中国科学: 数学 2010 年 第 40 卷 第 6 期: 533～537
www.springerlink.com math.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

关于 Thompson 问题

沈如林[①②], 施武杰[②*]

① 湖北民族学院数学系, 恩施 445000;
② 苏州大学数学科学学院, 苏州 215006
E-mail: shenrulin@hotmail.com, wjshi@suda.edu.cn

收稿日期: 2008-10-14; 接受日期: 2010-02-08; * 通信作者
国家自然科学基金 (批准号: 10571128), 湖北省教育厅青年基金 (批准号: Q20092905) 及湖北民族学院博士基金资助项目

摘要 1987 年本文第二作者给 J. G. Thompson 教授的信中提出猜想: 所有有限单群 S, 都能够用 S 的阶和 S 的元的阶的集合统一的刻画. 在回信中, Thompson 提出了他的关于有限群 G 可解性判断的问题. 当 G 的素图非连通时, 本文给出了 J. G. Thompson 问题的肯定回答.

关键词 Thompson 问题 同阶型 非连通素图

MSC (2000) 主题分类 20D45

1 引言

给定有限群 G, 怎样判断 G 的可解性? 著名的奇阶定理证明了任何奇数阶群都是可解的. 1987 年本文第二作者给 J. G. Thompson 教授的信中给出了如下的猜想:

猜想 设 G 是有限群, S 为有限单群. 则 $G \cong S$ 当且仅当 $\pi_e(G) = \pi_e(S)$, 这里 $\pi_e(G)$ 记 G 的所有元阶的集合, 且 $|G| = |S|$.

在以前工作的基础上, 文献 [1] 最后完成了上述猜想的证明, 从而该猜想成为一个定理.

在 Thompson 给本文第二作者的回信中提出了问题: 对于每个有限群 G 和每个整数 $d \geqslant 1$, 设 $G(d) = \{x \in G | x^d = 1\}$. 定义 G_1 和 G_2 是同阶型的当且仅当 $|G_1(d)| = |G_2(d)|$, $d = 1, 2, \ldots$

问题 (J. G. Thompson[2]) 设 G_1 和 G_2 是同阶型的群. 假设 G_1 可解, 是否 G_2 必然可解?

即对于偶阶群 G, 我们不能仅用 G 的阶来判断它的可解性, 但是如果上面 Thompson 问题正确, 我们可以通过同阶型来判断 G 的可解性.

特别在 Thompson 的信中写到: "我已经把关于同阶型的问题告诉了很多数学工作者. 这个问题起源于研究代数数域, 这是我非常感兴趣的".

设 $\pi(n)$ 是 n 的素因子集合, 记 $\pi(|G|)$ 为 $\pi(G)$. 用集合 $\pi(G)$, 定义 G 的素图为 (参见文献 [3]): $\pi(G)$ 为顶点集, 顶点 r 和 s 在 $\pi(G)$ 中连接, 当且仅当 $rs \in \pi_e(G)$.

在本文中我们证明了如下定理:

定理 设 G 是有限群使得 G 和 F 是同阶型. 如果 F 是可解且 F 的素图非连通, 则 G 也可解.

2 预备及引理

记 $M_G(n)$ 是 G 中 n 阶元的集合. 我们能够根据同阶元给出 G 的一个分拆, 即

引用格式: Shen R, Shi W. On Thompson problem (in Chinese). Sci Sin Math, 2010, 40(6): 533–537

$$G=\bigcup_{n\in\pi_e(G)} M_G(n),$$

这里 $\pi_e(G)$ 是 G 的谱, 即 G 的所有元阶的集合. 因为每个 n 阶元必定在某个 n 阶循环子群里面, 则 $|M_G(n)|=v_n(G)\phi(n)$, 这里 $v_n(G)$ 是 n 阶循环子群的个数, 称为阶 n 的循环次数, 且 $\phi(n)$ 表示 Euler 函数. 因此我们可以得到以下的一个方程, 叫做 G 的阶方程,

$$|G|=\sum_{n\in\pi_e(G)} v_n(G)\phi(n).$$

我们记这个方程为 $\mathrm{Ord}(G)$. 进一步, 对于有限群 G 和 H, 等式 $\mathrm{Ord}(G)=\mathrm{Ord}(H)$ 表示 $\pi_e(G)=\pi_e(H)$, 且对于每个 $d\in\pi_e(G)$ 有 $v_d(G)=v_d(H)$. 很容易看出阶方程相等与 Thompson 问题中的同阶型是一致的. 因此以下不妨把阶方程相等代替同阶型. Thompson 问题已经被引述在《群论中未解决的问题》的问题 12.37 (参见文献 [4]).

