

# (十五) 离散数学: 复习 (Review)

魏恒峰

hfwei@nju.edu.cn

2021 年 06 月 17 日





$\vdash$        $\models$

Theorem

$$\Sigma \vdash \alpha \iff \Sigma \models \alpha$$



$\rightarrow$        $\Rightarrow$

$\leftrightarrow$        $\Longleftrightarrow$

“ $\rightarrow$ ” and “ $\leftrightarrow$ ” are used in a **single** formula.

“ $\Rightarrow$ ” and “ $\Longleftrightarrow$ ” are used to connect **two** formulas.

$\rightarrow$        $\Rightarrow$

$\leftrightarrow$        $\Longleftrightarrow$

“ $\rightarrow$ ” and “ $\leftrightarrow$ ” are used in a **single** formula.

“ $\Rightarrow$ ” and “ $\Longleftrightarrow$ ” are used to connect **two** formulas.

$$x \in A \setminus B$$

$$\Longleftrightarrow x \in A \wedge x \notin B$$

$$\Longleftrightarrow x \in A \wedge (x \in U \wedge x \notin B)$$

$$\Longleftrightarrow x \in A \wedge x \in \overline{B}$$

$$\Longleftrightarrow x \in A \cap \overline{B}$$

$$\begin{aligned} p \oplus q &\triangleq (p \vee q) \wedge \neg(p \wedge q) \\ &= (p \wedge \neg q) \vee (\neg q \wedge q) \end{aligned}$$

$p$	$q$	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

$$\begin{aligned}
 p \oplus q &\triangleq (p \vee q) \wedge \neg(p \wedge q) \\
 &= (p \wedge \neg q) \vee (\neg q \wedge q)
 \end{aligned}$$

$p$	$q$	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

$$p \oplus q = q \oplus p$$

$$(p \oplus q) \oplus r = p \oplus (q \oplus r)$$



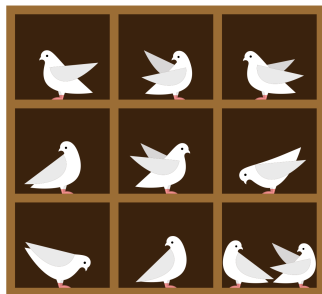
$\sqrt{2}$  is irrational.



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

## Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}. au + bv = d$$



## Theorem (Pigeonhole Principle)

If  $n$  **objects** are placed in  $r$  **boxes**, where  $r < n$ , then at least one of the boxes contains  $\geq 2$  ( $\geq \lceil \frac{n}{r} \rceil$ ) object.

## Numbers

Consider the numbers  $1, 2, \dots, 2n$ , and take any  $n + 1$  of them.

There are two among these  $n + 1$  numbers which are **relatively prime**.

## Numbers

Consider the numbers  $1, 2, \dots, 2n$ , and take any  $n + 1$  of them.

There are two among these  $n + 1$  numbers which are **relatively prime**.

There must be two numbers which are **only 1 apart**.

## Numbers

Consider the numbers  $1, 2, \dots, 2n$ , and take any  $n + 1$  of them. There are two among these  $n + 1$  numbers such as one **divides** the other.

## Numbers

Consider the numbers  $1, 2, \dots, 2n$ , and take any  $n + 1$  of them. There are two among these  $n + 1$  numbers such as one **divides** the other.

$$a = 2^k m, \quad (1 \leq m \leq 2n - 1 \text{ is odd})$$

There  $n + 1$  numbers have only  $n$  different odd parts.

There must be two numbers **with the same odd part**.

## Hand-shaking

If there are  $n > 1$  people who can shake hands with one another, there are two people who shake hands with the same number of people.



## Hand-shaking

If there are  $n > 1$  people who can shake hands with one another, there are two people who shake hands with the same number of people.

$$0 \sim n - 1$$

## Hand-shaking

If there are  $n > 1$  people who can shake hands with one another, there are two people who shake hands with the same number of people.

$$0 \sim n - 1$$

Either the '0' hole or the ' $n - 1$ ' hole or both must be empty.

## Sums

Suppose we are given  $n$  integers  $a_1, a_2, \dots, a_n$ .

Then there is a set of **consecutive numbers**  $a_{k+1}, a_{k+2}, \dots, a_l$  whose sum  $\sum_{i=k+1}^l a_i$  is a multiple of  $n$ .

## Sums

Suppose we are given  $n$  integers  $a_1, a_2, \dots, a_n$ .

Then there is a set of **consecutive numbers**  $a_{k+1}, a_{k+2}, \dots, a_l$  whose sum  $\sum_{i=k+1}^l a_i$  is a multiple of  $n$ .

$$A_i = \sum_{k=1}^{k=i} a_i$$

## Sums

Suppose we are given  $n$  integers  $a_1, a_2, \dots, a_n$ .

Then there is a set of **consecutive numbers**  $a_{k+1}, a_{k+2}, \dots, a_l$  whose sum  $\sum_{i=k+1}^l a_i$  is a multiple of  $n$ .

$$A_i = \sum_{k=1}^{k=i} a_i$$

$$A_0, A_1, A_2, \dots, A_n$$

## Sums

Suppose we are given  $n$  integers  $a_1, a_2, \dots, a_n$ .

Then there is a set of **consecutive numbers**  $a_{k+1}, a_{k+2}, \dots, a_l$  whose sum  $\sum_{i=k+1}^l a_i$  is a multiple of  $n$ .

$$A_i = \sum_{k=1}^{k=i} a_i$$

$$A_0, A_1, A_2, \dots, A_n$$

$$\exists 0 \leq i < j \leq n. A_i = A_j \pmod n$$

## Sums

Suppose we are given  $n$  integers  $a_1, a_2, \dots, a_n$ .

Then there is a set of **consecutive numbers**  $a_{k+1}, a_{k+2}, \dots, a_l$  whose sum  $\sum_{i=k+1}^l a_i$  is a multiple of  $n$ .

$$A_i = \sum_{k=1}^{k=i} a_i$$

$$A_0, A_1, A_2, \dots, A_n$$

$$\exists 0 \leq i < j \leq n. A_i = A_j \pmod n$$

$$A_j - A_i = a_{i+1} + \dots + a_j = 0 \pmod n$$

## Championship Match

“胡司令” (胡荣华) 要安排一次长达 77 天的象棋练习赛。

他想每天至少要有一场比赛, 但是总共不超过 132 场比赛。

请证明, 无论如何安排, 他都要在连续的若干天内恰好完成 21 场比赛。



## Championship Match

“胡司令” (胡荣华) 要安排一次长达 77 天的象棋练习赛。

他想每天至少要有一场比赛, 但是总共不超过 132 场比赛。

请证明, 无论如何安排, 他都要在连续的若干天内恰好完成 21 场比赛。

Let  $a_i$  denote the number of games he plays up through the  $i$ -th day.

## Championship Match

“胡司令” (胡荣华) 要安排一次长达 77 天的象棋练习赛。

他想每天至少要有一场比赛, 但是总共不超过 132 场比赛。

请证明, 无论如何安排, 他都要在连续的若干天内恰好完成 21 场比赛。

Let  $a_i$  denote the number of games he plays up through the  $i$ -th day.

$$a_1, a_2, \dots, a_{76}, a_{77}, a_1 + 21, a_2 + 21, \dots, a_{76} + 21, a_{77} + 21$$

## Championship Match

“胡司令” (胡荣华) 要安排一次长达 77 天的象棋练习赛。

他想每天至少要有一场比赛, 但是总共不超过 132 场比赛。

请证明, 无论如何安排, 他都要在连续的若干天内恰好完成 21 场比赛。

Let  $a_i$  denote the number of games he plays up through the  $i$ -th day.

$$a_1, a_2, \dots, a_{76}, a_{77}, a_1 + 21, a_2 + 21, \dots, a_{76} + 21, a_{77} + 21$$

There must be  $\geq 2$  elements having the same value.

## Championship Match

“胡司令” (胡荣华) 要安排一次长达 77 天的象棋练习赛。

他想每天至少要有一场比赛, 但是总共不超过 132 场比赛。

请证明, 无论如何安排, 他都要在连续的若干天内恰好完成 21 场比赛。

Let  $a_i$  denote the number of games he plays up through the  $i$ -th day.

$$a_1, a_2, \dots, a_{76}, a_{77}, a_1 + 21, a_2 + 21, \dots, a_{76} + 21, a_{77} + 21$$

There must be  $\geq 2$  elements having the same value.

It must be  $a_i + 21 = a_j$ .

