关于两个问题的一些研究

2011 级 ACM 班陈楠昕 5110309028

April 24, 2012

摘要:本文主要研究了对称群及置换群中的正规子群问题以及 Todd Coxeter 算法实现问题

关键词:**60 阶单群,Sn,对称群,An,置换群,Sn 正规子群,An 正规子群,Todd-Coxeter,Schreier graph,HLT plus lookahead,Felsch method ,Light,统筹,结合律测试,有限群生成**

Contents

Part I

理论研究

Chapter 1

对称群 Sn 以及置换群 An 的一些性质

Lemma 1. *任意两个正规子群交必为原群正规子群。*

Proof. 设群 H、M 皆为群 G 正规子群,即 $H,M \trianglelefteq G$,根据定义有

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H$$
$$\forall g \in G, \forall m \in M, gmg^{-1} \in M$$

则考虑群 $H \cap M$,显然 $\forall a \in H \cap M$, 有

$$\forall g \in G, gag^{-1} \in H, gag^{-1} \in M \Rightarrow gag^{-1} \in H \cap M$$

□

Lemma 2. *一个正规子群必为包含它的子群的正规子群。*

Proof. 设群 H 为群 G 正规子群,即 $H \trianglelefteq G$,根据定义有

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H$$

设 $H \leq M \leq G$,则显然有

$$\forall m \in M \leq G, \forall h \in H, mhm^{-1} \in H$$

□

Theorem 3. *对于置换群 A_n,其正规子群为* $\begin{cases} \{1\} & n = 1, 2 \\ \{1\}, A_n & n = 3 \\ \{1\} & n = 4 \\ \{1\}, A_n & n \geq 5 \end{cases}$

Proof. 对于 A_1, A_2, A_3,易见结论显然成立。

考虑群 A_4,非平凡子群共有 8 个:

- $\{(1), (12)(34)\}$
- $\{(1), (13)(24)\}$
- $\{(1), (14)(23)\}$
- $\{(1), (123), (132)\}$
- $\{(1), (124), (142)\}$
- $\{(1), (134), (143)\}$
- $\{(1), (234), (243)\}$
- $B_4 \triangleq \{(1), (12)(23), (13)(24), (14)(23)\}$

我们一一验证即发现只有 B_4 是 A_4 的正规子群。

对于 $n \geq 5$ 的情况, A_n 皆为单群,这里证明略,详情见 [**?**]$P78$ 页。

□

Fact 4. *任意两个奇置换乘积为偶置换。*

Theorem 5. *对于对称群 S_n,其正规子群为* $\begin{cases} \{1\} & n=1,2 \\ \{1\},A_n,S_n & n=3 \\ \{1\},B_4,A_4,S_4 & n=4 \\ \{1\},A_n,S_n & n\geq 5 \end{cases}$

Proof. 对于群 S_1,S_2,结论显然成立。

下面往证对于 $n\geq 3,n\neq 4$ 时结论成立,即 S_n 只有 $\{1\},A_n,S_n$ 这三个正规子群。设

$$H\trianglelefteq S_n,H\neq\{1\},H\neq S_n$$

由引理**??**知, $H\cap A_n\trianglelefteq S_n$。

由引理**??**知, $\because A_n\trianglelefteq S_n\therefore H\cap A_n\trianglelefteq A_n$

由定理**??**知,在这种情况下, $H\cap A_n=\{1\}orA_n$。

若 $H\cap A_n=\{1\}$,则考虑 $H\setminus\{1\}$,必全部为奇置换,且应用事实**??**可知

$$\forall x,y\in H\setminus\{1\},x\times y=1$$

考虑 $x=y$ 的情况,显然有

$$x\times x=x\times y=1,\forall y\in H\setminus\{1\}$$

所以 $H\setminus\{1\}$ 中任意两个奇置换均相等。那么我们不妨假设他们都等于 z,且

$$z=(ij)\cdots\cdots$$

然后设 $\sigma=(jk)$,其中 $k\neq j$,根据秘密武器有

$$\sigma z\sigma^{-1}=(ik)\cdots\cdots$$

因为是正规子群,所以有

$$\sigma z\sigma^{-1}\in H\Rightarrow\sigma z\sigma^{-1}=(ij)\cdots\cdots$$

矛盾,所以必然有 $H\cap A_n=A_n$。

而对于 $n=4$ 的情况,我们只须找出所有共轭类,取若干共轭类之并,逐个验证即可。

□

Chapter 2

60 阶单群性质

2.1 唯一性证明

Fact 6. *若* $H = \langle x \rangle$ 且 $H \leq G$，*其中* $|G| < \infty$，*若* $N_G(H) = \langle y \rangle$，*则* $\forall g \in G, gHg^{-1} \neq H \Rightarrow N_G\left(gHg^{-1}\right) = \langle z \rangle$，且 $|\langle y \rangle| = |\langle z \rangle|$。

Proof. 取 $z = gyg^{-1}$ 即可，则 $\langle z \rangle = \left\{gy^n g^{-1} | 0 \leq n < |\langle y \rangle|\right\}$，易见大小与 $\langle y \rangle$ 相同。

□

Fact 7. *若* $H = \langle x \rangle$ 且 $H \leq G$，*其中* $|G| < \infty$，*那么* $\forall g \in G, gHg^{-1} \neq H \Rightarrow N_G(H) \cap N_G\left(gHg^{-1}\right) = \{1\}$。

Proof. $gHg^{-1} = \left\langle gxg^{-1} \right\rangle$，若 $\exists y \in G, y \neq 1, yHy^{-1} = H$ 且 $ygHg^{-1}y^{-1} = gHg^{-1}$，则

$$yg \in N_G(H)$$

而由 $yHy^{-1} = H$，$(yg) H (yg)^{-1} = H$，知 $(y^n g) H (y^n g)^{-1} = H$，即 $y^n g \in N_G(H)$，从而可得 $g \in N_G(H)$，矛盾。

□

Theorem 8. 60 *阶单群在同构意义下只有一个。*

Proof. 设 G 是一个单群，故 G 的非单位同态像一定是同构像。考虑 G 的任意真子群左 (右) 陪集在乘法作用下的置换群，一定与 G 同构。$\because |G| \geq 4! \therefore \forall H \leq G, [G:H] \geq 5$。下面给出两种证明：

1. 设 n_2 为 G 中 $Sylow-2$ 子群个数，n_3 为 G 中 $Sylow-3$ 子群个数，n_5 为 G 中 $Sylow-5$ 子群个数。
   由 Sylow 定理可知有如下关系式：

$$\begin{cases} n_2 \mid 15 & n_2 \equiv 1(MOD\,2) \\ n_3 \mid 20 & n_3 \equiv 1(MOD\,3) \\ n_5 \mid 12 & n_5 \equiv 1(MOD\,5) \end{cases}$$

   由上可推出

$$\begin{aligned} n_2 &= 5\,or\,15 \\ n_3 &= 10 \\ n_5 &= 6 \end{aligned}$$

   下面证明 $n_2 \neq 15$。$\forall x \in G, order(x) = 2$，考虑其中心化子个数，即 $Z_G(x)$。因为有 $Z_G(x) \leq G$，
   若 $5 \mid |Z_G(x)|$，即 $Z_G(x)$ 中存在 5 阶元，不妨设为 y，则 $x \times y$ 为 10 阶元，且有

$$(x \times y) \langle y \rangle (x \times y)^{-1} = \langle y \rangle$$

   则 $N_G(\langle y \rangle)$ 中至少有 4 个 10 阶元，并且由事实**??**及事实**??**，知 10 阶元个数至少有 $4 \times 6 = 24$ 个。而 3 阶元共 $2 \times 10 = 20$ 个，5 阶元共 $4 \times 6 = 24$ 个，则 G 中至少有 $24 + 20 + 24 = 68$ 个元素，矛盾，所以 $5 \nmid |Z_G(x)|$。
   若 $3 || Z_G(x)|$，即 $Z_G(x)$ 中存在 3 阶元，同理可导出矛盾，所以 $3 \nmid |Z_G(x)|$。所以 $|Z_G(x)| \mid 4$。所以与 x 共轭的元素至少有 15 个，已知元素共 $20 + 24 + 15 + 1 = 60$ 个，所以 G 中共有 1 阶元 1 个，2 阶元 15 个，3 阶元 20 个，5 阶元 24 个。

   若 $n_2 = 15$，下面说明任意两个交只有 $\{1\}$。设 $|K1| = |K2| = 4$，$\exists y \neq 1$，$y \in K1\,and\,y \in K2$，因为 y 必为 2 阶元，而 4 阶群为交换群，所以 $K1$、$K2$ 中所有元素皆为 y 正规化子，则至少有 6 个，矛盾。所以 15 个 $Sylow-2$

子群至少包含 $15 \times 3 = 45$ 个,因此 $n_2 = 5$。对于这 5 个子群左 (右) 陪集在乘法作用下的置换群同构于 S_5 的一个子群,而 S_5 中的 60 阶子群必为正规子群 (指数为 2),再由定理**??**知 $G \cong A_5$。

2. 同理可证 $n_3 = 10$,$n_5 = 6$。下面证明 G 有指数为 5 的子群。
若 $n_2 = 5$,则 G 的 $Sylow - 2$ 子群正规化子指数为 5;
若 $n_2 = 15$,易见存在两个 $Sylow - 2$ 子群 $P1$、$P2$ 交不为单位子群,即为 2 阶子群 A。因为 4 阶群都是交换群,所以

$$P1、P2 \leq Z_G(A) < G$$

因此 $Z_G(A)$ 的阶数是 4 的倍数且大于 4,又不能等于 3,因此为 5。
综上所述存在一个指数为 5 的子群,按子群陪集的在乘法作用下同构于 S_5 的一个子群,同上有 $G \cong A_5$。

□

2.2 实例

Part II

算法及其实现

Chapter 3

Todd-Coxeter 算法

关于 Todd-Coxeter 算法本身，在课堂上已经有详细介绍。但是对于 Todd-Coxeter 算法的实现，我一直留有疑惑。经过查阅相关资料，我发现目前来看并没有特别好的方法实现，而难点主要体现在以下两个方面：

- 对于一个读入我们无法判断什么时候终止。特别如果群 G 是无限群，能在有限步内终止，但是对于时间复杂度方面不好保证。
- 处理比较大的数据时不能盲目设置变量，以防图太大不好处理。

目前知道的最好做法以及程序具体实现参考的是 [**?**]

3.1 Schreier Graph

首先 Todd-Coxeter 算法在实现中是用 Schreier graph 来表示的。我们用一个例子来说明：

考虑群

$$G :=< a, b; a^3 = b^3 = (ab)^2 = 1 >$$

以及子群

$$H :=< a >\leq G$$

考虑群作用 G/H,我们用红色键头表示作用 a,蓝色键头表示作用 b。在 Schreier Graph 中每个点每种颜色的边入度为 1,出度为 1,对应群作用映射。Todd-Coxeter 算法目标是我们要逐渐增加点与边,使得整个图每个点每种颜色边出度入度均为 1,且图中任意一条生成关系 (例如 $abab$) 对应路径形成一个封闭的环。

首先我们将 H 定义为 1,考虑到有 $a \in H$,于是有下图:

两条蓝色的边提醒我们存在两个点与 b 作用相关,但是我们目前没有给他们命名。

接着我们对于 1 考虑三种关系:

- 1 在 a 作用下不变,所以原图 1 满足 a^3 封闭;
- 为了满足 b^3,我们定义 2、3,分别为 $2 := 1 \times b$,$3 := 2 \times b$,关系 b^3 告诉我们这三个点形成蓝色封闭三角形。于是我们得到下图:

- 检查 1 处关系 $abab$,已经出现的有:

于是可以推断 $2 \times a = 3$,进而得到下图:

重复这些步骤,最终可得到:

3.2 HLT && Felsch

上面的例子相对来说是一个非常简单的例子,因为我们没有发现任何两个量相同。更加一般的情况下我们经常碰到设置了多个值相同的量,这时候我们需要把图中一些点合并。

在数据规模比较大的情况下为了控制图的大小，我们得采取一些方法。

Bibliography

[1]《The Todd – Coxeter procedure》,from Ken Brown, Cornell University, April 2011

[2]《应用近世代数》,from 胡冠章,王殿军,July 2006

[3]《有限群基础》,from 王萼芳,Sep 2002