对置换群有关算法的初步研究

浙江省镇海中学 岑若虚

问题的提出

- 对n个数进行操作。
  有n种操作，每种操作是一个置换，操作集合为S。
  问能否将一个状态变成另一个状态。

群

- 群是由一个非空集合以及一个二元运算组成的代数结构，满足封闭性、结合律、单位元和逆元。
- 群G中元素的个数称为群的阶，记作$|G|$。
- 单位元记作e，只含单位元的群记作1。

群

- 群是由一个非空集合以及一个二元运算组成的代数结构，满足封闭性、结合律、单位元和逆元。
- 群G中元素的个数称为群的阶，记作$|G|$。
- 单位元记作e，只含单位元的群记作1。
- 群$(G, \circ)$中，若H是G的子集，且$(H, \circ)$也是群，则称H是G的子群，记作$H \leq G$。
- 任意群G都有平凡子群G和1，其它子群称为真子群。
- 对于G的子集M，所有包含M的子群的交也是一个子群，称为M的生成子群，记作$\langle M \rangle$。
- M称为$\langle M \rangle$的生成集。

- 若H是G的子群，对任意$a \in G$，称

$$aH = \{ah | h \in H\}$$

为子群H的一个左陪集，称

$$Ha = \{ha | h \in H\}$$

为子群H的一个右陪集。

陪集

- 若H是G的子群，对任意$a \in G$，称
$$aH = \{ah | h \in H\}$$
为子群H的一个左陪集，称
$$Ha = \{ha | h \in H\}$$
为子群H的一个右陪集。
- 设G中H的右陪集作成的集合为S_R，左陪集作成的集合为S_L，可以证明映射
$$\phi : Ha \mapsto a^{-1}H$$
是S_R到S_L的一一映射。
下面我们只考虑右陪集。

例子

- $G=\{0,1,2,3,4,5\}$，运算是模6意义下的加法。
- 它的真子群有$H_1=\{0,2,4\}$和$H_2=\{0,3\}$。
- H_1也是$\{2\}$的生成子群，即$H_1=\langle\{2\}\rangle$。
- H_1的右陪集有

$$H_1 0=H_1 2=H_1 4=\{0,2,4\}$$

$$H_1 1=H_1 3=H_1 5=\{1,3,5\}$$

- H_2的右陪集有

$$H_2 0=H_2 3=\{0,3\}$$

$$H_2 1=H_2 4=\{1,4\}$$

$$H_2 2=H_2 5=\{2,5\}$$

拉格朗日定理

引理

设H为G的子群，任给H的右陪集Ha, Hb，则要么$Ha = Hb$，要么$Ha \cap Hb = \varnothing$.

证明

若存在$x \in Ha \cap Hb$，则存在$h_1, h_2 \in H$，使得$x = h_1 a = h_2 b$.
因此有

$$\forall ha \in Ha, ha = hh_1^{-1} h_1 a = hh_1^{-1} h_2 b = h' b \in Hb,$$

故$Ha \subseteq Hb$，同理$Hb \subseteq Ha$. 因此$Ha = Hb$，定理得证。

- 记$|G:H|$表示G中子群H的不同右陪集的个数。
  则$|G:1|$表示G的阶。

拉格朗日定理

若H是有限群G的子群，则$|G:1|=|G:H||H:1|$

证明

G的元被分成$|G:H|$个互不相交的右陪集，并且每个右陪集的阶为$|H:1|$。所以结论成立.

置换群

- 一个有限集合Ω到Ω的一个一一映射称为Ω的一个置换。
- 置换的运算是置换的合成，即$(f \circ g)(\alpha) = f(g(\alpha))$。

置换群

- 一个有限集合Ω到Ω的一个一一映射称为Ω的一个置换。
- 置换的运算是置换的合成，即$(f \circ g)(\alpha) = f(g(\alpha))$。
- n个元素的所有置换对于置换合成运算是一个群，
  称为n阶对称群S_n。
  置换群是S_n的子群，它的元素是置换。
- 元素β在置换g下的象记作β^g。
  元素β在置换群G中所有置换下的象的集合称为β的轨道，
  记作β^G。
- 置换群G中不改变元素集$A = \{a_1, \ldots, a_m\}$的置换组成的子群称为G中A的稳定集，记作G_A或$G_{a_1,\ldots,a_m}$。

回顾问题

- 给定$S \subseteq S_n, h \in S_n$，判断是否有$h \in \langle S \rangle$。

回顾问题

- 给定$S \subseteq S_n, h \in S_n$，判断是否有$h \in \langle S \rangle$。
- 下面介绍的Schreier－Sims算法能求出$\langle S \rangle$的基和强生成集，从而解决这两个问题。
- 假设$\Omega = \{1, 2, \ldots, n\}, G = \langle S \rangle \subseteq S_n$。

基和强生成集

- G的基是一个Ω的元素序列$B=(\beta_1,...,\beta_m)$，满足$G_B=1$。

基和强生成集

- G的基是一个Ω的元素序列$B=(\beta_1,...,\beta_m)$，满足$G_B=1$。
- B定义了一个子群链

$$G=G^{[1]}\geq G^{[2]}\geq ...\geq G^{[m]}\geq G^{[m+1]}=1$$

  其中$G^{[i]}=G_{\beta_1,...,\beta_{i-1}}$。
- 如果$\forall 1\leq i\leq m, G^{[i+1]}\neq G^{[i]}$，那么这个基称为无冗余的。

基和强生成集

- G的基是一个Ω的元素序列$B=(\beta_1,...,\beta_m)$，满足$G_B=1$。
- B定义了一个子群链

$$G=G^{[1]}\geq G^{[2]}\geq ...\geq G^{[m]}\geq G^{[m+1]}=1$$

其中$G^{[i]}=G_{\beta_1,...,\beta_{i-1}}$。

- 如果$\forall 1\leq i\leq m, G^{[i+1]}\neq G^{[i]}$，那么这个基称为无冗余的。
- 群G的一个生成集T是群G关于基B的强生成集，如果有

$$\forall 1\leq i\leq m+1, \langle T\cap G^{[i]}\rangle=G^{[i]}$$

即强生成集中必须包含B的子群链中所有子群的生成集。

例子

- $G = S_4$，序列$B = (1, 2, 3)$是G的一个无冗余基。
- 这里$G^{[1]}, G^{[2]}, G^{[3]}$分别是$\{1, 2, 3, 4\}, \{2, 3, 4\}$和$\{3, 4\}$的所有置换的集合，$G^{[4]} = 1$。
- 集合$T_1 = \{(1, 2, 3, 4), (3, 4)\}$
和$T_2 = \{(1, 2, 3, 4), (2, 3, 4), (3, 4)\}$
都是G的生成集。
- T_1不是关于B的强生成集，因为$\langle T_1 \cap G^{[2]} \rangle \neq G^{[2]}$。
而T_2是一个关于B的强生成集。

分解过程

- 假设已经求出了基B和强生成集T，尝试判定h是否属于G。

分解过程

- 假设已经求出了基B和强生成集T，尝试判定h是否属于G。
- 我们用$G^{[i+1]}$的陪集划分$G^{[i]}$。$G^{[i]}$中β_i可能变成$\beta_i^{G^{[i]}}$中的元素，而$G^{[i+1]}$是β_i的稳定集，因此$\beta_i^{G^{[i]}}$中的每个元素对应$G^{[i+1]}$的一个陪集。

分解过程

- 假设已经求出了基B和强生成集T，尝试判定h是否属于G。
- 我们用$G^{[i+1]}$的陪集划分$G^{[i]}$。$G^{[i]}$中β_i可能变成$\beta_i^{G^{[i]}}$中的元素，而$G^{[i+1]}$是β_i的稳定集，因此$\beta_i^{G^{[i]}}$中的每个元素对应$G^{[i+1]}$的一个陪集。
- 对于每个陪集，我们选取一个代表元r来表示陪集$G^{[i+1]}r$。这些代表元的集合记作R_i。