## Sequences

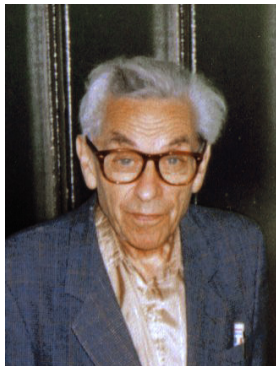
In any sequence  $a_1, a_2, \dots, a_{mn+1}$  of  $mn + 1$  **distinct** numbers, there exists an **increasing** subsequence

$$a_{i_1} < a_{i_2} < \dots < a_{i_{m+1}} \quad (i_1 < i_2 < \dots < i_{m+1})$$

of length  $m + 1$ , or a **decreasing** subsequence

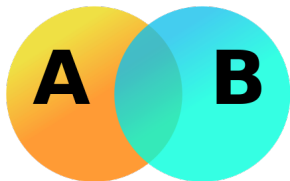
$$a_{j_1} > a_{j_2} > \dots > a_{j_{n+1}} \quad (j_1 > i_2 < \dots > j_{n+1})$$

of length  $n + 1$ , or both.

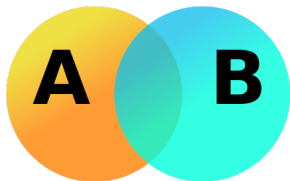


Paul Erdős (1913 ~ 1996)

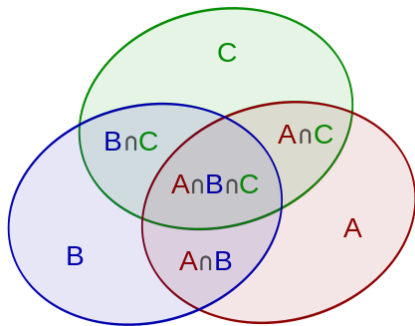
## Chapter 28 of “Proofs from THE Book”



$$|A \cup B| = |A| + |B| - |A \cap B|$$



$$|A \cup B| = |A| + |B| - |A \cap B|$$



$$\begin{aligned}
 |A \cup B \cup C| &= |A| + |B| + |C| \\
 &\quad - |A \cap B| - |A \cap C| - |B \cap C| \\
 &\quad + |A \cap B \cap C|
 \end{aligned}$$



## Theorem (Inclusion-Exclusion Principle)

$$\begin{aligned}\left| \bigcup_{i=1}^n A_i \right| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad - \dots \\ &\quad + (-1)^{n-1} |A_1 \cap \dots \cap A_n|.\end{aligned}$$

## Theorem (Inclusion-Exclusion Principle)

$$\begin{aligned}\left| \bigcup_{i=1}^n A_i \right| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad - \dots \\ &\quad + (-1)^{n-1} |A_1 \cap \dots \cap A_n|.\end{aligned}$$

$$\begin{aligned}\left| \bigcap_{i=1}^n \bar{A}_i \right| &= \left| S - \bigcup_{i=1}^n A_i \right| = |S| - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad - \dots + (-1)^n |A_1 \cap \dots \cap A_n|.\end{aligned}$$

## Counting Integers

How many integers in  $1, \dots, 100$  are not divisible by 2, 3 or 5?

## Counting Integers

How many integers in  $1, \dots, 100$  are not divisible by 2, 3 or 5?

$$100 - (50 + 33 + 20) + (16 + 10 + 6) - 3 = 26.$$

## Counting Derangements (错排)

Suppose there is a deck of  $n$  cards numbered from 1 to  $n$ .

Suppose a card numbered  $i$  is in the **correct** position if it is the  $i$ -th card in the deck. How many ways can the cards be shuffled **without any cards** being in the correct position?

## Counting Derangements (错排)

Suppose there is a deck of  $n$  cards numbered from 1 to  $n$ .

Suppose a card numbered  $i$  is in the **correct** position if it is the  $i$ -th card in the deck. How many ways can the cards be shuffled **without any cards** being in the correct position?

$A_m$  : all of the orderings of cards with the  $m$ -th card correct

## Counting Derangements (错排)

Suppose there is a deck of  $n$  cards numbered from 1 to  $n$ .

Suppose a card numbered  $i$  is in the **correct** position if it is the  $i$ -th card in the deck. How many ways can the cards be shuffled **without any cards** being in the correct position?

$A_m$  : all of the orderings of cards with the  $m$ -th card correct

$$\left| \bigcap_{i=1}^n \overline{A_i} \right| = \left| S - \bigcup_{i=1}^n A_i \right| = n! - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

## Counting Derangements (错排)

Suppose there is a deck of  $n$  cards numbered from 1 to  $n$ .

