置换群快速幂运算研究与探讨

江苏省苏州中学
潘震皓

基础知识

- 群 是集合 G 和定义在 G 上的二元运算符•组成的代数系统

- 群 满足 封闭性、结合律、单位元和逆元

基础知识

- **置换**

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & 4 & 2 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

置换 T

定义符号→ ，a 被 b 取代 => $b=a\rightarrow T$

$a(\rightarrow)^2T= a\rightarrow T\rightarrow T$

基础知识

- **连接运算**

$$a \rightarrow T1 \rightarrow T2 = a \rightarrow (T1 \bullet T2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 & 2 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

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

基础知识

- 循环

$$(1\ \ 3\ \ 2) \Longleftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

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

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

- 置换群基本操作

1. 存储 O(n)
2. 映射 O(1)
3. 连接运算 O(n)
4. 分解循环 O(n)
5. 整幂运算 $O(n \log k)$?
6. 开方运算 O(n+k) ?

例题

- 洗牌机（CEOI 98)

- 凯凯和凡凡有 N 张牌（依次标号为 1 ，2 ，……，N ）和一台洗牌机。假设 N 是奇数。洗牌机的功能是进行如下的操作：对所有位置 I （ $1 \le I \le N$ ），如果位置 I 上的牌是 J ，而且位置 J 上的牌是 K ，那么通过洗牌机后位置 I 上的牌将是 K 。
- 凯凯首先写下一个 1~N 的排列 a_i ，在位置 a_i 处放上数值 a_{i+1} 的牌，得到的顺序 $x_1, x_2, \ldots, x_N$ 作为初始顺序。他把这种顺序排列的牌放入洗牌机洗牌 S 次，得到牌的顺序为 $p_1, p_2, \ldots, p_N$ 。现在，凯凯把牌的最后顺序和洗牌次数告诉凡凡，要凡凡猜出牌的最初顺序 $x_1, x_2, \ldots, x_N$ 。

例题

位置 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$
牌

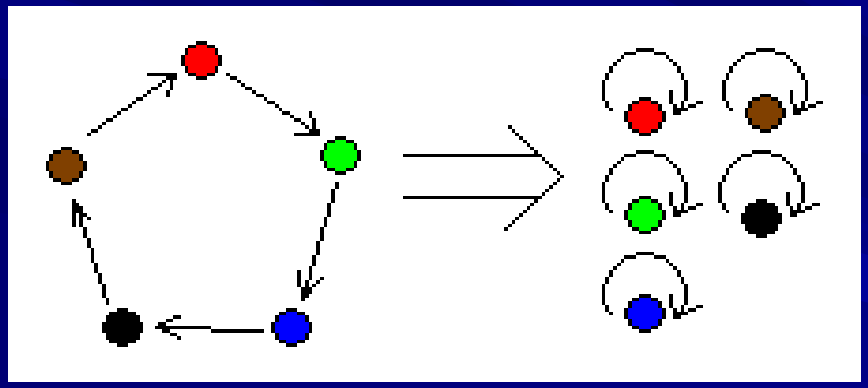
位置 i　　扑克牌 j　　位置 j　　扑克牌 k
位置 i　　扑克牌 k

a_i　　位置 a_i　　扑克牌 a_{i+1}

(1 3 4 2)

一个引子

- 设$T^k = e$，（T 为一循环，e 为单位置换），那么 k 的最小正整数解为 T 的长度。



- T=(1 3 5 2 4 6)

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

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

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

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

- $T=(1\ 3\ 5\ 2\ 4\ 6)$

- $T^2=(1\ 5\ 4)(2\ 6\ 3)$

- T^2 是两个循环的乘积，这两个循环分别是循环 T 的奇数项和偶数项

- $T=(1\ 3\ 5\ 2\ 4\ 6)$
- $T^3=(1\ 2)(3\ 4)(5\ 6)$
- T^3 是三个循环的乘积，这三个循环分别是循环 T 中编号 mod 3=0, 1, 2 的项
- 当 k|n 时，T^k 分裂成了 k 个循环的乘积，这 k 个循环分别是循环 T 中编号 mod k=0, 1…k-1 的项，按顺序的连接