分解过程

- 假设已经求出了基B和强生成集T，尝试判定h是否属于G。
- 我们用$G^{[i+1]}$的陪集划分$G^{[i]}$。$G^{[i]}$中β_i可能变成$\beta_i^{G^{[i]}}$中的元素，而$G^{[i+1]}$是β_i的稳定集，因此$\beta_i^{G^{[i]}}$中的每个元素对应$G^{[i+1]}$的一个陪集。
- 对于每个陪集，我们选取一个代表元r来表示陪集$G^{[i+1]}r$。这些代表元的集合记作R_i。
- R_i可以通过BFS求出：以元素为点，$T \cap G^{[i]}$中的置换为边，从β_i开始BFS。若能到达γ，说明它在$\beta_i^{G^{[i]}}$中。将β_i到γ的路径上的置换依次相乘，得到的就是将β_i变成γ的陪集的代表元。

例子

- $G = S_4, B = (1,2,3), T = \{(1,2,3,4),(2,3,4),(3,4)\}$。
- $G^{[3]} = \{e,(3,4)\}$，它把$G^{[2]}$分成三个陪集

$$G^{[3]}e = \{e,(3,4)\}$$

$$G^{[3]}(2,3) = \{(2,3)(2,3,4)\}$$

$$G^{[3]}(2,4) = \{(2,4)(2,3,4)\}$$

- 因此$R_2 = \{e,(2,3),(2,4)\}$。
  这三个陪集中的置换分别把$\beta_2 = 2$变为2,3和4。

分解过程

- 给定$g \in G$，先找出陪集代表元$r_1 \in R_1$满足$\beta_1^g = \beta_1^{r_1}$；然后令$g_2 = gr_1^{-1} \in G^{[2]}$，找出$r_2 \in R_2$满足$\beta_2^{g_2} = \beta_2^{r_2}$；令$g_3 = g_2 r_2^{-1}$，依次类推。

分解过程

- 给定$g \in G$，先找出陪集代表元$r_1 \in R_1$满足$\beta_1^g = \beta_1^{r_1}$；然后令$g_2 = gr_1^{-1} \in G^{[2]}$，找出$r_2 \in R_2$满足$\beta_2^{g_2} = \beta_2^{r_2}$；令$g_3 = g_2 r_2^{-1}$，依次类推。
- 通过以上分解过程，任意$g \in G$可以唯一表示成$g = r_m r_{m-1} \ldots r_1$的形式，其中$r_i \in R_i$。

分解过程

- 给定$g \in G$，先找出陪集代表元$r_1 \in R_1$满足$\beta_1^g = \beta_1^{r_1}$；然后令$g_2 = gr_1^{-1} \in G^{[2]}$，找出$r_2 \in R_2$满足$\beta_2^{g_2} = \beta_2^{r_2}$；令$g_3 = g_2 r_2^{-1}$，依次类推。
- 通过以上分解过程，任意$g \in G$可以唯一表示成$g = r_m r_{m-1} \ldots r_1$的形式，其中$r_i \in R_i$。
- 尝试用以上方法分解h，若能成功分解则$h \in G$，否则$h \notin G$。

分解过程

- 给定$g \in G$，先找出陪集代表元$r_1 \in R_1$满足$\beta_1^g = \beta_1^{r_1}$；然后令$g_2 = gr_1^{-1} \in G^{[2]}$，找出$r_2 \in R_2$满足$\beta_2^{g_2} = \beta_2^{r_2}$；令$g_3 = g_2 r_2^{-1}$，依次类推。
- 通过以上分解过程，任意$g \in G$可以唯一表示成$g = r_m r_{m-1} \ldots r_1$的形式，其中$r_i \in R_i$。
- 尝试用以上方法分解h，若能成功分解则$h \in G$，否则$h \notin G$。
- 分解失败的情况有两种，
  一是求出的$h_i = hr_1^{-1} r_2^{-1} \ldots r_{i-1}^{-1}$把$\beta_i$换到了$\beta_i^{G^{[i]}}$之外，这个$h_i$称为剩余置换。
  另一种是$h_{m+1} \neq e$，这个h_{m+1}也称为剩余置换。

