

(十五) 离散数学: 复习 (Review)


魏恒峰

hfwei@nju.edu.cn

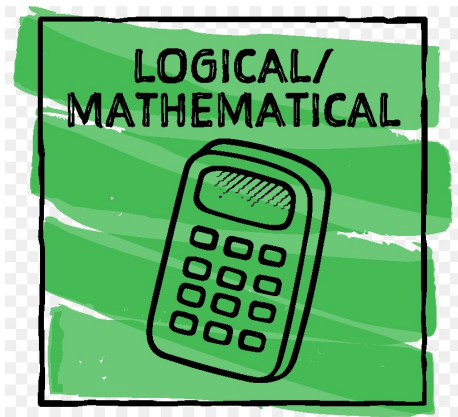
2021 年 06 月 17 日







Back to basics



\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.

$$x \in A \setminus B$$

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

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

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

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

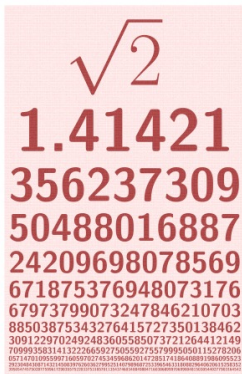
$$\begin{aligned}
 p \oplus q &\triangleq (p \vee q) \wedge \neg(p \wedge q) \\
 &= (p \wedge \neg q) \vee (\neg q \wedge q)
 \end{aligned}$$

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

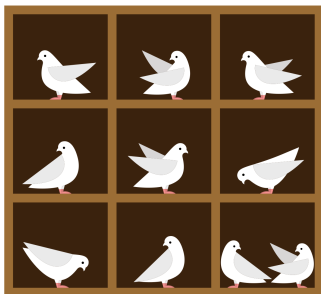
$$p \oplus q = q \oplus r$$

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

$\sqrt{2}$ is irrational.



The First Crisis in Mathematics



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.

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.

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

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.

$$0 \sim n - 1$$

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 .

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

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

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

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

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。

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 ≥ 2 elements having the same value.

It must be $a_i + 21 = a_j$.

Sequences

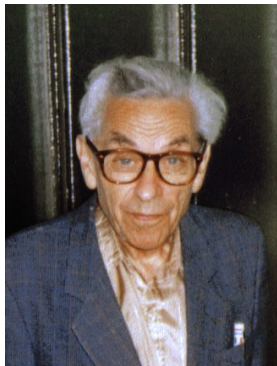
In any sequence $a_1, a_2, \dots, a_{mn+1}$ of $mn + 1$ **distinct** numbers, there exists an **increasing** subsequence

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

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

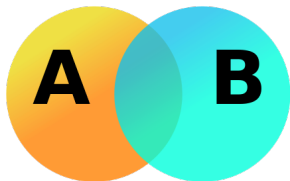
$$a_{j_1} > a_{j_2} > \dots > a_{j_{n+1}} \quad (j_1 > j_2 > \dots > j_{n+1})$$

of length $n + 1$, or both.

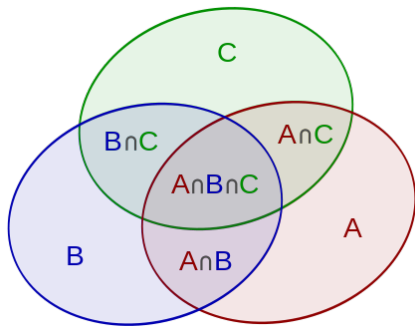


Paul Erdős (1913 ~ 1996)

Chapter 28 of “Proofs from THE Book”



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



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

Theorem (Inclusion-Exclusion Principle)

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

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

Counting Integers

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

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

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?

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

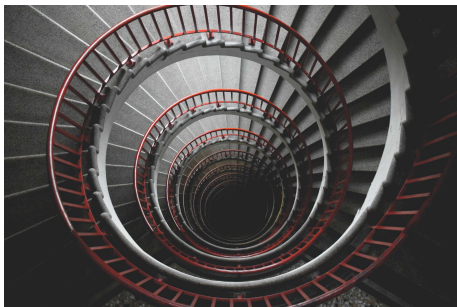
$$\left| \bigcap_{i=1}^n \overline{A_i} \right| = \left| S - \bigcup_{i=1}^n A_i \right| = n! - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ - \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.$$

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

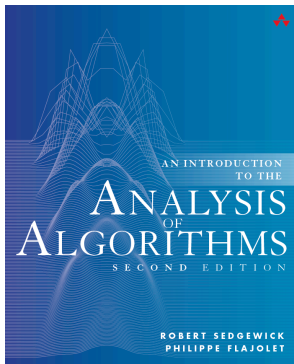
$$S_k = \frac{n!}{k!}$$

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

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



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



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

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



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

$$R \subseteq A \times A$$

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

Representing Relations as Matrices/Digraphs

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

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

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

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

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 .

