\ge 4$.

Idea: If $x^n-1=f_1(x)f_2(x)\cdots f_r(x)$ where each $f_i(x)$ is irreducible over F.

We associate polynomials $g_0(x), g_1(x),\cdots,g_{n-1}(x)\in F[x]$ by

letting $g_i(x)=f_l(x)$ if $x-\alpha_i$ is a factor of $f_l(x)$

(e.g. if $x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$, with $f_1 = x-1$, $f_2 = x^3+x+1$, $f_3 = x^3+x^2+1$, then $g_0(x)=f_1(x)$, $g_1(x)=g_2(x)=g_4(x)=f_2(x)$ and $g_3(x)=g_5(x)=g_6(x)=f_3(x)$.)

A BCH code of minimum distance d is a code generated by

$g(x) = \text{lcm of } g_{k+1}(x), g_{k+2}(x), \cdots, g_{k+d-1}(x)$ for some integer k.

(so at least $g(\alpha^{k+1}) = g(\alpha^{k+2}) = \cdots = g(\alpha^{k+d-1}) = 0$,

put $l = k+1$, $\delta = d-2$, we have $d(C) \geq \delta + 2 = d$)

proof of proposition 9.15 :

Suppose the contrary, $d < \delta + 2$. Then there exists $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ with $wt(c) = w \leq \delta + 1$

We write $c(x) = c_{i_1} x^{i_1} + c_{i_2} x^{i_2} + \cdots + c_{i_w} x^{i_w}$

Since $c \in C$, $c(x)$ is a multiple of $g(x)$ and we have $c(\alpha^l) = c(\alpha^{l+1}) = \cdots = c(\alpha^{l+\delta}) = 0$.

Then
$$\begin{pmatrix} \alpha^{l i_1} & \cdots & \alpha^{l i_w} \\ \alpha^{(l+1) i_1} & \cdots & \alpha^{(l+1) i_w} \\ \vdots & & \vdots \\ \alpha^{(l+w-1) i_1} & \cdots & \alpha^{(l+w-1) i_w} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_w} \end{pmatrix} = \begin{pmatrix} c(\alpha^l) \\ c(\alpha^{l+1}) \\ \\ c(\alpha^{l+w-1}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad -(*)$$

Note.
$$\begin{vmatrix} \alpha^{l i_1} & \cdots & \alpha^{l i_w} \\ \alpha^{(l+1) i_1} & \cdots & \alpha^{(l+1) i_w} \\ \vdots & & \vdots \\ \alpha^{(l+w-1) i_1} & \cdots & \alpha^{(l+w-1) i_w} \end{vmatrix} = \alpha^{l i_1 + \cdots + l i_w} \begin{vmatrix} 1 & \cdots & 1 \\ \alpha^{i_1} & \cdots & \alpha^{i_w} \\ \vdots & & \vdots \\ \alpha^{(w-1) i_1} & \cdots & \alpha^{(w-1) i_w} \end{vmatrix}$$

$$= \alpha^{l i_1 + \cdots + l i_w} \prod_{1 \leq j < k \leq w} (\alpha^{i_j} - \alpha^{i_k}) \quad \text{(Vandermonde determinant)}$$

$$\neq 0$$

Therefore, $(*)$ can only have trivial solution (Contradiction!)

Decoding of BCH Codes

Proposition 9.16

Let C be a cyclic code with generator polynomial $g(x) \in F[x]$.

Suppose that $\alpha_1, \alpha_2, \cdots, \alpha_r$ are zeros of $g(x)$.

Let $H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ & & \vdots & & \\ 1 & \alpha_r & \alpha_r^2 & \cdots & \alpha_r^{n-1} \end{pmatrix}$.

Then $v = (a_0, a_1, \cdots, a_{n-1}) \in C$ if and only if $vH^T = 0$.

proof: $v = (a_0, a_1, \cdots, a_{n-1}) \in C$

$\Leftrightarrow v(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = g(x)q(x)$ for some $q(x) \in F[x]$.

$\Leftrightarrow v(\alpha_i) = 0$ for $i = 1, 2, \cdots, r$

$\Leftrightarrow vH^T = 0$

Example 9.18

Using the setting of example 9.17.

Let $g(x) = x^3 + x + 1$ which is a factor of $x^7 - 1$ and $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$.

