Coding Theory

Yuan Luo
Shanghai Jiao Tong University
Contents

- **Part 1.** Block code: Equivalence; Radius; Decoding principles; Bounds
- **Part 2.** Linear block code (need some knowledge of Part 3): Generator matrix; Parity check matrix; RRE matrix; Dual code; Counting; Hamming code; Cyclic code
- **Part 3.** Finite field Characteristic; Coset; Three structure theorems; Extension; Irreducible polynomial; Minimal polynomial; Primitive polynomial
1.1 What is block code?

- **Alphabet:** We assume that information is coded using an alphabet $Q$ with $q$ distinct symbols. For example $Q=\{0, 1\}$, $Q=\{0, 1, 2, 3\}$

- **Block code:** A code is called a block code if the coded information can be divided into blocks of $n$ symbols which can be decoded independently.
Example: Over $Q=\{0, 1\}$, Code $C= \{(0 \ 1 \ 0), (0 \ 1 \ 1), (0 \ 0 \ 0), (1 \ 1 \ 1)\}$ has 4 codewords where $n = 3$.

Coding:

00 $\leftrightarrow (0 \ 1 \ 0)$
01 $\leftrightarrow (0 \ 1 \ 1)$
10 $\leftrightarrow (0 \ 0 \ 0)$
11 $\leftrightarrow (1 \ 1 \ 1)$
1.2 What is non-block code?

- An example of convolutional code:
  An infinite sequence of information symbols $i_0, i_1, i_2, \ldots$ is coded into a codeword: $i_0, i_0, i_1, i_1, i_2, i_2, \ldots$, which is a function of $i_0, i_1, i_2, \ldots$. 
1.3 Hamming distance and Hamming weight

* If \( x \in Q^n, y \in Q^n \), then the Hamming distance \( d(x, y) \) of \( x \) and \( y \) is defined by
  \[
  d(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|
  \]
  The weight \( w(x) \) of \( x \) is defined by
  \[
  w(x) = d(x, 0^n)
  \]
  We denote \((0, \ldots, 0)\) by \( 0^n \), and \((1, \ldots, 1)\) by \( 1^n \).

* Proposition: For any code \( C \) over \( Q = \{0, 1\} \), we have
  \[
  d(x, y) = w(x) + w(y) - 2 < x, y >
  \]
  where \( x, y \in C, and < x, y > = \sum_{i=1}^{n} x_i y_i \) (inner product over real field).
Trivial code: \(|C| = 1\).

极小距离: The minimum distance of a nontrivial code \(C\) is defined as:
\[
\min\{d(x,y) | x \in C, y \in C, x \neq y\}
\]

极小重量: The minimum weight of \(C\) with length \(n\) is defined as:
\[
\min\{w(x) | x \in C, x \neq 0^n\}
\]
* Code rate: If $|Q| = q$ and $\mathcal{C} \subset Q^n$, then
  $$R \triangleq n^{-1} \log q |\mathcal{C}|$$
  is called the code rate of $\mathcal{C}$.
* $(n,M,d)_q$: a code with $M$ codewords of length $n$ and minimum distance $d$ over a q-ary alphabet.
* $A_q(n,d)$: Maximal size of a code with parameter $n$, $d$ and $q$.
* For example: $A_q(n,1) = q^n$, $A_q(n,n) = q$
1.4 Equivalent codes

Let \( \sigma \) be a permutation on alphabet \( Q = \{s_1, ..., s_q\} \). Let \( \pi \) be a permutation on index alphabet \( \{1, 2, ..., n\} \).

\[
\sigma: \left( \begin{array}{c} s_1, ..., s_n \\ \sigma(s_1), ..., \sigma(s_n) \end{array} \right)
\]

\[
\pi: \left( \begin{array}{c} 1, ..., n \\ \pi(1), ..., \pi(n) \end{array} \right)
\]
Two basic transformations of a code $C^1$ are:

- $C^2 = \{(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)}) : (\alpha_1, \alpha_2, \ldots, \alpha_n) \in C^1\}$
- $C^2 = \{(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \sigma(\alpha_i), \alpha_{i+1}, \ldots, \alpha_n) : (\alpha_1, \alpha_2, \ldots, \alpha_n) \in C^1\}$

Two codes $C^1$ and $C^2$ are called to be equivalent if $C^2$ can be obtained from $C^1$ by using the two kinds of basic transformations.
* If $C^1$ is obtained from $C^2$ by using the two basic transformations, then $C^1 \leftrightarrow C^2$.