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

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 .

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

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 .

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

- ▶ 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 $R^i \subseteq T$.

$$f(x)$$

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

Surjection

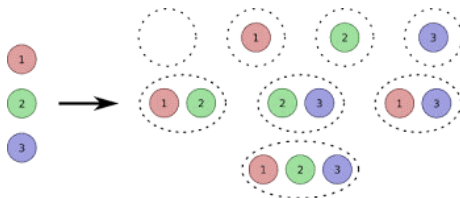
Bijection (one-to-one correspondence)

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

For a given subset $A \subseteq X$,

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

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



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

Definition (Natural Function)

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

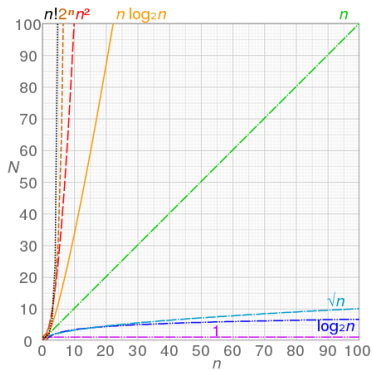
$$f : A \rightarrow A/R$$

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

is called the **natural function** on A .



Asymptotic Growth Rates of Functions



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



Ordering

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

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

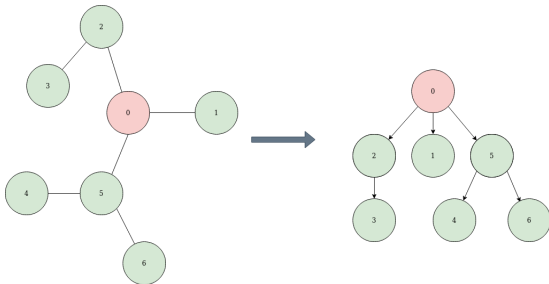
$$(\mathbb{R}, \leq) \xrightarrow[f: x \mapsto -x]{f: \mathbb{R} \rightarrow \mathbb{R}} (\mathbb{R}, \geq)$$

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 (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

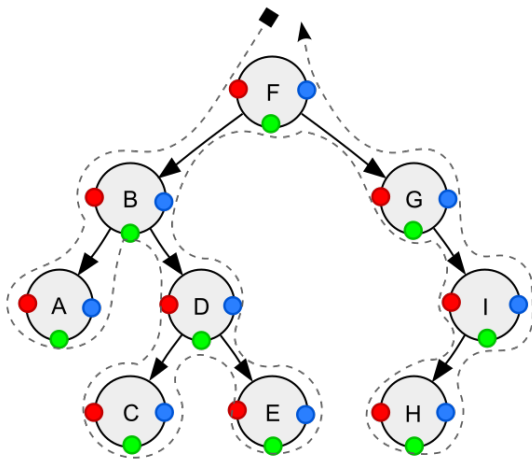
Definition (k -ary Trees (k -叉树))

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

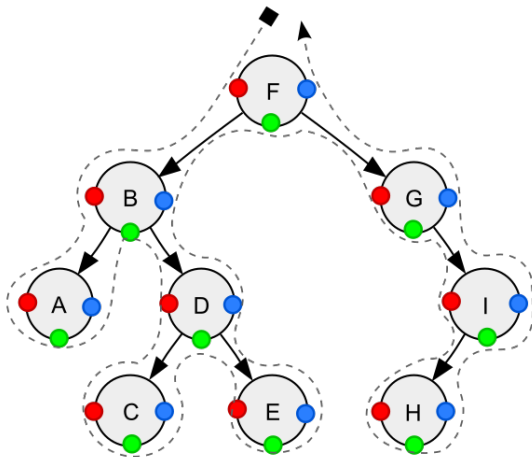
2-ary trees are often called binary trees.

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

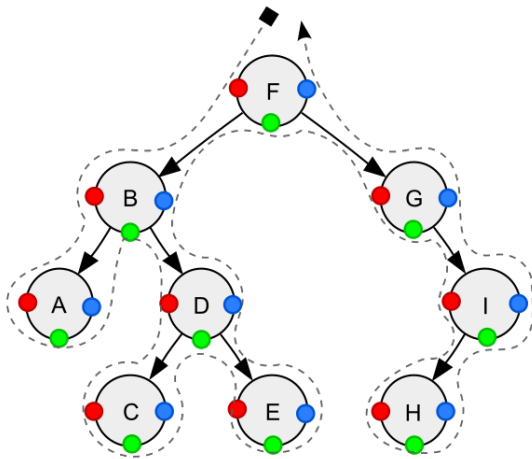
A complete k -tree is a k -ary tree in which each vertex, other than leaves, has $= k$ children.