In particular, $g(\alpha) = g(\alpha^2) = 0$ and so $d \geq 3$

Let $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & & \alpha^6 \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^6 \\ 1 & \alpha^4 & (\alpha^4)^2 & & (\alpha^4)^6 \end{pmatrix}$.

Let $v \in \mathbb{Z}_2^7$, $v \in C$ if and only if $vH^T = 0$

Let $\tilde{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^6 \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^6 \end{pmatrix}$ which is the first two rows of H.

$v \in C \Rightarrow v\tilde{H}^T = 0$ but the converse is not true, i.e. $\tilde{H}$ is not a parity matrix.

However, $\tilde{H}$ can be used for decoding as the following:

Suppose that $v \in \mathbb{Z}_2^7$ is a received message with at most one error,

then $v = c + r$ where $c \in C$ and $r = 0$ or $e_j = (0, 0, \cdots, \overset{j\text{-th}}{1}, \cdots, 0)$.

Therefore, $v\tilde{H}^T = (c+r)\tilde{H}^T = r\tilde{H}^T$.

If $v \in C$, $vH^T = 0$, no correction is needed.

If v contains one error, $vH^T = e_j\tilde{H}^T = (\alpha^{j-1} \quad \alpha^{2(j-1)})$

by computing $\alpha^{2(j-1)}/\alpha^{j-1} = \alpha^{j-1}$, then we know the error is in the j-th position.

$c = v - e_j$

For example,

(i) $v = (0,0,1,1,0,1,0)$ is received. $v\tilde{H}^T = (\alpha^2 + \alpha^3 + \alpha^5, \alpha^4 + \alpha^6 + \underset{\overset{\|}{\alpha^3}\ (\because \alpha^7 = 1)}{\alpha^{10}}) = (\alpha^2(1+\alpha+\alpha^3), \alpha^3(1+\alpha+\alpha^3)) = (0,0)$.

Then $v \in C$.

(ii) $v = (0,1,1,0,0,0,0)$ is received. $v\tilde{H}^T = (\alpha + \alpha^2, \alpha^2 + \alpha^4) = (\alpha^4, \alpha)$. $(\because \alpha^2 + \alpha^4 = \alpha(\alpha + \alpha^3) = \alpha \cdot 1 = \alpha$

Then $(S_1, S_2) = (\alpha^4, \alpha)$ and so $S_2/S_1 = \alpha^{-3} = \alpha^4$. $\alpha + \alpha^2 = \alpha(1+\alpha) = \alpha \cdot \alpha^3 = \alpha^4)$

$c = v - e_5 = (0,1,1,0,1,0,0)$ is the decoded message.

Example 9.19

Let $\alpha = 2 \in \mathbb{Z}_5$, we have $\alpha^2 = 4$, $\alpha^3 = 3$, $\alpha^4 = 1$.

Also, $x^4 - 1 = (x-1)(x-2)(x-4)(x-3) = \prod_{i=1}^{3}(x-\alpha^i)$

Let $g(x) = (x-2)(x-3) = x^2 + 4x + 3$

Then the cyclic code C generated by $g(x)$ is a $[4,2]$ code with $d(C) \geq 3$ and generating matrix $G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}$.

Also $H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{pmatrix}$ is a parity matrix

Suppose that $v = (3\ 2\ 4\ 1)$ is received.

$$vH^T = (s_1, s_2) = (3\ 2\ 4\ 1)\begin{pmatrix} 1 & 1 \\ 2 & 4 \\ 4 & 1 \\ 3 & 4 \end{pmatrix} = (1\ 4) = (1\ \alpha^2)$$

$s_2/s_1 = \alpha^2$ which means the error is located at 3-rd place.

Also $vH^T = (1\ 4) = 4(4\ 1) = 4e_3H^T$

Therefore, the decoded message is $c = v - 4e_3 = (3\ 2\ 0\ 1)$.

However, suppose that $v = (3\ 2\ 1\ 2)$ is received.

$$vH^T = (s_1, s_2) = (3\ 2\ 1\ 2)\begin{pmatrix} 1 & 1 \\ 2 & 4 \\ 4 & 1 \\ 3 & 4 \end{pmatrix} = (2\ 0) \neq ae_iH^T \text{ for any } a \in \mathbb{Z}_5 \text{ and } e_i.$$

Therefore, the received message contains more than 1 error.