* $C^1$ is an $(n,M,d)_q$ code, $C^1 \leftrightarrow C^2$, then $C^2$ is also an $(n,M,d)_q$ code.

* Any $(n,M,d)_q$ code is equivalent to a code with codeword $(0,0,\ldots,0)$.

* $C^1$ and $C^2$ are equivalent over $Q = GF(2)$, when $C^2 = \{\beta + \alpha : \alpha \in C^1\}$, where $\beta$ is a fixed vector over $GF(2)$. 
Size of block code

* **Th1.1.1:** $A_2(5, 3) = 4, A_2(8, 5) = 4$ over $Q = \{0, 1\}$.
* **Th1.1.2:** $A_2(n, 2) = 2^{n-1}$.
* **Th1.1.3:** If there is an $(n, M, d)_q$ code and $1 \leq d_1 \leq d$, then there is an $(n, M, d_1)_q$ code.
* **Th1.1.4:** Assume $d$ is odd. Over $Q = \{0, 1\}$, there is an $(n, M, d)_2$ code iff there is an $(n + 1, M, d + 1)_2$ code. So

$$A_2(n, d) = A_2(n + 1, d + 1) \text{ when } d \text{ is odd}.$$
* **Th1.1.5:** $2A_2(n - 1, d) \geq A_2(n, d)$. 
1.5 Packing radius and covering radius

- A sphere with radius $\rho$ and center $x$:

  Proposition 1.1.1: Define the volume of a ball 
  \[ B_\rho(x) \triangleq \{ y \in Q^n : d(x,y) \leq \rho \} \]

  It is easy to see that 
  \[ |B_\rho(x)| = \sum_{i=0}^{\rho} \binom{n}{i} (q - 1)^i. \]

  For $q = 2$, we have 
  \[ |B_\rho(x)| = \sum_{i=0}^{\rho} \binom{n}{i} \]
Packing radius: For an \((n, M, d)\) code \(C\) over \(Q\), its packing radius \(\rho\) is the largest integer such that the spheres \(B_\rho(c)\), where \(c \in C\), are disjoint.

Proposition 1.1.2 (calculate packing radius): \(d = 2\rho + 1\) or \(d = 2\rho + 2\).
Covering radius: The covering radius of an $(n,M,d)$ code $\mathcal{C}$ is the smallest $\rho$ such that the spheres $B_\rho(c)$ with $c \in \mathcal{C}$ cover the set $Q^n$, i.e.,

$$Q^n \subseteq \bigcup_{c \in \mathcal{C}} B_\rho(c)$$

Proposition 1.1.3 (calculate covering radius): If $\mathcal{C} \subseteq Q^n$, then the covering radius $\rho(\mathcal{C})$ of $\mathcal{C}$ is

$$\max\{\min\{d(x,c) : c \in \mathcal{C}\} : x \in Q^n\}.$$
1.6 Perfect code

A code is said to be perfect if its packing radius is equal to its covering radius.
in words, a code $\mathcal{C} \in Q^n$ is perfect if there exists a number $\rho$ for which the spheres $B_\rho(c) (c \in \mathcal{C})$ are disjoint and cover $Q^n$.

1.7 Quasi-perfect code

A code $\mathcal{C}$ is said to be quasi-perfect if

$$C_r(\mathcal{C}) = P_r(\mathcal{C}) + 1$$

where $C_r(\mathcal{C})$ is the covering radius of code $\mathcal{C}$, $P_r(\mathcal{C})$ is the packing radius of code $\mathcal{C}$. 
1.8 Bounds on size of block code

* **Hamming bound**

* **Th1.1.6** Hamming bound: Let $C$ be an $(n, M, d)_q$ code, we have

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q - 1)^i \leq q^n$$

where $e = \left\lfloor \frac{d-1}{2} \right\rfloor$
* Corollary 1.1.1: \( A_q(n,d) \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n, \quad e = \left\lfloor \frac{d-1}{2} \right\rfloor \)

* Corollary 1.1.2: For an \((n,M,2t+1)\) code, we have

\[
M \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n,
\]

and thus,

\[
A_q(n,2t+1) \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n,
\]