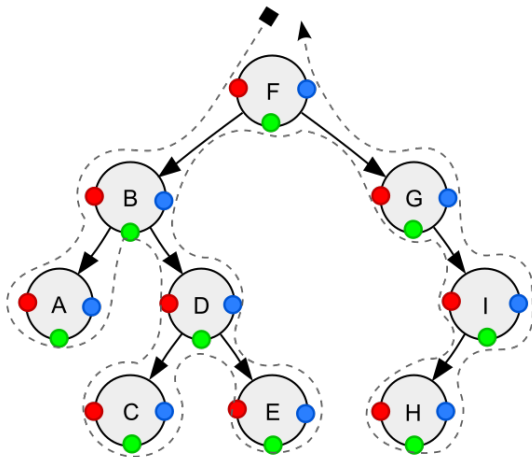
Depth-First Search (DFS)



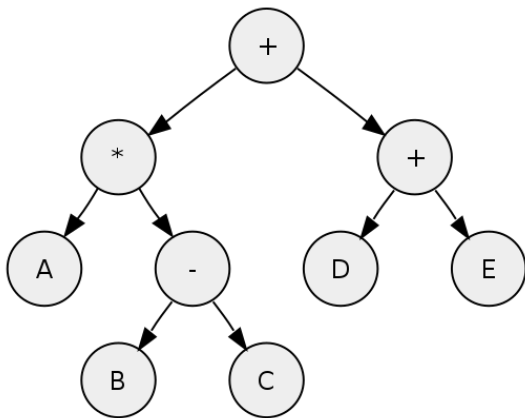
Pre-order (前序) Traversal: $F, B, A, D, C, E, G, I, H$



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



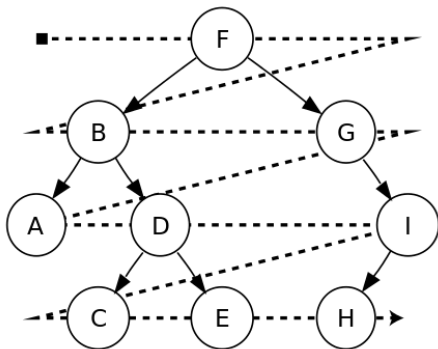
Post-order (后序) Traversal: $A, C, E, D, B, H, I, G, F$



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

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

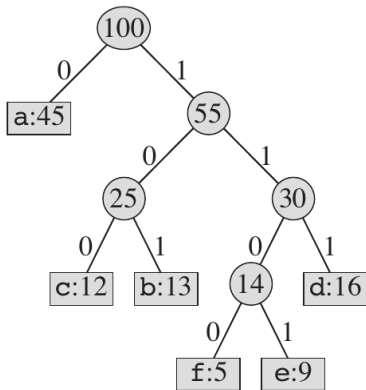
The Encoding Problem

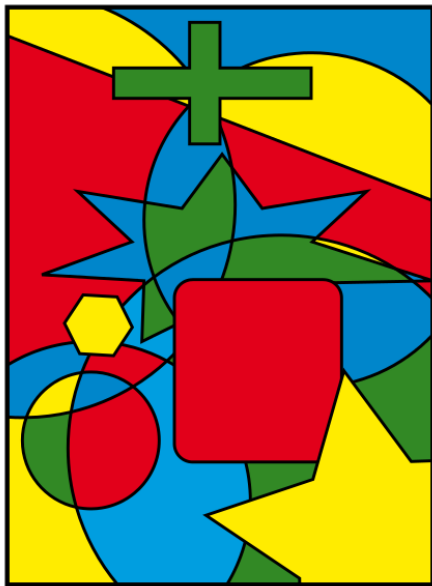
To find the **optimal** binary prefix code for C and F .