不难证明如果 G 是幂零的, 则 H 也是幂零的; 如果 G 是超可解, 则 H 是可解 (见文献 [5]). 当然, 如果 G 是有限非交换单群, 则 H 是非可解的, 因为引言中施的猜想 (见文献 [4] 中问题 12.39 或文献 [6]) 最近已经被解决.

集合 $\pi_e(G)$ 关于整除关系构成一个偏序, 记为 $\mu(G)$ 在这个偏序下极大的元. 设 $\pi(n)$ 是数 n 的素因子集, 而 $|n|_r$ 记为 n 的 r- 部分. 并记 $\pi(|G|)$ 为 $\pi(G)$. 在集 $\pi(G)$ 上我们定义一个图: 在顶点集 $\pi(G)$ 中的 r 和 s 连接当且仅当 $rs\in\pi_e(G)$. 这样图称为 G 的 Gruenberg-Kegel 图, 或 G 的素图, 并记为 $\mathrm{GK}(G)$. G 的素图分支记为 $\{\pi_i\mid i=1,\ldots,s:=s(G)\}$, $s(G)$ 叫做 G 的连通分支数, 且如果 G 是偶阶群, 规定 2 属于 π_1. 并记 $\mu_i(G)=\{a\in\mu(G)|\pi(a)\subseteq\pi_i(G)\}$. 在文献 [3, 7] 中, 运用一些数论的技巧确定了有限单群的连通分支数. 在近期的文章 [8] 给出了有限典型单群 G 极大环面的循环结构, 对于例外型的有限单群 G, 极大环面的循环结构在文章 [9] 中详细的给出, 因此很容易看出 $\mu_i(G)$ $(i\geqslant 2)$ 只有唯一元, 并记 $n_i(G)$ 为 $\mu_i(G)$ 的唯一元. 素图连通分支数大于 1 的群的结构由 Gruenberg 和 Kegel 给出 (参见文献 [3]).

定理 1(Gruenberg-Kegel) 如果 G 是一有限群, 其素图分支的个数 $s(G)\geqslant 2$, 则

(a) $s(G)=2$, 且 G 是 Frobenius 群或 2-Frobenius 群, 即 $G=ABC$, 这里 A 和 AB 是 G 的正规子群, AB 和 BC 分别是以 A, B 为核和 B, C 为补的 Frobenius 群.

(b) 存在非交换单群 S 使得 $S\leqslant\overline{G}=G/N\leqslant\mathrm{Aut}(S)$, 这里 N 是 G 的极大可解正规子群且 N 和 $\overline{G}/S$ 是 $\pi_1(G)$- 子群, $s(S)\geqslant s(G)\geqslant 2$, 且对每个 $2\leqslant i\leqslant s(G)$, 存在 $2\leqslant j\leqslant s(S)$, 使得 $\mu_i(G)=\mu_j(S)$.

由 Thompson 定理知 N 是幂零群. 如果我们限制定理 1 更强的条件, 我们得到如下更强的结果.

定理 2 假设 $s(F)\geqslant 2$. 如果对于有限群 G 有 $\mathrm{Ord}(G)=\mathrm{Ord}(F)$, 则以下之一成立:

(a) $s(G)=2$ 且 G 是 Frobenius 群或 2-Frobenius 群;

(b) 存在非交换单群 S 使得 $S\leqslant\overline{G}=G/N\leqslant\mathrm{Aut}(S)$, 这里 N 和 $\overline{G}/S$ 都是 $\pi_1(G)$- 子群. 素图 $\mathrm{GK}(G)$ 是非连通的, $s(S)\geqslant s(G)$, 且进一步, 下面成立:

(i) 若 i 满足 $2\leqslant i\leqslant s(G)$, 则存在 $j\,(2\leqslant j\leqslant s(S))$, 使得 $\mu_i(G)=\mu_j(S)$.