* Corollary 1.1.3: The hamming bound is achieved iff \( C \) is a perfect code.
All perfect codes:(under equivalence)

- \((n, q^n, 1)_q\) code.
- \((2m + 1, 2, 2m + 1)_{2}^2\), binary repetition code of odd length.
- Hamming code: an \((n, q^{n-r}, 3)_q\) linear code where \(n = \frac{q^{r-1}}{q-1}\)
- binary Golay code: \([23, 12, 7]_2\).
- ternary Golay code: \([11, 6, 5]_3\).
- some nonlinear codes having the same parameters \((n, M, d)_q\) of the Hamming code and the Golay code.
Gilbert bound

* Th 1.1.7. : \[ A_q(n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i} \]
Singleton bound

* Th1.1.8. For an \((n, M, d)_q\) code, we have

\[ n \geq d + \left\lceil \log_q M \right\rceil - 1 \]

* Corollary 1.1.4: For \([n, k, d]_q\) linear codes, \(d \leq n - k + 1\).

* Remark: If the Singleton bound is achieved, the corresponding code is called an MDS code. (MDS is the abbreviation of maximum distance separable)
Proof. Let $C$ be an $(n, M, d)q$ code. We puncture the code by deleting the last $d - 1$ components of each codeword, then all resulting codewords must still be pairwise different, so the resulting code has the same size $M$ but with length $n - (d - 1)$.

Thus $M \leq q^{n-d+1}$ and then $n \geq d + \lceil \log_q M \rceil - 1$. 
Example 1: trivial MDS codes: \([n,n,1]_q\) code, or, \([n,n-1,2]_q\), or, \([n,1,n]_q\) repetition code.

Example 2: non-trivial MDS codes: Reed-Solomon codes and generalized Reed-Solomon codes.

Example 3: MDS conjecture
For linear codes over GF\((q)\), let \(m(k, q)\) denote the maximal length of an MDS code with given dimension \(k\) over GF\((q)\):

\[
m(k, q) = \begin{cases} 
q + 1, & 2 \leq k \leq q; \\
k + 1, & q < k.
\end{cases}
\]

except for \(m(3,q) = m(q - 1,q) = q + 2\) when \(q = 2^l\).

Remark: for \(q \leq 19\), the guess is proved to be right.
MDS码的性质

1. 线性码的极小距离为 \( d \) ⇔ 校验矩阵中任意 \( d - 1 \) 列无关，存在 \( d \) 列相关。
   
   推论：一个 \([n, k]\) 码为 MDS 码 ⇔ 校验矩阵中任意 \( n - k \) 列无关。

2. 线性码的极小距离为 \( d \) ⇔ 生成矩阵中任意 \( n - d + 1 \) 列秩为 \( k - 1 \)。
   
   推论：一个 \([n, k]\) 码为 MDS 码 ⇔ 生成矩阵中任意 \( k \) 列秩为 \( k \)。

* 一个线性码为 MDS 码 ⇔ 其对偶码为 MDS 码
Plotkin bound

* **Th1.1.9.** \( A_q(n,d) \leq \frac{d}{d - \frac{q-1}{q} n} \), where \( d > \frac{q-1}{q} n \)

* **Corollary 1.1.5:** \( A_2(2d,d) \leq 4d \).
  
  When \( d \) is odd, \( A_2(2d + 1,d) \leq 4d + 4 \).

  **Proof.** Can not use Th1.1.9 directly. Using Th1.1.5,
  \[
  A_2(2d,d) \leq 2 A_2(2d - 1,d) \leq 2 \frac{d}{d - \frac{1}{2}(2d-1)} = 4d.
  \]

  Using Th1.1.4 and Th1.1.5, since \( d \) is odd,
  \[
  A_2(2d + 1,d) = A_2(2d + 2,d + 1) \leq 2 A_2(2d + 1,d + 1) \leq 4d + 4.
  \]
Proof. Let $C$ be an $(n, M, d)_2$ code, and the array of $C$ is an $M \times n$ matrix. Considering the rows of the array, we have

$$
\sum_{(x,y) \in C \times C, x \neq y} d(x, y) \geq M(M - 1)d.
$$

Considering the columns of the array, we have

$$
\sum_{(x,y) \in C \times C, x \neq y} d(x, y) = \sum_{i=1}^{n} 2s_i(M - s_i) \leq \sum_{i=1}^{n} 2 \frac{M^2}{4},
$$

where $s_i$ is the number of zeros contained in the $i$th column of the array. So

$$
M \leq \frac{d}{d - \frac{1}{2} n} \quad \text{if} \quad d - \frac{1}{2} n > 0.
$$

For q-ary case, the idea is similar. From the proof, we can see that the code achieving the Gilbert bound is equi-distant.
* Corollary 1.1.6: if $d$ is odd and $n < 2d + 1$, then

$$A_2(n,d) \leq \frac{2(d + 1)}{(2d + 1) - n}.$$  

Remarks: when $d$ is odd and $n < 2d$, the upper bound in Corollary 1.1.6 is better than the Plotkin bound.
1.9 Minimum distance decoding

* For a received vector $y \in Q^n$, if there is a codeword $c \in C \subseteq Q^n$ such that

$$d(y, c) = \min_{a \in C} d(y, a),$$

then $y$ is decoded into $c$. If there are two codewords $c \in C, b \in C$ such that

$$d(y, c) = d(y, b) = \min_{a \in C} d(y, a),$$

then $y$ is decoded into $c$ or $b$. 
1.10 Maximum likelihood decoding (MLD)

* **q-ary symmetric channel**: \( p < \frac{1}{2} \), \( Q = \{0, 1, 2, \ldots, q - 1\} \)

\[
p(\text{output symbol/input symbol}) = \begin{cases} 
  p(\alpha/\alpha) = 1 - p, & \alpha \in Q, \\
  p(\beta/\alpha) = \frac{p}{q-1}, & \beta \neq \alpha, \beta \in Q.
\end{cases}
\]

* **Discrete memoryless channel (DMC)**:

\[
p(y/x) = \prod_{i=1}^{n} p(y_i/x_i)
\]

where the codeword \( x \in C \) is sent through the q-ary symmetric channel and \( y \in Q^n \) is received.
* Definition of maximum likelihood decoding: For a received vector \( y \in Q^n \), if there is a codeword \( c \in C \subseteq Q^n \) such that

\[
p(y/c) = \max_{a \in c} p(y/a)
\]

then \( y \) is decoded into \( c \).

* Th1.1.10. Minimum distance decoding is equivalent to maximum likelihood decoding in a memoryless q-ary symmetric channel.
1.11 t-error detecting

- A code $C$ is $t$-error detecting if whenever at most $t$, but at least one, error is made in a codeword, the resulting word is not a codeword.
- A code $C$ is exactly $t$-error detecting if it is $t$-error detecting, but not $(t+1)$-error detecting.
- Th1.1.11. A code is $t$-error detecting if and only if $d \leq t + 1$.
- Th1.1.12. A code is exactly $t$-error detecting if and only if $d = t + 1$. 
1.12 t-error correcting

* A code $C$ is $t$-error correcting if "Minimum distance decoding" is able to correct all errors of size $t$ or less in any codeword.
* A code $C$ is exactly $t$-error correcting if it is $t$-error correcting, but not $(t+1)$-error correcting.
* Th1.1.13. A code is $t$-error correcting if and only if $d \geq 2t$.
* Th1.1.14. A code is exactly $t$-error correcting if and only if $d = 2t + 1$ or $2t + 2$, i.e., $t$ is the packing radius of the code $C$. 
1.13 Maximum a posteriori probability decoding (MAP)

* Definition: For a received vector \( y \in Q^n \), if there is a codeword \( c \in C \subseteq Q^n \) such that
  \[
p(c/y) = \max_{a \in C} p(a/y)
  \]
then \( y \) is decoded into \( c \).

* Th1.1.15. MAP is equivalent to MLD if \( c \in C \) is uniformly distributed.
2.1 Groups

- **Definition**: a group G is a nonempty set, together with a binary operation \( \odot \) that satisfies the following properties:
  - G is closed: \( \forall a, b \in G : a \odot b \in G \).
  - Associativity: for all \( a, b, c \in G \), \( (a \odot b) \odot c = a \odot (b \odot c) \).
  - Identity: there exists an element \( e \in G \) for which \( e \odot a = a \odot e = a \) for all \( a \in G \).
  - Inverse: for each \( a \in G \), there is an element \( a^{-1} \in G \) for which \( a \odot a^{-1} = a^{-1} \odot a = e \).
2.2 Abelian (or commutative) Group

Definition: a group $G$ is abelian, or commutative, if $a \odot b = b \odot a$, for all $a, b \in G$.