Suppose a card numbered  $i$  is in the **correct** position if it is the  $i$ -th card in the deck. How many ways can the cards be shuffled **without any cards** being in the correct position?

$A_m$  : all of the orderings of cards with the  $m$ -th card correct

$$\left| \bigcap_{i=1}^n \overline{A_i} \right| = \left| S - \bigcup_{i=1}^n A_i \right| = n! - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

$$S_k \triangleq \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| =$$



## Counting Derangements (错排)

Suppose there is a deck of  $n$  cards numbered from 1 to  $n$ .

Suppose a card numbered  $i$  is in the **correct** position if it is the  $i$ -th card in the deck. How many ways can the cards be shuffled **without any cards** being in the correct position?

$A_m$  : all of the orderings of cards with the  $m$ -th card correct

$$\left| \bigcap_{i=1}^n \overline{A_i} \right| = \left| S - \bigcup_{i=1}^n A_i \right| = n! - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

$$S_k \triangleq \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = \binom{n}{k} (n-k)! = \frac{n!}{k!}$$

$$S_k = \frac{n!}{k!}$$

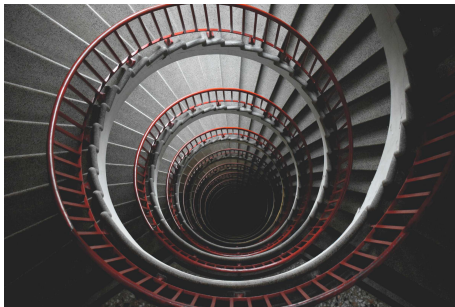
$$\left| \bigcap_{i=1}^n \overline{A_i} \right| = n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!}$$

$$= n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

$$S_k = \frac{n!}{k!}$$

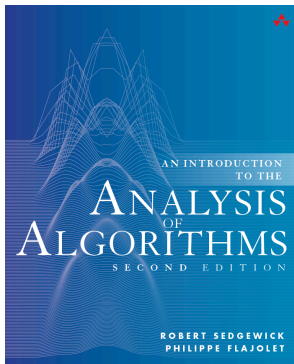
$$\begin{aligned} \left| \bigcap_{i=1}^n \overline{A_i} \right| &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!} \\ &= n! \sum_{k=0}^n \frac{(-1)^k}{k!} \end{aligned}$$

$$n \rightarrow \infty \implies \sum_{k=0}^n \frac{(-1)^k}{k!} \rightarrow e^{-1} \approx 0.368$$



$$a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-t}) + g(n)$$

$$a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-t}) + g(n)$$



recurrence type	typical example
first-order	
linear	$a_n = na_{n-1} - 1$
nonlinear	$a_n = 1/(1 + a_{n-1})$
second-order	
linear	$a_n = a_{n-1} + 2a_{n-2}$
nonlinear	$a_n = a_{n-1}a_{n-2} + \sqrt{a_{n-2}}$
variable coefficients	$a_n = na_{n-1} + (n-1)a_{n-2} + 1$
$t$ th order	$a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-t})$
full-history	$a_n = n + a_{n-1} + a_{n-2} \dots + a_1$
divide-and-conquer	$a_n = a_{\lfloor n/2 \rfloor} + a_{\lceil n/2 \rceil} + n$

**Table 2.1** Classification of recurrences

## Homogeneous Linear Recurrence Relations with Constant Coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_t a_{n-t}$$

## Homogeneous Linear Recurrence Relations with Constant Coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_t a_{n-t}$$

2020 年课程录屏 (Recurrence)



$$R \subseteq A \times A$$

$$\begin{cases} R^0 = I_A \\ R^{n+1} = R \circ R^n \end{cases}$$

## Representing Relations as Matrices/Digraphs

$$A = \{1, 2, 3, 4\}$$

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1)\}$$

## Representing Relations as Matrices/Digraphs

$$A = \{1, 2, 3, 4\}$$

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1)\}$$

$$R^2 \quad R^3$$

## Representing Relations as Matrices/Digraphs

$$A = \{1, 2, 3, 4\}$$

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1)\}$$

$$R^2 \quad R^3$$

$$R^+ = \bigcup_{i=1}^{\infty} R \quad R^* = \bigcup_{i=0}^{\infty} R$$

### Definition (Reflexive Closure (自反闭包))

The **reflexive closure**  $\text{cl}_{\text{ref}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** reflexive relation on  $X$  that contains  $R$ .

