arXiv:2301.03691v1 [math.GR] 9 Jan 2023

# 关于某些花环积型本原群的最小覆盖与两两生成

JULIA ALMEIDA 和 MARTINO GARONZI

Abstract. 有限群 $G$的覆盖数（记作 $\sigma(G)$）是满足以下条件的最小正整数 $k$：$G$是 $k$ 个真子群的并。我们计算了一族本原群 $G$ 的 $\sigma(G)$，这族群具有唯一极小正规子群 $N$，且该子群同构于 $A_n^m$，其中 $n$ 可被 6 整除，且 $G/N$ 为循环的。这是对 E. Swartz 关于对称群的一项结果的推广。我们还证明了一个关于两两生成的渐近结果。

## 1. Introduction

本文假设所有群都是有限群。群 $G$ 的一个覆盖是由 $G$ 的真子群构成的一个族，其并为 $G$；$G$的覆盖数（记作 $\sigma(G)$）是 $G$的一个覆盖所含子群的最小数目。这一有趣的不变量由 J. Cohn 在 [5] 中引入，后来受到许多作者的研究。本文关注一族与对称群密切相关的群，因此先简要回顾关于 $\sigma(S_n)$的已知结果。容易证明，$\sigma(S_3) = \sigma(S_4) = 4$。J. Cohn 在其论文中证明了包括以下结果在内的若干结论：$\sigma(S_5) = 16$。A. Abdollahi 等人 [1] 证明了 $\sigma(S_6) = 13$。A. Mar´oti [15] 证明了当 $n \geqslant 7$ 为奇数且 $n \neq 9$时，$\sigma(S_n) = 2^{n-1}$；L.-C. Kappe、D. Nikolova-Popova 和 E. Swartz [10] 证明了 $\sigma(S_8) = 64$、$\sigma(S_9) = 256$、$\sigma(S_{10}) = 221$、$\sigma(S_{12}) = 761$；R. Oppenheim 和 E. Swartz [16] 证明了 $\sigma(S_{14}) = 3096$；E. Swartz [19]证明了 $\sigma(S_{18}) = 36773$，并在 $n \geqslant 30$ 可被 6 整除时给出了 $\sigma(S_n)$的精确公式，该公式与下文定理 1 中令 $m = 1$所得的公式一致。

若 $G$ 可由两个元素生成，则 $G$ 的生成图是一个简单图，其顶点为 $G$ 的元素；若两个顶点共同生成 $G$，则它们之间以一条边相连。简单图的团是一个完全子图，其团数是团的最大规模。我们用 $\omega(G)$ 表示 $G$ 的生成图的团数，换言之，$\omega(G)$ 是 $G$ 的子集 $S$ 的最大规模，且该子集具有如下性质：当 $x$、$y \in S$ 且 $x \neq y$ 时，$\langle x$、$y\rangle = G$。由于 $G$ 的任何真子群至多包含此类集合 $S$ 中的一个元素，因此有 $\omega(G) \leqslant \sigma(G)$。很自然会问，对于某些群族，这个等式是否至少渐近成立。S. Blackburn [4] 证明，当 $n$ 为奇数且充分大时，$\sigma(S_n) = \omega(S_n)$；之后 L. Stringer [18] 证明，对于所有不等于 9 和 15 的奇数 $n$，$\omega(S_n) = \sigma(S_n)$，并且 $\sigma(S_9) \neq \omega(S_9)$。目前尚不清楚 $\omega(S_{15})$ 是否等于 $\sigma(S_{15})$。在与 F. Fumagalli 和 A.

*Key words and phrases.* 置换群，本原群，覆盖，群生成。作者感谢巴西国家科学技术发展委员会（CNPq）提供的博士奖学金和 Universal 资助（资助编号 402934/2021-0）。

Mar´oti 的一项合作研究中，第二作者证明，当 $n$ 为偶数并趋于无穷时， $\omega(S_n)/\sigma(S_n)$ 趋于 1。A. Lucchini 和 A. Mar´oti [13] 证明，若 $G$ 是 Fitting 长度至多为 2 的可解群，则 $\sigma(G) = \omega(G)$。

若一个群 $G$ 存在正规核平凡的极大子群，则称其为本原群。研究本原群的 $\sigma(G)$ 和 $\omega(G)$，对于理解这些不变量的一般行为至关重要。事实上，对于一般的 $G$，有 $\sigma(G) = \sigma(G/\Phi(G))$；若 $G$ 是 2-生成的，则 $\omega(G) = \omega(G/\Phi(G))$，其中 $\Phi(G)$表示 $G$的 Frattini 子群，而且容易看出， $G/\Phi(G)$是本原群的次直积。记 $d(G)$为 $G$ 的生成元集合的最小大小。若 $G$ 非循环且有唯一极小正规子群，将其记为 $N$，则 [12, 定理 1.1] 表明 $d(G) = \max\{2, d(G/N)\}$。此外，在这种情形下，若$\Phi(G) = \{1\}$，则 $G$ 是本原群。由于我们关注的是 2-生成群，首先要考虑的情形是 $G/N$ 为循环群。

本文旨在继续 [9] 和 [8] 中关于具有非阿贝尔底的特定本原群族的覆盖数的研究。回顾一下，群 $G$ 的底是由 $G$的极小正规子群生成的子群；若 $G$ 是具有非阿贝尔底 $N$的本原群，则 $N$是 $G$ 的唯一极小正规子群，且它是非阿贝尔单群 $T$ 的直积幂 $T^m$。假设 $G/N$ 是循环的，且 $T$ 同构于交错群 $A_n$，其中 $n \geqslant 5$。若 $T_1$ 表示 $N$ 的第一个直积因子，则 $G$ 的结构由几乎单群 $X = N_G(T_1)/C_G(T_1)$ 决定，该群的底同构于 $T$，因此若 $n \neq 6$，它可以是 $A_n$ 或 $S_n$之一。若 $X \cong A_n$，则 $G$是花环积 $A_n \wr C_m$，其中 $C_m$ 作为一个 $m$-循环作用。本文关注情形 $X \cong S_n$。在这种情形下， $G$ 的结构如下。

令 $G = G_{n,\ m}$为半直积 $A_n^m \rtimes \langle\gamma\rangle$，其中 $\gamma = (1, \dots, 1, \tau)\delta \in S_n \wr S_m$，且 $\tau = (1\ 2)$，$\delta = (1 \dots m)$。若 $x_1, \dots, x_m \in A_n$，则有

$$(x_1, \dots, x_m)^\gamma = ({x_m}^\tau, x_1, \dots, x_{m-1}).$$

本文建立以下结果，将 [19]关于 $\sigma(S_n)$ 的主要结果推广到情形 $m = 1$。

定理 1. 设 $G = G_{n,\ m}$，其中 $n \geqslant 30$ 可被 6 整除且 $m \geqslant 2$。记 $\alpha(x)$ 为正整数 $x$ 的不同素因子个数。则

$$\sigma(G) = \alpha(2m) + \left(\frac{1}{2}\binom{n}{n/2}\right)^m + \sum_{i=1}^{n/3-1}\binom{n}{i}^m.$$

此外， $G$ 有一个由极大子群组成的唯一最小覆盖。

设 $G$ 为上述陈述中的群。记 $d(G)$ 为生成 $G$ 所需元素的最小数目，并令 $N$ 为 $G$ 的底。由于 $N$ 是 $G$ 的唯一极小正规子群，且 $G/N$ 是循环的， [12] 的主要定理蕴含 $d(G) = 2$。因此，考虑 $\omega(G)$ 是有意义的。 $G$ 的两个显式生成元可按如下方式构造：取 $x_1, x_2 \in A_n$ 使得 $\langle x_1\tau, x_2\tau\rangle = S_n$。则$\langle\alpha_1, \alpha_2\rangle = G$，其中 $\alpha_i = (x_i, 1, \dots, 1)\gamma$，适用于 $i = 1, 2$。我们的第二个结果如下。

定理 2. 设 $G := G_{n,m}$. 对固定的 $m \geqslant 2$，当 $n \to \infty$, $n$ 为偶数时， $\omega(G)$ 与 $\left(\frac{1}{2}\binom{n}{n/2}\right)^m$ 渐近相等；并且当 $n \to \infty$, $n$ 为偶数时， $\omega(G)/\sigma(G)$ 趋于 1。

注意，利用 [8, 定理 1 (3)] 可由定理的第一条推出第二条。一个有趣的问题是，当 $G$ 是二生成本原群且 $|G| \to \infty$ 时， $\omega(G)/\sigma(G)$ 是否趋于 1。关于一个有趣的群族 $G$，对于该群族， $\omega(G)/\sigma(G)$ 趋于 0，参见 [13, 定理 1.2]。

## 2. Proof of Theorem 1

本节证明定理 1。我们的策略是应用 [19] 的引理3.1。为方便读者，现对此作出说明。设 $G$ 是一个有限群，其极大子群的共轭类由集合 $I_G$ 编号。对于 $j \in I_G$，令 $\mathcal{M}_j$ 表示 $G$ 的相应极大子群共轭类。令 $J$ 是 $I_G$ 的一个子集，并假设 $\mathcal{C} = \bigcup_{j\in J} \mathcal{M}_j$ 是对 $G$ 的覆盖。令 $\Pi$ 是 $G$ 的一个在共轭下封闭的子集，并将被共轭类 $\mathcal{M}_j$ 覆盖的 $\Pi$ 的子集记为 $\Pi_j$，因此，当 $\Pi$ 在共轭下封闭时， $\Pi_j$ 也在共轭下封闭。若情况如此，且 $M$、 $M'$ 是 $G$ 和 $j \in J$ 的共轭极大子群，则 $|M \cap \Pi| = |M' \cap \Pi|$ 和 $|M \cap \Pi_j| = |M' \cap \Pi_j|$。对于满足 $M \notin \mathcal{C}$ 的 $G$ 的极大子群 $M$，令

$$d(M) := \sum_{j\in J} \frac{|M \cap \Pi_j|}{|M_j \cap \Pi_j|}$$

其中 $M_j$ 是 $\mathcal{M}_j$中的任意一个固定元素。

引理 1（ [19]的引理3.1）。假设上述覆盖 $\mathcal{C}$ 满足以下条件。

(1) 对所有 $x \in \Pi$ 和 $g \in G$， $x^g \in \Pi$，即 $\Pi$ 在共轭下封闭。(2) 对每个 $\pi \in \Pi$，$\mathcal{C}$ 中恰有一个元素包含 $\pi$。(3) 对于每个不属于 $\mathcal{C}$的 $G$ 的极大子群 $H$， $d(H) < 1$。

那么 $\mathcal{C}$ 是 $G$的最小覆盖，也就是说， $\sigma(G) = |\mathcal{C}|$。此外， $\mathcal{C}$ 是由极大子群构成的 $G$ 的唯一最小覆盖。

设 $G$ 是定理 1陈述中定义的群。我们将构造$J$、 $\Pi$ 和 $\mathcal{C}$，以便将引理 1应用于群 $G$。采用我们常会提及的 [3], 的术语， $G$ 是一个2型本原群，也就是说， $G$ 有一个核自由极大子群，且恰有一个极小正规子群；该子群是非阿贝尔的，其底为 $N = A_n^m$。

设 $I = \{-1, 1, 2, \ldots, n/3 - 1\}$。与 [19], 中一样，我们定义如下的集合 $B_i$、 $i \in I$。为简化记号，我们用 $[a_1, \ldots, a_k]$ 表示 $S_n$ 的共轭类，该共轭类对应于循环结构为 $(a_1, \ldots, a_k)$ 的元素；显然， $a_i$ 均为和为 $n$ 的正整数。令

$B_{-1} := [n]$,$B_1 := [1, n/2 - 2, n/2 + 1]B_2 := [2, n/2 - 1, n/2 - 1]$ 若 $n/2$ 为偶数，$B_2 := [2, n/2 - 4, n/2 + 2]$ 若 $n/2$ 为奇数，$B_i := [i, (n - i - 1)/2, (n - i + 1)/2]$ 若 $i$ 为奇数， $3 \leqslant i < n/3$,$B_i := [i, (n - i)/2, (n - i)/2]$ 若 $i$ 为偶数，$(n - i)/2$ 为奇数， $4 \leqslant i < n/3$,$B_i := [i, (n - i)/2 - 1, (n - i)/2 + 1]$ 若 $i$ 为偶数，$(n - i)/2$ 为偶数， $4 \leqslant i < n/3$.

注意，对所有 $i \in I$， $B_i \cap A_n = \varnothing$。我们将对所有 $i \in I$ 的集合 $\Pi_i$ 定义如下:

$$\Pi_i = \{(x_1, x_2, \ldots, x_m)\gamma \in G \ : \ x_1 x_2 \ldots x_m \tau \in B_i\}.$$

注意，集合 $\Pi_i$ 两两不相交，集合 $B_i$ 也两两不相交。

注意，我们尚未定义 $\Pi_0$。我们将定义若干集合，而非定义一个唯一的 $\Pi_0$；对每个整除 $m$ 的素数 $r$，我们将这些集合记为 $\Pi_{0,\,r}$。对于这样的 $r$，令 $D_1$ 为 $S_n$ 中 $(n-2)$- 轮换的共轭类，并令 $D_i$ 为 $S_n$ 中 $n$-轮换的共轭类，其中 $i=2,\ \ldots,\ r$。令 $\nu := (1\ldots r)$。对于所有 $\sigma \in \langle \nu \rangle$，令

$$\Pi_{0,r,\sigma} := \{(x_1,\ldots,x_m)\gamma^r \in G \ :\ x_i x_{i+r} x_{i+2r} \ldots x_{i+m-r}\tau \in D_{\sigma(i)}\ \forall i = 1,\ldots,r\}.$$

假设 $m$ 为偶数，或者 $r \neq 2$。我们定义

$$\Pi_{0,r} := \bigcup_{\sigma\in\langle\nu\rangle} \Pi_{0,r,\sigma}.$$

这是一个不交并。事实上，设 $\sigma_1$、$\sigma_2 \in \langle\nu\rangle$ 满足 $\sigma_1 \neq \sigma_2$，并反设存在 $(x_1,\ldots,x_m)\gamma^r \in \Pi_{0,\,r,\,\sigma_1} \cap \Pi_{0,\,r,\,\sigma_2}$。由于 $\sigma_1 \neq \sigma_2$，且 $r$ 是素数，存在 $i \in \{1,\ldots,r\}$ 使得 $\sigma_1(i) = 1$ 且 $j = \sigma_2(i) \neq 1$。由于 $x_i x_{i+r} \ldots x_{i+m-r}\tau$ 属于 $D_{\sigma_1(i)} \cap D_{\sigma_2(i)} = D_1 \cap D_j$，我们推出 $D_1 = D_j$，矛盾。因此

$$|\Pi_{0,r}| = r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^{r} |D_i|.$$

现在假设 $m$ 为奇数。我们将定义 $\Pi_{0,2}$。考虑 $S_n$ 的共轭类 $C$，其元素的循环结构为 $(p, n-p)$，其中 $p$ 是一个满足 $n/3 < p < 2n/3$ 的固定素数。注意，根据伯特兰猜想，$p$ 存在。在这种情形下，我们定义

$$\Pi_{0,2} := \{(x_1,\ldots,x_m)\gamma^2 \in G \ :\ x_1 x_3 \ldots x_m\tau \cdot x_2 x_4 \ldots x_{m-1}\tau \in C\}.$$

注意

$$|\Pi_{0,2}| = |A_n|^{m-1} \cdot |C|.$$

令 $J$ 为由 $I$ 中的元素以及形如 $(0,r)$ 的数对组成的指标集，其中 $r$ 是 $2m$ 的一个素因子，并令 $\Pi := \bigcup_{j\in J} \Pi_j$。下面的命题表明，每个 $\Pi_j$ 在共轭下封闭，从而证明引理 1 的条件 (1) 成立。

命题 1. 对所有 $i \in I$，集合 $\Pi_i$、$i \in I$ 和 $\Pi_{0,r}$（$r$ 为 $2m$ 的任意素因子）在共轭下封闭。

证明。固定 $i \in I$。若 $(x_1,\ldots,x_m)\gamma \in \Pi_i$，则元素

$$((x_1,\ldots,x_m)\gamma)^\gamma = (\tau x_m \tau, x_1, \ldots, x_{m-1}) \cdot \gamma$$

属于 $\Pi_i$，因为

$$\tau x_m \tau \cdot x_1 \ldots x_{m-1} \cdot \tau = (x_1 \ldots x_m \tau)^{\tau x_m^{-1} \tau} \in B_i,$$

并且如果 $(y_1,\ldots,y_m) \in A_n^m$，则元素

$$((x_1,\ldots,x_m)\gamma)^{(y_1,\ldots,y_m)} = (y_1^{-1}x_1y_2, y_2^{-1}x_2y_3, \ldots, y_{m-1}^{-1}x_{m-1}y_m, y_m^{-1}x_m\tau y_1\tau)\gamma$$

属于 $\Pi_i$，因为

$$y_1^{-1}x_1y_2 \cdot y_2^{-1}x_2y_3 \cdot \ldots \cdot y_{m-1}^{-1}x_{m-1}y_m \cdot y_m^{-1}x_m\tau y_1\tau \cdot \tau = (x_1\ldots x_m\tau)^{y_1} \in B_i.$$

由于 $G$ 由 $A_n^m$ 和 $\gamma$ 生成，这证明了 $\Pi_i$ 在共轭下封闭。

现在证明 $\Pi_{0,r}$ 在共轭下封闭。以下论证也适用于 $m$ 为奇数的情形 $r=2$，因此我们假设 $m$ 为偶数或 $r\neq 2$。令 $(x_1,\ldots,x_m)\gamma^r\in\Pi_{0,r,\sigma}$。注意

$$((x_1,\ldots,x_m)\gamma^r)^\gamma=(\tau x_m\tau,x_1,\ldots,x_{m-1})\gamma^r$$

并且我们有如下结论。

$$\begin{aligned}&\tau x_m\tau x_r x_{2r}\ldots x_{m-r}\tau=(x_r x_{2r}\ldots x_{m-r}x_m\tau)^{\tau x_m^{-1}\tau}\in D_{\sigma(r)}=D_{\sigma\nu^{-1}(1)}\\&x_i x_{i+r}x_{i+2r}\ldots x_{i+m-r}\tau\in D_{\sigma(i)}=D_{\sigma\nu^{-1}(i+1)}\qquad\forall i=1,\ldots,r-1.\end{aligned}$$

由此可得 $((x_1,\ldots,x_m)\gamma^r)^\gamma\in\Pi_{0,\ r,\ \sigma\nu^{-1}}\subseteq\Pi_{0,\ r}$。

对于 $(y_1,\ldots,y_m)\in A_n^m$，我们有 $((x_1,\ldots,x_m)\gamma^r)_{(y_1,\ldots,y_m)}$ 等于

$$(y_1^{-1}x_1y_{r+1},\ldots,y_{m-r}^{-1}x_{m-r}y_m,y_{m-r+1}^{-1}x_{m-r+1}\tau y_1\tau,\ldots,y_m^{-1}x_m\tau y_r\tau)\cdot\gamma^r$$

此外，若 $1\leqslant i\leqslant r$，

$$y_i^{-1}x_iy_{r+i}\cdot y_{r+i}^{-1}x_{r+i}y_{2r+i}\cdot\ldots\cdot y_{m-r+i}^{-1}x_{m-r+i}\tau y_i\tau\cdot\tau=(x_ix_{i+r}x_{i+2r}\ldots x_{i+m-r}\tau)^{y_i}$$

属于 $D_{\sigma(i)}$。这意味着 $\Pi_{0,\ r}$ 在共轭作用下封闭。 □

对于 $i\in I, i\neq -1$，定义 $\mathcal{E}_i$ 为$A_n$的极大非传递子群集合，其轨道大小为 $i$和 $n-i$；定义 $\mathcal{E}_{-1}$为 $A_n$ 的具有 2 个块的极大非本原子群集合。令 $\mathcal{F}_i:=\{N_{S_n}(M):M\in\mathcal{E}_i\}$，对所有 $i\in I$,$\mathcal{E}:=\bigcup_{i\in I}\mathcal{E}_i$ 以及 $\mathcal{F}:=\bigcup_{i\in I}\mathcal{F}_i$均成立。注意到，正如 [19]中所述，$\{A_n\}\cup\mathcal{F}$ 是 $S_n$的一个覆盖。根据 [19, 引理 5，$n\equiv 0$ 模 6 时，$n\geqslant 30$ 和 $i\in I$，$\mathcal{F}$ 中包含 $B_i$ 元素的子群只有属于 $\mathcal{F}_i$的那些，因此 $\bigcup_{i\in I}B_i$ 的元素被 $\mathcal{F}$中的子群划分。此外，对所有 $i\in I$，$\mathcal{E}_i$ 和$\mathcal{F}_i$ 都是 $S_n$ 的子群的共轭类。

对于 $i\in I$，定义 $\mathcal{M}_i$ 为由 $G$ 中以下类型的子群组成的集合：$H=N_G(M^{a_1}\times\ldots\times M^{a_m})$，其中 $a_1$、.....、$a_m\in A_n$、$M\in\mathcal{E}_i$和$N_{S_n}(M)\cap B_i\neq\varnothing$。根据 [3, 命题 1.1.44] 和 [11]，$H$是 $G$ 的一个极大子群，它补充了 $G$的底 $N=A_n^m$；此外，$H\cap N$在 $N$中与 $M^m$共轭。因此，$|H|=2m\cdot|M|^m$和 $H$有 $G$中的 $|G:H|=|A_n:M|^m$个共轭子群。对于 $2m$的每个素因子 $r$，令 $\mathcal{M}_{0,\ r}=\{M_{0,r}\}$，其中 $M_{0,\ r}=A_n^m\rtimes\langle\gamma^r\rangle$是 $G$ 的一个指数为 $r$的正规子群。令 $\mathcal{C}$ 为所有 $\mathcal{M}_j$的并集，其中 $j\in J$。$\mathcal{C}$ 的大小等于定理 1 陈述中 $\sigma(G)$ 所声称的值。

命题 2. $\mathcal{C}$ 是 $G$的一个覆盖。

证明。设 $g=(x_1,\ldots,x_m)\gamma^k\in G$，其中 $x_i\in A_n$对所有 $i$均成立。若 $(k,m)\neq 1$，则$g$ 属于包含底的 $G$ 的 $\alpha(2m)$个子群之一。现在假设 $(k,m)=1$。由于 $\langle g\rangle=\langle g^t\rangle$，若 $t$ 与 $g$的阶互素，我们可以假设 $k=1$。由于 $\mathcal{F}$ 是 $S_n$的一个覆盖，存在 $M\in\mathcal{E}$，使得奇置换 $x_1\ldots x_m\tau$属于 $N_{S_n}(M)$，并且

$$H=N_G(M\times M^{x_1}\times M^{x_1x_2}\times\ldots\times M^{x_1\ldots x_{m-1}})$$

是包含 $g$的 $\mathcal{C}$ 的一个成员。 □

命题 3. 集合 $\mathcal{M}_i$、$i\in I$ 是 $G$ 的子群共轭类。

证明. $\mathcal{M}_i$ 中给定的一个子群与 $H = N_G(M^m)$ $A_n^m$-共轭，其中 $M \in \mathcal{E}_i$。因此，由于 $\mathcal{E}_i$ 的每个元素都是 $M$ 的 $A_n$-共轭，且为 $N_{S_n}(M)A_n = S_n$，我们只需证明 $H^\gamma = N_G(M^\tau \times M^{m-1})$ 与 $H$ $A_n^m$-共轭。这是因为 $M^\tau$ 与 $M$ $A_n$-共轭，且为 $N_{S_n}(M)A_n = S_n$。□

现在我们将描述 $G$ 的极大子群。以下讨论可参见 [3]。包含底 $N = \mathrm{soc}(G)$ 的 $G$ 的极大子群为 $M_{0,r}$，其中 $r$ 是 $2m$ 的任意一个素因子。设 $U$ 是 $G$ 的一个不包含 $N$ 的极大子群，因此 $UN = G$。注意到 $U \cap N \neq \{1\}$。事实上，若反设 $U \cap N = \{1\}$，则 $U \cong G/N$ 将是循环的，由元素 $u$ 生成，因此包含 $u$ 的 $G$ 的唯一真子群将是 $U$，这与 $\mathcal{C}$ 是 $G$ 的一个覆盖、且其成员并非循环群这一事实矛盾。接下来，$U$ 可以是以下两种类型之一。第一种类型是 $U = N_G(U \cap N)$，其中 $U \cap N = M \times M^{a_2} \times \ldots \times M^{a_m}$, $a_2, \ldots, a_m \in A_n$，且 $M$ 是 $A_n$ 与 $S_n$ 的一个极大子群的交。在这种情形下，$U$ 称为乘积型极大子群（见 [3, 命题 1.1.44, 定义 1.1.45]）。第二种类型由对角型极大子群构成（见 [3, 命题 1.1.55]）。固定 $\Omega = \{1, \ldots, m\}$ 的一个划分 $\{P_1, \ldots, P_k\}$，并记 $P_i = \{a_{ij} : j = 1, \ldots, r_i\}$。给定 $A_n$ 的一组自同构 $\varphi_{ij}$，其中 $i = 1, \ldots, k$ 且 $j = 2, \ldots, r_i$，令 $\Delta_\varphi$ 为满足如下性质的 $m$ 元组 $(x_1, \ldots, x_m)$ 的集合：$\in A_n^m$，且对所有 $i$，均有 $x_{a_{ij}} = x^{\varphi_i}_{,\,a_{i1}\,j}$。然后令 $U$ 为 $\Delta_\varphi$ 在 $G$ 中的正规化子。若 $U$ 补 $N$，则 $U$ 中存在一个元素 $u = (y_1, \ldots, y_m)\delta$，其中每个 $y_i$ 都属于 $S_n$，容易看出，划分 $P$ 被 $\delta$ 稳定。若 $U$ 是 $G$ 的一个极大子群，则可假设 $P$ 在所有被 $\delta$ 稳定的非平凡划分中，按照细化关系而言是极小的，换言之

$$\Delta_\varphi = \{(y_1, \ldots, y_{m/t}, y_1^{\varphi_{1,2}}, \ldots, y_{m/t}^{\varphi_{m/t,2}}, \ldots, y_1^{\varphi_{1,t}}, \ldots, y_{m/t}^{\varphi_{m/t,t}}) : y_1, \ldots, y_{m/t} \in A_n\}$$

其中，$t$ 是 $m$的一个素因子，$\varphi_{i,\,j}$ 是 $A_n$ 的一个自同构，其中 $1 \leqslant i \leqslant m/t$、$2 \leqslant j \leqslant t$，矩阵 $(\varphi_{i,\,j})_{\,i,\,j}$ 记作 $\varphi$。若 $U$ 是$G$的一个极大子群，补足底 $N$，且具有上述形式 $N_G(\Delta_\varphi)$，其中 $\varphi$ 如上所述，则称 $U$ 为对角型极大子群。若此情形成立，则 $U \cap N = \Delta_\varphi$。

在下面的讨论中，我们固定 $A_n$ 的一个子群 $M$，使得 $N_G(M^m)$ 是 $G$ 的一个极大子群，它补足底 $N = \mathrm{soc}(G)$，换言之，$N_G(M^m)\,N = G$。

引理 2。$N_{S_n}(M)\,A_n = S_n$，特别地，$N_{S_n}(M) \not\subseteq A_n$。

证明。设 $\alpha \in S_n$。若 $\alpha \in A_n$，则 $\alpha \in N_{S_n}(M)\,A_n$，因此现在假设 $\alpha \notin A_n$。于是 $\alpha\tau \in A_n$，从而 $(\alpha, \ldots, \alpha) = (\alpha\tau, \ldots, \alpha\tau)\,(\tau, \ldots, \tau) \in G$，因为 $(\tau, \ldots, \tau) = \gamma^m$。根据假设，我们可以写成 $(\alpha, \ldots, \alpha) = nh$，其中 $n = (a_1, \ldots, a_m) \in A_n^m$，且 $h = (b_1, \ldots, b_m)\,\gamma^k \in N_G(M^m)$。由此可得 $k = 0$，因此对所有 $i = 1, \ldots, m$，都有 $b_i \in N_{S_n}(M)$。所以 $\alpha = a_1 b_1 \in A_n N_{S_n}(M)$。□

引理 3. 设 $g \in G$，且令 $r$ 为 $2m$ 的一个素因子。若 $m$ 为偶数或$r \neq 2$，则

$$|N_G(M^m)^g \cap \Pi_{0,r}| = r \cdot \left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-r} \cdot \prod_{i=1}^{r} |D_i \cap N_{S_n}(M)|.$$

若 $m$ 为奇数，则

$$|N_G(M^m)^g \cap \Pi_{0,2}| = \left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-1} \cdot |C \cap N_{S_n}(M)|.$$

证明。由于 $\Pi_{0,\ r}$ 在共轭下封闭， $N_G(M^m)^g \cap \Pi_{0,\ r}$ 的大小等于 $N_G(M^m) \cap \Pi_{0,\ r}$ 的大小，因此我们可以假设 $g = 1$。先假设 $m$ 为偶数或 $r \neq 2$。我们将对每个 $\sigma \in \langle\nu\rangle$ 计算 $|N_G(M^m) \cap \Pi_{0,\ r,\ \sigma}|$，并将所有贡献相加。固定 $\sigma \in \langle\nu\rangle$。令 $(x_1, \ldots, x_m)\gamma^r \in N_G(M^m) \cap \Pi_{0,\ r,\ \sigma}$，则 $M^m$ 等于

$$(M \times \ldots \times M)^{(x_1,\ldots,x_m)\gamma^r} = M^{x_{m-r+1}\tau} \times \ldots \times M^{x_m\tau} \times M^{x_1} \times \ldots \times M^{x_{m-r}}.$$

因此 $x_{m-r+1}\tau, \ldots, x_m\tau \in N_{S_n}(M) \cap (S_n - A_n)$ 且 $x_1, \ldots, x_{m-r} \in N_{S_n}(M) \cap A_n$。由于 $N_{S_n}(M)$ 不包含于 $A_n$，集合 $N_{S_n}(M) \cap A_n$ 和 $N_{S_n}(M) \cap (S_n - A_n)$ 的基数相同。由于 $(x_1, \ldots, x_m)\gamma^r \in \Pi_{0,\ r}$， $x_i$ 们也必须满足 $\Pi_{0,\ r,\ \sigma}$ 定义中的方程。因此，对每个方程

$$x_i x_{i+r} \ldots x_{i+m-r}\tau \in D_{\sigma(i)},$$

其中 $i = 1, \ldots, r$，我们可以自由选择元素 $x_{i+r}, \ldots, x_{m-r+i}$，每个有 $|N_{S_n}(M) \cap A_n| = \frac{1}{2}|N_{S_n}(M)|$ 种选择；而为了满足定义 $\Pi_{0,\ r,\ \sigma}$ 的方程（即 $x_i z_i \in D_{\sigma(i)}$），只需选择元素 $x_i$，$i = 1, \ldots, r$，其中 $z_i = x_{i+r} \ldots x_{i+m-r}\tau \in N_{S_n}(M)$。由于

$$D_{\sigma(i)} z_i^{-1} \cap N_{S_n}(M) = (D_{\sigma(i)} \cap N_{s_n}(M)) z_i^{-1},$$

每个 $x_i$, $i = 1, \ldots, r$ 都有 $|D_{\sigma(i)} \cap N_{S_n}(M)|$ 种选择，结论即得。

现在假设 $m$ 为奇数。令 $(x_1, \ldots, x_m)\gamma^2 \in N_G(M^m) \cap \Pi_{0,\ 2}$。则 $M^m$ 等于

$$(M \times \ldots \times M)^{(x_1,\ldots,x_m)\gamma^2} = M^{x_{m-1}\tau} \times M^{x_m\tau} \times M^{x_1} \times \ldots \times M^{x_{m-2}}.$$

因此 $x_{m-1}\tau, x_m\tau \in N_{S_n}(M) \cap (S_n - A_n)$，且 $x_1, \ldots, x_{m-2} \in N_{S_n}(M) \cap A_n$。由于 $N_{S_n}(M)$ 不包含于 $A_n$，我们知道 $x_{m-1}$ 和 $x_m$ 各有 $\frac{1}{2}|N_{S_n}(M)|$ 种选择。现在可以在 $N_{S_n}(M) \cap A_n$ 中自由选择 $x_2, \ldots, x_{m-2}$，并且需要选择 $x_1$ 来满足定义 $\Pi_{0,2}$ 的方程，即 $x_1 t \in C$，其中 $t = x_3 x_5 \ldots x_m \tau x_2 x_4 \ldots x_{m-1}\tau \in N_{S_n}(M)$。我们可以在 $Ct^{-1} \cap N_{S_n}(M) = (C \cap N_{S_n}(M))t^{-1}$ 中自由选择 $x_1$，因此 $x_1$ 有 $|C \cap N_{S_n}(M)|$ 种选择。结论即得。□

推论 1. 假设 $m$ 为偶数或 $r \neq 2$。那么 $N_G(M^m) \cap \Pi_{0,\ r} = \varnothing$ 当且仅当至少存在一个 $i \in \{1, \ldots, r\}$ 使得 $N_{S_n}(M) \cap D_i = \varnothing$。此外，若 $m$ 为奇数且 $r = 2$，则 $N_G(M^m) \cap \Pi_{0,\ 2} = \varnothing$ 当且仅当 $N_{S_n}(M) \cap C = \varnothing$。

引理 4. 若 $i \in I$，则 $|N_G(M^m) \cap \Pi_i| = \left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M)|$。

证明. 设 $(x_1, \ldots, x_m)\gamma \in N_G(M^m) \cap \Pi_i$，则 $M^m$ 等于

$$(M^m)^{(x_1,\ldots,x_m)\gamma} = (M^{x_1} \times \ldots \times M^{x_m})^\gamma = M^{x_m\tau} \times M^{x_1} \times \ldots \times M^{x_{m-1}}.$$

因此， $x_m\tau \in N_{S_n}(M) \cap (S_n - A_n)$ 和 $x_1, \ldots, x_{m-1} \in N_{S_n}(M) \cap A_n$。由于 $N_{S_n}(M)$ 不包含于 $A_n$，$x_m$ 的可选数量为 $\frac{1}{2}|N_{S_n}(M)|$。现在，我们可以在 $N_{S_n}(M) \cap A_n$ 中自由选择 $x_2, \ldots, x_{m-1}$，并且需要选择 $x_1$ 以满足定义 $\Pi_i$ 的方程，即 $x_1 t \in B_i$，其中 $t = x_2 \ldots x_m\tau \in N_{S_n}(M)$。

换言之，我们可以在 $B_i t^{-1} \cap N_{S_n}(M) = (B_i \cap N_{S_n}(M))t^{-1}$中自由选择 $x_1$，因此 $x_1$ 的可选数量为 $|B_i \cap N_{S_n}(M)|$。结论得证。□

推论 2. 若 $i \in I$，则 $N_G(M^m) \cap \Pi_i = \varnothing$ 当且仅当 $B_i \cap N_{S_n}(M) = \varnothing$。

下述命题蕴含引理 1 的条件 (2) 成立。

命题 4. 设 $\pi \in \Pi$，则存在唯一的 $L \in \mathcal{C}$ 使得 $\pi \in L$。

证明. 若 $\pi \in \Pi_{0,\,r}$ 对某个整除 $2m$ 的素数 $r$ 成立，则 $M_{0,\,r}$ 是 $\mathcal{M}$ 中包含 $\pi$ 的唯一子群。这由推论 1 以及以下事实得出： $\mathcal{F}$ 中没有子群与集合 $D_1, \dots, D_r$ 均有非空交，因为 $n$-轮换不属于非传递子群，而 $(n-2)$-轮换不会稳定含有 2 个块的划分。

现在假设对某个 $i \in I$ 有 $\pi \in \Pi_i$。那么 $\pi = (x_1, \dots, x_m)\gamma$，其中 $x_1 \dots x_m \tau \in B_i$，特别是对每个整除 $2m$ 的素数 $r$，都有 $\pi \notin M_{0,\,r}$。存在唯一的 $H \in \mathcal{F}$ 使得 $x_1 \cdots x_m \tau \in H$ 且 $H = N_{S_n}(M)$，其中 $M = H \cap A_n \in \mathcal{E}$。假设 $\pi = (x_1, \dots, x_m)\gamma$ 属于 $N_G(M^{a_1} \times \dots \times M^{a_m})$。那么 $M^{a_1} \times \dots \times M^{a_m}$ 等于

$$(M^{a_1} \times \dots \times M^{a_m})^{(x_1,\dots,x_m)\gamma} = M^{a_m x_m \tau} \times M^{a_1 x_1} \times \dots \times M^{a_{m-1} x_{m-1}}.$$

因此，对于 $i$，有 $1 \leqslant i \leqslant m-1$、 $a_i x_i a_{i+1}^{-1} \in H$ 和 $a_m x_m \tau a_1^{-1} \in H$。从第 $i$ 个元素开始将这些元素相乘，得到

$$a_i x_i x_{i+1} \dots x_m \tau x_1 x_2 \dots x_{i-1} a_i^{-1} \in H,$$

这可以写成

$$(x_1 \dots x_m \tau)^{x_1 \dots x_{i-1}} = x_i x_{i+1} \dots x_m \tau x_1 x_2 \dots x_{i-1} \in H^{a_i}.$$

特别地，$x_1 \dots x_m \tau \in H^{a_1}$。由于 $\mathcal{F}$ 在共轭下封闭， $H$ 的唯一性意味着 $H^{a_1} = H$，因此 $a_1 \in N_{S_n}(H) = H$，因为它是 $S_n$ 的一个极大子群 $H$。现在我们可以将上述等式改写为

$$a_i \in H x_1 x_2 \dots x_{i-1}, \quad \forall i = 2, \dots, m.$$

由此可得，对于所有 $i = 2,$ ....., $m$，都有 $M^{a_1} = M$ 和 $M^{a_i} = M^{x_1 \dots x_{i-1}}$，因此 $\mathcal{C}$ 中包含 $\pi$ 的唯一子群是

$$N_G(M \times M^{x_1} \times M^{x_1 x_2} \times \dots \times M^{x_1 \dots x_{m-1}}).$$

证明至此完成。 □

为了完成定理 1 的证明，我们还需证明引理 1 的条件 (3) 成立，换言之，对于 $G$ 中不属于 $\mathcal{C}$ 的每个极大子群 $H$，都有 $d(H) < 1$。

引理 5. 对于 $n \geqslant 30$, $|\Pi_{0,2}|$ 的值在 $m$ 为偶数时最小。此外，若 $g \in G$，则 $|N_G(M^m)^g \cap \Pi_{0,2}|/|\Pi_{0,2}| \leqslant 2n(n-2)/|S_n : N_{S_n}(M)|^m$。

证明。我们有 $|D_1| = n!/(2(n-2))$, $|D_2| = (n-1)!$ 和 $|C| = n!/(p(n-p))$.

$$|\Pi_{0,2}| = \begin{cases} 2|A_n|^{m-2}|D_1||D_2| = |A_n|^m \cdot 4/(n(n-2)) & \text{if } m \text{ is even} \\ |A_n|^{m-1}|C| = |A_n|^m \cdot 4/(2p(n-p)) & \text{if } m \text{ is odd.} \end{cases}$$

注意到 $2p(n-p) < 2(2n/3)^2 \leqslant n(n-2)$ 是 $n/3 < p < 2n/3$ 和 $n \geqslant 30$。因此，当 $m$ 为偶数时，$|\Pi_{0,2}|$ 的值最小。现在我们来证明所述不等式。由于 $\Pi_{0,2}$ 在共轭下封闭，我们不妨假设 $g = 1$。根据引理 3，

$$\frac{|N_G(M^m) \cap \Pi_{0,2}|}{|\Pi_{0,2}|} = \begin{cases} \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^{m-2} \cdot \frac{|D_1 \cap N_{S_n}(M)||D_2 \cap N_{S_n}(M)|}{|D_1||D_2|} & \text{if } m \text{ is even} \\ \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^{m-1} \cdot \frac{|C \cap N_{S_n}(M)|}{|C|} & \text{if } m \text{ is odd.} \end{cases}$$

该陈述中的不等式可由以下事实得到： $D_1$、 $D_2$、 $C$中的任意一个与 $N_{S_n}$（$M$）的交集大小至多为 $|N_{S_n}$（$M$）$|$。□

引理 6. 若 $d$是 $n$的因数，且 $2 \leqslant d \leqslant n/2$，则（$n/d$）！ $^d \cdot d!$ 6 2（$n/2$）！ $^2$。

证明。我们按照 [14, 引理 21]的证明进行。首先假设 $d \leqslant n/d$。

$$\begin{aligned}(n/d)!^d \cdot d! &\leqslant (n/d)!^2 \cdot 2 \cdot ((n/d)! \cdot d)^{d-2} \leqslant (n/d)!^2 \cdot 2 \cdot ((n/d)! \cdot n/d)^{d-2} \\ &\leqslant (n/d)!^2 \cdot 2 \cdot ((n/d)^{n/d})^{d-2} = (n/d)!^2 \cdot 2 \cdot (n/d)^{2(n/2-n/d)} \\ &\leqslant (n/d)!^2 \cdot ((n/d)+1)^2 \cdot \ldots \cdot (n/2)^2 \cdot 2 = 2(n/2)!^2,\end{aligned}$$

其中，在第四个不等式中，我们使用了对所有 $r \geqslant 2$都有 $r!$ $\leqslant r^{r-1}$这一事实。

现在假设 $d > n/d$。由于 $2 \leqslant n/d \leqslant n/2$，在上述不等式中交换 $n/d$和 $d$ 的作用，我们得到 $d!$ $^{n/d} \cdot$（$n/d$）！ 6 2（$n/2$）！ $^2$。如果 $a > b \geqslant 2$ 为整数，则 $a!$ $^b \cdot b!$ $> b!$ $^a \cdot a!$，因为

$$\begin{aligned}a!^{b-1} &= (a \cdot (a-1) \cdot \ldots \cdot (b+1))^{b-1} \cdot b!^{b-1} \geqslant \left((b+1)^{(a-b)}\right)^{b-1} \cdot b!^{b-1} \\ &> b^{(a-b)(b-1)} \cdot b!^{b-1} \geqslant b!^{(a-b)} \cdot b!^{b-1} = b!^{a-1}.\end{aligned}$$

将此应用于 $a = d, b = n/d$，我们有 $(n/d)!^d \cdot d!$ $< d!^{n/d} \cdot (n/d)!$ 6 $2(n/2)!^2$。 □

引理 7. 设 $H$ 是 $S_n$ 的一个极大子群，使得 $H \notin \mathcal{F}$，并固定 $i \in I, M \in \mathcal{E}_i$。那么，要么 $|H| \leqslant |N_{S_n}(M)|$，要么 $H \cap B_i = \varnothing$。

证明. 根据奥南–斯科特定理， $S_n$ 的极大子群属于以下类型之一：(1) 本原；(2) 极大非传递，与某个 $k \in \{1, \ldots, n/2-1\}$ 对应的 $S_k \times S_{n-k}$ 同构；(3) 极大非本原，当 $2 \leqslant a, b < n$ 满足 $ab = n$ 时，与 $S_a \wr S_b$ 同构。若 $H$ 是非传递的，则 $H \cong S_k \times S_{n-k}$ 与$n/3 \leqslant k < n/2$，因此，如果 $N_{S_n}(M)$ 是非传递的，则 $|H| \leqslant (n/3)!(2n/3)!$ 6 $(n/3-1)!(2n/3+1)!$ $\leqslant |N_{S_n}(M)|$。另一方面，若 $N_{S_n}(M)$ 是传递的，则 $i = -1$ 且 $H \cap B_{-1} = \varnothing$。

现在假设 $H$ 是传递的。若 $H$ 是非本原的，则 $|H| = (n/d)!^d \cdot d!$ ，其中 $d$是 $n$，$d \neq 1, 2, n$ 的因数。由引理 6，若 $N_{S_n}(M)$ 是非本原的，则 $|H| = (n/d)!^d \cdot d!$ 6 $(n/2)!^2 \cdot 2!$ $= |N_{S_n}(M)|$。若 $N_{S_n}(M)$ 是非传递的，则$|H| = (n/d)!^d \cdot d!$ 6 $(n/2)!^2 \cdot 2!$ 6 $(n/3-1)!(2n/3+1)!$ $\leqslant |N_{S_n}(M)|$。若 $H$是本原的，则要么 $H = A_n$，此时 $H \cap B_i = \varnothing$；要么 $H \neq A_n$，此时由 [17]得 $|H| < 4^n$。由于 $n \geqslant 30$，我们有 $4^n \leqslant (n/2)!^2 \cdot 2 \leqslant (n/3-1)!(2n/3+1)!$，结论得证。□

命题 5. 设 $H$ 是 $G$ 的一个不属于 $\mathcal{C}$ 的极大子群。那么 $d(H) < 1$。

证明。假设 $H$ 是乘积型的。那么 $H$ 共轭于 $N_G(M^m)$，其中 $M$ 是 $A_n$ 与 $S_n$ 的一个极大子群的交，该极大子群既不具有 $A_n$ 的形式，也不具有 $S_{n/2} \wr S_2$ 或 $S_i \times S_{n-i}$, $i = 1, 2, \ldots, n/3 - 1$ 的形式。因此，根据引理 6 以及 $2(n/2)!^2 \leqslant (n/3)!\,(2n/3)!$ 为 $n \geqslant 30$ 这一事实，有 $|N_{S_n}(M)| \leqslant (n/3)!\,(2n/3)!$。如果 $M$ 是本原的，根据 [17]，我们有 $|N_{S_n}(M)| < 4^n \leqslant 2(n/2)!^2 \leqslant (n/3)!\,(2n/3)!$。由于对所有 $j \in J$，$\Pi_j$ 在共轭下封闭，因此对所有 $j \in J$，我们有 $|H \cap \Pi_j| = |N_G(M^m) \cap \Pi_j|$。我们将使用对所有 $k \geqslant 2$ 均成立的斯特林不等式：

$$\sqrt{2\pi k}\,(k/e)^k \leqslant k! \leqslant e\sqrt{k}\,(k/e)^k.$$

假设 $m$ 为偶数或 $r \neq 2$。由引理 3 以及 $\Pi_{0,r} \subseteq M_{0,r}$ 这一事实，

$$\begin{aligned}\frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} &= \frac{r \cdot \left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-r} \cdot \prod_{i=1}^{r} |D_i \cap N_{S_n}(M)|}{r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^{r} |D_i|} \\ &\leqslant \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^{m-r} \cdot \prod_{i=1}^{r} \frac{|N_{S_n}(M)|}{|D_i|} = \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^{m} \cdot 2(n-2)n^{r-1} \\ &\leqslant \left(\frac{(n/3)!\,(2n/3)!}{n!}\right)^{m} \cdot 2n^r \leqslant 2 \cdot \left(\frac{2^{2/3}}{3}\right)^{nm} \cdot \left(\frac{ne^2\sqrt{n}}{3\sqrt{\pi}}\right)^{m}.\end{aligned}$$

由引理 5，$|N_G(M^m) \cap \Pi_{0,2}|/|\Pi_{0,2}| \leqslant 2n(n-2)/|S_n| : N_{S_n}(M)|^m$，于是当 $m$ 为奇数时，在情形 $r = 2$ 下也有上述不等式。

根据 [19, 引理 5.4、5.5、5.9、5.10]，的证明，$\sum_{i \in I} \frac{|B_i \cap N_{S_n}(\quad M \quad)()|}{|B_i \cap N_{S_n}\ M_i|}$ 的最大值可通过将 $n = 30$ 代入表达式 $\frac{3n^2+27n+54}{4n^2-9}$ 得到，因此小于 0.9925。由引理 7，

$$\begin{aligned}\sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} &= \sum_{i \in I} \frac{\left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M)|}{\left(\frac{1}{2}\,|N_{S_n}(M_i)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M_i)|} \\ &\leqslant \sum_{i \in I} \frac{|B_i \cap N_{S_n}(M)|}{|B_i \cap N_{S_n}(M_i)|} < 0.9925\end{aligned}$$

我们得到

$$\begin{aligned}d(H) &= \sum_{r \in P(2m)} \frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} + \sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} \\ &< 2m \cdot \left[\left(\frac{2^{2/3}}{3}\right)^{n} \cdot \frac{ne^2\sqrt{n}}{3\sqrt{\pi}}\right]^{m} + 0.9925\end{aligned}$$

由于 $n \geqslant 30$，因此这小于 1。

现在我们转而研究 $G$ 的对角型极大子群以及补足底 $N$ 的子群。设 $H$ 是这样一个子群。回顾一下，$H \cap N = \Delta_\varphi$ 的阶为 $|A_n|^{m/t}$，其中 $t$ 是 $m$ 的一个素因子。我们有

$$\begin{aligned}d(H) &= \sum_{r \in P(2m)} \frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} + \sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} \\ &\leqslant |H| \cdot \left(\sum_{r \in P(2m)} \frac{1}{|\Pi_{0,r}|} + \sum_{i \in I} \frac{1}{|N_G(M_i^m) \cap \Pi_i|}\right).\end{aligned}$$

由于 $HN=G$，我们有 $C_{2m}\cong G/N=HN/N\cong H/H\cap N$，因此

$$|H|=|H:H\cap N|\cdot|H\cap N|=2m\cdot|\Delta_\varphi|=2m\cdot(n!/2)^{m/t}.$$

首先假设 $m$ 为偶数或 $r\neq 2$。由于 $2\leqslant r\leqslant m$,

$$\begin{aligned}|\Pi_{0,r}|&=r\cdot|A_n|^{m-r}\cdot\prod_{i=1}^{r}|D_i|=r\cdot\left(\frac{n!}{2}\right)^{m-r}\cdot\frac{n!}{n}\cdot\left(\frac{n!}{2(n-2)}\right)^{r-1}\\&=\frac{r\cdot n!^m}{2^{m-1}n(n-2)^{r-1}}\geqslant\frac{2\cdot n!^m}{2^{m-1}n^r}\geqslant\frac{n!^m}{2^{m-2}n^m}.\end{aligned}$$

由引理 5 可知，$|\Pi_{0,\,2}|$ 的最小值在 $m$ 为偶数时取得，因此上述关于 $|\Pi_{0,\,r}|$ 的不等式在所有情形下均成立。

对所有 $i\in I$，固定 $M_i\in\mathcal{E}_i$。$N_{S_n}(M_i)$ 的可能最小阶为 $i\in I$，此时 $M_i$ 是具有两个块的非本原群，因此 $|N_{S_n}(M_i)|\geqslant 2(n/2)!^2$。由于 $B_i\cap N_{S_n}(M_i)\neq\varnothing$，由引理 4 可得

$$|N_G(M_i^m)\cap\Pi_i|=\left(\frac{1}{2}\,|N_{S_n}(M_i)|\right)^{m-1}|B_i\cap N_{S_n}(M_i)|\geqslant(n/2)!^{2(m-1)}.$$

由此可得

$$\begin{aligned}d(H)&\leqslant 2m\left(\frac{n!}{2}\right)^{m/t}\cdot\left(\sum_{r\in P(2m)}\frac{2^{m-2}n^m}{(n!)^m}+\sum_{i\,\in\,I}\frac{1}{(n/2)!^{2(m-1)}}\right)\\&\leqslant 2m\left(\frac{1}{2}(n/e)^n e\sqrt{n}\right)^{m/t}\left(2^{m-1}\frac{mn^m}{(n/e)^{nm}}+\frac{n}{(n/(2e))^{n(m-1)}}\right)<1\end{aligned}$$

对于 $m\geqslant 3$ 和 $n\geqslant 30$，其中我们用到了这样的事实：若 $m=3$，则 $t\geqslant 2$ 和 $t=3$。

现在假设 $m=2$。我们将通过证明对所有 $i\in I$，$H\cap\Pi_{0,\,2}$ 和 $H\cap\Pi_i$ 均为空，来说明 $d(H)=0$。我们有 $H=N_G(\Delta_\varphi)$，其中 $\Delta_\varphi=\{(\alpha,\alpha^\varphi):\alpha\in A_n\}$，对于 $\varphi\in\mathrm{Aut}(A_n)\cong S_n$ 以及

$$\begin{aligned}\Pi_{0,\,2}&=\{(x_1,x_2)\gamma^2:\quad x_1\tau\in D_1,\ x_2\tau\in D_2\}\cup\{(x_1,x_2)\gamma^2:\quad x_1\tau\in D_2,\ x_2\tau\in D_1\},\\\Pi_i&=\{(x_1,x_2)\gamma:\ \ x_1x_2\tau\in B_i\},\qquad i\in I.\end{aligned}$$

对于 $i\in I$，我们有：若 $(x_1,x_2)\gamma\in H\cap\Pi_i$，则

$$(\alpha,\alpha^\varphi)^{(x_1,x_2)\gamma}=(\alpha,\alpha^\varphi)^{(x_1,x_2)(1,\tau)\delta}=(\alpha^{x_1},\alpha^{\varphi x_2\tau})^\delta=(\alpha^{\varphi x_2\tau},\alpha^{x_1})\in\Delta_\varphi,$$

因此 $\varphi x_2\tau\varphi=x_1$，等价地，$(\varphi x_2\tau)^2=x_1x_2\tau$，这不成立，因为 $(\varphi x_2\tau)^2\in A_n$ 且 $x_1x_2\tau\notin A_n$。因此，对于所有 $i\in I$，$H\cap\Pi_i=\varnothing$。

若 $(x_1,x_2)\gamma^2\in H\cap\Pi_{0,\,2}$，则对于所有 $\alpha\in A_n$,

$$(\alpha,\alpha^\varphi)^{(x_1,x_2)\gamma^2}=(\alpha,\alpha^\varphi)^{(x_1,x_2)(\tau,\tau)}=(\alpha^{x_1\tau},\alpha^{\varphi x_2\tau})\in\Delta_\varphi.$$

因此 $x_1\tau\varphi=\varphi x_2\tau$，即 $\varphi^{-1}x_1\tau\varphi=x_2\tau$。这是一个矛盾，因为根据 $\Pi_{0,\,2}$ 的定义，$x_1\tau$ 和 $x_2\tau$ 在 $S_n$ 中并不共轭。因此 $H\cap\Pi_{0,\,2}=\varnothing$。□

## 3. Proof of Theorem 2

对于 $\omega(G)$ 的计算，我们采用与 [7] 中相同的策略。我们使用以下结果，该结果可见于 [6]。我们采用的表述取自 [2,推论 5.1。2] （“对称情形”）。给定概率空间中的一个事件 $E$，我们用 $P(E)$ 表示其概率，用 $\overline{E}$ 表示其补集。按照惯例，$e$ 表示自然对数的底。

定理 3（Lov´asz 局部引理）。设 $E_1, E_2, \ldots, E_n$ 是任意概率空间中的事件。设 $(V, E)$ 是一个有向图，其中 $V = \{1, \ldots, n\}$ 是顶点集，并假设对于每个 $i \in V$，事件 $E_i$ 与事件集合 $E_j$ 相互独立，使得 $(i, j) \notin E$。设 $d$ 是图 $(V, E)$ 中顶点的最大度。若对每个 $i \in V$

$$P(E_i) \leqslant \frac{1}{e(d+1)}$$

那么 $P\left(\bigcap_{i\in V} \overline{E_i}\right) > 0$。

Lov´asz 局部引理中提到的相互独立条件如下：

$$P\left(E_i | \bigcap_{j\in S} \overline{E_j}\right) = P(E_i),$$

对所有 $i \in V$ 以及 $\{j \in V$ 的所有子集 $S : (i, j) \notin E\}$。

定义

$$\mathcal{N} = \{N_G(M \times M^{a_2} \times \ldots \times M^{a_m}) \ : \ M \in \mathscr{F}\},$$

其中，$\mathscr{F}$ 是 $A_n$ 中具有 2 个块的极大非本原子群族，$(S_{n/2} \wr S_2) \cap A_n$，且 $a_2, \ldots, a_m \in A_n$。注意，若 $H \in \mathcal{N}$，则对某个 $M \in \mathscr{F}$，$H$ 在 $G$ 中与 $N_G(M^m)$ 共轭。根据命题 1.1，$G$ 中包含于 $\mathcal{N}$ 的子群在 $G$ 中是极大的。[3, 44] 和 [11]。

令 $B$ 为 $S_n$ 中的 $n$-轮换集合，并令 $\Pi$ 为 $G$ 中具有形式 $(x_1, \ldots, x_m)\gamma$ 且满足性质 $x_1 \ldots x_m\tau \in B$ 的元素集合。注意，这些集合正是第 2 节中所称的 $B_{-1}$ 和 $\Pi_{-1}$。

引理 8. $\Pi$ 是 $G$ 的一个共轭类。

证明。注意 $B \nsubseteq A_n$，因此存在 $z \in A_n$ 使得 $z\tau \in B$。由此可得 $\pi := (z, 1, \ldots, 1)\gamma \in \Pi$。我们证明 $\Pi$ 是 $\pi$ 在 $G$ 中的共轭类。设 $(x_1, \ldots, x_m)\gamma \in \Pi$，我们将证明该元素在 $G$ 中与 $\pi$ 共轭。存在 $a \in S_n$ 使得 $(x_1 \ldots x_m\tau)^a = z\tau$。若 $a \notin A_n$，则 $b = x_1 \ldots x_m\tau a \in A_n$ 且 $(x_1 \ldots x_m\tau)^b = (x_1 \ldots x_m\tau)^a$，因此不妨设 $a \in A_n$。令 $y_1 := a$，并令 $y_i := x_i \ldots x_m\tau a\tau$，其中 $i = 2, \ldots, m$。则 $((x_1, \ldots, x_m)\gamma)_{(y_1,\ldots,y_m)}$ 等于

$$(y_1^{-1}x_1y_2, y_2^{-1}x_2y_3, \ldots, y_{m-1}^{-1}x_{m-1}y_m, y_m^{-1}x_m\tau y_1\tau)\gamma = (z, 1, \ldots, 1)\gamma = \pi.$$

证明到此结束。 □

对于 $H \in \mathcal{N}$ 和 $K \leqslant G$，定义

$$C(H) = \Pi \cap H, \qquad f_H(K) = \frac{|C(H) \cap K|}{|C(H)|}.$$

设 $g \in G$ 满足 $H = (N_G(M^m))^g$。由引理 4 和引理 8,

$$\begin{aligned}|C(H)| &= |H \cap \Pi| = |(N_G(M^m))^g \cap \Pi| = |N_G(M^m) \cap \Pi| \\ &= \left(\frac{1}{2}\,|N_{S_n}(M)|\right)^{m-1} \cdot |B \cap N_{S_n}(M)| = 2/n \cdot (n/2)!^{2m}.\end{aligned}$$

由于 $H$ 是 $G$ 的非正规极大子群，因此它是自正规化的。由于 $\mathcal{N}$ 是 $G$ 中 $H$ 的共轭类,

$$l = |\mathcal{N}| = |G : H| = \frac{(n!/2)^m \cdot 2m}{(n/2)!^{2m} \cdot 2m} = \frac{1}{2^m}\binom{n}{n/2}^m < 2^{m(n-1)}.$$

定义图 $\Gamma$，其顶点是 $\mathcal{N}$ 的二元子集 $v = \{H_1, H_2\}$，且满足 $H_1 \neq H_2$。若 $v \cap w \neq \varnothing$，则顶点 $v$ 与 $w$ 之间有一条边。图 $\Gamma$ 的每个顶点的度为 $d = 2(l-2) < 2^{m(n-1)+1}$。对所有 $H \in \mathcal{N}$，均匀且相互独立地选取 $g_H \in C(H)$，并令 $E_v$ 为事件 $\langle g_{H_1}, g_{H_2}\rangle \neq G$，等价地，$\langle g_{H_1}, g_{H_2}\rangle$ 包含于 $G$ 的某个极大子群中。容易看出，相互独立条件成立（另见 [7, 第 3] 节）。我们的目标是证明，对于图 $\Gamma$ 的每个顶点 $v$，都有 $P(E_v) \leqslant 1/(e(d+1))$。如果成立，那么局部引理表明，可以在每个 $C(H)$ 中选取一个 $g_H$，使得 $H \in \mathcal{N}$，且对 $\mathcal{N}$ 中所有 $H_1 \neq H_2$，都有 $\langle g_{H_1}, g_{H_2}\rangle = G$；因此这些元素构成 $G$ 的生成图中的一个团，换言之，$\omega(G) \geqslant |\mathcal{N}|$。结合 [8, 定理 1 (3)], ，即可得到定理 2 的结论。

在下面的讨论中，我们将讨论 $G$ 的各种类型的极大子群，这些子群已在第 2 节中进行了描述。

设 $\mathcal{M}_1$ 是 $S_n$ 的极大非传递子群族，$\mathcal{M}_2$ 是 $S_n$ 中不同于 $A_n$ 的本原极大子群族，$\mathcal{M}_j$ 是 $S_n$ 中具有 $j$ 个块的 $j \in \{3,4\}$ 的极大非本原子群族，$\mathcal{M}_5$ 是 $S_n$ 中至少具有 5 个块的极大非本原子群族。设 $\mathcal{H}$ 是 $G$ 中不属于 $\mathcal{N}$ 和 $J = \{1,2,3,4,5,6\}$ 的所有极大子群组成的族。我们将 $\mathcal{H}$ 写成并集 $\mathcal{H}_1 \cup \ldots \cup \mathcal{H}_6$，其中各个 $\mathcal{H}_j$ 定义如下。对于满足 $1 \leqslant j \leqslant 5$ 的 $j$，$\mathcal{H}_j$ 是 $\mathcal{H}$ 的子集，由形如 $N_G(M \times M^{a_2} \times \ldots \times M^{a_m})$ 的子群组成，其中 $a_2$、.....、$a_m \in A_n$，$N_{S_n}(M) \in \mathcal{M}_j$，且 $N_{S_n}(M) \cap A_n = M$。$\mathcal{H}_6$ 是 $G$ 的对角型极大子群族。

固定 $\Gamma$ 的一个顶点 $v = \{H_1, H_2\}$。对于 $j \in J$，令 $E_{v,j}$ 表示$\langle g_{H_1}, g_{H_2}\rangle$ 包含于 $\mathcal{H}_j$ 的一个成员中的概率。显然，我们有

$$P(E_v) \leqslant \sum_{j \in J} P(E_{v,j}).$$

设 $[H]$ 是 $G$ 中子群 $H$ 在 $G$ 中的共轭类，而 $m_{H_i}([H])$ 表示 $C(H_i)$ 中一个固定元素所属于的 $H$ 的不同共轭子群的个数，其中 $i = 1$，2。根据引理 8，这一定义良好。在下列求和中，$[H]$ 遍历 $\mathcal{H}_j$ 中元素的共轭类集合。仿照 [7] 中的论证，我们有，对于 $j \in J$,

$$P(E_{v,j}) \leqslant \sum_{[H]} m_{H_1}([H]) \max_{K \in [H]} (f_{H_2}(K)).$$

设 $c_{v,\ j}$ 表示 $\mathcal{H}_j$ 中满足以下条件的子群共轭类的个数：该共轭类中存在 $H$，使得 $H\cap C(H_1)\neq\varnothing$ 且 $H\cap C(H_2)\neq\varnothing$。由此可得

$$(\star)\qquad P(E_{v,j})\leqslant c_{v,j}\cdot\min_{\{i_1,i_2\}=\{1,2\}}\left(\max_{H\in\mathcal{H}_j,K\in[H]}(m_{H_{i_1}}([H])\cdot f_{H_{i_2}}(K))\right).$$

设 $s_{v,\ j}$ 为 $\mathcal{H}_j$ 中满足 $H\cap C(H_1)\neq\varnothing$ 且$H\cap C(H_2)\neq\varnothing$的子群 $H$ 的个数。那么

$$(\star\star)\qquad P(E_{v,j})\leqslant\sum_{H\in\mathcal{H}_j}f_{H_1}(H)f_{H_2}(H)\leqslant s_{v,j}\cdot\max_{H\in\mathcal{H}_j}(f_{H_1}(H)\cdot f_{H_2}(H)).$$

引理9. 设 Γ的一个顶点为 $v=\{H_1,H_2\}$。那么，对于足够大的 $n$，有 $c_{v,\ 2}\leqslant n$；对于 $j\in\{3,4\}$，有 $c_{v,\ j}\leqslant 1$；$c_{v,\ 5}\leqslant 2\sqrt{n}$；并且 $c_{v,\ 6}\leqslant m\cdot 2^m$。

界 $c_{v,\ 2}\leqslant n$ 取决于有限单群分类。

证明. 注意到 $c_{v,j}$ 不大于 $\mathcal{H}_j$中子群的共轭类数。此外，若 $H\in\mathcal{H}$，则可写成 $H=N_G(H\cap N)$，从而可将问题归结为计算 $N$中形如 $H\cap N$的子群的 $G$-共轭类。还要注意，若 $M$和 $L$在 $A_n$中共轭，则 $N_G(M^m)$ 和 $N_G(L^m)$ 在 $G$ 中通过形如 $(c,c,\ldots,c)\in A_n^m$且满足 $M^c=L$的元素共轭。因此，对于满足 $1\leqslant j\leqslant 5$ 的 $j$，$\mathcal{H}_j$ 中子群的共轭类数不大于属于 $\mathcal{M}_j$的 $S_n$的子群的共轭类数。因此，对于 $j\neq 6$，我们可以使用在引理 5]中计算得到的 $c_{v,j}$ 的界。换言之，对于足够大的 $n$，有 $c_{v,2}\leqslant n$；对于 $j\in\{3,4\}$，有 $c_{v,j}\leqslant 1$；并且 $c_{v,5}\leqslant 2\sqrt{n}$。

接下来需要对 $c_{v,\ 6}$ 进行界定。我们将使用以下事实：如果 $X\leqslant Y$ 是有限群，且 $Y$ 作用于有限集 Ω 上，那么记 $u_X$ 为该作用的 $X$-轨道数，记 $u_Y$ 为该作用的 $Y$-轨道数，则有 $u_Y\leqslant u_X\leqslant|Y\colon X|\cdot u_Y$。由于 $n$ 大于 6，$\mathrm{Aut}(A_n)\cong S_n$，因此，底 $N=A_n^m$ 中任意两个同构的对角子群 $\Delta_{\varphi_1}$、$\Delta_{\varphi_2}$ 在包含 $G$ 的群 $S_n^m\rtimes\langle\delta\rangle$ 中通过 $S_n^m$ 的某个元素共轭。由此可知，同构对角子群的 $G$-类数至多等于 $A_n^m$-类数，而后者至多为 $|S_n\colon A_n|^m=2^m$。我们知道，对角子群的同构类数等于 $m$ 的素因子数（见第 2 节）。因此 $c_{v,\ 6}\leqslant m\cdot 2^m$。□

引理 10. 设 $v$ 是 $\Gamma$ 的一个顶点，并假设 4 整除 $n$。则 $s_{v,\ 4}$ 6 1。

证明。设 $v=\{H_1,H_2\}$，并令 $H\in\mathcal{H}_4$。记

$$H=N_G(R^{b_1}\times\ldots\times R^{b_m})\in\mathcal{H}_4,\qquad H_i=N_G(M_i^{a_{i1}}\times\ldots\times M_i^{a_{im}})\in\mathcal{N},$$

对于 $i=1,2$，其中每个 $a_{ij}$和每个 $b_j$都属于 $A_n$，$N_{S_n}(M_i)$ 是 $S_n$ 的一个极大非本原子群，对 $i=1,2$ 有 2 个块，而 $N_{S_n}(R)$ 是 $S_n$ 的一个极大非本原子群，有 4 个块。假设对 $i=1,2$，$H\cap C(H_i)=H\cap\Pi\cap H_i\neq\varnothing$。我们需要证明，$H$ 由这些条件唯一确定，换言之，每个 $R^{b_j}$ 都唯一确定。根据引理 5],的证明，只需证明对 $i=1,2$ 以及对$j=1,\ldots,m$，$B\cap N_{S_n}(M_i^{a_{ij}})\cap N_{S_n}(R^{b_j})\neq\varnothing$。

固定 $i \in \{1,2\}$，并令 $h = (x_1, \ldots, x_m)\gamma \in H \cap C(H_i) = H \cap H_i \cap \Pi$。由于 $h \in \Pi$，根据定义 $x_1 \ldots x_m \tau \in B$。另一方面，作为 $h \in H$， $R^{b_1} \times \ldots \times R^{b_m}$等于

$$(R^{b_1} \times \ldots \times R^{b_m})^{(x_1,\ldots,x_m)\gamma} = R^{b_m x_m \tau} \times R^{b_1 x_1} \times R^{b_2 x_2} \times \ldots R^{b_{m-1} x_{m-1}}.$$

由此可得，对于 $j = 1, \ldots, m-1$， $b_m x_m \tau b_1^{-1} \in N_{S_n}(R)$ 和 $b_j x_j b_{j+1}^{-1} \in N_{S_n}(R)$。固定 $j \in \{1, \ldots, m\}$。从第 $j$ 项开始将所有项相乘，得到

$$b_j x_j x_{j+1} \ldots x_m \tau x_1 x_2 \ldots x_{j-1} b_j^{-1} \in N_{S_n}(R).$$

因此，元素 $x := x_j x_{j+1} \ldots x_m \tau x_1 x_2 \ldots x_{j-1}$ 属于 $N_{S_n}(R^{b_j})$。由于 $h \in H_i$，同样的论证表明 $x$ 属于 $N_{S_n}(M_i^{a_{ij}})$。此外

$$x = (x_j x_{j+1} \cdots x_m \tau) \cdot x_1 \cdots x_m \tau \cdot (x_j x_{j+1} \cdots x_m \tau)^{-1},$$

所以 $x$ 属于 $B$。因此 $x \in B \cap N_{S_n}(M_i^{a_{ij}}) \cap N_{S_n}(R^{b_j})$。 □

引理 11. 设 $L \leqslant G$ 和 $g \in \Pi$，则包含 $g$ 的 $L$ 的共轭子群个数至多为 $nm$。

证明。我们采用引理 [4, Lemma 4] 的证明中的论证。设 $a(L)$ 为包含 $g$ 的 $L$ 的共轭子群个数。注意， $a(L)$ 不依赖于 $g$，因为 $\Pi$ 是 $G$ 中的一个共轭类。考虑由满足以下条件的有序对 $(h, H)$ 构成的集合 $R$： $h \in H \cap \Pi$，且 $H$ 在 $G$ 中与 $L$ 共轭。一方面，由于 $\Pi$ 是 $G$ 的一个共轭类， $|R| = |\Pi| \cdot a(L)$。另一方面，由于 $L$ 有 $|G : N_G(L)|$ 个共轭子群属于 $G$，并且对所有 $g \in G$, $|L^g \cap \Pi| = |L \cap \Pi|$： $|R| = |G : N_G(L)| \cdot |L \cap \Pi| \leqslant |G : L| \cdot |L| = |G|$。因此 $|\Pi| \cdot a(L) \leqslant |G|$，故

$$a(L) \leqslant \frac{|G|}{|\Pi|} = \frac{2m \cdot (n!/2)^m}{(n-1)! \cdot (n!/2)^{m-1}} = nm.$$

这就完成了证明。 □

固定 $\Gamma$ 的一个顶点 $v = \{H_1, H_2\}$，并令 $i \in \{1,2\}$, $H := H_i$。由引理 11， $m_H([K]) \leqslant nm$ 对所有 $K \leqslant G$ 均成立。现在我们给出 $f_H(K) = |C(H) \cap K|/|C(H)|$ 对于 $K \in \mathcal{H}_j$ 的上界，以及 $P(E_{v,\,j})$ 对于 $j = 1, \ldots, 6$ 的上界。由于 $\Pi$ 在共轭下封闭，在估计 $f_H(K)$ 时，我们可以假设 $H = N_G(L^m)$，其中 $L$ 是 $A_n$ 的一个具有 2 个块的极大不可约子群。与第 2 节一样，我们将使用斯特林不等式。由引理 4， $C(H) = H \cap \Pi$ 的大小为 $(2/n) \cdot (n/2)!^{2m} \geqslant (2/n)(n/(2e))^{nm}$。

(1) 情形 $j = 1$。令 $K \in \mathcal{H}_1$ 为 $G$ 中 $N_G(M^m)$ 的一个共轭，其中 $M$ 是 $A_n$ 的一个极大非传递子群。注意，由引理 4， $K \cap \Pi = \varnothing$，因为 $N_{S_n}(M)$ 是非传递的，因此不包含 $n$-轮换。因此 $f_H(K) = 0$，这意味着 $P(E_{v,\,1}) = 0$。

(2) 情形 $j = 2$. 假设 $K$ 是 $G$ 的极大子群，且共轭于 $N_G(M^m)$，其中 $M^m = K \cap N$， $M$ 是 $A_n$ 与一个不同于 $A_n$ 的 $S_n$ 的本原极大子群的交。由 [17]、 $KN = G$ 和 $K \cap N$ 可知 $|M| \leqslant 4^n$ 共轭于 $M^m$，因此我们有 $|C(H) \cap K| \leqslant |K| = 2m \cdot |M|^m \leqslant 2m \cdot 4^{mn}$。因此，根据不等式（$\star$）以及引理 9、11，

$$P(E_{v,2}) \leqslant n \cdot mn \cdot \frac{mn \cdot 4^{mn}}{(n/(2e))^{mn}} = m^2 n^3 \cdot \left(\frac{8e}{n}\right)^{nm}.$$

(3) 情形 $j=3$. 假设 $K=N_G(M\times M^{a_2}\times\ldots\times M^{a_m})$, $M$ 是 $A_n$ 的一个具有 3 个块的极大非本原子群，且 $a_2,\ldots,a_m\in A_n$。我们将对 $C(H)\cap K$ 的大小给出上界。令 $g\in C(H)\cap K=H\cap\Pi\cap K$，则 $g=(x_1,\ldots,x_m)\gamma$，其中 $x_1\ldots x_m\tau\in B$，而由 $g\in H\cap K$ 可知 $x_1,\ldots,x_{m-1},x_m\tau\in N_{S_n}(L)$, $a_ix_ia_{i+1}^{-1}\in N_{S_n}(M)$ 对于 $i=1,\ldots,m-1$ 均成立，其中 $a_1=1$，且 $a_mx_m\tau\in N_{S_n}(M)$。我们推得

$$\begin{aligned}&x_1\ldots x_i\in N_{S_n}(L)\cap N_{S_n}(M)a_{i+1}\qquad\forall i=1,\ldots,m-1,\\&x_1\ldots x_m\tau\in B\cap N_{S_n}(L)\cap N_{S_n}(M)\end{aligned}$$

根据归纳法，$x_i$的选择数为 $|N_{S_n}(L)\cap N_{S_n}(M)a_{i+1}|$，至多为 $|N_{S_n}(L)\cap N_{S_n}(M)|$，对每个 $i=1,\ldots,m-1$ 均成立。此外，在选择了 $x_1,\ldots,x_{m-1}$ 之后，$x_m$的选择数为 $|B\cap N_{S_n}(L)\cap N_{S_n}(M)|$，至多为 $|N_{S_n}(L)\cap N_{S_n}(M)|$。因此

$$|C(H)\cap K|\leqslant|N_{S_n}(L)\cap N_{S_n}(M)|^m.$$

上述讨论表明，若 $B\cap N_{S_n}(L)\cap N_{S_n}(M)$ 为空，则$f_H(K)=0$，因此现在可以假设存在一个元素 $\sigma\in B\cap N_{S_n}(L)\cap N_{S_n}(M)$。那么 $\sigma$是一个正规化 $L$和 $M$ 的 $n$-循环。令 $\Delta$ 和 $\overline{\Delta}$ 为 $L$的块，即 $\langle\sigma^2\rangle$的两个轨道；令 $B_1$、$B_2$、$B_3$ 为 $M$的块，即 $\langle\sigma^3\rangle$的三个轨道。那么 $\langle\sigma^6\rangle$ 的六个轨道为$\Delta\cap B_i$、$i=1$、2、3，以及 $\overline{\Delta}\cap B_i$、$i=1$、2、3，它们构成 $\{1,\ldots,n\}$的一个划分 $P$，由 6 个大小为 $n/6$的块组成。显然，$N_{S_n}(L)\cap N_{S_n}(M)$ 包含于划分 $P$的稳定子中，而该稳定子与 $S_{n/6}\wr S_6$同构，因此

$$f_H(K)=\frac{|C(H)\cap K|}{|C(H)|}\leqslant\frac{|N_{S_n}(L)\cap N_{S_n}(M)|^m}{|C(H)|}\leqslant\frac{n}{2}\cdot\left(\frac{(n/6)!^6\cdot6!}{(n/2)!^2}\right)^m.$$

运用斯特林不等式可轻易证明，这至多为$n^{O(1)m}(1/3)^{nm}$。根据不等式（$\star$）以及引理 9、11，对于 $P(E_{v,\ 3})$，同样的上界成立。

（4）情形 $j=4$。假设 $K$ 是 $G$ 的一个极大子群，共轭于 $N_G(M^m)$，其中 $K\cap N=M^m$，而且 $M$是 $A_n$的一个具有 4 个块的极大非本原子群。由于 $KN=G$且 $K\cap N$共轭于 $M^m$，$|K|=2m\cdot|M|^m$，因此运用斯特林不等式可得

$$f_H(K)\leqslant\frac{|K|}{|C(H)|}=\frac{2m\cdot((n/4)!^4\cdot4!)^m}{2/n\cdot(n/2)!^{2m}}\leqslant n^{O(1)m}\cdot\left(\frac{1}{2}\right)^{nm}.$$

因此，根据不等式（$\star\star$）和引理 10，$P(E_{v,\ 4})\leqslant n^{O(1)m}(1/4)^{nm}$。

（5）情形 $j=5$。假设 $K$ 是 $G$ 的一个极大子群，共轭于 $N_G(M^m)$，其中 $K\cap N=M^m$，而且 $M$是 $A_n$的一个具有 5 个或更多块的极大非本原子群。根据 [4, 定理 3]，$|M|\leqslant n^{O(1)}\cdot(n/(5e))^n$，并且由于$|K|=2m\cdot|M|^m$，

$$f_H(K)\leqslant\frac{2m\cdot((n/(5e))^n\cdot n^{O(1)})^m}{2/n\cdot(n/(2e))^{nm}}\leqslant n^{O(1)m}\cdot\left(\frac{2}{5}\right)^{nm}.$$

由不等式（$\star$）和引理 9、11，同一上界也适用于 $P(E_{v,\ 5})$。（6）情形 $j=6$。设 $K=N_G(\Delta_\varphi)$ 是 $G$ 的对角型极大子群，因此 $|K|=2m\cdot|A_n|^{m/t}$，其中 $t$ 是 $m$ 的素因子。利用

$t \geqslant 2$ 以及斯特林不等式，

$$f_H(K) \leqslant \frac{|K|}{|C(H)|} = \frac{2m(n!/2)^{m/t}}{(2/n)(n/2)!^{2m}} \leqslant n^{O(1)m} \cdot \left(\frac{2\sqrt{e}}{\sqrt{n}}\right)^{mn}.$$

由不等式（$\star$）和引理 9、11，同一上界也适用于 $P$（$E_{v,\ 6}$）。

现在我们通过证明当 $n$ 充分大时， $P(E_v) \leqslant e^{\frac{1}{(d+1)}}$ 来完成证明。回顾一下， $d \leqslant 2^{mn}$。上述讨论意味着，对所有 $j = 1, \ldots, 6$， $P(E_{v,j}) \leqslant n^{O(1)m}(2/5)^{nm}$；又由于 $P(E_v) \leqslant \sum_{j=1}^{6} P(E_{v,j})$，因此归结为证明 $n^{O(1)m}(2/5)^{mn} \leqslant (1/2)^{mn}$，而当 $n$ 足够大时，这一结论成立。

## References


[1] A. Abdollahi、F. Ashraf 和 S. M. Shaker。“六次对称群可由 13 个真子群覆盖，且不能更少。”Bull. Malays. Math. Sci. Soc. (2). 30:1 (2007), 57–58.[2] N. Alon、J. H. Spencer。《概率方法》。第四版。Wiley 离散数学与优化丛书。John Wiley and Sons, Inc., 新泽西州霍博肯, 2016.[3] A. Ballester-Bolinches、L. M. Ezquerro。《有限群类》。Springer Netherlands, 2006. [4] S. R. Blackburn。“两两生成对称群的置换集。”J. Combin. Theory Ser. A. 113:7 (2006), 1572–1581. [5] J. H. E. Cohn。“论 n-和群。”Math. Scand. 75:1 (1994), 44–58. [6] P. Erd˝os、L. Lov´asz。“关于 3-色超图的问题与结果及若干相关问题。”A. Hajnal、R. Rado、V. S´os（编），Colloquium Math. Society Janos Bolyai，第 11 卷，North-Holland，阿姆斯特丹，1973 年，第 609–627 页。[7] F. Fumagalli、M. Garonzi、A. Mar´oti。“关于两两生成偶数次对称群的元素最大数。”Discrete Mathematics，第 345 卷，第 4 期（2022），112776。[8] M. Garonzi。“用真子群覆盖某些单体群。”Commun. Alge- bra. 41:2 (2013a), 471–491. [9] M. Garonzi、A. Mar´oti。“用真子群覆盖某些花环积。”Journal of Group Theory，第 14 卷，第 1 期（2011），103–125。[10] L.-C. Kappe、D. Nikolova-Popova 和 E. Swartz。“关于小对称群及某些散在单群的覆盖数。”Groups Complex. Cryptol. 8:2 (2016), 135– 154.[11] M. W. Liebeck、C. E. Praeger、J. Saxl。“有限交错群和对称群的极大子群分类。”Journal of Algebra 111, 365–383 (1987). [12] A. Lucchini、F. Menegazzo，《具有唯一极小正规子群的有限群的生成元》。Rendiconti del Seminario Matematico della Universit`a di Padova, tome 98 (1997), p. 173–191[13] A. Lucchini、A. Mar´oti。“有限群生成图的团数。”Proceedings of the American Mathematical Society，第 137 卷，第 10 期（2009），3207–3217。[14] A. Mar´oti。“关于本原群的阶。”Journal of Algebra，第 258 卷，第 2 期（2002），631 - 640。[15] A. Mar´oti。“用真子群覆盖对称群。”J. Combin. Theory Ser. A. 110:1 (2005), 97–111. [16] R. Oppenheim 和 E. Swartz。“关于 S14 的覆盖数。”Involve. 12:1 (2019), 89–96. [17] C. E. Praeger、J. Saxl。“关于本原置换群的阶。”Bulletin of the London Mathematical Society，第 12 卷，第 4 期（1980），303 – 307。[18] L. Stringer，《对称群与交错群的两两生成集》，博士论文，伦敦大学皇家霍洛威学院，2008 年。[19] E. Swartz。“关于次数被六整除的对称群的覆盖数。”Discrete Math. 339:11 (2016), 2593–2604.

Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília-DF, 70910-900, Brazil
*Email address*: julia_aredes_almeida@hotmail.com

Departamento de Matemática, Universidade de Brasília,
Campus Universitário DarcyRibeiro Brasília-DF 70910-900 Brazil , „
ORCID: https://orcid.org/0000-0003-0041-3131
*Email address*: mgaronzi@gmail.com