(ii) 设 $m>1$ 是 $\mu_i(F)$ $(i\geqslant 2)$ 的任何元的因子. 则 $|M_F(m)|=|M_{\overline{G}}(m)||N|$, $|M_{\overline{G}}(m)|=|M_S(m)|$.

证明 只需要证明 (b) 的 (i) 和 (ii). 设 $x\in G$ 且 $o(x)=m$. 因为 $\pi(N)\subseteq\pi_1(G)=\pi_1(F)$ 和 $\pi(m)\subseteq\pi_i(F)=\pi_i(G)$ $(i\geqslant 2)$, 我们有 $(m,|N|)=1$. 因此 $o(x)=o(xN)$. 事实上, 设 $o(xN)=n$, 因 $(xN)^m=x^mN=N$, 则 $n|m$. 反之, 根据 $N=(xN)^n=x^nN$, 我们有 $x^n\in N$. 当然, 可以推出

$o(x^n)||N|$, 但是

$$o(x^n)=\frac{o(x)}{(n,o(x))}=\frac{m}{(n,m)},$$

于是 $\frac{m}{(n,m)}\mid|N|$, 因此 $\frac{m}{(n,m)}=1$, 我们有 $m|n$. 即有 $m=n$. 另一方面, 如果存在 G 中的元 y, 使得 $o(y)\neq m$ 和 $o(yN)=o(xN)$, 则 $o(xN)|o(y)$, 即 $m|o(y)$, 我们可以假定 $o(y)=mq$ $(q\neq 1)$ 且存在 q 的素因子 r 使得 $r\in\pi_j(G)$ $(i\neq j)$ (否则, q 是 $\mu_i(G)$ 的某个元的因子, 我们从上面有 $o(yN)=o(y)=mq$, 矛盾). $\pi_i(G)$ 和 $\pi_j(G)$ 在 G 的素图中是连通的, 矛盾. 因此, $o(y)=m$. 于是 $|M_{\overline{G}}(m)|\leqslant|M_F(m)|=|M_G(m)|$. 进一步, 陪集 xN 中的每个元都有阶 m, 这样就有 $|M_G(m)|=|M_{\overline{G}}(m)||N|$. 对于剩下的部分, 因为 $\overline{G}$ 是几乎单群, $\overline{G}$ 是单群 S 被 $\overline{G}/S$ 的扩张. 我们选择 $\overline{G}/S$ 的一个陪集表示 $\{y_1,y_2,\ldots,y_l\}$, 这里 $y_i\in\overline{G}$, 当然, 根据陪集分解, $\overline{G}$ 中每个元都能写成 y_is 的形式, 这里 $1\leqslant i\leqslant l$ 且 $s\in S$. 因为 $o(y_iS)=o(y_isS)$, 我们有 $o(y_iS)|o(y_is)$. 如果 $y_iS\neq S$, 根据如上条件 $\overline{G}/S$ 是 $\pi_1(G)$- 子群, 我们有 $\pi(o(y_iS))\subseteq\pi_1(\overline{G})$, 因此存在 $o(y_is)$ 的一个素因子使得它也属于 $\pi_1(G)$. 如果 $\pi(o(s))\subseteq\pi_i(\overline{G})$ $(i\geqslant 2)$, 因为 $\pi_1(\overline{G})$ 和 $\pi_i(\overline{G})$ 在 $\overline{G}$ 的素图中不连通, 则 $\overline{G}$ 中的每个不属于 S 的元没有 $o(s)$ 因子的阶. 因此, $|M_{\overline{G}}(m)|=|M_S(m)|$. □

为了完成定理的证明, 我们还需要 Frobenius 群和 2-Frobenius 群的具体结构. 如下给出一些引理.