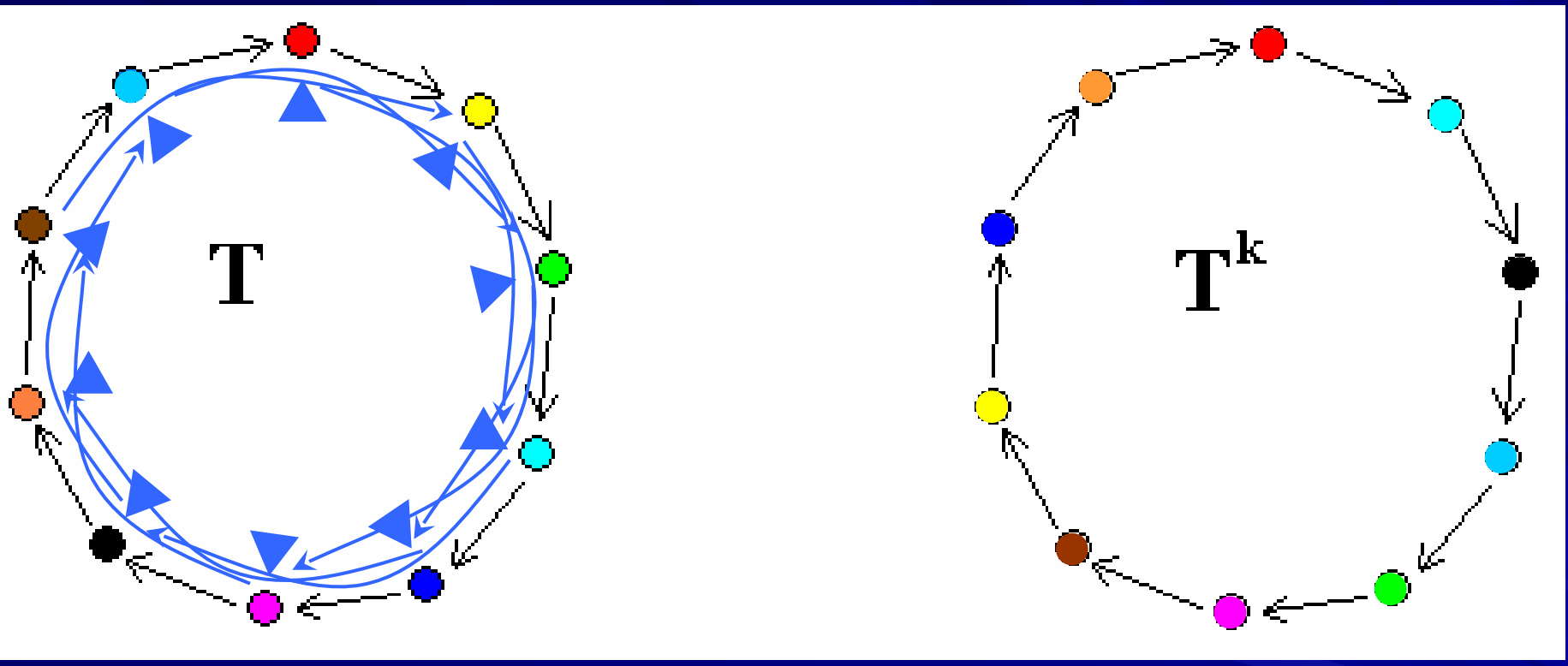
- $T^{a*b}=(T^a)^b$
- a=gcd(n,k) b=k/a
- $T^k=(T^a)^b$
- 所以说，现在问题就转换到了长度 n 和指数 k 互质时 的 整幂运算。

- 若 $T=(a_1 \quad a_2 \quad \dots \quad a_n)$，
  假设 $T^k=(b_1 \quad b_2 \quad \dots \quad b_n)$

- 则 :$a_i \to T=a_{i+1}$，$b_i \to T^k=b_{i+1}$

- 显然，$b_i \to T^k=b_i(\to)^k T=b_i \to T \to T \dots \to T$

- 所以，令 $a_i=b_j$，$a_{i+k}=b_{j+1}$


T
T^k

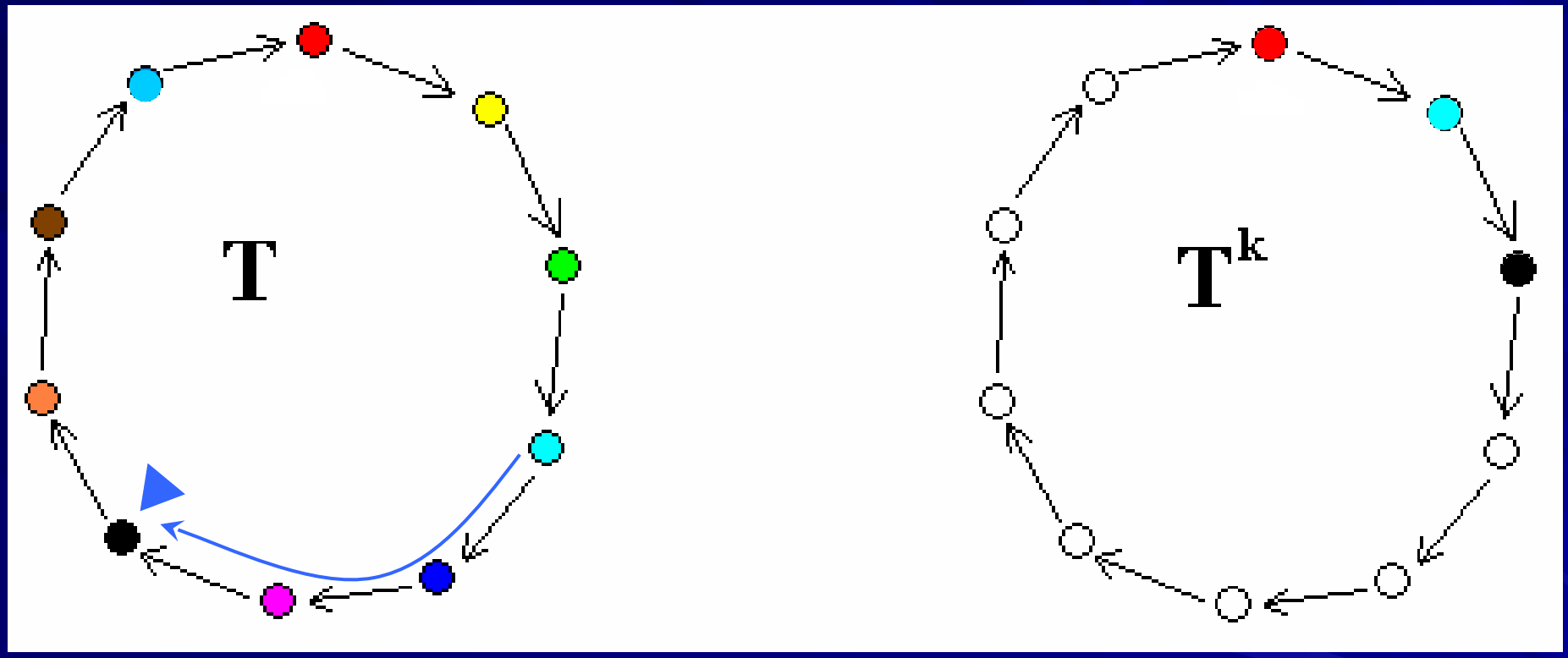
- 置换群整幂运算可以在线性时间复杂度内解决

- 算法：
  - 分解循环
  - 从每个未扫描元素，按上述方法求得一个循环
  - 将所有求得循环合并成置换

开方运算

- 开方运算比整幂运算复杂
  1. 有多解
  2. 有无解
  3. 多解规律性不强

- 需要解决的问题
  1. 一个可行解
  2. 解的个数


T
T^k

- $T=(1\ 6\ 4)(2\ 3\ 5)$

  $(1\ 6\ 4)(3\ 5\ 2)$
- $T_1=(1\ 4\ 6)(2\ 5\ 3)$
- $T_2=(1\ 2\ 6\ 3\ 4\ 5)$
- $T_3=(1\ 3\ 6\ 5\ 4\ 2)$

- $T_1^2=T_2^{2=}T_3^2=T$

- T=(1 3 4 2)
- 经过枚举，不存在一个 T_1 满足 $T_1^2=T$

- T=(1 3 4 2)(5 7 6 8)
- T_1=(1 5 3 7 4 6 2 8) ，满足 $T_1^2=T$

- 如果 gcd(n,k)>1 ，那么开方时就必须找 k’ 个长度皆为 n 的循环合并（k’ 是 gcd(n,k) 的倍数，同时是 k 的因数）；否则，不能进行开方运算

- 可行解生成的算法：
  - 将置换分解成循环
  - 对于每个可以不合并的循环，进行整幂运算的逆运算
  - 对于必须合并的循环，每次选择 gcd(n,k) 个合并
  - 将所得到的循环化为置换

- 多解的产生
  1. 合并与不合并之间
  2. 选择几个循环合并
  3. 选择哪几个循环合并
  4. 合并时的“圆组合”

- $T=(1\ 6\ 4)(2\ 3\ 5)$

  $(1\ 6\ 4)(3\ 5\ 2)$
- $T_1=(1\ 4\ 6)(2\ 5\ 3)$
- $T_2=(1\ 2\ 6\ 3\ 4\ 5)$
- $T_3=(1\ 3\ 6\ 5\ 4\ 2)$

- $T_1^2=T_2^{2=}T_3^2=T$

- 多解的产生
  1. 合并与不合并之间
  2. 选择几个循环合并
  3. 选择哪几个循环合并
  4. 合并时的“圆组合”

例题

- 单个循环，长度奇数
- 指数是 2 的幂次

总结

- 置换群的幂运算这一问题是从最后一个例子洗牌机想到的，这一切都是对问题的深入研究带来的结果；分裂是自然而然的，而合并却是我们自己捏出来的，这一切又都是思想逆转所造成的结果；通过分裂和合并，置换群的幂运算被完美地解决了，这一切又都是多举例子多作猜想而得到的结果。
- 每当发现问题，探寻问题，解决问题的时候，我们就会找到进步的道路。而完成这一切时，我们就进步了。

谢谢大家

- 排列矩阵 (Permutation Matrix)
  - 每行每列有且仅有一个元素值非零
  - 此值为 1
  - 稀疏矩阵可以被表示为少量排列矩阵的和

- $O(n^3 \log k) \Rightarrow O(n+k)$

  $O(nm+km)$