2.3 Finite Group

Definition: a group $G$ is finite if it contains only a finite number of elements, which is denoted by $|G|$. $|G|$ is called the order of the group.
Th1.2.1: Let $G$ be any group, then the following hold.

* The identity is unique.
* For any $a \in G, a^{-1}$ is unique.
2.4 Subgroup

* Definition: Let $G$ be a group with respect to $\circ$, and $H$ is a nonempty subset of $G$. If $H$ is a group with respect to $\circ$, $H$ is called a subgroup of $G$.

* Th1.2.2: Let $G$ be a group with respect to $\circ$, and $S$ be a nonempty subset of $G$. Then $S$ is a subgroup of $G$ iff $\forall a, b \in S : a \circ b^{-1} \in S$. 
2.5 Order of an element in a group

* Let $G$ be a finite group with respect to $\circ$, for any fixed element $g \in G, \{g, g \circ g, g \circ g \circ g, \ldots\}$ is a subgroup with finite order.

Since there exists $i < j$ such that $g_i = g_j$, we have $e = g_{i-1}. Let k = j - i$, the smallest possible positive integer $k(g^k = e)$ is called “the order of $g$. If the order of $g$ is $n$, then $\{g, g^2, g^3, \ldots, g^n = g^0 = e\}$ is a subgroup of $G$. 
2.6 Cyclic Group

If G is a group and \( a \in G \), then the set of all powers of \( a : < a > = \{ a^i | i \in \mathbb{Z} \} \) is a subgroup of G, called the cyclic subgroup generated by a. A group G is cyclic if it has the form \( G = < a > \), for some \( a \in G \).
2.7 Cosets

Let $G$ be a group and $H$ be a subgroup of $G$. Let $a$ be an element of $G$. The set of elements $\{a \circ h : h \in H\}$ is called a coset of “$a$” relative to $H$ and is denoted by $aH$. 
Example: let \( H = \{ h_1 = e, h_2, ..., h_n \} \) be a subgroup of a finite group \( G \).

\[
\begin{align*}
  h_1 &= e \cdot h_2, h_3, ..., h_n \\
  g_1 \odot e, g_1 \odot h_2, g_1 \odot h_3, ..., g_1 \odot h_n \\
  g_2 \odot e, g_2 \odot h_2, g_2 \odot h_3, ..., g_2 \odot h_n \\
  &\vdots \\
  g_{m-1} \odot e, g_{m-1} \odot h_2, g_{m-1} \odot h_3, ..., g_{m-1} \odot h_n
\end{align*}
\]

where \( g_i \) is not in the first \( i \) rows, and

\[
g_iH(1 \leq i \leq m-1) = \{ g_i \odot e, g_i \odot h_2, g_i \odot h_3, ..., g_i \odot h_n \}
\]

is called a coset relative to \( H \), and

\[
G = \bigcup_{i=1}^{m-1} g_iH.
\]
Th1.2.3: (1) The array has finite rows since $G$ is finite.
(2) Each element of $G$ appears once in the array.
(3) $|H|||G|$.
(4) $G$ can be decomposed into a disjoint union of cosets relative to $H$.
(5) The order of any element of $G$ is a factor of $|G|$.
2.8 Ring

* A ring $R$ is a nonempty set, together with two binary operations, called addition (denoted by $\oplus$), and multiplication (denoted by $\odot$), such that
  * $R$ is an abelian group under the operation $\oplus$
  * $\forall a, b \in R, a \odot b \in R$.
  * $\forall a, b, c \in R, (a \odot b) \odot c = a \odot (b \odot c)$.
  * $\forall a, b, c \in R, a \odot (b \oplus c) = (a \odot b) \oplus(a \odot c)$, $\ (b \oplus c) \odot a = b \odot a \oplus c \odot a$
2.9 Field

* A field $F$ is a nonempty set, together with two binary operations, called addition (denoted by $\oplus$), and multiplication (denoted by $\odot$), such that
  * $F$ is an abelian group under the operation $\oplus$.
  * $F\setminus\{0\}$ is an abelian group under the operation $\odot$, where 0 is the identity of $F$ under $\oplus$.
  * $\forall a, b, c \in F, a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
2.10 Finite Field

- A finite field is called a Galois field. A Galois field with $q$ elements is denoted by $GF(q)$. It is easy to see that $|GF(q)| \geq 2$.