### Definition (Reflexive Closure (自反闭包))

The **reflexive closure**  $\text{cl}_{\text{ref}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** reflexive relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{ref}}(R) = R \cup I_X$$

### Definition (Symmetric Closure (对称闭包))

The **symmetric closure**  $\text{cl}_{\text{sym}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** symmetric relation on  $X$  that contains  $R$ .

### Definition (Symmetric Closure (对称闭包))

The **symmetric closure**  $\text{cl}_{\text{sym}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** symmetric relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{sym}}(R) = R \cup R^{-1}$$



## Definition (Transitive Closure (传递闭包))

The **transitive closure**  $\text{cl}_{\text{trn}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** transitive relation on  $X$  that contains  $R$ .

## Definition (Transitive Closure (传递闭包))

The **transitive closure**  $\text{cl}_{\text{trn}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** transitive relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{trn}}(R) = R^+$$

## Definition (Transitive Closure (传递闭包))

The **transitive closure**  $\text{cl}_{\text{trn}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** transitive relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{trn}}(R) = R^+$$

- ▶  $R^+$  contains  $R$
- ▶  $R^+$  is transitive
- ▶  $R^+$  is minimal

## Definition (Transitive Closure (传递闭包))

The **transitive closure**  $\text{cl}_{\text{trn}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** transitive relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{trn}}(R) = R^+$$

- ▶  $R^+$  contains  $R$
- ▶  $R^+$  is transitive
- ▶  $R^+$  is minimal

If  $T$  is any transitive relation containing  $R$ , then  $R^+ \subset T$ .

## Definition (Transitive Closure (传递闭包))

The **transitive closure**  $\text{cl}_{\text{trn}}(R)$  of a relation  $R \subseteq X \times X$  is the **smallest** transitive relation on  $X$  that contains  $R$ .

$$\text{cl}_{\text{trn}}(R) = R^+$$

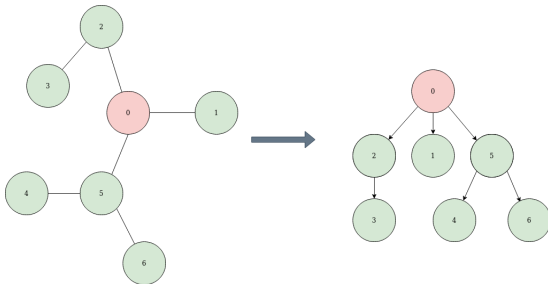
- ▶  $R^+$  contains  $R$
- ▶  $R^+$  is transitive
- ▶  $R^+$  is minimal

If  $T$  is any transitive relation containing  $R$ , then  $R^+ \subseteq T$ .

By induction on  $i$ , we can show that  $R^i \subseteq T$ .

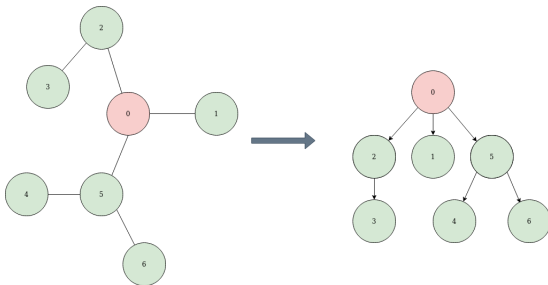
## Definition (Rooted Tree (有根树))

A **rooted tree** is a **tree** where one vertex has been **designated the root**.



## Definition (Rooted Tree (有根树))

A **rooted tree** is a **tree** where one vertex has been **designated the root**.



## Definition (Directed Rooted Tree (有向有根树))

A **directed rooted tree** is a **rooted tree** where all edges directed **away from** or **towards** the root.

## Definition

Parent, Child; Sibling; Ancestor, Descendant



## Definition

Parent, Child; Sibling; Ancestor, Descendant

## Definition ( $k$ -ary Trees ( $k$ -叉树))

A  $k$ -ary tree is a rooted tree in which each vertex has  $\leq k$  children.

2-ary trees are often called binary trees.

