

求特殊射影线性群 $PSL(2, q)$ 的元阶集的搜索算法^{*}The Search Algorithm for Set of Element Orders Set of Projective Special Linear Group $PSL(2, q)$ 王志刚¹ 王绍恒²(湖南师范大学理学院 长沙410081)¹ (重庆三峡学院计算机科学系 重庆404000)²

Abstract In this paper, in order to find a set of element orders of projective special liner group $PSL(2, q)$ and numbers of elements every order and order of group, we give a search algorithm and discuss complexity of the algorithm.

Keywords Finite group, Order of group, Order of element, Matrix, Algorithm

1 引言

设群 G 是一个有限群, 以 $\pi_e(G)$ 表示群 G 的元阶集^[1], 在文[1~3]中, 给出了用 $\pi_e(G)$ 刻画群 G 的性质的方法, 在这些刻画中, 通常要先计算已知群的元阶集 $\pi_e(G)$ 及各阶元的个数, 对于特殊射影线性群 $G = PSL(2, q)$ (其中 q 为素数) 而言, 已有了求 $\pi_e(G)$ 的公式, 但还没有求各阶元的个数的公式, 各阶元的代表元及群的阶的公式, 本文给出求以上各项数值的搜索算法, 并讨论了算法复杂性。

设 q 为素数, 域 $F = GF(q)$, 则 F 上全体二级可逆方阵的全体对矩阵乘法组成全线性群 $GL(2, q)$, 而 F 上全体行列式为1的二级可逆方阵的全体对矩阵乘法组成特殊线性群 $SL(2, q)$, 设 $GL(2, q)$ 的中心为 Z , 则 Z 由 F 上全体二级非零纯量阵组成, 令 $D = Z \cap SL(2, q)$, 则特殊射影线性群 $PSL(2, q) = SL(2, q)/D$, 由商群的构造知 $PSL(2, q)$ 中元的形式为 Dx , 其中 x 为 F 上行行列式为1的二级非零纯量阵:

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_q = \begin{pmatrix} q-1 & 0 \\ 0 & q-1 \end{pmatrix}$$

下面讨论 $PSL(2, q)$ 的元的阶的求法, 因为 $PSL(2, q)$ 中的单位元为 D , 而 $(Dx)^r = D$ 当且仅当 $Dx^r = D$, 即 $x^r \in D$, 也就是

$$x^r = E_1 \text{ 或 } x^r = E_q \quad (1)$$

可见, 要求 Dx 的阶, 只需求满足条件(1)的最小正整数 r 即可。又当 x 取遍 $SL(2, q)$ 中所有元时, Dx 取遍 $PSL(2, q)$ 中所有元, 且 $SL(2, q)$ 中每两个元 x 及 $E_q x$ 对应 $PSL(2, q)$ 中同一个元 Dx , 因此下文中统计出的 $SL(2, q)$ 中行行列式为1的 x 的个数的一半就是 $PSL(2, q)$ 中相应元 Dx 的个数。 $SL(2, q)$ 的元可如下构造:

由于 $F = GF(q)$ 与模 q 的剩余类环 Z_q 同构, 取 $x = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $a_{i,j} \in Z_q$, 则 $x \in SL(2, q)$ 当且仅当 $\det(x) \equiv 1 \pmod{q}$ 。在计算中, 只需对 $a_{i,j}$ 循环取值0到 $q-1$, 对每一个 x 求其行列式的值并对模 q 取余, 结果为1者就是 $SL(2, q)$ 中的元素。

2 算法分析

为使结构清晰, 下面以主程序及其过程的方式说明求 $\pi_e(G)$ 及各阶元的个数, 各阶元的代表元及群的阶的算法。

过程1: 求矩阵 x 的行列式 $\det(x) = a_{11}a_{22} - a_{12}a_{21}$ 按模 q 取余, 若值为1, 则令 $Determinant(x)$ 取1, 否则取0。

过程1.1: 求矩阵 x 与 y 的乘积并把值赋给矩阵 y 。

过程2: 求 Dx 的阶。

若 $x = E_1$ 或 $x = E_q$, 则取 $r = 1$ 。否则

取 $r = 1$, 矩阵 y 取初值 x 。

循环开始

$r = r + 1$

调用过程2.1求矩阵 x 与 y 的乘积并把结果赋给矩阵 y 。

若 $y = E_1$ 或 $y = E_q$, 则 r 即为 x 的阶, 跳出循环; 否则继续循环。

循环结束。

过程3: 求元阶集 $\pi_e(G)$, 统计各阶元的个数及群的阶, 记录各阶元的代表元。

以数组 $paieg()$ 记录元的阶之集, 以 k 记录元阶集中元素的个数, 由于单位元是1阶元, 可令初值 $k = 1$; $paieg(1) = 1$ 。用数组 $Number()$ 记录 $PSL(2, q)$ 中各个相同阶的元对应于 $SL(2, q)$ 中元的个数, 用数组 $Element()$ 记录各阶元的一个代表元素对应的矩阵。

由过程2求出 Dx 的阶 r 后, 将 r 与数组 $paieg()$ 中各元进行比较, 如果数组 $paieg()$ 中第 k 个元素与 r 相同, 表明阶为 r 的元已在此之前出现过, 赋值使 r 阶元的个数增1: $Number(k) = Number(k) + 1$ 。如果 $paieg()$ 中没有一个与 r 相同, 表明找到第一个 r 阶元, 把 r 放到数组 $paieg()$ 中, 并以该 x 作为 r 阶元的代表, 赋值: $k = k + 1$, $paieg(k) = r$, $Number(k) = 1$, $Element(k) = x$ 。

过程4: 输出结果。

i 从1到 k 循环, 输出 $paieg(i)$ 就得 $\pi_e(G)$ 。

i 从1到 k 循环, 输出 $Number(i)/2$ 就得各阶元的个数。

i 从1到 k 循环, 输出 $Element(i)$ 就得各阶元的代表元素对应的

二级矩阵。

输出群 $PSL(2, q)$ 的阶 $Matrixnumber/2$ 。

主程序:

定义有关数组。

输入奇素数 q 。

循环: $a_{11}, a_{12}, a_{21}, a_{22}$ 分别从0到 $q-1$ 取值产生一个矩阵 $x = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 。

调用过程1, 求出 $Determinant(x)$ 。

如果 $Determinant(x) = 1$, 令 $Matrixnumber = Matrixnumber + 1$ (统计 $SL(2, q)$ 中行行列式为1的矩阵个数), 同时调用过程2求 Dx 的阶 r 。

调用过程3更新元阶集 $paieg()$; 统计 r 阶元的个数; 记录第一次出现的 r 阶元对应的矩阵。

循环结束。

调用过程4输出统计结果。

3 实例

例1 设 $G = PSL(2, 7)$, 由上述算法求得 $\pi_e(G) = \{1, 2,$

$3, 4, 7\}$, $x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 对应1阶元 Dx_1 , $x_2 = \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix}$ 对应2阶元

Dx_2 , $x_3 = \begin{pmatrix} 0 & 1 \\ 6 & 1 \end{pmatrix}$ 对应3阶元 Dx_3 , $x_4 = \begin{pmatrix} 0 & 1 \\ 6 & 3 \end{pmatrix}$ 对应4阶元

Dx_4 , $x_5 = \begin{pmatrix} 0 & 1 \\ 6 & 2 \end{pmatrix}$ 对应7阶元 Dx_5 。其中 $D = \{E_1, E_q\}$, 而 $E_1 =$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ 及 } E_q = \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}。$$

各阶元个数如下:

1阶元1个; 2阶元21个; 3阶元56个; 4阶元42个; 7阶元48个, 群的阶为168。

^{*} 本课题受湖南省青年骨干教师基金资助。王志刚 副教授, 主要从事算法和网络的教学与研究工作。

例2 设 $G=PSL(2,17)$, 由上述算法求得 $\pi_r(G)=\{1,2,3,4,8,9,17\}$,

$x_1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 对应1阶元 Dx_1 , $x_2=\begin{pmatrix} 0 & 1 \\ 16 & 0 \end{pmatrix}$ 对应2阶元 Dx_2 , $x_3=\begin{pmatrix} 0 & 1 \\ 16 & 1 \end{pmatrix}$ 对应3阶元 Dx_3 , $x_4=\begin{pmatrix} 0 & 1 \\ 16 & 6 \end{pmatrix}$ 对应4阶元 Dx_4 , $x_5=\begin{pmatrix} 0 & 1 \\ 16 & 5 \end{pmatrix}$ 对应8阶元 Dx_5 , $x_6=\begin{pmatrix} 0 & 1 \\ 16 & 3 \end{pmatrix}$ 对应9阶元 Dx_6 , $x_7=\begin{pmatrix} 0 & 1 \\ 16 & 2 \end{pmatrix}$ 对应17阶元 Dx_7 . 其中 $D=\{E_1, E_9\}$, 而 $E_1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 及 $E_9=\begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}$.

各阶元个数如下:

1阶元1个; 2阶元153个; 3阶元272个; 4阶元306个; 8阶元612个; 9阶元816个; 17阶元288个; 群的阶为2448.

4 复杂度分析

本算法的输入尺寸由 q 决定, 算法执行的运算次数取决于 q 的大小. 下面只对在最坏情况下的时间复杂度作粗略的估计.

在过程一中, 求一个二级矩阵的行列式要2次乘法, 主程序中由于二级矩阵的4个元分别从0到 $q-1$ 循环, 共调用过程一 q^4 次, 共计算了 $2q^4$ 次乘法.

特殊线性群 $SL(2, q)$ 的阶为 $q(q^2-1)$, 说明其中行列式为1的矩阵 x 有 $q(q^2-1)$ 个, 每个这样的矩阵都要调用过程二求 x 的阶. 在求阶过程中每个 r 阶元 x 要进行矩阵乘法 $r-1$ 次, 每次矩阵乘法要进行8次数的乘法, 在最坏情况下 r 取 q

(q^2-1) (而在平均情况下 r 取 q), 因此最坏要进行 $8q(q^2-1)$ 次乘法. 此外每个矩阵 x 还需进行 $2r$ 次判断与 E_1 及 E_q 是否相等, 每判断一次要进行4次数的比较, 最坏时要进行 $8q^2(q^2-1)^2$ 次数的比较.

在过程三中进行统计时, 还要多次对数组 $paieg()$ 进行搜索, 由搜索算法^[5]知, 在最坏的情况下每搜索一次的运算量为 N , 其中 N 为数组 $paieg()$ 的大小, 从而总的搜索次数 $W(N) < q^2(q^2-1)^2 < q^6$.

综上所述, 整个计算过程中的工作量在最坏的情况下也不超过

$$2q^4 + q(q^2-1)[8q(q^2-1) + 8q^2(q^2-1)^2 + q(q^2-1)] < 10q^9.$$

可见, 其工作量是与输入尺寸 q 成多项式增长的.

参考文献

- 1 施武杰. 元的阶给定的有限群[J]. 科学通报, 1997, (11): 1702~1706
- 2 施武杰. A5的一个特征性质[J]. 西南师范学院学报(自然科学版), 1986, (3): 11~14
- 3 Lipschutz S, Shi WujiE. FINITE GROUPS WHOSE ELEMENT ORDERS DO NOT EXCEED TWENTY [J]. PROGRESS IN NATURAL SCIENCE. 2000
- 4 Shi wujiE. A CHARACTERISTIC PROPERTY OF $PSL_2(7)$ [J]. J. AusTral. Math. (SeriEs A0 36 (1984). 354~356
- 5 徐士良. 计算机常用算法[M]. 北京: 清华大学出版社, 1989. 43~47
- 6 Proc. European Conf. on Computer Vision, April 1996
- 7 Swets D, Weng J. Hierarchical Discriminant Analysis for Image Retrieval. IEEE PAMI, 1999, 21(5)
- 8 Bian Zhao-Qi, Zhang Xue-Gong, et al. Pattern Recognition. Beijing: Publishing House of QingHua University, 2000 (in Chinese)
- 9 Pelikan M, Goleberg D E, Cauntr-Paz E. BOA: The Bayesian optimization algorithm. GECCO-99. In: Proc. of the Genetic and Evolutionary Computation Conf. CA, Morgan Kaufmann, 1999. 525~532
- 10 Turk M A, Pentland A P. Eigenfaces for recognition. Journal of Cognitive Neuroscience, 1991, 3(1): 71~86
- 11 Moses Y, Adimi Y, Ullman S. Face recognition: The problem of compensating for changes in illumination direction. In: Proc. of the European Conf. on Computer Vision, 1994, A. 286~296
- 12 Sandy A, Pentland, Choudhury T. Face Recognition for Smart Environments. IEEE Computer, 2000, 33(2): 34~36
- 13 Li S Z, Lu Juwei. Face Recognition Using the Nearest Feature Line Method. IEEE Transactions on Neural Networks, 1999
- 14 O'Toole A, Abdi H, Deffenbacher K A, Valentin D. Low-dimensional representation of faces in higher dimensions of the face space. Journal of The Optical society of America, 1993, A(10): 405~411
- 15 Pentland A, Moghaddam B, Starner T. View-based and modular eigenspaces for face recognition. In: Proc. IEEE Conf. on Computer Vision and Pattern Recognition CVPR 94, (Seattle, Washington), 1994. 84~91
- 16 Phillips P J, Wechsler H, Huang J, Rauss P. The FERET database and evaluation procedure for face recognition algorithms. Image and Vision Computing, 1998, 16(5): 295~306
- 17 Cover T M, Hart P E. Nearest Neighbor Pattern Classification. IEEE Transactions on Information Theory, 1967, IT-13(1): 21~27
- 18 Zhao W, Chellappa P, Rosenfeld A. Face recognition: A Literature Survey. ACM Journal of Computing Surveys, 2000
- 19 Zhao W, Krishnaswamy A, Chellappa R, Swets D, Weng J. Discriminant analysis of principal components for face recognition. In: Wechsler, Philips, Bruce, Fogelman-Soulie, Huang, eds. Face Recognition: From Theory to Applications, Springer-Verlag, 1998. 73~85
- 20 Brunelli R, Poggio T. Face recognition: Features versus templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, 15: 1042~1052
- 21 Chellappa R, Wilson C L, Sirohey S. Human and Machine Recognition of Faces, A Survey. Proc. of the IEEE, 1995, 83: 705~740
- 22 Cox I J, Ghosn J, Yianilos P N. Feature-based face recognition using mixture-distance. In: Proc. of IEEE Computer Society Conf. on Computer Vision and Pattern Recognition, 1996. 209~216
- 23 Chellappa R, Wilson C L, Sirohey S. Human and machine recognition of faces: A survey. PIEEE, 1995, 83: 705~740
- 24 Kirby M, Sirovich L. Application of the Karhunen-Loeve procedure for the characterization of human faces. IEEE Trans. Pattern Analysis and Machine Intelligence, 1990, 12(1)
- 25 Belhumeur P N, Hespanha J P, Kriegman D J. Eigenfaces vs. fisher-faces: Recognition using class specific linear projection. In:

(上接第163页)

为其他脸面识别算法的基础. 同时本文实验还发现对于大型脸面训练库, 同样不需要更多的特征数表达脸面.

致谢 作者感谢 J. Ross Beveridge 对本文实验的帮助, 感谢 Defense Advanced Research Products Agency (DARPA) 为本文的研究提供的 FERET 脸面数据库及标准化程序.

参考文献