浅谈群论在信息学竞赛中的简单应用

宁波市镇海中学 虞皓翔

摘 要

本文介绍了有关群论中 Polya 定理，群的判定和表示以及 Schreier-Sims 等算法，以及它们在 OI 中的应用，并对计算群论及其算法进行了初步的研究。

引 言

群论是抽象代数中研究群的理论。群在抽象代数中具有重要的地位。群的概念在数学的许多分支中都有出现，而且群论的研究方法对抽象代数的其他分支也有重要影响。

1 置换

1.1 定义

1.1.1 置换

定义 1.1.1 (置换)**.** 一个置换可以看成一个一一映射 (双射) $g : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$，满足 $g(i) = p_i$。

为了强调置换是一种变换/映射，我们通常使用 $2 \times n$ 的矩阵来表示一个置换：

$$g = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$$

通常，我们将 n 称为该置换的**大小**或**长度**，大小为 n 的置换又称为 n 元置换。

1.1.2 逆序数和奇偶性

定义 1.1.2 (逆序数和奇偶性)**.** 对于一个 n 元置换 g，如果 $i, j \in \{1, 2, \cdots, n\}$ 满足 $i < j$ 且 $g(i) > g(j)$，则称 (i, j) 是一个**逆序对**。

一个置换 g 中所有逆序对的总数叫做这个排列的**逆序数**，记作 $N(g)$。

若一个置换的逆序数为奇数，则称它为**奇置换**，否则称它为**偶置换**。

一个置换 g 的符号定义为 $\operatorname{sgn}(g) = (-1)^{N(g)}$，即奇置换的符号为 -1，偶置换的符号为 1。

1.1.3 置换的合成和逆

定义 1.1.3 (置换的合成)**.** 设 $f=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}, g=\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}$。则它们的**合成**就是按照先 f 后 g 的顺序做两次变换，记作 $g\circ f$，简写为 gf。具体地，就是将 f 的下行和 g 的上行对应，则新的置换就是以 f 的上行为上行，以 g 的下行为下行。

用公式表达就是，$(g\circ f)(k)=g(f(k))=j_{i_k}$。

定义 1.1.4 (逆置换)**.** 对于置换 $g=\begin{pmatrix}1 & 2 & \cdots & n\\ p_1 & p_2 & \cdots & p_n\end{pmatrix}$，定义它的逆 $g^{-1}=\begin{pmatrix}p_1 & p_2 & \cdots & p_n\\ 1 & 2 & \cdots & n\end{pmatrix}$。即 g^{-1} 满足 $g^{-1}(g(i))=i$。

1.2 置换的循环表示

1.2.1 循环

定义 1.2.1 (循环)**.** 对 L 个元素的一个排列 $a_1,a_2,\cdots,a_L$，如果置换 g 满足 $g(a_1)=a_2, g(a_2)=a_3,\cdots,g(a_{L-1})=a_L, g(a_L)=a_1$，则称置换 g 为一个**循环** (或轮换)[1]，简记为 $(a_1\ a_2\ a_3\cdots a_{L-1}\ a_L)$，$L$ 称为该循环的**长度**。

1.2.2 循环分解和循环表示

定义 1.2.2 (循环表示)**.** 对 n 元置换 g，称下式为 g 的循环表示：

$$g=(a_{11}a_{12}\cdots a_{1L_1})(a_{21}a_{22}\cdots a_{2L_2})\cdots\left(a_{y1}a_{y2}\cdots a_{yL_y}\right)$$

其中 $g\left(a_{ij}\right)=a_{i,j+1}, g(a_{iL_i})=a_{i1}, L_1+L_2+\cdots+L_y=n\ (1\le j<L_i)$，且所有 a_{ij} 互不相同。

在上式中，把 $(a_{i1}a_{i2}\cdots a_{iL_i})$ 为一个**循环**，L_i 为该循环的**长度**，y 为置换 g 的循环表示中的**循环数**，记作 $\#(g)$，在上下文已知的情况下可记为 $\#$。

如果有一个循环的**长度**为 1，则可以省略不写。

设 $g=(a_{11}a_{12}\cdots a_{1L_1})(a_{21}a_{22}\cdots a_{2L_2})\cdots\left(a_{y1}a_{y2}\cdots a_{yL_y}\right)$，则 g 等于组成它的所有循环的合成。

1.3 置换的循环指标

刻画置换性质的另一大工具是循环指标[2]。它在置换中的地位就像组合数学的生成函数一样。

循环指标是这样一个东西，它关注的是置换的骨架结构——即各个循环的长度。

[1] Cycle
[2] Cycle index

1.3.1 循环指标

定义 1.3.1 (循环指标)**.** *对 n 元置换 g，设 g 的循环表示为*

$$g = (a_{11}a_{12}\cdots a_{1L_1})(a_{21}a_{22}\cdots a_{2L_2})\cdots\left(a_{y1}a_{y2}\cdots a_{yL_y}\right)$$

*设这些循环中有 $\#_i$ 个循环大小为 i，则定义 g 的**循环指标**为 $t_1^{\#_1}t_2^{\#_2}\cdots t_n^{\#_n}$，其中 t_i 为形式变元，就像生成函数中的 x 一样。*

它也有另一种理解方式：对于 g 的每一个循环 c_i，设它的长度为 L_i。则它会对“循环指标”贡献 t_{L_i}，最后将每个循环对“循环指标”的贡献相乘，即得最终的循环指标。

如：置换 $(1\ 4\ 2\ 5\ 3)$ 的循环指标为 t_5；而置换 $(1\ 4)(2\ 5)(3\ 6\ 7)$ 的循环指标为 $t_2^2t_3$。

2 群

2.1 定义

2.1.1 群

定义 2.1.1 (群)**.** *若一个非空集合 G 和其上的二元运算 $\circ$ 满足以下四个条件，则称二元组 $(G,\circ)$ 构成**群**，或称 G 在 $\circ$ 下构成**群**。在不混淆的情况下，也可称 G 是群。*

1. *(封闭性) $\forall f,g\in G, f\circ g\in G$。*
2. *(结合律) $\forall f,g,h\in G,(f\circ g)\circ h = f\circ(g\circ h)$。*
3. *(单位元存在性) $\exists g\in G$，使得 $\forall g\in G, e\circ g = g\circ e = g$。*
4. *(逆存在性) $\forall f\in G,\exists g\in G$，使得 $f\circ g = g\circ f = e$。*

其中 e 叫做 g 的单位元 (幺元)，对满足 $f\circ g = g\circ f = e$ 的 g，称为 f 的逆元，记作 f^{-1}。

需要注意的是，群的定义中**并没有说明**群中元素的运算需要满足交换律。因为事实上，在这类问题中，结合律显得比交换律更基本些，更重要些。一个经典的例子是满足结合律的代数系统中可以定义幂 (Power)，而只满足交换律不满足结合律的代数系统中无法定义幂。

定义 2.1.2 (交换群)**.** *当群 G 的运算满足交换律时，我们称 G 是一个交换群或阿贝尔群[3]。*

[3] Abelian group

2.1.2 一些特殊的群

1. 整数集合 $\mathbb{Z}$ 关于加法 $+$ 构成群 $(\mathbb{Z}, +)$。
2. 对于任何正整数 m，在模 m 的意义下的加法也构成群。称为 m **阶循环群** (Cyclic group)，记作 Z_m。
3. 所有 $n!$ 个 n 元置换构成一个群，这个群被称为 n **元对称群** (Symmetric group)，记作 S_n。
4. 所有 $\left\lceil \frac{n!}{2} \right\rceil$ 个偶置换也构成一个群，这个群被称为 n **元交错群** (Alternating group)，记作 A_n。
5. 对于一个正 n 边形，它的**旋转群**和 Z_n 是同构，故没必要取一个新的名称；而它的**旋转/翻转群**共有 $2n$ 个元素，被称为 $2n$ **阶二面体群** (Dihedral group)，记作 D_{2n}。

2.1.3 阶和子群

定义 2.1.3 (阶)**.** *群 G 的元素个数称为 G 的阶，简记为 $|G|$。*

*若 G 有无穷多个元素，称 G 为**无限群**，若 G 的元素个数有限，则称 G 是**有限群**。*

定义 2.1.4 (子群)**.** *设 $(G, \circ)$ 是群，若 G 的子集 H 对于**同一种运算** $\circ$ 也构成群，则称 $(H, \circ)$ 是 $(G, \circ)$ 的子群。记作 $(H, \circ) \leq (G, \circ)$。*

