Todd – Coxeter 算法的证明

刘文海,李忠森
(福建对外经济贸易职业技术学院,福建 福州 350016)

摘 要: 提出了 Todd – Coxeter 算法在有限步内终止的条件,并作出了论证. 结论可以作为 Todd – Coxeter 算法应用的理论依据.

关键词: 群论; 群作用; Todd – Coxeter; 陪集枚举
中图分类号: O29; TP301.6 **文献标识码:** A **文章编号:** 1008 – 4681(2013)05 – 0005 – 02

Todd 和 H. S. M. Coxeter 在 1936 年发明了最原始的陪集列举算法[1]. Todd – Coxete 算法是一种枚举策略,能有效地解决陪集列举问题. 当时还没有计算机,人们还没有发现其中的价值. 该算法是一种机械式的,不需要用到任何思维的技巧. 因此在计算机问世之后,该算法顺利地在计算机上实现,很受欢迎. 之后有很多对原始 Todd – Coxeter 算法的改进被提出,其中的经典代表作有 V. Felsch、HLT(Haselgrove, Leech 和 Trotter) 和 lookahead.

陪集列举最大的难点在于,只能证明在有限阶群下是可以结束的[2]. 但是到目前为止,仍不能预测需要多少内存,需要多少时间算法会结束. 如果一个群是有限群,虽然最后必然会结束,但在过程中可能花任意长的时间,用任意多的存储空间. 此外,找不到一个最适合的群表示,使算法运行最优. 也就是说,对于同一个群,不同的群表示,算法所花的时间和存储空间有可能迥然不同.

1 算法描述

设 H 是有限群 G 的一个子群. Todd – Coxeter 算法是一个计算 H 在 G 中的陪集个数和确定 G 在陪集上作用的直接方法.

群 G 和子群 H 都要以具体的方式给出,考虑一个群

$$G = \langle x_i \mid i \in I; r_k \mid k \in K \rangle$$

由生成元 x_i 和关系 r_k 表示. 这样的 G 实现为一个商群 F/N,其中 F 是集合 $\{x_i \mid i \in I\}$ 上的自由群,而 N 是 $\{r_k \mid k \in K\}$ 的最小正规闭包. 假设 G 的子群 H 由一个在自由群 F 中的子集合 $\{h_j \mid j \in J\}$ 生成.

对于 $[G:H] < \infty$ 的情况,Todd – Coxeter 算法可以给出陪集的个数及它们之间的关系.

建立一个陪集的乘法表,用行表示陪集的标号,列表示 G 的生成元及它们的逆:

	x_1	x_2	x_3	…	x_1^{-1}	x_2^{-1}	x_3^{-1}	…
1								
2								
3								
⋮								

(1) 用标号 1 来表示子群 H,把子群的生成元 h_j 应用在陪集 1 上得到 1. $h_j = 1(\forall j \in J)$,在此过程中根据需要定义新的陪集.

(2) 对数列 1,2,3,…中的任意陪集 m.

a. 如果陪集 mx_i 和 $mx_i^{-1}(\forall i \in I)$ 没有被定义过,那么为它们定义新的陪集.

b. 把 G 中的关系应用在陪集 m 上,得到 $mr_k = m(\forall k \in K)$,在此过程中根据需要定义新的陪集.

注意到(1)和(2)中新定义的任何陪集都由前面定义过的陪集乘以一个生成元 x_i 或一个生成元的逆来定义. 同时 $mx_i^{\varepsilon} = n$ 表明 $nx_i^{-\varepsilon} = m$,其中 $\varepsilon \in \{1, -1\}$.

(3) 冲突问题. 如果表格中的一个格子可以有两个标号,则说明两个标号代表同一个陪集,则将它们合并,用较小的标号代替较大的标号.

最后,一个陪集的标号应该选择最小的可以使用的自然数,这就是 Todd – Coxeter 算法. 当 G 和 H 为可有限表示群且 H 在 G 中的陪集个数有限时,可以证明 Todd – Coxeter 算法在有限步结束.

2 算法证明

引理 1 设 F 为自由群,$H = \langle h_j \mid j \in J \rangle$ 为 F 中的有

* 收稿日期:2013 – 05 – 24
作者简介:刘文海(1962 –),男,福建南安人,福建对外经济贸易职业技术学院副教授. 研究方向:算法分析、数据挖掘.

限生成子群. $\{x_i \mid i \in I\}$ 是 F 的生成元集合. 若恒等式 $Hh_j = H(\forall j \in J)$, $Hgx_i^{\varepsilon_i}x_i^{-\varepsilon_i} = Hg(\forall Hg \in F/H, \forall i \in I, \varepsilon_i = \pm 1)$ 成立,则可以判断任意两个陪集是否相等.

证明 设陪集 $H\mu = H\nu$,其中 μ 和 ν 是由 F 的生成元组成的字. 那么 $\mu\nu^{-1} \in H$,既 $\mu\nu^{-1} = h_{j_1}^{\varepsilon_1}h_{j_2}^{\varepsilon_2}\cdots h_{j_n}^{\varepsilon_n}$,$\{j_i\}_{i=1,2,\cdots,n} \in J$,$\{\varepsilon_i\}_{i=1,\cdots,n} \in \{-1,1\}$.

若 $Hh_j = H(\forall j \in J)$,则 $H\mu\nu^{-1} = H$. 再由 $Hgx_i^{\varepsilon_i}x_i^{-\varepsilon_i} = Hg$,得 $H\mu = H\nu$. 所以只要 $Hh_j = H(\forall j \in J)$ 和 $Hgx_i^{\varepsilon_i}x_i^{-\varepsilon_i} = Hg(\forall Hg \in F/H, \forall i \in I, \varepsilon_i = \pm 1)$ 成立,就可以找出所有相等的陪集.

引理2 有限生成子群 $H = <h_j \mid j \in J>$,在有限生成群 $G = <x_i \mid i \in I; r_k \in K>$ 中的指数可数. 若恒等式 $Hh_j = H(\forall j \in J)$, $Hgr_k = Hg(\forall k \in K)$, $Hgx_i^{\varepsilon_i}x_i^{-\varepsilon_i} = Hg(\forall Hg \in F/H, \forall i \in I, \varepsilon_i = \pm 1)$ 成立,则可以判断任意两个陪集是否相等.

证明 命题等价于列举由集合 $\{h_j \mid j \in J\}$ 和 $N(\{r_k \mid k \in K\}$ 的最小正规闭包) 生成的子群 H' 在自由群 $F = <x_i \mid i \in I>$ 中的陪集. H' 的生成元集是

$$\{h_j \mid j \in J\} \cup \{w^{-1}r_kw \mid k \in K, w \in <x_i \mid i \in I>\}$$

$w^{-1}r_kw$ 是上述子群的生成元,等价于 $H'gr_K = H'g$,其中 $H'g$ 为陪集 $H'w^{-1}$. 为了证明命题,只需检查对任意关系 r_k,任意陪集 $H'g$,有 $H'gr_k = H'g$. 因此,在引理1给出的几个恒等式中加入 $Hgr_k = Hg$ 就可以判断任意两个陪集是否相等.

定理 有限生成子群 $H = <h_j \mid j \in J>$,在有限生成群 $G = <x_i \mid i \in I; r_k \in K>$ 中的指数有限. 那么 Todd – Coxeter 算法可以在有限步结束.

证明 由步骤(2)a 可以知道:任意一个陪集 Hg 都会在有限步之后被标号. 根据引理2,可以合并所有代表同一个陪集的标号,这时算法就结束了.

Todd – Coxeter 算法的陪集计数,已经成为了研究有限群的基本工具,在数学界和计算机界广泛应用,包括由生成元和其关系能得到群的结构,计算小的有限李群的舒尔乘子,通过已知子群 H,K 的陪集表计算重陪集 $H \times K$,和决定一个子群的陪集代表元的集合. 而 Todd – Coxeter 的基本思想被应用到了其他领域,产生了很多类似算法.

参考文献:

[1] Todd J A, Coxeter H S M. A practical method for enumerating cosets of a finite abstract group[A]. Proceedings of the Edinburgh Mathematical Society[C]. Cambridge: Cambridge University Press,1936.

[2] Beetham M J, Campbell C M. A note on the Todd – coxeter coset enumeration algorithm[A]. Proceedings of the Edinburgh Mathematical Society[C]. Cambridge: Cambridge University Press, 1976.

The Proving of Todd – Coxeter Algorithm

LIU Wenhai, LI Zhongsen

(Fujian International Business & Economic College, Fuzhou Fujian 350016, China)

Abstract: The paper has put forward the condition to terminate the Todd – Coxeter algorithm within finite steps and also proves it. The theorem can be used as the theoretical basis of the application of Todd – Coxeter algorithm.

Key Words: group theory; action of group; Todd – Coxeter; coset enumeration

(责任编校:晴川)