Schreier引理

- 如果R是G中H的陪集代表元的集合，那么对任意$g \in G$，$Hg \cap R$只有一个元素，用$\overline{g}$表示。

引理

设$H \leq G = \langle S \rangle$，$R$为$G$中$H$的陪集代表元的集合，$e \in R$。那么集合

$$T = \{rs(\overline{rs})^{-1} | r \in R, s \in S\}$$

是H的生成集。

证明

- 由定义，T中元素都属于H，$\langle T\rangle \subseteq H$。
- 任取$h \in H \leq G$，h可以写成$h = s_1 s_2..s_k$的形式，$s_i \in S$。
- 我们定义一个G中元素的序列$h_0, h_1, \ldots, h_k$使得

$$h_j = t_1 t_2 \ldots t_j r_{j+1} s_{j+1} s_{j+2} \ldots s_k$$

其中$t_i \in T, r_{j+1} \in R, h_j = h$。

证明

- 由定义，T中元素都属于H，$\langle T \rangle \subseteq H$。
- 任取$h \in H \leq G$，h可以写成$h = s_1 s_2 .. s_k$的形式，$s_i \in S$。
- 我们定义一个G中元素的序列$h_0, h_1, \dots, h_k$使得

$$h_j = t_1 t_2 \dots t_j r_{j+1} s_{j+1} s_{j+2} \dots s_k$$

  其中$t_i \in T, r_{j+1} \in R, h_j = h$。
- 首先令$h_0 = e s_1 s_2 \dots s_k = h$。
- 如果h_j已定义，
  令$t_{j+1} = r_{j+1} s_{j+1} (\overline{r_{j+1} s_{j+1}})^{-1}, r_{j+2} = \overline{r_{j+1} s_{j+1}}$。
- 显然，$h_{j+1} = h_j = h$，符合上式。
- 我们有$h = h_k = t_1 t_2 \dots t_k r_{k+1}$。由于$h \in H$
  且$t_1 t_2 \dots t_k \in \langle T \rangle \leq H$，一定有$r_{k+1} \in H \cap R = 1$。

证明

- 由定义，T中元素都属于H，$\langle T\rangle \subseteq H$。
- 任取$h \in H \le G$，h可以写成$h = s_1 s_2..s_k$的形式，$s_i \in S$。
- 我们定义一个G中元素的序列$h_0, h_1, \ldots, h_k$使得

$$h_j = t_1 t_2 \ldots t_j r_{j+1} s_{j+1} s_{j+2} \ldots s_k$$

  其中$t_i \in T, r_{j+1} \in R, h_j = h$。
- 首先令$h_0 = e s_1 s_2 \ldots s_k = h$。
- 如果h_j已定义，
  令$t_{j+1} = r_{j+1} s_{j+1} (\overline{r_{j+1} s_{j+1}})^{-1}, r_{j+2} = \overline{r_{j+1} s_{j+1}}$。
- 显然，$h_{j+1} = h_j = h$，符合上式。
- 我们有$h = h_k = t_1 t_2 \ldots t_k r_{k+1}$。由于$h \in H$
  且$t_1 t_2 \ldots t_k \in \langle T\rangle \le H$，一定有$r_{k+1} \in H \cap R = 1$。
- 因此$h \in \langle T\rangle$。综上所述，$H \subseteq \langle T\rangle$。所以$\langle T\rangle = H$。

Schreier - Sims算法

- 我们维护元素序列$B = (\beta_1, \beta_2, \ldots, \beta_m)$，生成集序列$T_1, T_2, \ldots, T_{m+1}$。
- 保证T_i是$\{\beta_1, \ldots, \beta_{i-1}\}$的稳定集，并保证$\langle T_i \rangle \geq \langle T_{i+1} \rangle$对$1 \leq i \leq m$成立，$\langle T_1 \rangle = G, T_{m+1} = 1$。

Schreier - Sims算法

- 我们维护元素序列$B = (\beta_1, \beta_2, \ldots, \beta_m)$，生成集序列$T_1, T_2, \ldots, T_{m+1}$。
- 保证T_i是$\{\beta_1, \ldots, \beta_{i-1}\}$的稳定集，并保证$\langle T_i \rangle \geq \langle T_{i+1} \rangle$对$1 \leq i \leq m$成立，$\langle T_1 \rangle = G, T_{m+1} = 1$。
- 还要维护$\langle T_i \rangle$中$\langle T_i \rangle_{\beta_i}$的陪集代表元集合$R_i$。