引理 3 (参见文献 [10, 引理 1] 及 [11, 定理 1]) 设 F 是以 K 为核 H 为补 Frobenius 群, 则以下结论成立:

(i) K 幂零且 K 的 Sylow p- 子群循环, 这里 p 是奇素数;

(ii) 如果 $2\in\pi(H)$, 则 K 是交换群. 进一步, 如果 H 是可解的, 则 H 的 Sylow 2- 子群或者循环或者 (广义) 四元素 Q_{2^n}. 如果 H 是非可解, 则存在子群 H_0 使得 $|H:H_0|\leqslant 2$ 且 $H_0\cong Z\times SL_2(5)$, 这里 Z 的每个 Sylow 子群都循环且 $(|Z|,30)=1$.

引理 4 (参见文献 [10, 定理 2]) 设 E 是 2-Frobenius 群, 即 $G=ABC$, 这里 A 和 AB 是 G 的正规子群, AB 和 BC 分别是以 A, B 为核和 B, C 为补的 Frobenius 群. 则以下结果成立:

(i) $s(E)=t(E)=2$ 且 $\pi_1(E)=\pi(A)\cup\pi(C),\pi_2(E)=\pi(B)$;

(ii) E 是可解的, B 是 E 的 Hall 子群且是奇阶的, 且 C 循环群.

3 定理证明

以下我们使用定理 1 和先前的一些引理完成证明, 本质上我们使用单群分类定理. 首先, 我们考虑 Frobenius 群的情形. 设 F 是 Frobenius 群, 其核为 K, 补为 H, 并且有限群 G 使得 $\mathrm{Ord}(G)=\mathrm{Ord}(F)$. 当然, 我们有 $|G|=|F|$, $\pi_e(G)=\pi_e(F)$ 且循环次数 $v_n(G)=v_n(F)$, 这里 $n\in\pi_e(F)$.

论断 1 如果 G 是有限群, F 是 Frobenius 群, 使得 $\mathrm{Ord}(G)=\mathrm{Ord}(F)$, 则 G 是 Frobenius 群. 进一步, 如果 F 是可解的, 则 G 也是可解的.

我们使用 Gruenberg-Kegel 定理完成论断 1.

情形 1 G 是 2-Frobenius 群. 设 $G=ABC$, 这里 A 和 AB 是 G 的正规子群, AB 和 BC 分别是以 A, B 为核和 B, C 为补的 Frobenius 群. 根据引理 3 和 4, 我们有 $\pi(B)=\pi_2(F)$, 即 $\pi(B)=\pi(K)$ 或 $\pi(H)$. 当然, 据引理 4 知 B 是奇阶循环的.

(i) 如果 $\pi(B)=\pi(K)$, 因为 K 是 F 的 Hall 子群且 $|B|=|K|$, 则 F 中存在 $|B|$ 阶元, 因此 K 循环. 进而, K 是正规子群, 于是 $v_{|B|}(F)=1$. 另一方面, AB 是 Frobenius 群, 其补为 B, 则 $v_{|B|}(G)\geqslant v_{|B|}(AB)=|A|>1$, 因此 $v_{|B|}(G)>v_{|B|}(F)$, 矛盾.

(ii) 如果 $\pi(B)=\pi(H)$, 同样 H 是循环的, 则 $v_{|B|}(F)=|K|$. 因为 A 和 AB 都在 G 中正规, 则 $G=ABC=C(AB)=C(BA)=CBA$, 因此每个元 $g\in G$ 能够写成 cba 的形式, 这里 $a\in A, b\in B$ 和 $c\in C$. 于是我们有 $B^g=B^{cba}=((B^c)^b)^a=B^a$, 这样 B 在 G 中的共轭子群的个数为 B 在 A 中的个数, 而 G 可解, 则所有 $|B|$ 阶子群都共轭, 因此 $v_{|B|}(G)=v_{|B|}(AB)=|A|$. 但是 $|H||K|=|F|=|G|=|A||B||C|$ 和 $|B|=|H|$, 于是 $|A|=|K|/|C|$. 因此, $v_{|B|}(F)=|K|<|K|/|C|=|A|=v_{|B|}(G)$, 矛盾.

情形 2 存在非交换单群 S 使得 $S\leqslant\overline{G}=G/N\leqslant \mathrm{Aut}(S)$. 如果 $2\in\pi(H)$, 则 K 是 Abel 群. 选择 $r\in\pi(K)$, 根据定理 2, 我们有 $|K|_r=|G|_r=|S|_r$. 因为 K 是 Abel 且正规, 则 K 中 r- 元数目为 $|K|_r$, 即 $|S|_r$. 但是因 S 中 Sylow r- 子群一直存在, 则 S 的 r- 元个数也为 $|S|_r$, 因此 S 中仅有一个 Sylow r- 子群, 即存在一个真正规子群, 矛盾.

如果 $2\in\pi(K)$, 则 K 的 Sylow p- 子群 $(p\in\pi(K))$ 在 F 中正规, 而由 $\mathrm{Ord}(F)=\mathrm{Ord}(G)$, 我们有 G 的 Sylow p- 子群也正规. 因为 $N=O_p(G)$, 我们有 $p=2$, 且 N 是 G 的正规 Sylow 2- 子群. 因此 G/N 是奇阶群, 有著名的 Feit-Thompson 定理, G/N 是可解的, 矛盾.

因此由定理 2 有 G 是 Frobenius 群. 进一步, 如果 F 是非可解, 则由引理 3, 存在子群 H_0 使得 $|H:H_0|\leqslant 2$ 且 $H_0\cong Z\times SL_2(5)$, 这里 Z 的每个 Sylow 子群都循环且 $(|Z|,30)=1$. 故 $|H|=2^3\cdot 3\cdot 5\cdot|Z|$ 或 $2^4\cdot 3\cdot 5\cdot|Z|$. 很容易知道 H 中不存在 15 阶元 (因为 15 不属于 $\pi_e(SL_2(5))$). 现设 G 的补为 V. 则由 $\mathrm{Ord}(F)=\mathrm{Ord}(G)$ 有 $\pi_e(H)=\pi_e(V)$ 且 $|H|=|V|$. 如果 G 是可解, 则存在 V 的 15 阶 Hall 子群. 这样 $15\in\pi_e(V)$, 矛盾. 故 G 也是非可解.

下面我们考虑 2-Frobenius 群的情形. 设 E 是 2-Frobenius 群且 $E=ABC$, 这里 A 和 AB 是 G 的正规子群, AB 和 BC 是分别以 A, B 为核和 B, C 为补的 Frobenius 群.

论断 2 如果 G 是有限群, E 是 2-Frobenius 群使得 $\mathrm{Ord}(G)=\mathrm{Ord}(E)$, 则 G 也是 2-Frobenius 群.

由论断 1, 我们可以假设存在非交换单群 S 使得 $S\leqslant\overline{G}=G/N\leqslant\mathrm{Aut}(S)$. 因为 B 是 E 循环 Hall 子群, 则任何两个 $|B|$ 阶 Hall 子群的交是平凡的, 且 $v_{|B|}(E)=|A|$, 于是在 G/N 中任何两个 $|B|$ 阶 Hall 子群的交是平凡的且 $v_{|B|}(G/N)=\frac{|A|}{|N|}$, 因此 S 也有定理 2(b) 的性质, 即 S 中任何两个 $|B|$ 阶 Hall 子群的交是平凡的, 且 $v_{|B|}(S)=\frac{|A|}{|N|}$.

如果 $S=L_2(r^f)$, 其中 r 是奇素数且 $\pi(B)=\{r\}$, 则 $|B|=r^f$. 因此 S 中存在 r^f 阶元, 但是 $L_2(r^f)$ 的 Sylow r- 子群是 $Z_r\times Z_r\times\cdots\times Z_r$ (个数为 f). 因此 $f=1$. 如果 $S=L_3(4)$ 且 $|B|=\mu_i(S)=3$, 则 S 包含一个自中心化的 9 阶初等交换 Sylow 3- 子群, 因此 $|M_S(3)|=2^6\cdot 5\cdot 7$ (参见文献 [12]). 于是 G 中 3 阶元素的个数 $|M_G(3)|$ 是 $|M_S(3)|\cdot|N|=2^6\cdot 5\cdot 7\cdot|N|$. 另一方面, 我们知道 $|G|=|A||B||C|=|N||S|$ 且 $|A|=|M_G(3)|$, 则我们有 $|S|=3|M_S(3)|\cdot|C|=3\cdot 2^6\cdot 5\cdot 7\cdot|C|$. 因此 $|C|=3$, 这矛盾于 $|C|\mid(|B|-1)$.