- Th1.2.4: $Z_q$ is a field $\iff q$ is prime.
Subfield: a subset $G$ of field $F$ is called a subfield if $G$ is a field under the addition and the multiplication.

The characteristic of a field: denote by $0$ the identity of a field $F$ under addition, and denote by $e$ the identity of a field $F$ under multiplication.

Definition: let $F$ be a field, if for any positive integer $m$, we have $me \neq 0$ (scalar product), then we say that the characteristic of $F$ is 0. Otherwise, the smallest positive integer $p$ satisfying $pe = 0$ is called the characteristic of $F$. 
Th1.2.5: let F be any field, then the characteristic of F is either 0 or “a prime p”.

Th1.2.6: let F be a field of characteristic p and e be its identity element. Let

\[ \pi = \{0, e, 2e, 3e, \ldots, (p - 1)e\}. \]

\[ \pi \] is the smallest subfield of F and called the prime field of F.
2.11 Isomorphic, Isomorphism

- Let $F$ and $F'$ be two fields, assume that a bijective map from $F$ to $F'$
  \[ \sigma : \alpha \rightarrow \sigma(\alpha) (\alpha \in F, \sigma(\alpha) \in F') \]
  can be established such that it ”preserves” the addition and multiplication of fields. Then we say that $F$ and $F'$ are isomorphic.

- Th1.2.7: denote by $\pi$ the prime field of $F$ with characteristic $p$ (prime), then $\pi$ and $Z_p$ are isomorphic.
* Th1.2.8: let $F$ be a field of characteristic $p$ and $a$, $b$ be any two elements of $F$, then

$$(a \oplus b)^p = a^p \oplus b^p$$

* Corollary 1.2.9: let $F$ be a field of characteristic $p$ and $a$, $b$ be any two elements of $F$, then

$$(a \ominus b)^p = a^p \ominus b^p$$

* Corollary 1.2.10: let $F$ be a field of characteristic $p$ and $a_1, a_2, \ldots, a_m$ be any $m$ elements of $F$, then

$$(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_2^p + \cdots + a_m^p$$
Th1.2.11: the multiplicative group of any finite field is cyclic.
2.12 Primitive element

Definition: the generators of the multiplicative group of a finite field are called the primitive elements.
2.13 Three structure theorems of finite fields

* Th1.2.12: let $F$ be a finite field of characteristic $p$, then the number of elements of $F$ must be a power of $p$.

* Th1.2.13: let $p$ be prime and $n$ be a positive integer, then there exists a finite field which contains exactly $p^n$ elements.

* Th1.2.14: Any two finite fields containing the same number of elements are isomorphic.
2.14 域和多项式

* 令$F$为一个域，$F[x] = \{f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n : f_i \in F\}$ (where $n$ is a non-negative integer) 在通常多项式的加法和乘法下构成一个有单位元的多项式交换环。

* 若$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$ 且$a_n \neq 0$，则称$p(x)$的阶为$n$，i.e., $deg p(x) = n$ or $\partial p(x) = n$。若$a_n = 1$ 则称$p(x)$是首1多项式。零多项式的阶定义为$-\infty$。
* **Th1.2.15:** 设 \( a(x), b(x) \in F[x] \)，则存在唯一的一对多项式 \( q(x), r(x) \in F[x] \) 满足：

\[
a(x) = q(x)b(x) + r(x), \quad \partial r(x) < \partial b(x).
\]

此时记 \( r(x) = (a(x))_{b(x)} \)。
Th1.2.16：（最大公因子）

设 \( a(x) \neq 0, b(x) \neq 0 \in F[x] \) 则 \( a(x) \) 和 \( b(x) \) 的最大公因子 \( \gcd(a(x), b(x)) \) 为满足下列关系的唯一首1多项式 \( p(x) \in F[x] \):

* \( p(x) | a(x), p(x) | b(x) \)
* \( \text{If } r(x) | a(x), r(x) | b(x), \text{ 则 } r(x) | p(x) \)。