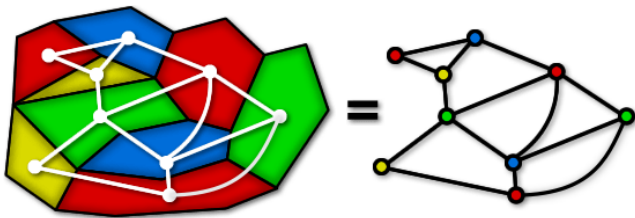
Let E be a binary prefix code for C and F . The length $L(E)$ is

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

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



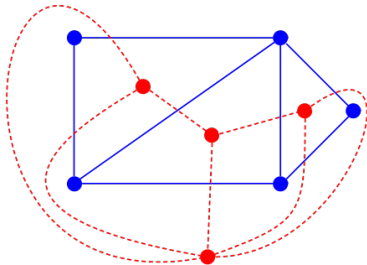


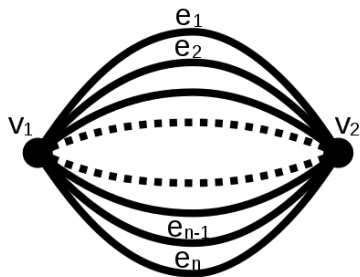
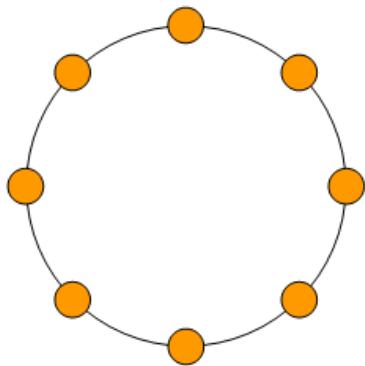


Definition (Dual Graph (对偶图))

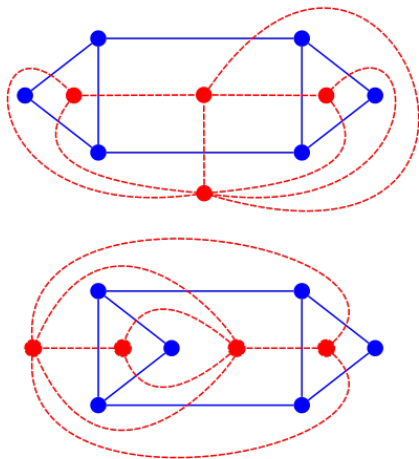
The **dual graph** of a **plane graph** G is a graph G'

- ▶ G' has a **vertex** for each face of G ;
- ▶ G' has an **edge** for each pair of faces in G that are separated from each other by an edge, and a **self-loop** when the same face appears on both sides of an edge.



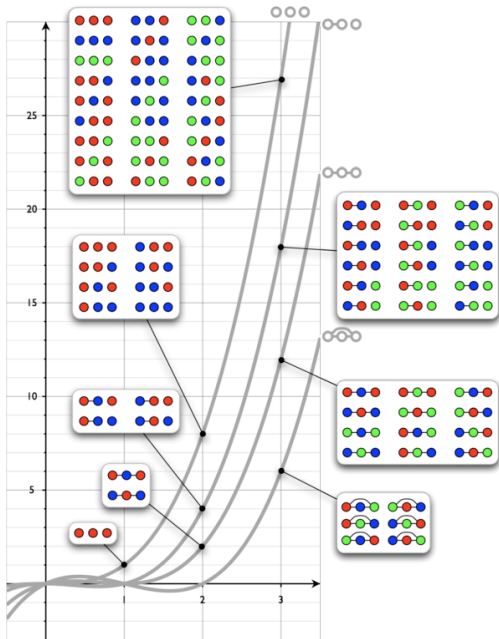


The dual graph G' depends on **the choice of embedding** of the graph G .



Theorem

G is a bipartite graph $\iff \chi(G) = 2 \iff G$ has no odd cycles.



Definition (Chromatic Polynomial (色多项式; 非严格定义))

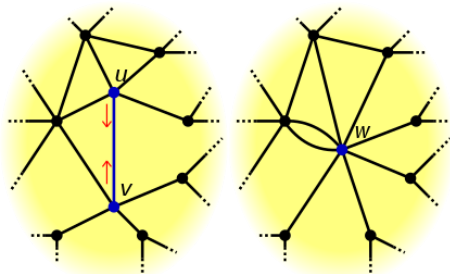
The **chromatic polynomial** $P(G, k)$ counts the number of colorings of graph G as a function of the number k of colors.