注意这里强调的是同一种运算，H 不能另辟一个新的运算。

2.1.4 生成子群

定义 2.1.5 (生成子群)**.** *设 $(G, \circ)$ 是群，S 为 G 的一个非空**子集**，则称包含 S 的所有子群的交称为 S 在 G 中生成的子群，记作 $\langle S \rangle$。*

在这里，$\langle S \rangle$ 可以看作是 S 在 $\circ$ 运算下的闭包。如果 $\langle S \rangle = G$，则称 S 是 G 的一组生成集。

定义 2.1.6 (一个元素的阶)**.** *对于一个元素，我们同样可以定义它的阶——对于元素 $g \in G$，如果存在 $n \in \mathbb{N}^*$，使得 $g^n = e$，则称满足 $g^n = e$ 的最小者为它的阶，记作 $|g| = n$。*

*若这样的 n 不存在，则称它是**无限阶的**。*

对于有限群，由抽屉原理和群的逆元素存在性可知，任何一个元素的阶都是有限的。

由阶的定义和生成子群的定义，容易验证：

对于任何群 G 和任何元素 $a \in G$，有 $|\langle a \rangle| = |a|$。即 a 在 G 中生成的子群大小等于 a 的阶数。

2.1.5 陪集，Lagrange 定理

定义 2.1.7 (陪集)**.** *对于群 G 和它的子群 $H \leq G$，对于一个元素 $g \in G$，记集合 $gH = \{g \circ h | h \in H\}$ 为 H 在 G 中导出的一个左陪集，同理可以定义右陪集。*

容易证明，对于确定的子群 H，它导出的所有陪集大小都是相等的，就等于 $|H|$。

陪集有一个比较好的性质：

定理 2.1.1. *对于子群 $H \leq G$，它导出的任意两个陪集，要么完全相同，要么交集为空。*

事实上，若存在 $a, b \in G$ 与 $h_1, h_2 \in H$ 满足 $a \circ h_1 = b \circ h_2$，则 $a = b \circ \left(h_2 \circ h_1^{-1}\right) \in bH$，即 $a \in bH \Rightarrow aH \subseteq bH$，同理 $bH \subseteq aH$，因此有 $aH = bH$。

从而，可以直接导出 Lagrange 定理：

定理 2.1.2 (Lagrange)**.** *对于有限群 G 及其子群 $H \leq G$，有 $|G| = |H| \cdot [G : H]$，其中 $[G : H]$ 表示 H 可以导出的陪集个数。*

2.2 置换群、Burnside 引理和 Pólya 计数定理

置换群是 OI 中最常见的一类群了，本节将介绍与置换群相关的基础理论以及 Pólya 计数定理。

定义 2.2.1 (置换群)**.** *由大小相同的置换作为元素构成的群称为置换群。如果置换的大小为 n，则称对应的群是一个 n 元置换群。*

2.2.1 染色

接下来引入群论中的一个重要概念——染色。

为了方便，以下我们约定问题均在 n 元的情况下。即置换群中的置换大小均为 n。

定义 2.2.2 (染色)**.** *一个 n 元染色，指的是对集合 $\{1, 2, \cdots, n\}$ 的每个元素分配一个物品 (可以是颜色、数，等等) 的分配方案。*

通常，用 $\mathbf{c}$ 表示一个染色，$\mathbf{c}[i]$ 表示该染色中 i 位置的物品。记所有染色的集合为 C。

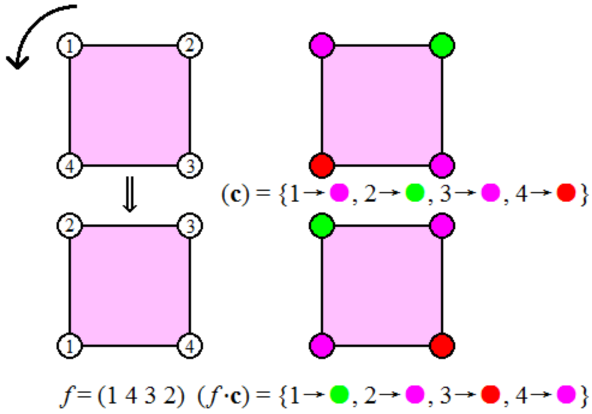
2.2.2 置换的作用

置换是可以**作用**于染色，得到其它的染色的。

定义 2.2.3 (作用)**.** *对于置换 $f \in S_n$ 和染色 $\mathbf{c} \in C$，定义满足 $f(i)$ 的颜色是 $\mathbf{c}[i]$ 的染色 $\mathbf{c}'$，为 f **作用**于 $\mathbf{c}$ 的结果，记为 $f \cdot \mathbf{c}$，简记为 $f\,\mathbf{c}$。*

即 $(f \cdot \mathbf{c})[i] = \mathbf{c}\left[f^{-1}(i)\right]$。

下面是一个具体的例子：



2.2.3 作用的性质，广义染色

不难验证，置换对染色的作用满足如下两个性质：

1. $e \cdot \mathbf{c} = \mathbf{c}$。

2. $(f \circ g) \cdot \mathbf{c} = f \cdot (g \cdot \mathbf{c})$。

而且，关于之后的所有结论和证明，也只需要用到这两个性质。因此，可以通过这两个性质，定义出抽象的染色概念：

定义 2.2.4 (广义染色). *对于群 G (无须是置换群) 和一个全集 C，对于 G 中任意一个元素和 C 中任意一个元素 $\mathbf{c}$，定义运算 $\cdot$ 满足 $g \cdot \mathbf{c} \in C$，且满足如下两个性质：*

1. $e \cdot \mathbf{c} = \mathbf{c}$。

2. $(f \circ g) \cdot \mathbf{c} = f \cdot (g \cdot \mathbf{c})$。

*则称 C 是广义染色集合，C 中的元素 $\mathbf{c}$ 是**广义染色**。*

2.2.4 轨道和稳定子群

定义 2.2.5 (轨道). *对于一个置换群 G 和一个染色 $\mathbf{c}$，对于群中的所有元素，我们都对 $\mathbf{c}$ “作用”一下，可以得到一个 C 的子集，记作 $G \cdot \mathbf{c}$，即*

$$G \cdot \mathbf{c} = \{g \cdot \mathbf{c} | g \in G\}$$

*这个集合 $G \cdot \mathbf{c}$，被称作 $\mathbf{c}$ 在 G 中的**轨道**。*

和轨道相对立的一个概念，称为**稳定子群**，它的定义如下：

定义 2.2.6 (稳定子群)**.** *对于一个置换群 G 和一个染色 $\mathbf{c}$，群中满足 $g \cdot \mathbf{c} = \mathbf{c}$ 的置换 g 构成一个群，称为染色 $\mathbf{c}$ 的稳定子群，记为 $G_{\mathbf{c}}$。*

此外，对一个染色集合 $X \subseteq C$，定义 $G \cdot X = \{g \cdot \mathbf{c} | g \in G, \mathbf{c} \in X\}$。若 $G \cdot X = X$，则称 X 在 G 下**固定**。

2.2.5 轨道——稳定子群定理

有了这样的两个概念后，就可以得到群作用中奠基的定理：轨道——稳定子群定理。

定理 2.2.1 (轨道——稳定子群定理)**.** *对于置换群 G 和染色 $\mathbf{c}$，有 $|G \cdot \mathbf{c}| \cdot |G_{\mathbf{c}}| = |G|$。*

证明. *考虑置换群 G 以及对应的染色 $\mathbf{c}$，由定义，$G_{\mathbf{c}}$ 是一个子群.*

任取 $g \in G$，对于左陪集 $gG_{\mathbf{c}} = \{g \circ h | h \in G_{\mathbf{c}}\}$ 中的元素 $f = g \circ h_0$，有 $f \cdot \mathbf{c} = (g \circ h_0) \cdot \mathbf{c} = g \cdot (h_0 \cdot \mathbf{c}) = g \cdot \mathbf{c}$，因此左陪集 $gG_{\mathbf{c}}$ 中的所有置换作用于 $\mathbf{c}$ 产生相同的染色。

另一方面，对于两个不同的左陪集 $g_1G_{\mathbf{c}}, g_2G_{\mathbf{c}}$，它们作用于 $\mathbf{c}$ 不能产生相同的染色。否则 $g_1 \cdot \mathbf{c} = g_2 \cdot \mathbf{c}$，有 $\left(g_1^{-1} \circ g_2\right) \cdot \mathbf{c} = g_1^{-1} \cdot (g_2 \cdot \mathbf{c}) = g_1^{-1} \cdot (g_1 \cdot \mathbf{c}) = \mathbf{c}$，从而由定义，$g_1^{-1} \circ g_2 \in G_{\mathbf{c}}$，于是 $g_2 \in g_1G_{\mathbf{c}}$，矛盾。

所以，设子群 $G_{\mathbf{c}}$ 导出的陪集数量为 K，每个陪集作用于 $\mathbf{c}$ 可以得到一个独一无二的染色，因此 K 就等于整个置换群中所有元素作用于 $\mathbf{c}$ 所得到的染色数量，即 $|G \cdot \mathbf{c}|$。

由 Lagrange 定理，$|G| = |G_{\mathbf{c}}| \cdot [G : G_{\mathbf{c}}] = |G \cdot \mathbf{c}| \cdot |G_{\mathbf{c}}|$。

2.2.6 Burnside 引理

轨道——稳定子群定理的一个直接推论就是 **Burnside 引理**。

为了方便阐述这个定理，首先需要一些定义：

定义 2.2.7 (置换的不动点)**.** *对于一个置换 g 和一个染色集合 $X \subseteq C$，X 中满足 $g \cdot \mathbf{c} = \mathbf{c}$ 的染色 $\mathbf{c}$ 的集合记为 X^g。*

定义 2.2.8 (染色的等价)**.** *对于置换群 G 和两个染色 $\mathbf{c}_1, \mathbf{c}_2$，称两个染色**等价** (或**本质相同**) 当且仅当 $\exists g \in G$，使得 $g \cdot \mathbf{c}_1 = \mathbf{c}_2$，记作 $\mathbf{c}_1 \sim \mathbf{c}_2$。*

不难证明，两个染色 c_1, c_2 等价，当且仅当下列条件之一成立：

1. $\mathbf{c}_2 \sim \mathbf{c}_1$。
2. $\exists g \in G$，使得 $g \cdot \mathbf{c}_1 = \mathbf{c}_2$。
3. $\mathbf{c}_2$ 在“$\mathbf{c}_1$ 在 G 中的轨道”中。
4. $\mathbf{c}_1$ 在 G 中的轨道与 $\mathbf{c}_2$ 在 G 中的轨道相同。

这说明我们可以将 X 中不等价的染色数量看成 X 中元素在 G 中形成的不同轨道数目。我们用 X/G 表示 X 中元素形成的互异轨道的集合，$|X/G|$ 表示不同轨道数目。则有：

定理 2.2.2 (Burnside)**.** 对于置换群 G 和它固定的染色集合 X，有

$$|G|\,|X/G| = \sum_{g\in G} |X^g|$$

即在 G 的作用下，X 中元素形成的不同轨道数目，等于 G 中所有置换的不动点个数的平均值。

证明. 考虑计算集合 $\{(g,\mathbf{c})|g\cdot\mathbf{c}=\mathbf{c}, g\in G, \mathbf{c}\in X\}$ 的大小。

一方面，我们枚举每个置换，它就等于每个置换的不动点个数的和，即 $\sum_{g\in G}|X^g|$。

另一方面，枚举每个染色，它就等于该染色的稳定子群大小 $\sum_{\mathbf{c}\in X}|G_{\mathbf{c}}|$。

由轨道——稳定子群定理，

$$\sum_{\mathbf{c}\in X}|G_{\mathbf{c}}| = \sum_{\mathbf{c}\in X}\frac{|G|}{|G\cdot\mathbf{c}|} = |G|\cdot\sum_{\mathbf{c}\in X}\frac{1}{|G\cdot\mathbf{c}|}$$

对于等式右端，考虑每一个完整的轨道 $G\cdot\mathbf{c}$，其中每个染色都会产生 $\dfrac{1}{|G\cdot\mathbf{c}|}$ 的贡献，因此每个轨道恰对右端的和式贡献 1，于是 $\sum\limits_{\mathbf{c}\in X}\dfrac{1}{|G\cdot\mathbf{c}|}=|X/G|$，*Burnside* 引理成立。

2.2.7 Pólya 计数定理——简单版

注意到我们在推导 Burnside 引理的整个过程中，对于置换的“作用”，都只用到了两个性质 (单位性和结合性)，因此 Burnside 引理其实是对一般的群和广义染色成立的。

而当我们限制群为**置换群**，染色为**一般的染色**时，那么或许可以到更进一步的结果。

在 Burnside 引理中，考虑置换 $g\in G$。我们要计数在置换 g 下，X 中使得在 g 作用下不变的染色数量。

由之前置换的理论，设 g 的循环表示是 $g = c_1\circ c_2\circ\cdots\circ c_y$，则考虑一个循环 $c = (a_1\ a_2\cdots)$，将这个循环作用于染色 $\mathbf{c}$，由定义，有 $\mathbf{c}[a_i]=\mathbf{c}[a_{i+1}]$。因此，我们可以得到：

引理 2.2.1. 对于置换 g 和染色 $\mathbf{c}$，设 g 的循环表示是 $g=c_1\circ c_2\circ\cdots\circ c_y$，则 $g\cdot\mathbf{c}=\mathbf{c}$ 的充要条件是：对于 g 的每个循环 $(a_1\ a_2\cdots)$，$\mathbf{c}$ 中对 $a_1,a_2,\cdots$ 分配的颜色是相同的。

于是，假设颜色一共有 m 种，且每个位置可分配的颜色集合都是相同的，那么，如果 g 有 $\#(g)$ 个循环，那么，在 g 的作用下不变的染色数量就应该是 $m^{\#(g)}$，从而可以得到

定理 2.2.3 (Pólya)**.** 对于置换群 G 和它固定的染色集合 X，如果这 n 个位置可分配的颜色集合都是相同的，一共 m 种，那么对于 $g\in G$，有

$$|X^g| = m^{\#(g)}$$

从而代入 *Burnside* 引理，有

$$|G||X/G| = \sum_{g\in G} m^{\#(g)}$$

其中 n 为置换的大小，$\#(g)$ 表示置换 g 的**循环数**。

2.3 Pólya 定理的完整版及其扩展

在上文我们定义了一个置换的循环指标，它可以较为方便地描述**生成函数版的 Pólya 定理**。

定义 2.3.1 (置换群的循环指标)**.** 定义一个置换群 G 的循环指标，为**群中所有置换的循环指标的平均值**，记作 $Z_G(t_1, t_2, \cdots, t_n)$。

定理 2.3.1 (Pólya)**.** 假设普通生成函数 $f(t) = f_0 + f_1 t + f_2 t^2 + \cdots$，其中 f_w 为权值为 w 的**颜色**数量。

定义一个染色的权值为 n 个位置所分配的颜色的权值之和。

用生成函数 $F(t)$ 表示在 G 的作用下不同轨道数的普通生成函数，则 *Pólya* 定理表明：

将 $t_i = f\left(t^i\right)$ 代入 G 的循环指标中，所得到的结果就是 $F(t)$，即：

$$F(t) = Z_G\left(f(t), f\left(t^2\right), \cdots, f(t^n)\right)$$

此定理可以推广到多元生成函数的情形中。特别地，当 $f(t)$ 为常数时该定理就是之前所述的简单版 *Pólya* 定理。

2.3.1 广义 Burnside 引理/Pólya 定理

接下来考虑对一般的 Burnside 引理进行推广。

在一般的 Burnside 引理中，我们是对下式进行算两次：

$$\sum_{g\in G}\sum_{\mathbf{c}\in X}[g\cdot\mathbf{c} = \mathbf{c}]$$

现在考虑对每个置换 g 赋予一个权值 $\omega(g)$，那么，对于一个子群 $H \le G$，定义它的权值 $\omega(H) = \sum\limits_{g\in H}\omega(g)$，然后对

$$\sum_{g\in G}\sum_{\mathbf{c}\in X}[g\cdot\mathbf{c} = \mathbf{c}]\,\omega(g)$$

算两次，可以得到：

定理 2.3.2 (广义 Burnside 引理)**.** 对于置换群 G 和它固定的染色集合 X，记群中的置换 g 的权值为 $\omega(g)$，子群 H 的权值为 $\omega(H)$，则：

$$\sum_{O\in X/G} \omega(G_O)|O| = \sum_{g\in G} \omega(g)|X^g|$$

即在 G 的作用下，X 中元素形成的所有轨道的大小与对应稳定子群的权值的乘积之和，等于 G 中所有置换的不动点个数与对应置换权值乘积之和。

同理，当 $\omega(g)$ 仅和置换的循环指标相关时，就能导出广义 Pólya 定理。

广义 Burnside 定理一般有两个用途：其一是通过合理给置换赋权，来解决带权轨道的计数问题，其二是推出接下来所要介绍的 **Pólya 容斥**。

2.3.2 Pólya 容斥

特别地，在广义 Burnside 定理的式子中，取 $\omega(g) = \mathrm{sgn}(g)$ (即符号，奇置换为 -1，偶置换为 1)。

考虑染色集合在 S_n 的作用下形成的不同轨道，可知一种染色 $\mathbf{c}$ 的稳定子群 $G_{\mathbf{c}}$ 同构于若干个对称群的直积。

而这些小的对称群中，一旦有 ≥ 2 元的对称群，那么其中所有置换的符号之和等于 0，从而稳定子群 $G_{\mathbf{c}}$ 的权值 $\omega(G_{\mathbf{c}}) = 0$。

也就是说，最终一个轨道的权值非零，当且仅当它的稳定子群是平凡群，也就是说 n 个位置的“颜色”互不相同，这就是 Pólya 容斥。

推论 2.3.1 (Pólya 容斥)**.** *对于置换群 $G = S_n$ 和它固定的染色集合 X，有*

$$|G| \sum_{O\in X/G} \left[O \text{ 是颜色互异的轨道} \right] = \sum_{g\in G} \mathrm{sgn}(g)|X^g|$$

即在 G 的作用下，X 中元素形成的各颜色互不相同的轨道数，等于 G 中所有置换的不动点个数乘以其符号的平均值。

2.4 例题

例题 1. 树 [4]

定义 n 阶带标号有根树的集合 $\mathcal{T}$，满足以 1 为根，i 的父节点标号 p_i 满足 $1 \leq p_i < i$。易知 $|\mathcal{T}| = (n-1)!$。

现在按顺序等概率随机取 k 个 $\mathcal{T}$ 中的元素 $T_1, T_2, \cdots, T_k$ (可以相同)，求 $T_1, T_2, \cdots, T_k$ (作为有根树) 两两同构的概率。

$n \leq 2000; k \leq 10^9$，对大素数取模。

[4] 来源：ZJOI2018，有改动

先转化题意，显然两棵树同构是一个等价关系，因此我们可以将 $\mathcal{T}$ 划分为若干个等价类 $\mathcal{T} = E_1 \cup E_2 \cup \cdots \cup E_\lambda$，于是我们就要求 $\sum\limits_{i=1}^{\lambda} |E_i|^k$。

考虑 DP ——记 f_i 表示 i 个点时的答案，那么它也就等于将其去掉后森林的答案，因此转而考虑有根森林的等价类。森林中树的大小参差不齐，故按照大小为 $1, 2, \cdots, n$ 的顺序依次在森林中加入对应大小的树。记 $g_{i,s}$ 表示所有树大小不超过 i 的大小为 s 的森林所对应的答案 (各等价类大小的 k 次方和)，则有 $f_i = g_{i-1,i-1}, g_{1,s} = 1$。考虑转移，那么就是在森林中加入若干个大小为 i 的树。枚举加入了 d 个，那么有

$$g_{i,s} = \sum_{0 \le d \le \lfloor \frac{s}{i} \rfloor} g_{i-1,s-d\cdot i} \cdot I_{i,d} \cdot \binom{s}{d \cdot i}^k$$

其中 $I_{i,d}$ 表示对于所有 d 棵大小为 i 的树构成的带标号有根森林，各等价类大小的 k 次方和。

下面考虑求解 $I_{i,d}$，我们换一个字母，用 $I_{n,m}$ 表示，即 m 棵大小为 n 的树。

首先，对于带标号的问题，外面的标号已经由一个二项式系数解决，实际 DP 时可以统统除以阶乘然后直接乘，因此里面的标号设为 $1 \sim n$ 也无妨。因此，在一般情况下，这个标号分配方案就等于 $\binom{m \cdot n}{n, n, \cdots, n}$，但是这里不行，因为同构的两棵树之间换一下标号，得到的还是同一棵树。

考虑一个 m 维的，元素为 n 阶树等价类的向量的全集 X，两个向量“本质相同”当且仅当 n 阶树构成的等价类集合相同。设 n 阶树的等价类划分为 $\mathcal{T}_n = E_1 \cup E_2 \cup \cdots \cup E_\lambda$，然后记 $P_n(\delta) = \sum\limits_{i=1}^{\lambda} |E_i|^\delta$。那么，可以发现 X 中每个元素其实就是一个**染色** ——对于每个位置分配一个 E_i。于是问题就转化为了等价类计数的问题，考虑使用 Pólya 定理来处理。

使用多元生成函数的 Pólya 定理，定义 $f(t_1, t_2, \cdots, t_\lambda) = t_1^k + t_2^k + \cdots + t_\lambda^k$。则最后我们要求的即为 $F(|E_1|, |E_2|, \cdots, |E_\lambda|)$。在 X 上作用的变换群显然是 S_m，因此我们将其代入 S_m 的循环指标，就得到一个关于 $f(|E_1|, |E_2|, \cdots, |E_\lambda|), f\left(|E_1|^2, |E_2|^2, \cdots, |E_\lambda|^2\right), \cdots,$ $f(|E_1|^m, |E_2|^m, \cdots, |E_\lambda|^m)$，亦即 $P_n(k), P_n(2k), \cdots, P_n(mk)$ 的表达式。

假设我们已经知道了这些 $P_n(ik)$，那么考虑 Pólya 定理，其实质就是对于一个大小为 c 的循环给出 $P_n(ck)$ 的贡献。而熟知置换可以由循环之间的**带标号无序组**来刻画，也就是多项式 exp。

但是这里有个致命的问题——每个轨道的贡献不一定是 1：具体地，考虑一个轨道 (“本质相同”的向量组)，设其中包含了 κ_i 个 E_i 中的元素，那么在**最终分配标号**的时候，这些树它们之间的标号是可以任意互换的，因此最后还需要除以 $\kappa_i!$。

也就是说，对于一个轨道，它会产生 $\prod\limits_{i=1}^{\lambda} \dfrac{1}{(\kappa_i!)^k}$ 倍的贡献。

可以发现这里我们需要统计带权轨道的权值和，因此我们需要使用**广义 Pólya 定理**：

$$\sum_{O \in X/G} \omega(G_O)|O| = \sum_{g \in G} \omega(g)|X^g|$$

我们希望对于满足 $(\kappa_1, \kappa_2, \cdots, \kappa_\lambda)$ 的轨道 O，有 $\omega(G_O)|O| = \prod\limits_{i=1}^{\lambda} \dfrac{1}{(\kappa_i!)^k}$。

考察 G_O 的结构，可得 $G_O = S_{\kappa_1} \times S_{\kappa_2} \times \cdots \times S_{\kappa_\lambda}$。

注意到在 Pólya 定理中，一个置换的权值仅仅和它的循环指标相关，以及两个群的直积的循环指标等于两个群的循环指标的乘积 (卷积)。因此有 $Z_{G_O} = Z_{S_{\kappa_1}} \cdot Z_{S_{\kappa_2}} \cdot \cdots \cdot Z_{S_{\kappa_\lambda}}$，从而有 $\omega(G_O) = \omega(S_{\kappa_1})\,\omega(S_{\kappa_2})\cdots\omega(S_{\kappa_\lambda})$。

结合轨道——稳定子群定理，得 $|O| = \dfrac{|G|}{|G_O|} = \dfrac{m!}{\kappa_1!\kappa_2!\cdots\kappa_\lambda!}$，而 $m!$ 可以看成常数，因此对比前式可知要

$$\omega(G_O) = \prod_{i=1}^{\lambda} \frac{1}{(\kappa_i!)^{k-1}} \Rightarrow \omega(S_\kappa) = \frac{1}{(\kappa!)^{k-1}}$$

而现在我们需要知道每个循环大小所产生的贡献，记大小为 c 的循环产生的贡献为 χ_c，于是通过对称群 S_κ 的权值我们可以通过 $\chi_1, \chi_2, \cdots$ 来推导出 χ_κ。其实，这里的置换还是可以由循环之间的带标号无序组来刻画，因此之前的多项式 exp 仍是可行的。

设 $f(x) = \sum_{i\ge1} \chi_i \dfrac{x^i}{i!}$，则 $\exp f(x) = 1 + \sum_{i\ge1} \omega(S_i)\dfrac{x^i}{i!} = \sum_{i\ge0} \dfrac{x^i}{(i!)^k}$，于是做一次多项式 ln 就能得到诸 χ_i 了。

当然，这里还剩最后一个问题：当时是假设已经知道 $P_n(k), P_n(2k), \cdots, P_n(mk)$，但事实上除了 $P_n(k)$，其余的值都是不知道的。这说明我们不仅仅要 DP 所有等价类的 k 次方和，还有 $2k$ 次方和，$3k$ 次方和……

不过注意到 $d \cdot i \le n$，也就是说，对于 i 阶树的等价类，我们只需要知道其 k 次方和，$2k$ 次方和，……，$\left\lfloor \dfrac{n}{i} \right\rfloor \cdot k$ 次方和，这是一个调和级数。于是我们对多组 $(i, d\cdot k)$ $(i \cdot d \le n)$ 分别计算即可，考虑平方实现的 exp/ln，则这部分的时间复杂度为

$$\sum_{i\cdot d\le n} \left(\frac{n}{i\cdot d}\right)^2 = O\left(n^2\right)$$

其余部分转移的时间复杂度为

$$\sum_{i=1}^{n} \sum_{e=1}^{\left\lfloor \frac{n}{i} \right\rfloor} \sum_{s=1}^{\left\lfloor \frac{n}{e} \right\rfloor} \left\lfloor \frac{s}{i} \right\rfloor = O\left(n^2\right)$$

即总时间复杂度 $O\left(n^2\right)$。

3 群的判定和表示

3.1 基础知识

3.1.1 不变子群、商群

定义 3.1.1 (不变子群). 设群 $(G, \circ)$ 的子群 $H \le G$ 满足：对于是 $\forall g \in G, h \in H$，有

$$g \circ h \circ g^{-1} \in H$$

则称 H 是 G 的**不变子群**或**正规子群**，记作 $H \trianglelefteq G$。

若 $H \trianglelefteq G$ 且 $H \neq G$，则记 $H \triangleleft G$ (真不变子群)。

定义 3.1.2 (商群)**.** 对于群 $(G, \circ)$ 和它的不变子群 $N \trianglelefteq G$，在 N 的所有陪集 (左右都一样) G/N 上定义运算 $\cdot$ 满足：

$$(aN) \cdot (bN) = (a \circ b) N$$

则称 $(G/N, \cdot)$ 为 G 对 N 的**商群**。

3.1.2 同态和核

定义 3.1.3 (同态)**.** 设有群 $(G, \circ), (H, \cdot)$，若映射 $f : G \to H$ 满足，对于 $\forall a, b \in G$ 均有

$$f(a \circ b) = f(a) \cdot f(b)$$

则称 f 是 G 到 H 的**同态**映射，简称同态。

根据 f 是否是单射、满射、双射，可以定义同态映射是否是单同态、满同态和同构。

定义 3.1.4 (核)**.** 设 f 是 G 到 H 的同态，e_H 为 H 的单位元，则集合 $f^{-1}(e_H) = \{g | g \in G, f(g) = e_H\}$ 被称为 f 的**核**，记为 $\ker f$。

3.1.3 同构定理

同态和同构有着密切的联系，比如下面的群同态基本定理 (群同构第一定理) 和群同构第三定理：

定理 3.1.1 (群同态基本定理)**.** 设 f 是 $(G, \circ)$ 到 $(H, \cdot)$ 的**满同态**，那么 $G/\ker f$ 和 H 同构。

这是群同态中奠基的一个定理，在同态与熟悉的同构之间搭建了一座桥梁。

证明. 设 $K = \ker f$。定义映射 $\phi : G/K \to H$，满足：

$$\phi(gK) = f(g)$$

首先需要证明这个定义的合理性，即它没有歧义。事实上，设 $g \circ h_1, g \circ h_2 \in gK$，则

$$f(g \circ h_1) = f(g) \cdot f(h_1) = f(g) \cdot f(h_2) = f(g \circ h_2)$$

因此这个定理是合理的。

现在我们欲证明 ϕ 是同构 (双同态)，因此我们就需要分别证明 ϕ 是同态、单射和满射。

- 取 $gK, hK \in G/\ker f$，有

  $$\phi((g \circ h) K) = f(g \circ h) = f(g) \cdot f(h) = \phi(gK) \cdot \phi(hK)$$

  即 ϕ 是同态。

- 若 $\phi(gK) = \phi(hK)$，则 $f(g) = f(h) \Rightarrow$

$$f\left(g \circ h^{-1}\right) = f(g) \cdot f\left(h^{-1}\right) = f(g) \cdot f(h)^{-1} = e_G$$

  即 $g \circ h^{-1} \in K \Rightarrow gK = hK$，即 ϕ 是单射。

- 任取 $h \in H$，由于 f 是满射，故存在 $g \in G$ 使得 $f(g) = h$，于是 $\phi(gK) = f(g) = h$，从而 ϕ 是满射。

综上，ϕ 是双同态，即 G/K 和 H 同构。

下面的群同构第三定理，可以用来简化一些代码的实现，限于篇幅，这里只给出定理，略去证明。

定理 3.1.2 (群同构第三定理)**.** 设 N 是 G 的不变子群，则：

- G 的子群 H 满足 $N \leq H \leq G$，当且仅当 $H/N \leq G/N$。
- G 的子群 H 满足 $N \leq H \trianglelefteq G$，当且仅当 $H/N \trianglelefteq G/N$，如果两者成立，则商群 $\dfrac{G/N}{H/N} \cong G/H$。

3.2 群的判定

3.2.1 根据定义判定群

考虑一个经典的问题，就是给定一张乘法表，如何检验其中的元素是否构成一个群？

尝试通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下约定该代数结构中的运算用 $\circ$ 表示。

- 封闭性。

  直接检验即可。

- 单位元。

  设 e 是单位元，则 $e \circ e = e$。同时，若 g 满足 $g \circ g = g$，则两边同乘 g^{-1} 得 $g = e$。也就是说，e 是满足 $g \circ g = g$ 的唯一元素。

  通过这一点，我们可以得到群的单位元，设为 e (如果不存在或不唯一说明不是群)。接下来根据定义对每个 g 检验是否有 $e \circ g = g \circ e = e$。

- 逆元。

  对于 $\forall g \in G$，我们寻找满足 $g \circ h = h \circ g = e$ 的元素 h，如果不存在或不唯一说明不是群。否则通过检验。

接下来就是最后一步——结合律的检验。

如果直接按照定义检验，我们需要枚举元素 f,g,h，而这样做的时间复杂度是 $O\left(n^3\right)$。

而前面三种性质的检验都可以在输入复杂度 ($O\left(n^2\right)$) 内完成，那结合律的检验是否有更优秀的方法呢？

对于一个一般的代数结构结合律的检验，到笔者写本文时，学术界尚未有复杂度低于 $O\left(n^3\right)$ 的**确定性**算法 (但存在复杂度较为优秀的随机算法)。

不过，如果我们检验的对象是群，则可以利用群的性质，可以得到一个在 $O\left(n^2\log n\right)$ 时间内的算法。

3.2.2 检验结合律的 Light 算法

引理 3.2.1. 对于任意 n 阶有限群 G，存在一个大小不超过 $\lfloor\log_2 n\rfloor$ 的子集 $S\subseteq G$，它生成 G (即 $G=\langle S\rangle$)。[5]

证明. 定义子群链 $\{e\}=G_0\le G_1\le\cdots\le G_k=G$，其中 $G_i=\langle\{g_1,g_2,\cdots,g_i\}\rangle$，具体构造方法如下：

- 设我们已经知道 $G_0,G_1,\cdots,G_{i-1}$，现在要确定 G_i。
- 若 $G_{i-1}=G$，则构造结束。否则，有 $G_{i-1}<G$。
- 任取 $g_i\in G\setminus G_{i-1}$，令 $G_i=\langle G_{i-1}\cup\{g_i\}\rangle$。
- 则 $G_{i-1}\le G_i\le G$ 且 $G_{i-1}\ne G_i$ ($g_i\in G_i\wedge g_i\notin G_{i-1}$)。
- 于是 $|G_i|\ge 2|G_{i-1}|$。
- 因此 $n=|G|=|G_k|\ge 2^k|G_0|=2^k$，即 $k\le\lfloor\log_2 n\rfloor$，证毕。

引理 3.2.2. 设 $(G,\circ)$ 是一个满足封闭性、单位元、逆元的代数结构，设 $G=\langle S\rangle$，则 G 满足结合律当且仅当：

- 对 $\forall s\in S,g,h\in G,(g\circ s)\circ h=g\circ(s\circ h)$。

证明. 必要性显然。下证充分性：

设 $A=\{s|\forall g,h\in G,(g\circ s)\circ h=g\circ(s\circ h)\}$，即所有满足结合律的**中间元素**。

我们证明：若 $a,b\in A$，则 $a\circ b\in A$。

事实上，有

$$\begin{aligned}(g\circ(a\circ b))\circ h&=((g\circ a)\circ b)\circ h=(g\circ a)\circ(b\circ h)\\&=g\circ(a\circ(b\circ h))=g\circ((a\circ b)\circ h)\end{aligned}$$

其中 g,h 为任意元素，四个等号分别运用了 a,b,a,b 作为中间元素的结合律。

故 $a\circ b\in A$。由条件知 $S\subseteq A$，由上述结论并结合生成子群的性质知 $\langle S\rangle\subseteq A$，即 $G\subseteq A\Rightarrow G=A$，即代数结构 G 满足结合律。

[5]下界可以取到，如 $G=Z_2^k$

结合上述两个引理，我们就得到了 Light 算法，流程如下：

1. 按照 Lemma 2.1 所述方法找到大小不超过 $\lfloor \log_2 n \rfloor$ 的集合 S，满足 $G = \langle S \rangle$。[6]
2. 对于 S 中的每个元素 s，检验 s 作为中间元素时是否满足结合律，即是否对于 $\forall g, h \in G$，有 $(g \circ s) \circ h = g \circ (s \circ h)$。

   如果成立，则 G 是群，否则 G 不是群。

分析一下算法的时间复杂度：对于第一步，容易在 $O\left(n^2\right)$ 或 $O\left(n^2 \log n\right)$ 时间内找到一组生成集 S；而对于第二步，检验时间等于 $O\left(n^2 |S|\right) = O\left(n^2 \log n\right)$。

故总时间复杂度为 $O\left(n^2 \log n\right)$。

3.3 群的表示

那么，对于一个一般的群，除了使用乘法表外，还有哪些方法能表示它呢？

在 OI 中比较常见的群就是置换群，因此我们希望用置换群来表示一个一般群。

定义映射 $\lambda_g(x) = g \circ x$，则 λ_g 是一个双射。

考虑两个映射 λ_g, λ_h 的复合，有

$$\lambda_g(\lambda_h(x)) = g \circ (h \circ x) = (g \circ h) \circ x = \lambda_{g \circ h}(x)$$

同理，可以证明 λ_g 和 $\lambda_{g^{-1}}$ 互为逆映射。

而且，变换 λ_g 将 G 中的所有元素变换为了 G 中的所有元素，只是其中的对应关系发生了改变，即 λ_g 实质上可以看成是 G 上的一个**置换**。而置换 $\left\{\lambda_g \middle| g \in G\right\}$ 就构成了一个置换群，即 $|G|$ 元对称群的子群。

于是，我们得到了 **Cayley 定理**：

定理 3.3.1 (Cayley)**.** *每个 n 阶有限群都同构于一个不超过 n 元的置换群 (不超过 n 元的对称群的子群)。*

换句话说，对于 n 阶有限群 G，至少存在一个 G 到 S_n 的**单同态**。

3.4 例题

例题 2. *列队*[7]

给定群 G，求 G 到 n 元对称群 S_n 的单同态个数。

$|G| \le 30; n \le 1000$，对 998244353 取模。

[6]因为我们假设 G 是群，因此这个过程一定可以进行。但是如果 G 不是群，这个过程也可能成功进行。但是这个过程一旦不能成功进行，就能说明 G 已经不是群了，那么后面也没必要再去检验结合律了。

[7]来源：UOJ Round #10，Problem C (uoj154)，有改动

对于群 G, H，记 G 到 H 的**同态**数量为 $\operatorname{homo}(G, H)$ [8]，**单同态**数量为 $\operatorname{mono}(G, H)$ [9]。

考虑一个同态 $f : G \to H$，记 $K = \ker f$，由群同态基本定理知 G/K 和 $\operatorname{im} f$ 之间存在同构 ϕ，那么将同构 ϕ 的陪域扩展到 H 即得 G/K 到 H 的一个**单同态**。也就是说，$G \to H$ 的每一个同态都对应到 G/N 到 H 的一个单同态，其中 N 是 H 的一个不变子群。于是，有

$$\operatorname{homo}(G, H) = \sum_{N \trianglelefteq G} \operatorname{mono}(G/N\ , H)$$

根据上式，我们就可以将计算 $\operatorname{mono}(G, H)$ 的问题通过类似于反应的手段转化为了若干个计算 $\operatorname{homo}(G, H)$ 的子问题。

现在考虑给定群 G，计算它到 S_n 的**同态**个数。

设 f 是 G 到 S_n 的一个同态，设置换群 $H = \operatorname{im} f \le S_n$。定义 i 的特征染色 χ_i 为：i 位置为黑色，其余位置为白色。那么诸轨道 $H \cdot \chi_i$ 中黑色出现的所有位置构成的集合，构成了集合 $\{1, 2, \cdots, n\}$ 的一个划分。

考虑其中一个集合 A ($|A| = k$)，不妨设 $1 \in A$，则 $|H \cdot \chi_1| = k$。由轨道——稳定子群定理，$\left|H_{\chi_1}\right| = \dfrac{|H|}{|H \cdot \chi_1|} = \dfrac{|H|}{k}$。由同态的性质知，稳定子群 H_{χ_1} 的原像是 G 的一个 $\dfrac{|G|}{k}$ 阶子群。

之前讨论的是给定 f 后 G 的结构，接下来尝试从 G 的结构去构造 f。

对于 $\{1, 2, \cdots, n\}$ 的任意一个划分，作为诸元素的轨道。考虑其中一个集合 A ($|A| = k$)，仍然不妨设 $1 \in A$。在 G 中任意寻找一个大小为 $\dfrac{|G|}{k}$ 的子群 S，令它的像为特征染色 χ_1 的稳定子群。那么 S 导出的 k 个左陪集，作用于 χ_1 后将黑色分别移到 $1, 2, \cdots, k$。

记这 k 个左陪集分别为 $S, g_2S, g_3S, \cdots, g_kS$，由于单位元在 S 中，因此陪集 S 中元素的像会将黑色移到 1。对于剩下的 $2 \le i \le n$，合理调整 g_i 的顺序，不妨设陪集 g_iS 中元素的像会将黑色移到 i。

于是，对于这样一种 g_i 的顺序，考虑其中任意一个置换 g，我们有 $(\forall s \in S)$

$$g(j) = g\left(\left(g_j \circ s\right)(1)\right) = \left(g \circ g_j \circ s\right)(1) = \left(g \circ g_j\right)(1)$$

即 $g(j)$ 由 $g \circ g_j$ 唯一确定，和 s 无关，于是这个定义没有歧义 (合理)，因而也就得到一个所有元素在 A 中唯一的变换。但是我们还能调整 g_i 的顺序，这里一共有 $(k-1)!$ 种调整的方式，每种方式都能对应到一个 A_1 上独一无二的变换。综上，对于一个大小为 k 的集合，我们需要一个大小为 $\dfrac{|G|}{k}$ 的子群作为其稳定子群的原像。且对于每个这样的子群，都能得到 $(k-1)!$ 种该等价类中变换的方式。

接下来就可以直接计数了，只需要作出 $\{1, 2, \cdots, n\}$ 的一个划分，然后对划分中的每个集合找到一个对应大小的子群与之对应即可。

由于划分可以看成**带标号无序组**，因此设

$$f(x) = \sum_k \frac{x^k}{k} \sum_{H \le G, |H| = \frac{|G|}{k}} 1 = \sum_{H \le G} \frac{x^{|G|/|H|}}{|G|\ /\ |H|}$$

[8]homomorphism

[9]monomorphism

则 $\operatorname{homo}(G, S_n) = n!\,[x^n] \exp f(x)$。

此外，对于这题的实现，其实是不需要递归的求解的，我们可以通过**群同构第三定理**来简化过程。考虑我们递归解决规模为 G/N 的子问题，我们需要枚举 G/N 的子群和不变子群。由群同构第三定理，G/N 的子群和不变子群对应于 G 的子群和不变子群 (中满足 N 是其子群者)，如果继续递归，所得到的商群 $\dfrac{G/N}{H/N}$ 其实是同构于 G/H 的。因此在整个过程中所涉及到的群，其实都是 G 的商群。

也就是说，我们只需要一次 bfs 得到 G 的所有子群和不变子群，然后按照阶数从大到小的顺序枚举不变子群 N，解决规模为 G/N 的问题。于是扫描到不变子群 N 时，这些商群的子群所对应的答案都是已知的，像 Möbius 反演一样操作即可。

如果使用 $O\left(n^2\right)$ 的多项式 exp，则总时间复杂度为 $O\left(M\,|G|^2 + M_N \cdot M + M_N \cdot n^2\right)$ (M (M_N) 分别表示 30 阶以内的群的 (不变) 子群数量的最大值，其值等于 67，在 Z_2^4 处取到)。

4 计算群论初步

下面介绍的内容是一些计算群论的基础算法。

计算群论是研究某一类问题的利器：对于一些大小不大的置换构成的集合 S，它们可能生成一个很大的置换群 $\langle S \rangle$，而计算群论可以对形如 $\langle S \rangle$ 的置换群维护出一个有很多功能的“群论结构”。其中 Schreier-Sims 算法是计算群论中最基础的算法。

4.1 引入

考虑一个最基本的问题：给定若干个 n 元置换构成的集合 S，求 S 生成的子群大小 $|\langle S \rangle|$，这里 $n \le 50$。

怎么求一个巨大的群的大小呢？一个比较直观的思路是：

如果我们有个子群链 $\langle S \rangle = G_0 \ge G_1 \ge G_2 \ge \cdots \ge G_k = \{e\}$，那么由 Lagrange 定理，有

$$|G| = \prod_{i=0}^{k-1} \frac{|G_i|}{|G_{i+1}|} = \prod_{i=0}^{k-1} [G_i : G_{i+1}]$$

于是我们就尝试去构造这样一个子群链。

根据之前的经验，对于一个置换群 G，对 $\forall 1 \le i \le n$，诸轨道 $G \cdot \chi_i$ 构成了 $\{1, 2, \cdots, n\}$ 的一个划分。

考虑特征染色 χ_1 的稳定子群 G_{χ_1}，由轨道——稳定子群定理，有 $\left[G : G_{\chi_1}\right] = |G \cdot \chi_1|$，而轨道的大小显然不超过 n，因此这个数值是可接受的。

而且，这个稳定子群它**固定了元素** 1，也就是说它可以被嵌入到 $n-1$ 元置换群中，这就是原问题的一个子问题。

如果我们能对其进行递归求解，那就得到了我们所要的子群链了。

这就是 Schreier-Sims 算法的主要思想。

4.2 元素判定和截面

知道了算法的思想后，接下来考虑如何对这样的群进行操作。

由于 G 是置换群，那么可以比较容易知道 $G\cdot\chi_1$ 的大小，以及这些元素的轨道。但是现在我们无法方便地表示 G_{χ_1}。事实上，G_{χ_1} 也是一个庞大的置换群，也只能用生成集来表示。

因此，Schreier 和 Sims 选择了**增量构造法**，即逐渐向 S 中添加元素，然后对子群链中的每个子群进行维护。

初始时，$S=\varnothing$，那么 $G=\{e\}$，这些都是平凡的。

考虑向 S 中添加一个新元素 g。首先，我们需要检验 g 是否已经在 $\langle S\rangle$ 中。

也就是说，我们维护的群论结构需要支持查询一个置换是否在 $\langle S\rangle$ 中。

我们仍然考虑递归求解，那么此时不能显然只存储轨道划分了，我们需要存储一下 G_{χ_1} 导出的陪集的有关信息。

为了统一起见，本文接下来一律使用右陪集。

其实，虽然 G_{χ_1} 很大，但它导出的陪集并不多，我们可以在每个陪集中取一个代表元，构成一个集合。这个集合在计算群论被称为**截面** [10]。

定义 4.2.1 (截面)**.** *对于群 G 和它的子群 $H\le G$，设 H 导出的左陪集集合为 $C_1,C_2,\cdots,C_k$，则**包含单位元的**集合 $R=\{r_1,r_2,\cdots,r_k\}$ (其中 $r_i\in C_i$) 称为 H 的一个左截面，同理可以定义右截面。*

由于现在统一了使用右陪集，因此只需要考虑右截面。

考虑 G_{χ_1} 的一个右截面 $R=\{r_1=e,r_2,r_3,\cdots,r_k\}$，它满足如下性质：

- 由定义知对于 $i\ne j$ 有 $Hr_i\ne Hr_j$，即 $r_i\circ r_j^{-1}\notin H$。
- 考虑陪集 Hr_i，任取其中元素 $h_0\circ r_i$，那么有 $(h_0\circ r_i)^{-1}(1)=\left(r_i^{-1}\circ h_0^{-1}\right)(1)=r_i^{-1}\left(h_0^{-1}(1)\right)=r_i^{-1}(1)$，也就是说，同一个陪集中的置换，具有相同的 1 的**原像**；而不同陪集中的置换则有不相同的原像。
- 那么，对于 $\forall g\in G$，我们根据 g 中 1 的原像 $g^{-1}(1)$ 就可以**唯一确定**它所在的陪集 Hr_i，也就是说，$Hg\cap R$ 包含唯一元素，我们称其为 g 的**标准置换**，记作 $\operatorname{norm} g$。

截面在 Schreier-Sims 算法中扮演着非常重要的角色，在后面的 Schreier 引理中会得到充分体现。

现在先回到元素判定，此时我们要判断 g 是否在 $\langle S\rangle$ 中。

我们希望找到一个 r_i 使得 $(r_i\circ g)(1)=1$，也就是说 $r_i\circ g\in H\Leftrightarrow r_i\in Hg^{-1}$，也就是说求 $\operatorname{norm}\left(g^{-1}\right)$。

[10] Transversal

注意到置换群的特殊性，一个置换的**标准置换**可以比较方便地求出：假设我们要求 $\operatorname{norm} g$，则可以先求出 $g^{-1}(1)$，找到 1 的原像和它相同的 r_i 即可。当然，如果不存在显然可以说明 $g \notin \langle S \rangle$。

找到了对应的 r_i 后，我们就得到了一个固定元素 1 的置换 $r_i \circ g$。那么，易知 $g \in G \Leftrightarrow r_i \circ g \in G_{\chi_1}$，于是我们成功转化为了子问题。

4.3 增量构造的过程

4.3.1 增量构造—— S 影响 R

现在继续考虑增量构造，首先可以假设欲添加元素 $g \notin \langle S \rangle$，否则问题已经解决。

那么，改变了 S 后，考虑截面 R 会发生哪些变化。

回到置换群，R 中每个元素记录的是 1 的不同的**原像**。从这一点考虑，我们只需要知道 1 多了哪些原像即可。

设原先 1 的原像集合为 A_1，那么，当新增置换 g 后，考虑置换 $r_i \circ g\ (r_i \in R)$，也就是说对于 $\forall p \in A_1$，假设 $r_i(p) = 1$，现在 $(r_i \circ g)^{-1}(1) = \left(g^{-1} \circ r_i^{-1}\right)(1) = g^{-1}\left(r_i^{-1}(1)\right) = g^{-1}(p)$ 也成了 1 的原像。