- 我们维护元素序列$B = (\beta_1, \beta_2, \ldots, \beta_m)$，生成集序列$T_1, T_2, \ldots, T_{m+1}$。
- 保证T_i是$\{\beta_1, \ldots, \beta_{i-1}\}$的稳定集，并保证$\langle T_i \rangle \geq \langle T_{i+1} \rangle$对$1 \leq i \leq m$成立，$\langle T_1 \rangle = G, T_{m+1} = 1$。
- 还要维护$\langle T_i \rangle$中$\langle T_i \rangle_{\beta_i}$的陪集代表元集合$R_i$。
- 我们使用一个指示器cur，保证$i > cur$时有

$$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$$

从而$(\beta_{cur+1}, \ldots, \beta_m)$是$\langle T_{cur} \rangle$的基，$\bigcup_{cur+1 \leq j \leq m} T_j$ 是$\langle T_{cur} \rangle$ 的强生成集。

- 开始时令$m = 1$，β_1为任意会被S中置换改变的数，$T_1 = S$，$cur = 1$，用BFS求出R_1。

- 开始时令$m=1$，β_1为任意会被S中置换改变的数，$T_1=S$，$cur=1$，用BFS求出R_1。
- 每次判断$i=cur$时$\langle T_i\rangle_{\beta_i}=\langle T_{i+1}\rangle$是否成立。

- 开始时令$m = 1$，β_1为任意会被S中置换改变的数，$T_1 = S$，$cur = 1$，用BFS求出R_1。
- 每次判断$i = cur$时$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$是否成立。
- 根据我们的保证，$\langle T_{cur} \rangle_{\beta_{cur}} \supseteq \langle T_{cur+1} \rangle$成立，只要判断$\langle T_{cur} \rangle_{\beta_{cur}} \subseteq \langle T_{cur+1} \rangle$ 是否成立。
- 我们利用Schreier引理求出$\langle T_{cur} \rangle_{\beta_{cur}}$的生成集$T'$，并利用分解过程判断是否有$T'$中的每个元素都属于$\langle T_{cur+1} \rangle$。

Schreier－Sims算法

- 如果$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$成立，可以将$cur$减1。

- 如果$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$成立，可以将$cur$减1。
- 如果不成立，有T'中的元素$h \notin \langle T_{cur+1} \rangle$。将$h$在分解过程中得到的剩余置换加入$T_{cur+1}$。
  若$cur = m$，我们要任选会被S_{cur}改变的元素作为β_{m+1}。重新进行BFS更新R_{cur+1}。
  现在$i = cur + 1$时$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$不一定成立，需要将$cur$加1。

Schreier - Sims算法

- 如果$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$成立，可以将$cur$减1。
- 如果不成立，有T'中的元素$h \notin \langle T_{cur+1} \rangle$。将$h$在分解过程中得到的剩余置换加入$T_{cur+1}$。
  若$cur = m$，我们要任选会被S_{cur}改变的元素作为β_{m+1}。重新进行BFS更新R_{cur+1}。
  现在$i = cur + 1$时$\langle T_i \rangle_{\beta_i} = \langle T_{i+1} \rangle$不一定成立，需要将$cur$加1。
- 重复以上过程，直至$cur = 0$，我们就得到了G的基B和强生成集$T = \bigcup_{1 \le j \le m} T_j$。

复杂度分析

- 基的大小最多为n。每个T_i最多改变n次，因为每次改变后β_i的轨道都会增加一个元素。

复杂度分析

- 基的大小最多为n。每个T_i最多改变n次，因为每次改变后β_i的轨道都会增加一个元素。
- 如果已经知道$\langle T_{cur} \rangle_{\beta_{cur}}$的生成集的某个元素属于$\langle T_{cur+1} \rangle$，之后就不必再对它执行分解过程。
  因此对于每个$1 \le cur \le m$ 都只要进行$O(|R_{cur}||T_{cur}|) = O(n^2)$次分解操作。
  每次分解过程需要$O(n^2)$。