## Definition

Parent, Child; Sibling; Ancestor, Descendant

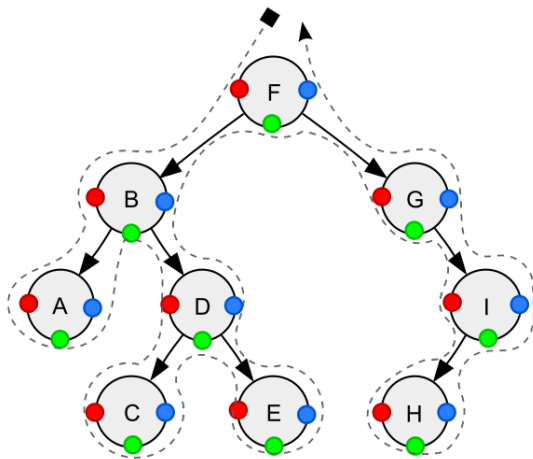
## Definition ( $k$ -ary Trees ( $k$ -叉树))

A  $k$ -ary tree is a rooted tree in which each vertex has  $\leq k$  children.

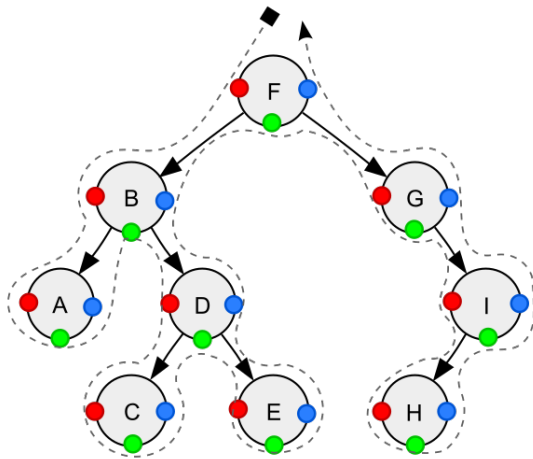
2-ary trees are often called binary trees.

## Definition (Complete $k$ -Tree (完全 $k$ -叉树))

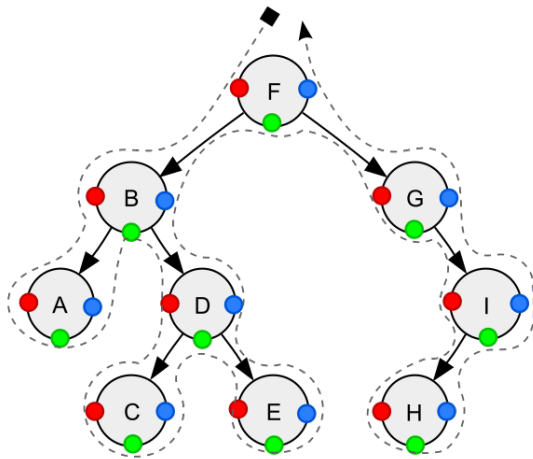
A complete  $k$ -tree is a  $k$ -ary tree in which each vertex, other than leaves, has  $= k$  children.



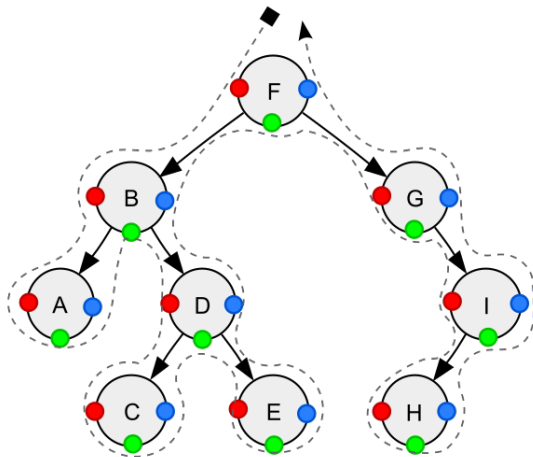
Depth-First Search (DFS)



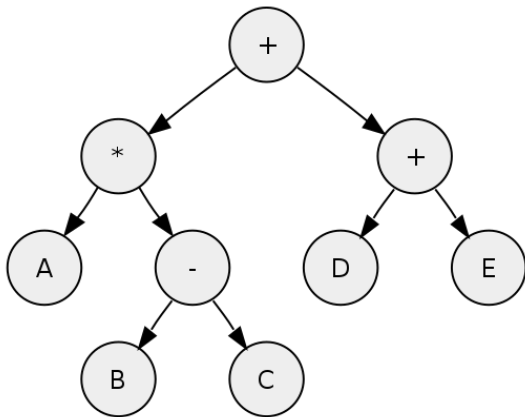
Pre-order (前序) Traversal:  $F, B, A, D, C, E, G, I, H$