那么必然存在 \( u(x), v(x) \in F[x] \) 使得：

\[
\gcd(a(x), b(x)) = u(x)a(x) + v(x)b(x).
\]

更进一步，如果 \( \partial a(x) > 0, \partial b(x) > 0, a(x) \neq cb(x) \) for any \( c \in F \)，那么我们可以使得上式中的 \( u(x) \) 和 \( v(x) \) 满足

\[
\partial u(x) < \partial b(x) - \partial \gcd(a(x), b(x))
\]
\[
\partial v(x) < \partial a(x) - \gcd(a(x), b(x))
\]

同时这样的 \( u(x) \) 和 \( v(x) \) 是唯一的。
|  | 定义：设\(a(x), b(x) \in F[x]\)，若\(\text{gcd}(a(x), b(x)) = e\)，则称\(a(x)\)与\(b(x)\)互素。 |
|  | * Corollary 1.2.17：设\(F[x]\)中，\(a(x)\)与\(b(x)\)互素，则存在\(u(x), v(x) \in F[x]\)满足：
|  | \[e = u(x)a(x) + v(x)b(x).\] |
|  | 若\(\partial a(x) > 0, \partial b(x) > 0\)，则存在唯一的\(u(x), v(x) \in F[x]\)满足：
|  | \[
|  | \partial u(x) < \partial b(x), \partial v(x) < \partial a(x).
|  | \]
Definition (irreducible polynomial):

Let $F$ be a field, and $p(x)$ be a polynomial over $F$, i.e. in $F[x]$. If the factor of $p(x)$ must be

$$c \in F \text{ or } c \ p(x) \text{ over } F, \ i.e. \ in \ F[x],$$

$p(x)$ is said to be irreducible.

For example,

- $y^2 - 2$ is irreducible over the field of rational numbers, but reducible over the field of real numbers, see $y^2 - 2 = (y + \sqrt{2})(y - \sqrt{2})$.
- $y^2 + y + 1$ is irreducible over $F_2$, but reducible over $F_4 = F_2[x]_{x^2 + x + 1}$, see $y^2 + y + 1 = (y - x)(y - x - 1)$.
- $y^2 + 1$ is reducible over $F_2$, see $y^2 + 1 = (y + 1)(y + 1)$. 
Th1.2.18 (Field Extension) : Let $F$ be a field, and $p(x)$ be an irreducible polynomial of degree $n$ in $F[x]$, i.e. over $F$. The set \( \{ a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} : a_i \in F \} \) with following addition $\oplus$ and multiplication $\odot$, is a field denoted by $F[x]_p(x)$, where for $a(x), b(x) \in F[x]_p(x)$,

\[
\begin{align*}
    a(x) \oplus b(x) &= a(x) + b(x) \\
    a(x) \odot b(x) &= (a(x)b(x))_p(x).
\end{align*}
\]
**Advanced Relations**

- **Irreducible Polynomial**
  - Field Extension
  - Subfield
  - Subfield
  - Field Extension

- **Minimal Polynomial**
  - Construction
  - Factorization
  - P is a special M

- **Primitive Polynomial**

\[ \phi(q^n - 1)/n \]

**Counting**
Definition. Minimal polynomial (Wan p.118):

Let $F$ be a big finite field with a small subfield $F_q$. “The minimal polynomial of $\alpha \in F$ over $F_q$” is the lowest (degree) monic polynomial with root $\alpha$.

Example (not limited to finite field):
For $F = R$ the field of real numbers, and $F_q = Q$ the field of rational numbers,

“The minimal polynomial of $\sqrt{2} \in R$ over $Q$” is $x^2 - 2$. 
Example: For $F_q = F_2$, let $F = F_2[x]_{x^3 + x + 1}$. There are 8 elements in $F$:

0,
1,
$x$,
$x^2$,
$x^3 = x + 1$,
$x^4 = x^2 + x$
$x^5 = x^2 + x + 1$
$x^6 = x^2 + 1$.

Note that $x^7 = x^3 + x = 1$. 
It is easy to see that,

<table>
<thead>
<tr>
<th>element</th>
<th>minimal polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$y$</td>
</tr>
<tr>
<td>1</td>
<td>$y + 1$</td>
</tr>
</tbody>
</table>

In addition, if $x \in F$ is a root of $f(y)$ over $F_2$, i.e. $f(x)=0$, then $f(x^2) = f(x)^2 = 0$ and $f(x^4) = f(x)^4 = 0$. Because of the 3 roots $x$, $x^2$, $x^4$, the degree of $f(x)$ should be 3.

<table>
<thead>
<tr>
<th>element</th>
<th>minimal polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$, $x^2$, $x^4$</td>
<td>$y^3 + y + 1 = (y - x)(y - x^2)(y - x^4)$</td>
</tr>
</tbody>
</table>

Similarly,

<table>
<thead>
<tr>
<th>element</th>
<th>minimal polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^3$, $x^6$, $x^{12} = x^5$</td>
<td>$y^3 + y^2 + 1 = (y - x^3)(y - x^6)(y - x^5)$</td>
</tr>
</tbody>
</table>
**Theorem.** Let $F$ be a big finite field with a small subfield $F_q$. Any element of $F$ has a unique **minimal polynomial** over $F_q$, which is **irreducible** over $F_q$. 

---

**From minimal polynomial to irreducible polynomial**
From irreducible polynomial to minimal polynomial

* **Theorem.** Let $f(y) \neq y$ be an irreducible polynomial over $F_q$ with degree $n$, then
  * $f(y)$ has $n$ roots in $F[x]_{f(x)}$.
  * The $n$ roots have the same order in $F[x]_{f(x)}$.
  * For any of the $n$ roots in $F[x]_{f(x)}$, $f(y)$ is the minimal polynomial of it over $F_q$. 
Example. $f(y) = y^3 + y + 1$ is irreducible over $F_2$. But over $F[x]_{f(x)}$, i.e. $F[x]_{x^3 + x + 1}$,

$$f(y) = y^3 + y + 1 = (y - x)(y - x^2)(y - x^4).$$

- $f(y)$ has 3 roots $x, x^2, x^4$ in $F[x]_{x^3 + x + 1}$.
- The 3 roots have the same order 7 in $F[x]_{x^3 + x + 1}$.
- For any of the 3 roots in $F[x]_{x^3 + x + 1}$, $f(y)$ is the minimal polynomial of it over $F_2$. 
Cyclotomic Cosets
Definition. Primitive polynomial (Wan P.126)

For an irreducible polynomial \( f(y) \neq y \) over \( F_q \), if \( x \) is a primitive element in \( F[x]_{f(x)} \), we say \( f(y) \) is a primitive polynomial.

Example: For \( F_q = F_2 \), let \( F = F_2[x]_{x^3 + x + 1} \). It is easy to see from above example that \( f(y) = y^3 + y + 1 \) is primitive since

\[
f(x) = 0 \quad \text{and} \quad F = \{0, 1, x, x^2, x^3, x^4, x^5, x^6\}.
\]

In addition, \( g(y) = y^3 + y^2 + 1 \) is also primitive since

\[
g(x^3) = 0 \quad \text{and} \quad F = \{0, 1, x^3, (x^3)^2 = x^6, (x^3)^3 = x^2, (x^3)^4 = x^5, (x^3)^5 = x^1, (x^3)^6 = x^4\}.
\]
Theorem. Wan P.127 shows that the number of monic primitive polynomials of degree $n$ over $F_q$ is

$$\phi(q^n - 1)/n,$$

where $\phi(m)$ is the number of positive integers that are relatively prime to $m$.

Example. From last example, we can see that the number of monic primitive polynomials of degree 3 over $F_2$ is

$$\frac{\phi(2^3-1)}{3} = \frac{\phi(7)}{3} = 2.$$

They are reciprocal

$$y^3 + y + 1 \text{ and } y^3 + y^2 + 1.$$
**Definition.** If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, its reciprocal polynomial is defined to be 
$$x^n f(x^{-1}) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

**Theorem.** If $\alpha \neq 0$ is a root of $f(x)$, $\alpha^{-1}$ is a root of the reciprocal polynomial. So 
$f(x)$ is irreducible $\iff$ its reciprocal polynomial is irreducible, 
$f(x)$ is primitive $\iff$ its reciprocal polynomial is primitive.

See $y^3 + y + 1$ and $y^3 + y^2 + 1$.

See $y^3 + y$ and $y^2 + 1$. 

Reciprocal Polynomial
Thank you!