Triangle K_3	$x(x-1)(x-2)$
Complete graph K_n	$x(x-1)(x-2)\cdots(x-(n-1))$
Edgeless graph \overline{K}_n	x^n
Path graph P_n	$x(x-1)^{n-1}$
Any tree on n vertices	$x(x-1)^{n-1}$
Cycle C_n	$(x-1)^n + (-1)^n(x-1)$
Petersen graph	$x(x-1)(x-2)(x^7 - 12x^6 + 67x^5 - 230x^4 + 529x^3 - 814x^2 + 775x - 352)$

Theorem (Recurrence for Chromatic Polynomial)

Given a graph G and an edge $e \in E(G)$, then

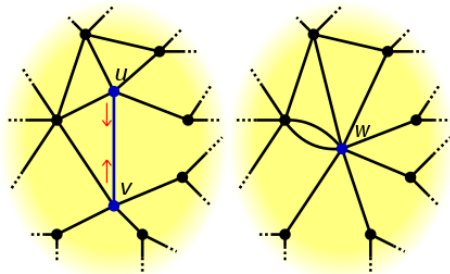
$$P(G, k) = P(G - e, k) - P(G/e, k)$$



G/e : 边的收缩

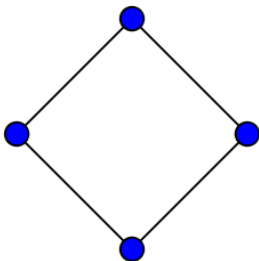
$$P(G, k) = P(\textcolor{red}{G} - e, k) - P(\textcolor{red}{G}/e, k)$$

$$P(G - e, k) = P(\textcolor{violet}{G}/e, k) + P(\textcolor{violet}{G}, k)$$



In $G - \{u, v\}$, $\textcolor{violet}{Color}(u) = \textcolor{violet}{Color}(v)$ or $\textcolor{violet}{Color}(u) \neq \textcolor{violet}{Color}(v)$.

$$P(G, k) = P(\textcolor{red}{G} - e, k) - P(\textcolor{red}{G}/e, k)$$



$$\begin{aligned} P(C_4, k) &= P(P_4, k) - P(K_3, k) \\ &= k(k-1)^3 - k(k-1)(k-2) \\ &= k(k-1)(k^2 - 3k + 3) \\ &= (k-1)^4 + (-1)^4(k-1) \end{aligned}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\sigma = (1\ 4)(2\ 3\ 6)(5)$$

$$= (1\ 4)(2\ 3\ 6)$$

$$= (2\ 3\ 6)(1\ 4)$$

$$= (2\ 3\ 6)(4\ 1)$$

$$= (3\ 6\ 2)(4\ 1)$$

$$= (3\ 6)(6\ 2)(4\ 1)$$

$$(i_1\ i_2\ \dots\ i_r) = (i_1\ i_2)(i_2\ i_3)\dots(i_{r-2}\ i_{r-1})(i_{r-1}\ i_r)$$

By induction on the length r .

$$\begin{aligned}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 2 & 5 & 4 & 1 \end{pmatrix} &= (1\ 7)(2\ 3)(3\ 6)(6\ 4) \\ &= (1\ 7)(3\ 6)(2\ 5)(6\ 4)(4\ 5)(2\ 5)\end{aligned}$$

Theorem (Parity (奇偶性) of Permutations)

将一个置换表示成若干对换的乘积, 所用对换个数的奇偶性是唯一的。

Definition (Even/Odd Permutations (偶置换/奇置换))

可表示为偶数个对换的乘积的置换称为偶置换; 否则, 称为奇置换。

Definition (Alternating Group (交错群; A_n))

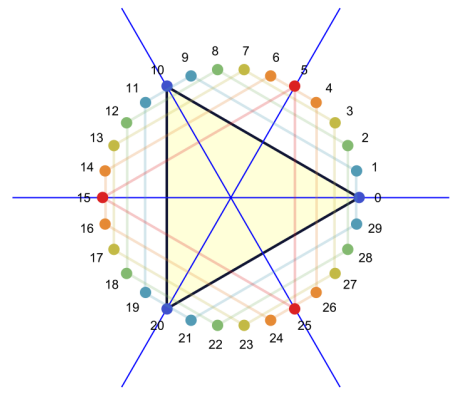
由 S_n 的全体偶置换构成的子群称为 n 次交错群。

$$A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$\operatorname{sgn} : S_n \rightarrow \{1, -1\}$$

$$\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$$

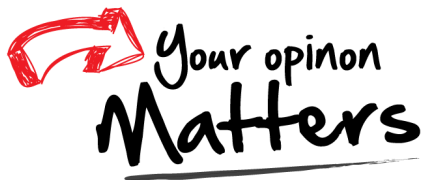
$$S_n/A_n \cong \{1, -1\}$$



$$A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$(1\ 2)A_3 = \{(1\ 2), (2\ 3), (1\ 3)\}$$

Thank
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn