(十五) 离散数学: 复习 (Review)

魏恒峰

hfwei@nju.edu.cn

2021年06月17日



1/47

Theorem

$$\Sigma \vdash \alpha \Longleftrightarrow \Sigma \models \alpha$$

3/47





" \rightarrow " and " \leftrightarrow " are used in a single formula.

" \Longrightarrow " and " \Longleftrightarrow " are used to connect two formulas.



" \rightarrow " and " \leftrightarrow " are used in a single formula.

" \Longrightarrow " and " \Longleftrightarrow " are used to connect two formulas.

$$x \in A \setminus B$$

$$\iff x \in A \land x \notin B$$

$$\iff x \in A \land (x \in U \land x \notin B)$$

$$\iff x \in A \land x \in \overline{B}$$

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

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

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

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

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

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

Theorem

$\sqrt{2}$ is irrational.



The First Crisis in Mathematics

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 ≥ 2 ($\geq \lceil \frac{n}{r} \rceil$) object.

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

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

Consider the numbers $1, 2, \ldots, 2n$, 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.

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

There are two among these n+1 numbers such as one divides the other.

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

There are two among these n+1 numbers such as one divides the other.

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

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.

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

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

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

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

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

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

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

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

$$A_0, A_1, A_2, \ldots, A_n$$

$$\exists 0 \le i < j \le n. \ A_i = A_j \mod n$$

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

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

$$A_0, A_1, A_2, \ldots, A_n$$

$$\exists 0 \le i < j \le n. \ A_i = A_j \mod n$$

$$A_i - A_i = a_{i+1} + \dots + a_i = 0 \mod n$$



"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。

"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.

"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.

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

"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.

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

There must be ≥ 2 elements having the same value.

"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.

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

There must be ≥ 2 elements having the same value.

It must be
$$a_i + 21 = a_j$$
.

4□ > 4回 > 4 = > 4 = > = 9 < ○</p>

Sequences

In any sequence $a_1, a_2, \ldots, a_{mn+1}$ 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

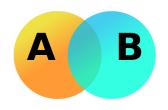
$$a_{j_1} > a_{j_2} > \dots > a_{j_{n+1}} \quad (j_1 > i_2 < \dots > j_{n+1})$$

of length n+1, or both.

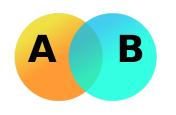


Paul Erdős (1913 \sim 1996)

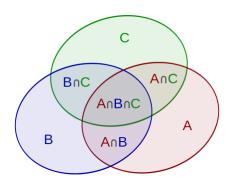
Chapter 28 of "Proofs from THE Book"



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



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



$$|A \cup B \cup C| = |A| + |B| + |C|$$

$$-|A \cap B| - |A \cap C| - |B \cap C|$$

$$+|A \cap B \cap C|$$

Theorem (Inclusion-Exclusion Principle)

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j|$$

$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k|$$

$$- \cdots$$

$$+ (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

Theorem (Inclusion-Exclusion Principle)

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

$$+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k|$$

$$- \cdots$$

$$+ (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

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

Counting Integers

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

Counting Integers

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

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

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?

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?

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?

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

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?

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

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

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?

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

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

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

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

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

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

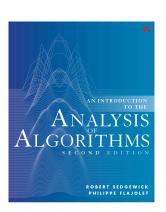
$$n \to \infty \implies \sum_{k=0}^{n} \frac{(-1)^k}{k!} \to e^{-1} \approx 0.368$$



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

22 / 47

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



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	$a_n = na_{n-1} + (n-1)a_{n-2} + 1$
tth 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

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

Homogeneous Linear Recurrence Relations with Constant Coefficients

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



https://www.bilibili.com/video/BV1Cf4y187Cu?share_source=copy_web

23 / 47

$$R \subseteq A \times A$$

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

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

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

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

$$R^2 \qquad R^3$$

Representing Relations as Matrices/Digraphs

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

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

$$R^{2} \qquad R^{3}$$

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

Definition (Reflexive Closure (自反闭包))

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

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

Definition (Symmetric Closure (对称闭包))

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

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

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

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

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

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

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

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

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

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

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

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

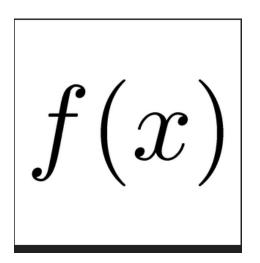
The transitive closure $\operatorname{cl}_{\operatorname{trn}}(R)$ of a relation $R \subseteq X \times X$ is the smallest transitive relation on X that contains R.

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

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

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

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



29/47

Injection (one-to-one; 1-1)

Surjection

Bijection (one-to-one correspondence)

Definition (Characteristic Function (特征函数) of a Subset)

For a given subset $A \subseteq X$,

$$\chi_A:X\to\{0,1\}$$

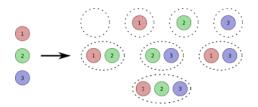
$$\chi_A(x) = 1 \iff x \in A.$$

Definition (Characteristic Function (特征函数) of a Subset)

For a given subset $A \subseteq X$,

$$\chi_A: X \to \{0, 1\}$$

$$\chi_A(x) = 1 \iff x \in A.$$



$$\chi_A: X \to \{0,1\}$$
 vs. $\mathcal{P}(X)$

Definition (Natural Function)

Let $R \subseteq A \times A$ be an equivalence relation. The following function f

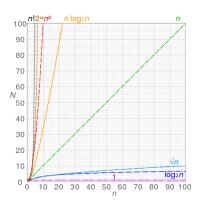
$$f:A\to A/R$$

$$f: a \mapsto R(a)$$

is called the natural function on A.



Asymptotic Growth Rates of Functions





https://www.bilibili.com/video/BV175411T7ph?share_source=copy_web



Definition (Order Isomorphism (同构))

Given two posets (S, \leq_S) and (T, \leq_T) , an order isomorphism from (S, \leq_S) to (T, \leq_T) is a bijection from S to T such that

$$\forall x, y \in S. \ x \leq_S y \leftrightarrow f(x) \leq_T f(y).$$

Definition (Order Isomorphism (同构))

Given two posets (S, \leq_S) and (T, \leq_T) , an order isomorphism from (S, \leq_S) to (T, \leq_T) is a bijection from S to T such that

$$\forall x, y \in S. \ x \leq_S y \leftrightarrow f(x) \leq_T f(y).$$

$$(\mathbb{R}, \leq) \xrightarrow{f \colon \mathbb{R} \to \mathbb{R}} (\mathbb{R}, \geq)$$

Definition (Order Isomorphism (同构))

Given two posets (S, \leq_S) and (T, \leq_T) , an order isomorphism from (S, \leq_S) to (T, \leq_T) is a bijection from S to T such that

$$\forall x, y \in S. \ x \leq_S y \leftrightarrow f(x) \leq_T f(y).$$

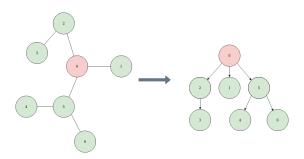
$$(\mathbb{R}, \leq) \xrightarrow{f: \mathbb{R} \to \mathbb{R}} (\mathbb{R}, \geq)$$

Definition (Order Automorphism (自同构))

An order isomorphism from a poset to itself is an order automorphism.

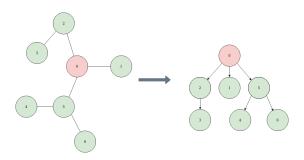
Definition (Rooted Tree (有根树))

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

 $Parent,\,Child;\quad Sibling;\quad Ancestor,\,Descendant$

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

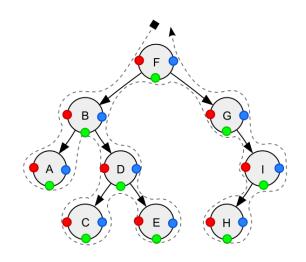
Definition (k-ary Trees (k-叉树))

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

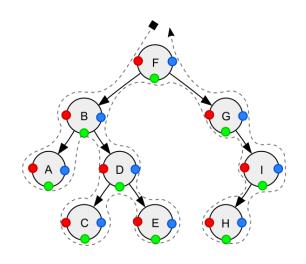
2-ary trees are often called binary trees.

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

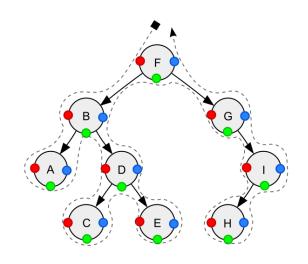
A complete k-tree is a k-ary tree in which each vertex, other than leaves, has = k children.



Depth-First Search (DFS)

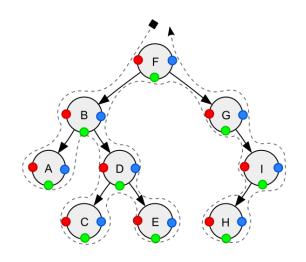


Pre-order (前序) Traversal: F, B, A, D, C, E, G, I, H



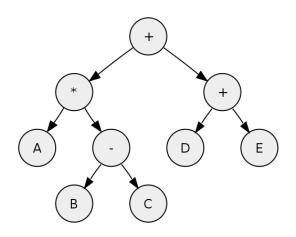
In-order (中序) Traversal: A, B, C, D, E, F, G, H, I

40/47

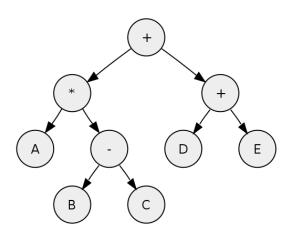


Post-order (后序) Traversal: A, C, E, D, B, H, I, G, F

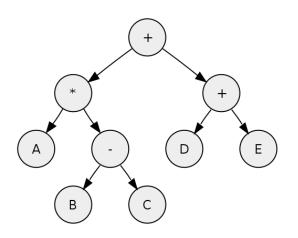
41/47



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



Prefix Expression (前缀表达式): +*A - BC + DEInfix Expression (中缀表达式): A*(B-C) + (D+E)

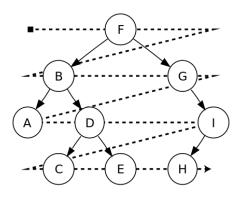


Prefix Expression (前缀表达式): +*A - BC + DE

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

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

2021 年 06 月 17 日



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



David A. Huffman (1925 $\sim 1999)$

$C[1 \dots n]$	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

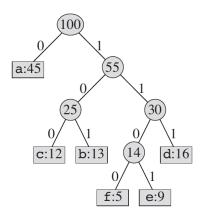
The Encoding Problem

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