现记 $S^*=\overline{G}/S$. 对于其余的情形, 根据文献 [10] 中的引理 1.1, 如果 $\mu_i(S)$ 不为 $L_2(r^f)$ (r 为奇数且 $f>1$) 的分支 $\{r\}$ 和 $L_3(4)$ 的分支 $\{3\}$, 则 S^* 包含一个循环的 Hall 子群 U 满足 $|U|=\mu_i(S)$, 这里 $i>1$. 进一步, U 在 S^* 中是自中心化的, 则 $\mu_i(S)$ 阶元的共轭类的长度为 $\frac{|S^*|}{\mu_i(S)}$. 因此

$$|M_{S^*}(\mu_i(S))|\geqslant\frac{|S^*|}{\mu_i(S)}. \tag{3.1}$$

因为 $\mathrm{Ord}(E)=\mathrm{Ord}(G)$, 我们有

$$|G|=|A|\cdot|B|\cdot|C|=|S^*|\cdot|N|. \tag{3.2}$$

根据引理 4 (ii), 我们有 B 是 E 的循环子群, 并且根据定理 1 可以得到以下的公式:

$$|B| = \mu_i(S), \tag{3.3}$$

$$|A| = |M_{S^*}(|B|)| \cdot |N|. \tag{3.4}$$

由 (3.2)–(3.4) 式, 我们得到

$$|S^*| = \mu_i(S) \cdot |M_{S^*}(|B|)| \cdot |C|. \tag{3.5}$$

据 (3.1) 式和 $|C| > 1$, 有

$$|S^*| \leqslant \mu_i(S) \cdot |M_{S^*}(\mu_i(S))| = \mu_i(S) \cdot |M_{S^*}(|B|)| < \mu_i(S) \cdot |M_{S^*}(|B|)| \cdot |C|,$$

这个矛盾于 (3.5). 因此 G 是 2-Frobenius 群. □

致谢 作者感谢 Marston Conder 教授的交流及帮助.

参考文献

1 Vasilev A V, Grechkoseeva M A, Mazurov V D. Characterization of the finite simple groups by spectrum and order. Algebra Logic, 2009, 48: 385–409
2 Thompson J G. Private communication. 1987
3 Williams J S. Prime graph components of finite groups. J Algebra, 1981, 69: 487–513
4 Mazurov V D. Unsolved Problems in Group Theory, The Kourovka Notebook, 16th ed. Novosibirsk: Inst Mat Sibirsk Otdel Akad, 2006
5 许明春. 与 σ-Sylow 塔群同阶型的群. 海南大学学报 (自然科学版), 1996, 14: 103–105
6 Shi W. A new characterization of the sporaolic simple groups. In: Group Theory, Proceeding of the 1987 Conference. Berlin-New York: Walter de Gruyter, 1989, 531–540
7 Kondrat'ev A S. Prime graph components of finite simple groups. Math USSR Sbornik, 1989, 67: 235–247
8 Buturlakin A A, Grechkoseeva M A. The cyclic structure of maximal tori in the finite classical groups. Algebra Logic, 2007, 46: 129–156
9 Kantor W M, Seres A. Prime power graphs for groups of Lie type. J Algebra, 2002, 247: 370–434
10 Mazurov V D. Characterizations of groups by arithmetic properties. Algebra Colloq, 2004, 11: 129–140
11 陈贵云. Frobenius 群与 2-Frobenius 群的结构. 西南师范大学学报 (自然科学版), 1995, 20: 485-487
12 Conway J H, Curtis R T, Norton S P, et al. Atlas of Finite Groups. Oxford: Clarendon Press, 1985

On Thompson problem

SHEN RuLin & SHI WuJie

Abstract In 1987, the second author of this paper reported his conjecture, all finite simple groups S can be characterized uniformly using the order of S and the set of element orders in S, to Prof. Thompson. In their communications, Thompson posed his problem about the judgment of solvability of finite groups G. In this paper we give a positive answer for Thompson's problem if the prime graph of G is not connection.

Keywords: Thompson problem, same order type, disconnected prime graph
MSC(2000): 20D45