复杂度分析

- 基的大小最多为n。每个T_i最多改变n次，因为每次改变后β_i的轨道都会增加一个元素。
- 如果已经知道$\langle T_{cur} \rangle_{\beta_{cur}}$的生成集的某个元素属于$\langle T_{cur+1} \rangle$，之后就不必再对它执行分解过程。
  因此对于每个$1 \le cur \le m$ 都只要进行$O(|R_{cur}||T_{cur}|) = O(n^2)$次分解操作。
  每次分解过程需要$O(n^2)$。
- 总的时间复杂度是$O(n^5)$。
  如果群的大小为$|G|$，时间复杂度也可以表示成$O(n^2 \log^3 |G|)$。
- 在实际运行中算法的常数很小，一般不需要这么多操作。
  我的程序能在2秒内跑出$n = 100$的数据。

复杂度分析

- 基的大小最多为n。每个T_i最多改变n次，因为每次改变后β_i的轨道都会增加一个元素。
- 如果已经知道$\langle T_{cur}\rangle_{\beta_{cur}}$的生成集的某个元素属于$\langle T_{cur+1}\rangle$，之后就不必再对它执行分解过程。
  因此对于每个$1 \le cur \le m$ 都只要进行$O(|R_{cur}||T_{cur}|) = O(n^2)$次分解操作。
  每次分解过程需要$O(n^2)$。
- 总的时间复杂度是$O(n^5)$。
  如果群的大小为$|G|$，时间复杂度也可以表示成$O(n^2 \log^3 |G|)$。
- 在实际运行中算法的常数很小，一般不需要这么多操作。
  我的程序能在2秒内跑出$n = 100$的数据。
- 空间复杂度是$O(n^3)$。

求阶

- 应用：给定置换集合S，求$|\langle S\rangle|$。

求阶

- 应用：给定置换集合S，求$|\langle S\rangle|$。
- 我们用Schreier－Sims算法求出$\langle S\rangle$的基B。B定义了一个子群链

$$G = G^{[1]} \geq G^{[2]} \geq \ldots \geq G^{[m]} \geq G^{[m+1]} = 1$$

求阶

- 应用：给定置换集合S，求$|\langle S\rangle|$。
- 我们用Schreier－Sims算法求出$\langle S\rangle$的基B。B定义了一个子群链

$$G = G^{[1]} \geq G^{[2]} \geq \ldots \geq G^{[m]} \geq G^{[m+1]} = 1$$

- 由拉格朗日定理，

$$|G| = \prod_{i=1}^{m} |G^{[i]} : G^{[i+1]}|$$

- 而$G^{[i]}$中$G^{[i+1]}$的陪集个数就是$|R_i|$。

求阶

- 应用：给定置换集合S，求$|\langle S\rangle|$。
- 我们用Schreier－Sims算法求出$\langle S\rangle$的基B。B定义了一个子群链

$$G = G^{[1]} \geq G^{[2]} \geq \ldots \geq G^{[m]} \geq G^{[m+1]} = 1$$

- 由拉格朗日定理，

$$|G| = \prod_{i=1}^{m} |G^{[i]} : G^{[i+1]}|$$

- 而$G^{[i]}$中$G^{[i+1]}$的陪集个数就是$|R_i|$。
- Schreier－Sims算法求出了R_i，我们直接求$\prod_{i=1}^{m} |R_i|$即可。

总结

- Schreier－Sims算法是计算群论的基本算法。
- 还有一些更优秀的类似算法以及对该算法的优化，由于本人水平有限，以及考虑到在OI中的实现难度不作介绍。

总结

- Schreier－Sims算法是计算群论的基本算法。
- 还有一些更优秀的类似算法以及对该算法的优化，由于本人水平有限，以及考虑到在OI中的实现难度不作介绍。
- 该算法实际上清晰地表示出了置换群的结构，因此可以方便地完成成员性判定、求阶等任务。

总结

- Schreier – Sims算法是计算群论的基本算法。
- 还有一些更优秀的类似算法以及对该算法的优化，由于本人水平有限，以及考虑到在OI中的实现难度不作介绍。
- 该算法实际上清晰地表示出了置换群的结构，因此可以方便地完成成员性判定、求阶等任务。
- 但是该算法是个一般化的算法，并没有利用具体的置换群的特殊性质，因此时间复杂度较大。我们在面对具体问题的时候要挖掘题目的特殊性质再设计算法。

- 谢谢大家。
- 欢迎提问。