浅谈群论在 OI 中的应用

虞皓翔

Zhenhai High School

August 2, 2020

- 置换及其基本运算，逆序数、奇偶性及循环表示。

- 置换及其基本运算，逆序数、奇偶性及循环表示。
- 群的基础概念：阶、子群、陪集和 Lagrange 定理。

- 置换及其基本运算，逆序数、奇偶性及循环表示。
- 群的基础概念：阶、子群、陪集和 Lagrange 定理。
- 常见的四类群：n 元对称群 S_n，n 元交错群 A_n，n 阶循环群 Z_n 以及 $2n$ 阶二面体群 D_{2n}。

- 置换及其基本运算，逆序数、奇偶性及循环表示。
- 群的基础概念：阶、子群、陪集和 Lagrange 定理。
- 常见的四类群：n 元对称群 S_n，n 元交错群 A_n，n 阶循环群 Z_n 以及 $2n$ 阶二面体群 D_{2n}。
- 置换群对染色的作用、轨道——稳定子群定理和 Burnside 引理。

- 置换及其基本运算，逆序数、奇偶性及循环表示。
- 群的基础概念：阶、子群、陪集和 Lagrange 定理。
- 常见的四类群：n 元对称群 S_n，n 元交错群 A_n，n 阶循环群 Z_n 以及 $2n$ 阶二面体群 D_{2n}。
- 置换群对染色的作用、轨道——稳定子群定理和 Burnside 引理。
- 一些基础的生成函数技巧。

下文中的染色，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。

下文中的染色，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。

置换 g 对染色 $\mathbf{c}$ 的作用，记为 $g \cdot \mathbf{c}$，其满足 $(g \cdot \mathbf{c})[i] = \mathbf{c}\left[g^{-1}(i)\right]$。

下文中的染色，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。

置换 g 对染色 $\mathbf{c}$ 的作用，记为 $g\cdot\mathbf{c}$，其满足 $(g\cdot\mathbf{c})[i]=\mathbf{c}\left[g^{-1}(i)\right]$。

染色 $\mathbf{c}$ 在 G 中的轨道，即 G 中所有置换作用于 $\mathbf{c}$ 所得的染色集合，用 $G\cdot\mathbf{c}$ 表示，即 $G\cdot\mathbf{c}=\{g\cdot\mathbf{c}|g\in G\}$。

下文中的染色，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。

置换 g 对染色 $\mathbf{c}$ 的作用，记为 $g\cdot\mathbf{c}$，其满足 $(g\cdot\mathbf{c})[i]=\mathbf{c}\left[g^{-1}(i)\right]$。

染色 $\mathbf{c}$ 在 G 中的轨道，即 G 中所有置换作用于 $\mathbf{c}$ 所得的染色集合，用 $G\cdot\mathbf{c}$ 表示，即 $G\cdot\mathbf{c}=\{g\cdot\mathbf{c}|g\in G\}$。

染色 $\mathbf{c}$ 的稳定子群，为满足 $g\cdot\mathbf{c}=\mathbf{c}$ 的置换构成的子群，用 $G_{\mathbf{c}}$ 表示。

下文中的染色，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。

置换 g 对染色 $\mathbf{c}$ 的作用，记为 $g\cdot\mathbf{c}$，其满足 $(g\cdot\mathbf{c})[i]=\mathbf{c}\left[g^{-1}(i)\right]$。

染色 $\mathbf{c}$ 在 G 中的轨道，即 G 中所有置换作用于 $\mathbf{c}$ 所得的染色集合，用 $G\cdot\mathbf{c}$ 表示，即 $G\cdot\mathbf{c}=\{g\cdot\mathbf{c}|g\in G\}$。

染色 $\mathbf{c}$ 的稳定子群，为满足 $g\cdot\mathbf{c}=\mathbf{c}$ 的置换构成的子群，用 $G_{\mathbf{c}}$ 表示。

轨道——稳定子群定理，用上述定义表示就是 $|G\cdot\mathbf{c}|\cdot|G_{\mathbf{c}}|=|G|$。

Burnside 引理，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。

Burnside 引理，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。

如果用 X/G 表示不同轨道的集合，X^g 表示置换 g 的不动点集合，则 Burnside 引理可以写成

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

Definition 1.1 (Cycle index)

对 n 元置换 g，设 g 的循环表示为

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

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。

Definition 1.1 (Cycle index)

对 n 元置换 g，设 g 的循环表示为

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

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。

Definition 1.1 (Cycle index)

对 n 元置换 g，设 g 的循环表示为

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

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 $t_2^2t_3$。

Definition 1.2 (Cycle index of a permutation group)

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 $Z_G(t_1, t_2, \cdots, t_n)$。

循环指标可以比较方便地描述**生成函数版的 Pólya 定理**。

循环指标可以比较方便地描述**生成函数版的 Pólya 定理**。

Theorem 1.1 (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：

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

同理，这个定理在多元生成函数的情形中也是成立的。

接下来考虑对一般的 Burnside 引理进行推广。

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：

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

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：

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

当外层枚举 g 时，我们就得到了 $\sum\limits_{g\in G}|X^g|$。

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：

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

当外层枚举 g 时，我们就得到了 $\sum\limits_{g\in G}|X^g|$。

当外层枚举 $\mathbf{c}$ 时，我们就得到了 $\sum\limits_{\mathbf{c}\in X}|G_{\mathbf{c}}|=|G|\cdot\sum\limits_{\mathbf{c}\in X}\dfrac{1}{|G\cdot\mathbf{c}|}$。

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：

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

当外层枚举 g 时，我们就得到了 $\sum_{g\in G}|X^g|$。
当外层枚举 $\mathbf{c}$ 时，我们就得到了 $\sum_{\mathbf{c}\in X}|G_{\mathbf{c}}|=|G|\cdot\sum_{\mathbf{c}\in X}\frac{1}{|G\cdot\mathbf{c}|}$。

也就是说，对于染色 $\mathbf{c}$，其稳定子群 $G_{\mathbf{c}}$ 中的每个元素对最终的和式产生 1 的贡献，那么最终 $\mathbf{c}$ 的贡献就等于 $|G_{\mathbf{c}}|$，整条轨道 $G\cdot\mathbf{c}$ 的贡献就等于轨道大小乘稳定子群大小，即 $|G|$。

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 $H \leq G$，它就有一个属于它自己的权值，记作 $\omega(H) = \sum_{g \in H} \omega(g)$。

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 $H \leq G$，它就有一个属于它自己的权值，记作 $\omega(H) = \sum_{g \in H} \omega(g)$。

现在考虑对

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

算两次，

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 $H \leq G$，它就有一个属于它自己的权值，记作 $\omega(H) = \sum_{g \in H} \omega(g)$。

现在考虑对

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

算两次，考虑外层枚举 $\mathbf{c}$，可以得到：

$$\begin{aligned}\sum_{g \in G} \sum_{\mathbf{c} \in X} [g \cdot \mathbf{c} = \mathbf{c}] \, \omega(g) &= \sum_{\mathbf{c} \in X} \sum_{g \in G_{\mathbf{c}}} \omega(g) \\ &= \sum_{\mathbf{c} \in X} \omega(G_{\mathbf{c}})\end{aligned}$$

于是，对于一个染色 $\mathbf{c}$，它的稳定子群会对最终的和产生 $\omega\left(G_{\mathbf{c}}\right)$，考虑它所在的轨道 $G\cdot\mathbf{c}$，则该轨道中所有染色共享一个稳定子群，因此该轨道 (等价类) 产生的贡献就等于 $\left|G\cdot\mathbf{c}\right|\cdot\omega\left(G_{\mathbf{c}}\right)$。

于是，对于一个染色 $\mathbf{c}$，它的稳定子群会对最终的和产生 $\omega(G_{\mathbf{c}})$，考虑它所在的轨道 $G\cdot\mathbf{c}$，则该轨道中所有染色共享一个稳定子群，因此该轨道 (等价类) 产生的贡献就等于 $|G\cdot\mathbf{c}|\cdot\omega(G_{\mathbf{c}})$。

对于外层枚举 g，则是比较平凡的：

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

于是，对于一个染色 $\mathbf{c}$，它的稳定子群会对最终的和产生 $\omega\left(G_{\mathbf{c}}\right)$，考虑它所在的轨道 $G\cdot\mathbf{c}$，则该轨道中所有染色共享一个稳定子群，因此该轨道 (等价类) 产生的贡献就等于 $\left|G\cdot\mathbf{c}\right|\cdot\omega\left(G_{\mathbf{c}}\right)$。

对于外层枚举 g，则是比较平凡的：

$$\sum_{g\in G}\sum_{\mathbf{c}\in X}\left[g\cdot\mathbf{c}=\mathbf{c}\right]\omega\left(g\right)=\sum_{g\in G}\omega\left(g\right)\left|X^{g}\right|$$

于是就得到了**广义 Burnside 引理**：

Theorem 2.1 (Generalized Burnside's lemma)

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：

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

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。

Theorem 2.1 (Generalized Burnside's lemma)

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：

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

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 $\omega(g)$ 仅仅和置换的循环指标相关时，就能导出广义 Pólya 定理。具体就是把 $\omega(g)|X^g|$ 换成对应的循环指标表达式即可，这里就不再列举了。

特别地，取 $\omega(g)$ 为该置换的符号 (奇置换为 -1，偶置换为 1)。

特别地，取 $\omega(g)$ 为该置换的符号 (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。

特别地，取 $\omega(g)$ 为该置换的符号 (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 $\omega(G_{\mathbf{c}}) = 0$。

特别地，取 $\omega(g)$ 为该置换的符号 (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。

Corollary 2.1 (Pólya)

对于置换群 $G=S_n$ 和它固定的染色集合 X，有

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

(其中 $\operatorname{sgn}(g)$ 表示置换 g 的符号)

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。

Problem (小 ω 的魔方（自编题）)

你需要对一个 $n \times n \times n$ 的魔方上的 $6n^2$ 个小格子上贴贴纸，贴纸共有六种颜色，每种颜色的贴纸均有无限多个。

每种颜色的贴纸分为三类，权值分别为 $-1, 0, 1$。用 C_i 表示颜色为 C 且权值为 i 的贴纸种数。

现在需要将这些贴纸贴在魔方上，要求每个小格子恰好贴一张贴纸，每种颜色的贴纸各用 n^2 个。

定义一个最终方案的权值等于所有 $6n^2$ 张贴纸的权值之和，两个方案是本质相同的当且仅当可以在三维空间中旋转而重合。

求对于每个 $k \in \left[-6n^2, 6n^2\right]$，求出有多少种本质不同的权值为 k 的方案。

$n \leq 1000$，对 10^9+7 取模，通过某种方式压缩输出。

Solution

考察立方体的转动群，可知它同构于 S_4，考虑该群对面的置换，可以将这些置换分为五类：

Solution

考察立方体的转动群，可知它同构于 S_4，考虑该群对面的置换，可以将这些置换分为五类：

1. 恒等变换，共一个。

Solution

考察立方体的转动群，可知它同构于 S_4，考虑该群对面的置换，可以将这些置换分为五类：

1. 恒等变换，共一个。
2. 固定上下底面，将立方体转体 $\pm 90°$，共两个变换，又由于立方体有三对底面，故有 6 个这样的变换。

Solution

考察立方体的转动群，可知它同构于 S_4，考虑该群对面的置换，可以将这些置换分为五类：

1. 恒等变换，共一个。
2. 固定上下底面，将立方体转体 $\pm 90^{\circ}$，共两个变换，又由于立方体有三对底面，故有 6 个这样的变换。
3. 固定上下底面，将立方体转体 180°。这一类变换有 3 个。

Solution

考察立方体的转动群，可知它同构于 S_4，考虑该群对面的置换，可以将这些置换分为五类：

1. 恒等变换，共一个。
2. 固定上下底面，将立方体转体 $\pm 90^\circ$，共两个变换，又由于立方体有三对底面，故有 6 个这样的变换。
3. 固定上下底面，将立方体转体 180°。这一类变换有 3 个。
4. 固定一对顶点 (要求这对顶点的连线为体对角线)，将立方体沿着这条体对角线进行~~糖葫芦式的~~转体，可以旋转 $\pm 120^\circ$，故有 2 种这样的变换。同样，由于立方体有四条体对角线，故第 4 类变换一共有 8 个。

Solution

1. 恒等变换，共一个。
2. 固定上下底面，将立方体转体 $\pm 90^\circ$，共两个变换，又由于立方体有三对底面，故有 6 个这样的变换。
3. 固定上下底面，将立方体转体 180°。这一类变换有 3 个。
4. 固定一对顶点 (要求这对顶点的连线为体对角线)，将立方体沿着这条体对角线进行~~糖葫芦式的~~转体，可以旋转 $\pm 120^\circ$，故有 2 种这样的变换。同样，由于立方体有四条体对角线，故第 4 类变换一共有 8 个。
5. 固定一条棱，将这条棱连接的两个面 (顶点) 交换。对于每一种这样的交换，其实恰好有 (立方体的) 两条平行的对棱满足这个性质，而立方体一共有 6 对棱，故这样的变换一共有 6 个。

Solution

由于对每种颜色的使用次数有限制，因此使用生成函数版的 Pólya 定理。

Solution

由于对每种颜色的使用次数有限制，因此使用生成函数版的 Pólya 定理。

在这道题中，可以定义七个形式变元 $x_1, x_2, x_3, x_4, x_5, x_6, y$，分别表示六种颜色使用的贴纸数和权值 (可以将 $-1 \sim 1$ 转化为 $0 \sim 2$ 以避免负数)。

Solution

由于对每种颜色的使用次数有限制，因此使用生成函数版的 Pólya 定理。

在这道题中，可以定义七个形式变元 $x_1, x_2, x_3, x_4, x_5, x_6, y$，分别表示六种颜色使用的贴纸数和权值 (可以将 $-1 \sim 1$ 转化为 $0 \sim 2$ 以避免负数)。

下面约定颜色 x_1 的生成函数为 $F_1(x_1, y) = \left(a + by + cy^2\right) x_1$，其余颜色类同。

Solution

由于对每种颜色的使用次数有限制，因此使用生成函数版的 Pólya 定理。

在这道题中，可以定义七个形式变元 $x_1, x_2, x_3, x_4, x_5, x_6, y$，分别表示六种颜色使用的贴纸数和权值 (可以将 $-1 \sim 1$ 转化为 $0 \sim 2$ 以避免负数)。

下面约定颜色 x_1 的生成函数为 $F_1(x_1, y) = \left(a + by + cy^2\right) x_1$，其余颜色类同。

以第 2 类置换为例，由于两个底面不动，因此它的循环指标需要根据 n 的奇偶性来讨论。

Solution

- 若 n 为奇数，则循环指标为 $t_1^2t_4^{(3n^2-1)/2}$，那么生成函数为 $(1+F_1(x_1,y)+F_2(x_2,y)+\cdots+F_6(x_6,y))^2\cdot\left(1+F_1\left(x_1^4,y^4\right)+F_2\left(x_2^4,y^4\right)+\cdots+F_6\left(x_6^4,y^4\right)\right)^{(3n^2-1)/2}$。取 $(x_1x_2\cdots x_6)^{n^2}$ 项系数可知贡献为 0。

Solution

- 若 n 为奇数，则循环指标为 $t_1^2 t_4^{(3n^2-1)/2}$，那么生成函数为 $(1+F_1(x_1,y)+F_2(x_2,y)+\cdots+F_6(x_6,y))^2 \cdot \left(1+F_1\left(x_1^4,y^4\right)+F_2\left(x_2^4,y^4\right)+\cdots+F_6\left(x_6^4,y^4\right)\right)^{(3n^2-1)/2}$。取 $(x_1x_2\cdots x_6)^{n^2}$ 项系数可知贡献为 0。
- 当 n 为偶数时，循环指标为 $t_4^{3n^2/2}$，生成函数为 $\left(1+F_1\left(x_1^4,y^4\right)+F_2\left(x_2^4,y^4\right)+\cdots+F_6\left(x_6^4,y^4\right)\right)^{3n^2/2}$。取 $(x_1x_2\cdots x_6)^{n^2}$ 项系数可知贡献为

$$\frac{6\cdot(3n^2/2)!}{(n^2/4)!^6}\cdot\left[F_1(1,y)\,F_2(1,y)\ldots F_6(1,y)\right]^{n^2/4}$$

Solution

最后只需要快速计算对若干 N,
$\left[F_1(1,y)\,F_2(1,y)\cdots F_6(1,y)\right]^N$ 的所有次项系数。

Solution

最后只需要快速计算对若干 N, $\left[F_1(1,y)\,F_2(1,y)\cdots F_6(1,y)\right]^N$ 的所有次项系数。

注意到被求幂的多项式的次数不会超过 12 次，因此可以首先展开，然后化为低次多项式的快速幂问题。

Solution

最后只需要快速计算对若干 N,
$\left[F_1(1,y)F_2(1,y)\cdots F_6(1,y)\right]^N$ 的所有次项系数。

注意到被求幂的多项式的次数不会超过 12 次，因此可以首先展开，然后化为低次多项式的快速幂问题。

而这是一个经典问题：设 $g(x)=f^N(x)$，则 $g'(x)f(x)=k\cdot f'(x)g(x)$，两边取某一项系数即可得到关于系数的长度不超过 $\deg f$ 的递推式。

Solution

最后只需要快速计算对若干 N, $\left[F_1(1,y)F_2(1,y)\cdots F_6(1,y)\right]^N$ 的所有次项系数。

注意到被求幂的多项式的次数不会超过 12 次，因此可以首先展开，然后化为低次多项式的快速幂问题。

而这是一个经典问题：设 $g(x)=f^N(x)$，则 $g'(x)f(x)=k\cdot f'(x)g(x)$，两边取某一项系数即可得到关于系数的长度不超过 $\deg f$ 的递推式。

于是这个问题就能在约 $12n^2$ 的时间内解决。

Definition 1.1 (Invariant subgroup/Normal subgroup)

设群 $(G,\circ)$ 的子群 $H\leq G$ 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** (Invariant subgroup) 或**正规子群** (Normal subgroup)，记作 $H\trianglelefteq G$。

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

Definition 1.1 (Invariant subgroup/Normal subgroup)

设群 $(G, \circ)$ 的子群 $H \leq G$ 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** (Invariant subgroup) 或**正规子群** (Normal subgroup)，记作 $H \trianglelefteq G$。

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

Definition 1.2 (Quotient group)

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**。

Definition 1.3 (Homomorphism)

设有群 $(G,\circ),(H,\cdot)$，若映射 $f\colon G\to H$ 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** (Homomorphism) 映射，简称同态。

Definition 1.3 (Homomorphism)

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** (Homomorphism) 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。

Definition 1.4 (Kernel)

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** (Kernel)，记为 $\ker f$。

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：

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：

Theorem 1.1 (Fundamental theorem on homomorphisms)

设 f 是 $(G, \circ)$ 到 $(H, \cdot)$ 的**满同态**，那么 $G/\ker f$ 和 H 同构。

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：

Theorem 1.1 (Fundamental theorem on homomorphisms)

设 f 是 $(G, \circ)$ 到 $(H, \cdot)$ 的**满同态**，那么 $G/\ker f$ 和 H 同构。

Theorem 1.2 (The third isomorphism theorem)

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 $\dfrac{G/N}{H/N} \cong G/H$。

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？

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，运算用 $\circ$ 表示。

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，运算用 $\circ$ 表示。

- 封闭性。

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，运算用 $\circ$ 表示。

- 封闭性。
  直接检验即可。

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，运算用 $\circ$ 表示。

- 封闭性。
  直接检验即可。
- 单位元。

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，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。

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？

考虑通过群的定义——封闭性、结合律、单位元和逆元来检验。为了方便起见，以下假设群中的元素是 $0 \sim n-1$，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)。那么对每个 g 检验是否有 $e \circ g = g \circ e = e$。

- 逆元。

- 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。

- 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 $O\left(n^3\right)$。

- 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 $\left(O\left(n^2\right)\right)$ 内完成，那结合律的检验是否有更优秀的方法呢？

- 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 $\left(O\left(n^2\right)\right)$ 内完成，那结合律的检验是否有更优秀的方法呢？

至少到现在为止，检验一个**一般**的代数结构是否满足结合律还没有低于 $O\left(n^3\right)$ 的**确定性**算法，但存在复杂度较为优秀的随机算法。

- 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 $\left(O\left(n^2\right)\right)$ 内完成，那结合律的检验是否有更优秀的方法呢？

至少到现在为止，检验一个**一般**的代数结构是否满足结合律还没有低于 $O\left(n^3\right)$ 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。

- 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 $\left(O\left(n^2\right)\right)$ 内完成，那结合律的检验是否有更优秀的方法呢？

至少到现在为止，检验一个**一般**的代数结构是否满足结合律还没有低于 $O\left(n^3\right)$ 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。

在这之前，我们需要用到两个引理：

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Proof

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

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Proof

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。

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Proof

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 $G_{i-1} < G$。

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Proof

定义子群链 $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_k = G$，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 $G_i = \langle G_{i-1} \cup \{g_i\} \rangle$。

Lemma 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 $G = \langle S \rangle$)。

(注：下界可以取到，比如 $G = Z_2^k$)

Proof

定义子群链 $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_k = G$，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 $G_{i-1} \leq G_i \leq G$ 且 $G_{i-1} \neq G_i$ ($g_i \in G_i \wedge g_i \notin G_{i-1}$)。

Proof

定义子群链 $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_k = G$，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 $G_{i-1} \leq G_i \leq G$ 且 $G_{i-1} \neq G_i$ $(g_i \in G_i \wedge g_i \notin G_{i-1})$。
- 于是 $|G_i| \geq 2\,|G_{i-1}|$。

Proof

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。

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

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

Proof

必要性显然。下证充分性：

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

Proof

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**。

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

Proof

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 $a\circ b\in A$。

Proof

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。

Proof

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。

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 $G = \langle S \rangle$。

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 $G = \langle S \rangle$。
(注：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)

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 $G = \langle S \rangle$。
   (注：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)
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 $(g \circ s) \circ h = g \circ (s \circ h)$。

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 $G = \langle S \rangle$。
   (注：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)
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。

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 $G = \langle S \rangle$。
   (注：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)
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 $O\left(n^2 |S|\right) = O\left(n^2 \log n\right)$。

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 $G = \langle S \rangle$。
   (注：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)
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 $O\left(n^2 \log n\right)$。

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。

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。

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

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

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。

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 $\{\lambda_g | g \in G\}$ 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**：

于是，我们得到了 **Cayley 定理**：

Theorem 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)。

于是，我们得到了 **Cayley 定理**：

Theorem 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**。

于是，我们得到了 **Cayley 定理**：

Theorem 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**。

那么，这样的**单同态**的个数有多少呢？

Problem (列队（uoj154）)

给定群 G，求 G 到 n 元对称群 S_n 的单同态个数。

(注：原题需要判定 G 是否构成群，这里略去)

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

Solution

对于群 G, H，记 G 到 H 的**同态**数量为 $\mathrm{homo}\,(G, H)$，**单同态**数量为 $\mathrm{mono}\,(G, H)$。

考虑一个同态 $f\colon G \to H$，记 $K = \ker f$，由群同态基本定理知 G/K 和 $\mathrm{im}\, f$ 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**。

Solution

对于群 G, H，记 G 到 H 的**同态**数量为 $\mathrm{homo}(G, H)$，**单同态**数量为 $\mathrm{mono}(G, H)$。

考虑一个同态 $f\colon G \to H$，记 $K = \ker f$，由群同态基本定理知 G/K 和 $\mathrm{im}\, f$ 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。

Solution

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

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

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

Solution

对于群 G, H，记 G 到 H 的**同态**数量为 $\text{homo}\,(G, H)$，**单同态**数量为 $\text{mono}\,(G, H)$。

考虑一个同态 $f\colon G \to H$，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

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

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

Solution

现在考虑给定群 G，计算它到 S_n 的**同态**个数。

Solution

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 $H = \operatorname{im} f \leq S_n$。

Solution

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 $H = \operatorname{im} f \leq S_n$。
定义 i 的特征染色 χ_i 为：i 位置为黑色，其余位置为白色。

Solution

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 $H = \operatorname{im} f \leq S_n$。

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。

Solution

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 $H = \operatorname{im} f \leq S_n$。

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 $|H \cdot \chi_1| = k$。

Solution

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，$|H_{\chi_1}| = \dfrac{|H|}{|H \cdot \chi_1|} = \dfrac{|H|}{k}$。

Solution

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，$|H_{\chi_1}| = \dfrac{|H|}{|H \cdot \chi_1|} = \dfrac{|H|}{k}$。

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。

Solution

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。

Solution

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 $1\in A$。

Solution

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 $1, 2, \cdots, k$。

Solution

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。

Solution

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。

Solution

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 $(\forall s \in S)$

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

Solution

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 $(\forall s \in S)$

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

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。

Solution

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 $(\forall s \in S)$

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

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 $\frac{|G|}{k}$ 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。

Solution

接下来就可以直接计算了，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。

Solution

接下来就可以直接计算了，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

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

Solution

接下来就可以直接计算了，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

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

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

Solution

接下来就可以直接计算了，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

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

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

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。

Solution

接下来就可以直接计算了，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

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

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

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。

Solution

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。

Solution

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。

Solution

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。

Solution

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)。

除了一些阶数不大的群外，更加常见的群就是置换群了。

除了一些阶数不大的群外，更加常见的群就是置换群了。

有些置换群，虽然里面的置换的大小不大，群也仅仅由几个简单的置换生成，但是作为整体构成的群就很庞大了。

除了一些阶数不大的群外，更加常见的群就是置换群了。

有些置换群，虽然里面的置换的大小不大，群也仅仅由几个简单的置换生成，但是作为整体构成的群就很庞大了。

一个经典的例子就是魔方群 G_{C}，比如三阶魔方，只有简单的 6 种基本置换，就能生成 $|G_{\mathrm{C}}| = 43\,252\,003\,274\,489\,856\,000$ 种不同的置换。

除了一些阶数不大的群外，更加常见的群就是置换群了。

有些置换群，虽然里面的置换的大小不大，群也仅仅由几个简单的置换生成，但是作为整体构成的群就很庞大了。

一个经典的例子就是魔方群 G_C，比如三阶魔方，只有简单的 6 种基本置换，就能生成 $|G_\mathrm{C}| = 43\,252\,003\,274\,489\,856\,000$ 种不同的置换。

计算群论就是研究这一类问题的利器：它可以对这类置换群维护出一个有很多功能的“群论结构”。Schreier-Sims 算法是计算群论中最基础的算法。

考虑从一个最基本的问题开始：

考虑从一个最基本的问题开始：

Problem

给定若干个 n 元置换构成的集合 S，求 S 生成的子群大小 $|\langle S\rangle|$。

$n \le 50$。

考虑从一个最基本的问题开始：

Problem

给定若干个 n 元置换构成的集合 S，求 S 生成的子群大小 $|\langle S\rangle|$。

$n \le 50$。

怎么求一个巨大的群的大小呢？一个比较直观的思路是：

考虑从一个最基本的问题开始：

Problem

给定若干个 n 元置换构成的集合 S，求 S 生成的子群大小 $|\langle S\rangle|$。

$n \le 50$。

怎么求一个巨大的群的大小呢？一个比较直观的思路是：

如果我们有一个子群链 $\langle S\rangle = G_0 \ge G_1 \ge G_2 \ge \cdots \ge G_k = \{e\}$，那么由 Lagrange 定理，有

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

考虑从一个最基本的问题开始：

Problem

给定若干个 n 元置换构成的集合 S，求 S 生成的子群大小 $|\langle S\rangle|$。

$n \le 50$。

怎么求一个巨大的群的大小呢？一个比较直观的思路是：

如果我们有一个子群链 $\langle S\rangle = G_0 \ge G_1 \ge G_2 \ge \cdots \ge G_k = \{e\}$，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 $\forall 1 \leq i \leq n$，诸轨道 $G \cdot \chi_i$ 构成了 $\{1, 2, \cdots, n\}$ 的一个划分。

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 $[G : G_{\chi_1}] = |G \cdot \chi_1|$，而轨道的大小显然不超过 n，因此这个数值是可接受的。

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 $[G : G_{\chi_1}] = |G \cdot \chi_1|$，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。

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 $[G : G_{\chi_1}] = |G \cdot \chi_1|$，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。

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 $[G : G_{\chi_1}] = |G \cdot \chi_1|$，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。

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。

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

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，你可以比较容易知道 $G \cdot \chi_1$ 的大小，以及这些元素的轨道。但是你现在无法方便地表示 G_{χ_1}。事实上，G_{χ_1} 也是一个庞大的置换群，你现在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。

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，你可以比较容易知道 $G \cdot \chi_1$ 的大小，以及这些元素的轨道。但是你现在无法方便地表示 G_{χ_1}。事实上，G_{χ_1} 也是一个庞大的置换群，你现在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。

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，你可以比较容易知道 $G\cdot\chi_1$ 的大小，以及这些元素的轨道。但是你现在无法方便地表示 G_{χ_1}。事实上，G_{χ_1} 也是一个庞大的置换群，你现在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。

那现在我们向 S 中添加一个新元素 g，那么会产生怎样的“链式反应”呢？

假设现在我们要向 S 中添加 g。那么在这一切之前，我们需要检验 g 是否已经在 $\langle S\rangle$ 中。

假设现在我们要向 S 中添加 g。那么在这一切之前，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滋磁查询一个置换是否在 $\langle S\rangle$ 中。

假设现在我们要向 S 中添加 g。那么在这一切之前，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滋磁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。

假设现在我们要向 S 中添加 g。那么在这一切之前，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滋磁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。

假设现在我们要向 S 中添加 g。那么在这一切之前，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滋磁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 $G_{\chi 1}$ 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 $G_{\chi 1}$ 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中其实由它专业的术语：**截面**。

Definition 2.1 (Transversal)

对于群 G 和它的子群 $H \leq G$，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。

Definition 2.1 (Transversal)

对于群 G 和它的子群 $H \leq G$，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。

Definition 2.1 (Transversal)

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 $G_{\chi 1}$ 的一个右截面 $R = \{r_1 = e, r_2, r_3, \cdots, r_k\}$，它满足如下性质：

Definition 2.1 (Transversal)

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 $G_{\chi 1}$ 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 $i \neq j$ 有 $Hr_i \neq Hr_j$，即 $r_i \circ r_j^{-1} \notin H$。

Definition 2.1 (Transversal)

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 $i \neq j$ 有 $Hr_i \neq Hr_j$，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同的原像。

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 $i \neq j$ 有 $Hr_i \neq Hr_j$，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。

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。

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 $\operatorname{norm}\left(g^{-1}\right)$。

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 $\operatorname{norm}\left(g^{-1}\right)$。

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 $g \notin \langle S\rangle$。

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 $\operatorname{norm}\left(g^{-1}\right)$。

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。

现在就可以继续增量构造了。

现在就可以继续增量构造了。

首先，可以假设欲添加元素 $g \notin \langle S \rangle$，否则问题已经解决。

现在就可以继续增量构造了。

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，首当其冲的就是截面 R，我们看看 R 会发生哪些变化。

现在就可以继续增量构造了。

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，首当其冲的就是截面 R，我们看看 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。

现在就可以继续增量构造了。

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，首当其冲的就是截面 R，我们看看 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。

现在就可以继续增量构造了。

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，首当其冲的就是截面 R，我们看看 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涵起来。

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 S' 的影响。

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 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。

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 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。

那如何得到稳定子群的 $\langle S' \rangle$ 呢？这里我们需要用到一个引理：**Schreier 引理**。

Lemma 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 $H = \langle S' \rangle$。

Lemma 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 $H=\langle S'\rangle$。

Proof

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

Lemma 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 $H=\langle S'\rangle$。

Proof

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 $r=e$。

Proof

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。

Proof

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 $h \in \langle S' \rangle$。

Proof

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

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

Proof

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。

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

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：

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 $(r \circ s) \circ (\operatorname{norm}(r \circ s))^{-1}$。

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 $(r \circ s) \circ (\mathrm{norm}\,(r \circ s))^{-1}$。

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 $(r \circ g) \circ (\mathrm{norm}\,(r \circ g))^{-1}$。

事实上，这两个搜索可以并到一起进行：

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 $(r \circ s) \circ (\mathrm{norm}(r \circ s))^{-1}$。

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 $(r \circ g) \circ (\mathrm{norm}(r \circ g))^{-1}$。

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：

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 $G_{\chi 1}$ 中尝试添加 $(r \circ s) \circ (\mathrm{norm}\,(r \circ s))^{-1}$。

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 $(r \circ g) \circ (\mathrm{norm}\,(r \circ g))^{-1}$。

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 $\mathrm{norm}\,\pi$ 不存在)，则将其加入 R，并继续搜索 $\pi' = \pi \circ s$，回到第二步。

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 $G_{\chi 1}$ 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 $G_{\chi 1}$ 中尝试添加 $\pi \circ (\operatorname{norm} \pi)^{-1}$ 即可。

这个过程就可以用算法来描述了，即 **Schreier-Sims 算法**，伪代码如下：

这个过程就可以用算法来描述了，即 **Schreier-Sims 算法**，伪代码如下：

```
function TEST(g)
    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
end function
```

```
function UPDATE_TRANSVERSAL(g)
    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
end function
```

```
function UPDATE_GENERATOR(g)
    if TEST(g) then
        return
    else
        S ← S ∪ {g}
        for r ∈ R do
            UPDATE_TRANSVERSAL(r ∘ g)
        end for
    end if
end function
```

function UPDATE_GENERATOR(g)
    if TEST(g) **then**
        return
    else
        $S \leftarrow S \cup \{g\}$
        for $r \in R$ **do**
            UPDATE_TRANSVERSAL($r \circ g$)
        end for
    end if
end function

以上就是 Schreier-Sims 算法的全部内容，接下来分析一下它的时间复杂度。

首先还是考虑固定元素 1 的群论结构 (维护 $[G : G_{\chi 1}]$ 的)，容易证明 $|S| < n$。

(只需注意到 S 中每增加一个元素和引起两个连通块的合并)

首先还是考虑固定元素 1 的群论结构 (维护 $[G : G_{\chi_1}]$ 的), 容易证明 $|S| < n$。

(只需注意到 S 中每增加一个元素和引起两个连通块的合并)

先考虑计算 `test` 函数的时间复杂度, 易知它的时间复杂度为 $O\left(n^2\right)$。

首先还是考虑固定元素 1 的群论结构 (维护 $[G : G_{\chi 1}]$ 的)，容易证明 $|S| < n$。

(只需注意到 S 中每增加一个元素和引起两个连通块的合并)

先考虑计算 `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 $O(n)$。

首先还是考虑固定元素 1 的群论结构 (维护 $[G:G_{\chi_1}]$ 的)，容易证明 $|S|<n$。

(只需注意到 S 中每增加一个元素和引起两个连通块的合并)

先考虑计算 `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。

首先还是考虑固定元素 1 的群论结构 (维护 $[G : G_{\chi_1}]$ 的), 容易证明 $|S| < n$。

(只需注意到 S 中每增加一个元素和引起两个连通块的合并)

先考虑计算 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 $O\left(n^5\right)$。

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。

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。

($O\left(n^5\right)$ 的上确界性已经被 Knuth 证明，但是在随机数据下期望是 $O\left(n^4\right)$ 的，因此在实践中非常有用)

1. Rajagopalan, Sridhar; Schulman, Leonard J. (2000). *Verification of Identities*.
2. Seress, A. (2002), *Permutation Group Algorithms*, Cambridge U Press.
3. Knuth, Donald E. (1991), *Efficient representation of perm groups*, Combinatorica.
4. 罗雨屏 (2014)，抽象代数入门.

Thanks for watching and listening!