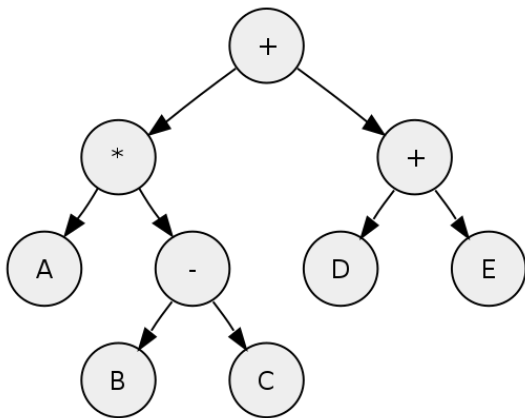
In-order (中序) Traversal:  $A, B, C, D, E, F, G, H, I$



Post-order (后序) Traversal:  $A, C, E, D, B, H, I, G, F$



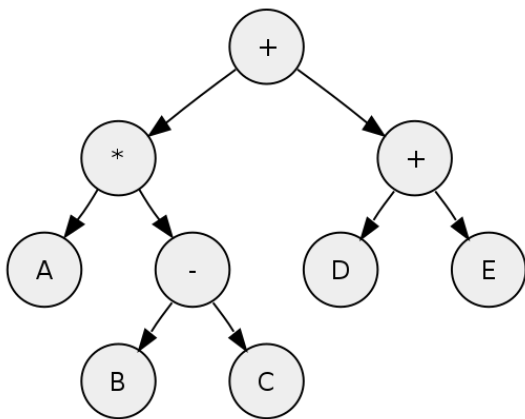
Prefix Expression (前缀表达式):  $+ * A - BC + DE$



Prefix Expression (前缀表达式):  $+ * A - BC + DE$

Infix Expression (中缀表达式):  $A * (B - C) + (D + E)$

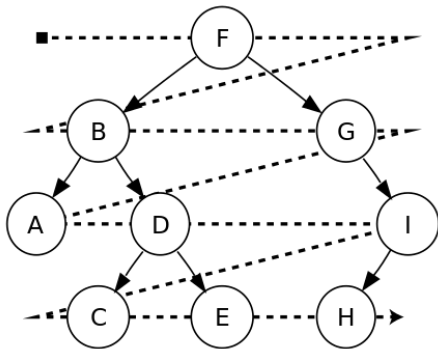




Prefix Expression (前缀表达式):  $+ * A - BC + DE$

Infix Expression (中缀表达式):  $A * (B - C) + (D + E)$

Postfix Expression (后缀表达式):  $ABC - * DE + +$



Breadth-First Search (BFS):  $F, B, G, A, D, I, C, E, H$



David A. Huffman (1925 ~ 1999)

$C[1 \dots n]$	$a$	$b$	$c$	$d$	$e$	$f$
$F[1 \dots n]$	45	13	12	16	9	5
Fixed Length Code	000	001	010	011	100	101
Variable Length Code	0	101	100	111	1101	1100

Prefix code (前缀码): No code is a **prefix** of some other code

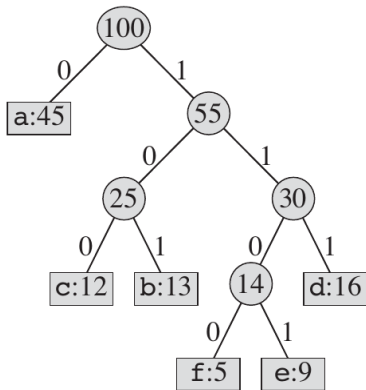
## The Encoding Problem

To find the **optimal** binary prefix code for  $C$  and  $F$ .

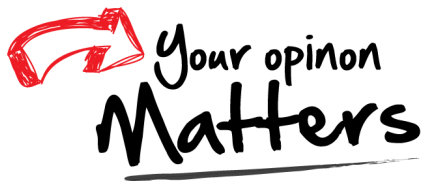
Let  $E$  be a binary prefix code for  $C$  and  $F$ . The length  $L(E)$  is

$$L(E) = \sum_{c \in C} f_c \cdot l_E(c)$$

$C[1 \dots n]$	$a$	$b$	$c$	$d$	$e$	$f$
$F[1 \dots n]$	45	13	12	16	9	5



Thank  
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn