1 群作用和轨道

记 $S=\{\sigma_1,\sigma_2,\ldots,\sigma_m\},G=\langle S\rangle$，考虑 G 在 Ω 上天然的群作用 $*$（即“置换”一词的本来意义），则对于任一元素 $\beta\in\Omega$，我们可以求得它的轨道 $O(\beta)=\{g*\beta|g\in G\}$。

虽然我们不知道 G 的具体结构，但是我们拥有它的一个生成元集 S。对于任意 $g\in G$，都可以找到一组 $s_1,s_2,\ldots,s_k\in S\cup S^{-1}$，使得 $g=s_1\cdot s_2\cdots s_k$。此时群作用变为

$$g*\beta=(s_1\cdot s_2\cdots s_k)*\beta=s_1*(s_2*(\cdots s_k*\beta))$$

，可以看出 G 在 Ω 上的作用，实际上是由 $S\cup S^{-1}$ 在 Ω 不断作用得到的。

受上面观察的启发，我们构造一个无向图 $G=\langle V,E\rangle$，其中 $V=\Omega$，而

$$E=\{(a,b)|\exists s\in S\cup S^{-1},s*a=b\}$$

在无向图 G 中，我们可以清楚地看到，$\gamma\in O(\beta)$ 当且仅当 β 和 γ 属于同一个连通分量。由于我们只关心 $O(\beta)$，不妨做出以 β 为根的一颗生成树 T。一个附加的好处是，对于任意给出的 γ，可以求出一个满足 $g*\beta=\gamma$ 的 g。具体的做法非常简单，只需要将 T 上从 β 到 γ 唯一的路径上所有置换相乘，即得所求的 g。

在上述算法中，建图的复杂度是 $O(|\Omega|\cdot|S|)$，构建生成树的时间复杂度是 $O(|\Omega|^2)$。如果预处理根到每个节点的置换之积，则之后每次询问都能在 $O(1)$ 的复杂度内得到。

2 稳定子群降链和强生成集

我们知道，轨道 $O(\beta)$ 和群 G 关于稳定化子 $\mathrm{stab}(\beta)$ 的陪集划分是一一对应的。所以我们知晓了轨道 $O(\beta)$，实际上就是知道了关于 $\mathrm{stab}(\beta)$ 陪集划分的代表元。

不甚自然地，引入稳定子群降链的定义：

对于元素序列 $(\beta_1,\beta_2,\ldots,\beta_k)$，其中 $\beta_i\in\Omega$，其对应的稳定子群降链 $G=G^1\geq G^2\geq\cdots\geq G^{k+1}$ 满足

$$\forall g\in G^i,\forall 1\leq j<i,g*\beta_j=\beta_j$$

换句话说，G^i 是 $\beta_1,\beta_2,\ldots,\beta_{i-1}$ 的稳定化子。

额外地，如果 $G^{k+1}=\{1\}$ 是平凡群，则 $(\beta_1,\beta_2,\ldots,\beta_k)$ 称为关于 G 的一组基。

进一步地，对于某个生成元集 S 和关于基 $(\beta_1,\beta_2,\ldots,\beta_k)$ 的子群降链 $G^1\geq G^2\geq\cdots\geq G^{k+1}$，如果有 $\langle S\cap G^i\rangle=G^i$，则称 S 是关于基 $(\beta_1,\beta_2,\ldots,\beta_k)$ 的一个强生成元集。

2.1 计算 $\langle S\rangle$ 的阶数

如果我们把 G^i 写成关于 G^{i+1} 的陪集划分，由拉格朗日定理，有：

$$|G^i|=|G^{i+1}|\cdot|G^i:G^{i+1}|$$

不断递推得到

$$|G|=[G^1:G^2]\cdot[G^2:G^3]\cdots[G^k:G^{k+1}]$$

因为 G^{i+1} 是 G^i 中元素 β_i 的稳定化子，根据轨道和陪集划分的对应关系，我们有 $[G^i:G^{i+1}]=|O(\beta_i)|$，代入得到

$$|G|=|O(\beta_1)|\cdot|O(\beta_2)|\cdots|O(\beta_k)|$$

剩下的工作只是计算 β_i 在 G^i 中的轨道数 $O(\beta_i)$，因为 S 是强生成元集，又因为 G^i 是元素 $\beta_1,\beta_2,\ldots,\beta_k$ 的稳定化子，所以容易求得 $S\cap G^i$，由定义 $\langle S\cap G^i\rangle=G^i$ 知道 $S\cap G^i$ 是 G^i 的生成元集。根据上一节的内容，我们知道在具有生成元集的情况下，计算元素的轨道数是简单的。

2.2 测试 $g\in\langle S\rangle$ 是否成立

若 $g\in G$，通过不断把陪集表示展开，可以得到

$$g=r_1\cdot r_2\cdots r_k(r_i\in G^i/G^{i+1})$$

（注意，我们借用了商群的符号了表示陪集的划分）

所以，测试 $g\in G$ 等价于把 g 按照陪集表示展开。对等式取关于 β_1 的轨道，因为 $r_2\cdot r_3\cdots r_k\in G^2=\mathrm{stab}(\beta_1)$，有：

$$g*\beta_1=r_1*((r_2\cdot r_3\cdots r_k)*\beta)=r_1*\beta_1$$

因为我们可以求得 β_1 的轨道，所以求得 r_1 也是自然的，之后只要递归地在 G^2 中展开 $r_1^{-1}\cdot g$ 即可。

容易分析得到，一次展开的时间复杂度是 $O(|\Omega|^2)$。

3 强生成元集的构造

余下的工作只有一件，对于任意给出的生成元集 T，如何构造等价的强生成元集 S 及其对应的基 $(\beta_1, \beta_2, \ldots, \beta_k)$。

为此，需要 Schreier 引理：如果 $G = \langle S \rangle, H \leq G$，$\overline{r}$ 表示 G/H 中 r 所在陪集的代表元，则：

$$H = \langle r \cdot s \cdot (\overline{r \cdot s})^{-1} | r \in G/H, s \in S \rangle$$

引理实际上是说，如果我们拥有 G 和生成元集和 G/H 的代表元，则可以得到 H 的生成元集。

于是我们可以从 $G^1 = G = \langle T \rangle$ 出发，取任一 β_1 满足 $\mathrm{stab}(\beta_1) \neq G^1$，容易计算出 $O(\beta_1)$，即 G^1/G^2。根据引理，我们已经可以枚举出 G^2 的生成元集。

需要注意的是，如果把所有可能的生成元全部作为 G^2 的生成元，可能导致整体复杂度的退化。为此，需要对这个生成元集作极小化，也就是说每次添加生成元时，如果已经属于生成元集，则应该被忽略。为了快速做到这点，需要利用上节介绍的算法，为此需要得到 G^2 的一个稳定子群降链，即是说每次加入元素，需要递归调用算法。