然后我们只需要枚举 S 中元素继续搜索即可。

从图论的角度来看，就是：把原先的轨道划分看成连通块，作出 g 对应的循环图 G_g，将这些边对应的连通块“连通”起来，就得到了新的轨道划分。于是我们先去找这些连接两个不同连通块的边 (即 g)，然后再将其它连通块中的值包含起来。

4.3.2 增量构造—— R 影响 S'

我们现在已经成功处理了生成集 S 的变化对截面 R 的影响，现在就需要处理截面 R 的变化对稳定子群 G_{χ_1} 生成集，记为 S' 的影响。

看起来 S' 中添加了很多的置换，但是我们所维护的 $\langle S' \rangle$ 的增量必须是有限的，而且最好是可接受的。下面的 **Schreier 引理**就可以说明。

引理 4.3.1 (Schreier). *设群 H 是群 $G = \langle S \rangle$ 的子群，R 为 H 的一个右截面，定义集合*

$$S' = \left\{ (r \circ s) \circ (\operatorname{norm}(r \circ s))^{-1} \middle| r \in R, s \in S \right\}$$

则 $H = \langle S' \rangle$。

证明. *显然，$\langle S' \rangle \subseteq H$。下证 $H \subseteq \langle S' \rangle$。*

注意到 $e \in R$，因此 H 中任意一个元素 h 可以表示成：

$$h = r \circ s_1 \circ s_2 \circ \cdots \circ s_k$$

其中 $r \in R; s_1, s_2, \cdots, s_k \in S$。特别地，这里可以取 $r = e$。

接下来对 k 归纳证明：形如上式表示的元素一定在 $\langle S' \rangle$ 中。

当 $k = 0$ 时，$h = r \in H \cap R = \{e\}$，故 $h \in \langle S' \rangle$。

设结论对 $k-1$ 成立，考虑 k，有

$$\begin{aligned} h &= r \circ s_1 \circ s_2 \circ \cdots \circ s_k \\ &= (r \circ s_1) \circ (\operatorname{norm}(r \circ s_1))^{-1} \circ \operatorname{norm}(r \circ s_1) \circ s_2 \circ \cdots \circ s_k \end{aligned}$$

注意到 $(r \circ s_1) \circ (\operatorname{norm}(r \circ s_1))^{-1} \in \langle S' \rangle, \operatorname{norm}(r \circ s_1) \in R$，故 $h \in \langle S' \rangle \Leftrightarrow \operatorname{norm}(r \circ s_1) \circ s_2 \circ \cdots \circ s_k \in \langle S' \rangle$，即 $k-1$ 的子问题，由归纳假设知结论成立。

4.3.3 主要流程

有了 Schreier 引理后，我们就对 $\langle S' \rangle$ 有一个有限的刻画了。

由 Schreier 引理，我们可以通过 Cartesian 积 $R \times S$ 来构造 S'。因此，在增量构造中，R 对 S' 的影响就可以如下处理：

设 R 中新增了元素 r，我们枚举 S 中所有的元素 s，向 G_{χ_1} 中尝试添加 $(r \circ s) \circ (\operatorname{norm}(r \circ s))^{-1}$。

当然，由于之前是先在 S 中增加 g，因此我们也需要枚举 $r \in R$ 并加入 $(r \circ g) \circ (\operatorname{norm}(r \circ g))^{-1}$。

事实上，这两个搜索可以并到一起进行：

- 在“S 影响 R”的过程中，我们枚举 $\pi = r \circ g$，进入第二步：
- 如果 $G_{\chi_1}\pi \cap R = \varnothing$ (即 $\operatorname{norm}\pi$ 不存在)，则将其加入 R，并继续搜索 $\pi' = \pi \circ s$，回到第二步。否则，由于 $\operatorname{norm}\pi = \operatorname{norm}(r \circ g)$ 存在，因此直接向 G_{χ_1} 中尝试添加 $\pi \circ (\operatorname{norm}\pi)^{-1}$ 即可。

4.3.4 Schreier-Sims 算法的伪代码

这个过程就可以用算法来描述了，它就被称为 Schreier-Sims 算法，它的伪代码如下：

Algorithm 1 test

```
Require: A permutation g
Ensure: Report whether g ∈ ⟨S⟩
  pos ← g(1)
  if R[pos] = nil then
    return false
  else
    if next = nil then
      return true
    else
      return next.test(R[pos] ∘ g)
    end if
  end if
```

Algorithm 2 update_transversal

Require: A permutation g

Ensure: Update g as a transversal

```
pos ← g^{-1}(1)
if R[pos] = nil then
    R[pos] ← g
    for s ∈ S do
        update_transversal(g ∘ s)
    end for
else
    if next ≠ nil then
        next.update_generator(g ∘ R[pos]^{-1})
    end if
end if
```

Algorithm 3 update_generator

Require: A permutation g

Ensure: Update g as a generator

```
if test(g) then
    return
else
    S ← S ∪ {g}
    for r ∈ R do
        update_transversal(r ∘ g)
    end for
end if
```

4.3.5 Schreier-Sims 算法的时间复杂度

上述就是 Schreier-Sims 代码的核心框架，下面分析它的时间复杂度。

首先还是考虑固定元素 1 的群论结构 (维护 $\left[G : G_{\chi_1}\right]$ 的)。

由上文 Light 算法的过程可知，按照上述算法产生的 n 阶群的生成集大小不超过 $\lfloor \log_2 n \rfloor$，因为每次添加元素后子群大小至少翻倍。

于是，对于 n 元对称群，这个生成集的大小不超过 $\log_2 |n!| = O(n \log n)$。

事实上，这其实是对称群的真子群链问题，由参考文献 [5] 可知生成集的大小不超过 $\frac{3}{2}n$，即 $|S| = O(n)$。

考虑计算 test 函数的时间复杂度，易知它的时间复杂度为 $O\left(n^2\right)$。对于每个群论结构，它调用 update_generator 的次数 (仅考虑通过 *test* 的)，为 $O(n)$，调用的 update_transversal 中使得截面 R 大小改变的次数也为 $O(n)$。于是调用的 update_transversal 中使得截面 R 大小不变的次数就不超过 $O\left(n^2\right)$，这也可以通过结论“S' 中每个元素可以通过 $R\times S$ 来构造”中看出。

故该群论结构调用子结构的 test 函数至多 $O\left(n^2\right)$ 次，摊到该结构上的时间复杂度为 $O\left(n^4\right)$。因此 Schreier-Sims 算法的总时间复杂度为 $O\left(n^5\right)$。

不过由上述分析过程知，该算法的常数本身就非常小而且通常卡不满，因此实用价值比较高。不过，$O\left(n^5\right)$ 的确是该算法的上确界性，已经被 Knuth 证明，见参考文献 [4]。不过，在随机数据下的期望仍然是 $O\left(n^4\right)$。

5 总结

本文介绍了群论在 OI 中一些常见的运用，从置换、群、群的判定和表示以及计算群论等方面多角度介绍了群论。群论作为组合数学和抽象代数中极其重要的一个分支，但在信息学竞赛中目前并不普及，出现的题目也不是很多。

同时，计算群论中，除了 Schreier-Sims 作为其基础算法外，还有如 Todd-Coxeter, Product-replacement 等其它算法，以及很多很多东西等待我们去探索，可以说这里的水很深。

希望本文能起到一个抛砖引玉的作用，吸引更多读者来研究群论以及抽象代数类的问题。

感谢

感谢中国计算机学会提供学习和交流的平台。

感谢国家集训队高闻远教练的指导。

感谢符水波老师、应平安老师对我的关心与教导。

感谢罗煜翔、钱易等同学为本文验稿。

感谢父母对我的照顾与支持。

参考文献

[1] Wikipedia contributors. Group action. *Wikipedia*, https://en.wikipedia.org/wiki/Group_action.

[2] Rajagopalan, Sridhar; Schulman, Leonard J. (2000), *Verification of Identities*.

[3] Seress, A. (2002), *Permutation Group Algorithms*, Cambridge U Press.

[4] Knuth, Donald E. (1991), *Efficient representation of perm groups*, Combinatorica.

[5] Peter J. Cameron, Ron Solomon, Alexandre Turull (1988), *Chains of Subgroups in Symmetric Groups*.

[6] 罗雨屏 (2014)，抽象代数入门.