

七个 Ramsey 数 $R_n(5)$ 的下界

罗海鹏

苏文龙

(广西科学院 南宁市 530031) (广西梧州一中)

摘 要 用群论和数论研究素数阶循环图, 探讨循环群的正规子群的结构, 给出探索 Ramsey 数 $R_n(5)$ 下界的一般方法, 得到若干 Ramsey 数 $R_n(5)$ 的新的下界。

关键词 Ramsey 数; 下界; 循环图; 正规子群; 图论

分类号 0157.5

0 引 言

在图论中有著名的 Ramsey 定理。对于任意 $n \geq 2$ 个正整数 $k_1, k_2, \dots, k_n \geq 2$, 存在最小正整数 R , 当 $s \geq R$ 时用 n 种颜色把 s 阶完全图 G 的边任意着色, 则一定存在各边同着第 i 种颜色的 k_i 阶完全子图, 这里 i 是 $1, 2, \dots, n$ 中的某一个。

上述正整数 R 称为 Ramsey 数 $R(k_1, k_2, \dots, k_n; 2)$ 。当 $k_1 = k_2 = \dots = k_n = k$ 时简记为 $R_n(k)$ 。确定 Ramsey 数是组合数学和图论中非常困难的问题。1990 年 B. D. McKay 和我国的张克民采用穷举法, 在高速电子计算机上连续运算一个月证明了 $R(3, 8) = 28^{[1]}$, 得到迄今已知的第 9 个不平凡的 Ramsey 数。但当 Ramsey 数增大时, 这种方法的运算量将呈指数级的增长, 所需要的运算时间是人们难以接受的, 因此近 30 年来人们往往沿用文献 [2] 的方法研究阶数较小的循环图, 在计算机上得到一些 Ramsey 数的新下界^[3, 4], 鉴于这种方法在产生参数时存在一定的随机性, 运算效率也不高, 进展非常缓慢。因此, 作者在文献 [5] 中作了新的尝试: 用群论和数论研究了素数阶循环图的基本性质, 提高了运算效率, 一举获得了 20 个广义 Ramsey 数的新下界, 其中 $R_4 \geq 458$ 刷新了 $R_4 \geq 382^{[6]}$ 的记录。本文是文献 [5] 的继续, 阐明了寻求 Ramsey 数 $R_n(5)$ 的下界的一般方法, 得到了 Ramsey 数 $R_n(5)$ 的 7 个新的下界。

定理 1:

(1) $R_9(5) \geq 22\,484$, $R_{11}(5) \geq 27\,480$, (3) $R_{12}(5) \geq 42\,170$, (4) $R_{15}(5) \geq 80\,222$,

(5) $R_{16}(5) \geq 109\,314$, (6) $R_{17}(5) \geq 111\,318$, (7) $R_{18}(5) \geq 205\,238$

上述成果尚未见于其他文献报道, 并且远远优于据文献 [7] 的下界公式计算出来的结果。

1 素数阶循环图的线性变换

给定整数 $n \geq 2$, 素数 $p = 2mn + 1$, 记 $Z_p = \{-mn, \dots, -2, -1, 0, 1, 2, \dots, mn\}$ 为模 p 的一个完整剩余系。约定, 以下所有小写英文字母都表示模 p 整数, 并且任何若干个整数的加、

1997 年 5 月 30 日收稿。

第一作者简介: 罗海鹏, 男, 1947 出生, 研究员, 计算机软件专业。

减、乘、乘方运算的结果(为了简便, 仍用普通等号“=”写出)都应取模 p 同余归结到 Z_p , 除非另外声明. 设 g 是 p 的原根, 记

$$\begin{aligned} Z_p &= \{x \mid x = g^i, 0 \leq i < 2mn\}. \\ \alpha_i &= \{x \mid x = g^{nj+i}, 0 \leq j < 2m\}, 0 \leq i < n. \\ \alpha_i \alpha_j &= \{x \mid x = ab, a \in \alpha_i, b \in \alpha_j\}. \end{aligned}$$

熟知 Z_p 是有限域, Z_p 是在模 p 同余的乘法运算下的 $2mn$ 阶交换群, α_0 是生成元为 g^n 的 $2m$ 阶循环群, 它是 Z_p 的正规子群, α_1 是 α_0 的陪集, $Z_p/\alpha_0 = \{\alpha_0, \dots, \alpha_{n-1}\}$ 是 Z_p 的商群且有

引理 1. $\alpha_i \alpha_j = \alpha_{i+j}$, 其中 $\alpha_{i+j} = \alpha_r$, $r = i+j \pmod{n}$ 且 $0 \leq r < n$. (约定, 以下关于 α_i 的下标均仿此: 取模 n 同余且归结到模 n 的最小非负剩余系 $\{0, 1, \dots, n-1\}$).

定义 1 设 G 是 P 个顶点的完全图, 顶集 $V_G = Z_p$, 边集的参数集 $S_G = \{\alpha_0, \dots, \alpha_{n-1}\}$ (即以命名为 $0, 1, \dots, n-1$ 的 n 种颜色把各边着色): 当且仅当 $x-y \in \alpha_i$ 时, 两个顶点 x, y 称为 α_i 相邻的 (即顶点 x, y 的联边是着色 i 的). 象这样命名了各顶点并且规定了各边着色方法的完全图称为 p 阶循环图.

定义 2 在 p 阶循环图 G 中, $k \geq 2$ 个不同的顶点 x, y, \dots, z 如果其中任意两个顶点都是 α_i 相邻的, 就称它们作成 k 阶 α_i 团 (即各边都着色 i 的 k 阶完全子图), 记为 $(x, y, \dots, z)_i$. 在不致误会时略去 α_i 团的下标简记为 (x, y, \dots, z) . 其中 x, y, \dots, z 称为这个团的元素. 包含同样元素 (不论各元素排列顺序是否相同) 的两个团看作是同一个团而不加区别.

定义 3 给定两个 p 阶循环图 G 与 G' , 如果 V_G 与 $V_{G'}$ 之间存在 1-1 对应关系 f , 并且 f 把图 G 中的 α_i 团映射为图 G' 中的 α_j 团, 则这两个图称为同构的. 约定, 两个同构的 p 阶循环图 (其顶集均为 Z_p) 看作是同一个图, 上述同构映射 f 称为图 G 的变换.

引理 2 设 $a \in \alpha_j$, $b \in Z_p$, 则 $f(x) = ax + b$ ($x \in Z_p$) 作成图 G 的变换 (线性变换), 它把 k 阶 α_i 团变换成 k 阶 α_{i+j} 团.

证明: 由 $a \in \alpha_j$ 知 $a \neq 0$. 对于任意 $x, y \in Z_p$ 有 $x=y \Leftrightarrow ax=ay \Leftrightarrow f(x)=f(y)$, 即 f 作成顶集 V_G 的 1-1 变换. 据引理 1 有 $x-y \in \alpha_i \Leftrightarrow f(x)-f(y) = a(x-y) \in \alpha_{i+j}$, 即图 G 中 α_i 相邻的两个顶点变换成 α_{i+j} 相邻的其它两个顶点, 因此图 G 中 α_i 团变换成 α_{i+j} 团. 证毕.

2 循环群的正规子群与 $R_n(5)$ 的下界

引理 3 记 $\alpha_0^+ = \{x \mid x \in \alpha_0 \text{ 且 } x > 0\}$, 则在取模 p 同余 (归结到 Z_p) 的乘法运算再取绝对值的复合运算下, α_0^+ 作成以 g^n 为生成元的 m 阶循环群:

$$\alpha_0^+ = \{x \mid x \equiv g^{ni} \pmod{p}, 0 \leq i < m\}, \text{ 并且有 } x-y \in \alpha_0 \Leftrightarrow |x-y| \in \alpha_0^+.$$

证明: 注意到 α_0 是生成元为 g^n 的 $2m$ 阶循环群, 知 $g^{2m} \neq 1$ 且 $g^{2nm} = 1$, 有 $g^{nm} = -1 \in \alpha_0$. 由此易知在上述复合运算下 α_0^+ 作成生成元为 g^n 的 m 阶循环群并且有 $x \in \alpha_0 \Leftrightarrow x = (-1) \times x \in \alpha_0$, 这就得到引理 3 的后一个结论, 证毕.

引理 4 记 α_0 的子集

$$\theta = \{x \mid x \in \alpha_0 \text{ 且 } x-1 \in \alpha_0\}, \quad \theta^+ = \{x \mid x \in \alpha_0^+ \text{ 且 } x-1 \in \alpha_0^+\}$$

则当 $\theta \neq \Phi$ 时有 $\theta = \{x \mid x \in \theta^+ \text{ 或 } 1-x \in \theta^+; \text{ 或者当 } 2 \in \theta^+ \text{ 时 } x=2^{-1}\}$ 。

证明: 设 $x \in \theta$, 则 $x \in \alpha_0$ 且 $x-1 \in \alpha_0$ 。由引理 3 知 $-x \in \alpha_0$ 且 $1-x = -(x-1) \in \alpha_0$, 故有 $1-x \in \theta$, 从而一般地有 $x \in \theta^+$ 或 $1-x \in \theta^+$, 特别地当 $x=1-x$ 时有 $x=2^{-1}$, 据引理 1 易知此时 $2 \in \theta^+$ 。证毕。

定义 4 设 $\theta \neq \Phi$ 且 $a \in \theta$ 。令

$$\theta(a) = \{x \mid x \in \theta \text{ 且 } |x-a| \in \alpha_0^+\}$$

用 $[\theta(a)]$ 表示集合 $\theta(a)$ 的特征数; 如果 $\theta(a) = \Phi$, 就记 $[\theta(a)] = 0$; 如果 $\theta(a)$ 只含一个元素或者对于任意 $b, c \in \theta(a)$ 都有 $|c-b| \in \alpha_0^+$, 就记 $[\theta(a)] = 1$ 。其他情况记为 $[\theta(a)] > 1$ 。

引理 5 设 $\theta \neq \Phi$ 。如果对于任意 $a \in \theta^+$ 恒有 $[\theta(a)] \leq 1$, 那么 $R_n(5) \geq p+1$ 。

证明: 假设在 p 阶循环图 G 中存在某个 5 阶 α_i 团 $(x_1, x_2, x_3, x_4, x_5)$ 。据定义 2 知 $x_2-x_1 \in \alpha_i$, 据引理 1 知 $(x_2-x_1)^{-1} \in \alpha_{-i}$, 据引理 2 知变换

$$f(x) = (x_2-x_1)^{-1} \circ (x-x_1)$$

把这 5 阶 α_i 团变换成 5 阶 α_0 团 $(0, 1, a, b, c)$, 其中 $a=f(x_3)$, $b=f(x_4)$, $c=f(x_5)$ 。据定义 2 有

① $a, a-1; b, b-1; c, c-1 \in \alpha_0 \Rightarrow a, b, c \in \theta$ 。

② $1-a, -a; 1-b, -b; 1-c, -c \in \alpha_0 \Rightarrow 1-a, 1-b, 1-c \in \theta$ 。

不失一般性, 设 $a \in \theta^+$ 。否则, 如果 a, b, c 三个元素都不属于 θ^+ , 那么据引理 4 知 $1-a, 1-b, 1-c$ 这 3 个元素中至少有 2 个属于 θ^+ , 此时在以下讨论中把 a, b, c 分别换成 $1-a, 1-b, 1-c$ 也能得到相应的结论。

设 $a \in \theta^+$ 并考察 5 阶 α_0 团 $(0, 1, a, b, c)$, 据定义 2 知

③ $b-a, c-a, c-b \in \alpha_0$ 。

据引理 3 知 $|b-a|, |c-a|, |c-b| \in \alpha_0^+$, 据定义 4 有

④ $b, c \in \theta(a)$ 且 $|c-b| \in \alpha_0^+$, 故有 $[\theta(a)] > 1$ 。

这与引理 5 的条件是不相容的。因此根据定义 1 构造一个 p 阶循环图 G 并且证明了: 在命题 5 的条件下, 这 p 阶循环图 G 中任何 5 阶 α_i 团 ($0 \leq i < n$) 都不存在。据著名的 Ramsey 定理知 $R_n(5) \leq p$ 是不可能的, 只能有 $R_n(5) \geq p+1$ 。证毕。

3 定理 1 的证明

(1) 给定 $n=9$, 素数 $p=22\,483$, 则 $g_n=3$ 循环群 α_0^+ 的最小生成元。据引理 3 有

$$\alpha_0^+ = \{x \mid x \equiv 2^i \pmod{22\,483}, x \in \mathbb{Z}_p, 0 \leq i < 1\,249\}.$$

限于篇幅, 集合 α_0^+ 的 1 249 个元素这里不一一列出, 仅指出据引理 4 得到 α_0 的子集 $\theta^+ = \{81, 110, 207, 299, 377, 456, 579, 621, 657, 668, 720, 765, 791, 862, 1053, 1179, 1267, 1332, 1431, 1437, 1537, 1593, 1655, 1737, 1855, 1907, 1971, 2027, 2187, 2218, 2254, 2416, 2524, 2530, 3095, 3096, 3799, 3802, 3869, 3874, 3899, 4293, 4308, 4339, 4700, 4701, 4779, 4963, 5038, 5056, 5092, 5211, 5551, 5644, 5778, 5924, 6195, 6206, 6228, 6636, 6654, 6854, 6877, 6902, 6903, 7043, 7226, 7245, 7564, 7588, 7655, 7725, 7750, 7841, 7845, 8156, 8224, 8252, 8330, 8387, 8505, 8829, 9129, 9221, 9288, 9469, 9563, 9713, 9780, 10046, 10109, 10146, 10213,$

10271, 10319, 10611, 10790, 10805, 10806, 10843, 10934, 11080}

注意到 $\theta(81) = \{110, 1855, -10045, -6901, -4307, -1430, -667, -206\}$ 。容易验证, 对于任意 $b, c \in \theta(81)$ 都有 $|c-b| \notin \alpha_0^+$, 故有 $[\theta(81)] = 1$ 。仿此可证: 对于任意 $a \in \theta^+$ 恒有 $[\theta(a)] \leq 1$ 。据引理 5 即得 $R_9(5) \geq 22\,484$ 。这就证明了定理 1 中的第 (1) 个结论。

仿上述, 考查下面给出的 6 组数据:

(2) $n=11$, 素数 $p=27\,479$ 与循环群 α_0^+ 的生成元 $g^n=12$;

(3) $n=12$, 素数 $p=42\,169$ 与循环群 α_0^+ 的生成元 $g^n=12$;

(4) $n=15$, 素数 $p=80\,221$ 与循环群 α_0^+ 的生成元 $g^n=66$;

(5) $n=16$, 素数 $p=109\,313$ 与循环群 α_0^+ 的生成元 $g^n=4$;

(6) $n=17$, 素数 $p=111\,317$ 与循环群 α_0^+ 的生成元 $g^n=20$;

(7) $n=18$, 素数 $p=205\,237$ 与循环群 α_0^+ 的生成元 $g^n=3$ 。

利用微机作辅助运算, 可以验证相应的集合 θ 都满足引理 5 的条件, 因此根据引理 5 就证明了定理 1 中的其余的 6 个结论。

参 考 文 献

- McKay B D, Zhang K M. The value of the Ramsey number $R(3, 8)$. J. Graph Theory, 1992, 16 (1): 99~105
- Graver J E, Yackel J. Some graph theoretic results associated with Ramsey's theorem. J. Comb. Theory, 1968, 4: 125~175
- Exoo G. A lower bound for $R(5, 5)$. J. Graph Theory, 1989, 13 (1): 97~98
- 谢继国, 张忠辅. 经典 Ramsey 数 $R(5, 9)$ 和 $R(5, 10)$ 的下界. 科学通报, 1996, 41 (20): 1918~1919
- 苏文龙. The Estimation of Lower Bounds about Some Ramsey Number $R_n(3)$ and $R_n(4)$. 广西科学, 1996, 3 (3): 4~7
- 宋恩民, 陈亮. 求 Ramsey 数最优下界值的递归算法. 华中理工大学学报, 1992, 20 (6): 169~171
- 阚家海. Ramsey 数的下界. 科学通报, 1990, 35 (18): 1437

LOWER BOUNDS OF SEVEN RAMSEY NUMBERS $R_n(5)$

Luo Haipeng

Su Wenlong

(Guangxi Academy of Sciences)

(Wuzhou No. 1 Middle School, Guangxi)

Abstract The prime order cyclic graph is studied by Group-theory and Number-theory, and the constuction of normal subgroup of cyclic group is discussed. The universal method for looking for the lower bound of Ramsey number $R_n(5)$ and some new lower bounds of Ramsey numbers $R_n(5)$ have been given.

Key words Ramsey number; lower bound; cyclic graph; normal subgroup; graph-theory