arXiv:2303.01957v1 [cs.DS] 3 Mar 2023

具有常数查询时间的有限群线性空间数据结构

Bireswar Das[1], Anant Kumar[1], Shivdutt Sharma[2], 和 Dhara Thakkar[1] *

[1] 印度理工学院甘地讷格尔分校，甘地讷格尔[2] 印度信息技术学院乌纳分校，印度 {bireswar,kumar_anant,thakkar_dhara}@iitgn.ac.in shiv@iiitu.ac.in

摘要。 阶为 n 的有限群可以用其凯莱表表示。在字 RAM 模型中，阶为 n 的群的凯莱表可以用 $O(n^2)$ 个字存储，并可用于在常数时间内回答乘法查询。一个值得探讨的问题是，我们能否设计一种数据结构，以 $o(n^2)$ 的空间存储阶为 n 的群，同时仍能在常数时间内回答乘法查询。

我们设计了一种常数查询时间数据结构，可以用 $O(n)$ 个字存储任意有限群，其中 n 是群的阶。

Farzan 和 Munro（ISSAC 2006年）给出了存储一个阶为 n 的群所需字数的一个信息论下界 $\Omega(n)$。由于我们的数据结构达到了这一下界，并且能够在常数时间内回答查询，因此它在空间使用和查询时间两方面都是最优的。

该过程中的一个关键步骤，本质上是为非阿贝尔单群设计线性空间和常数查询时间的数据结构。非阿贝尔单群的数据结构利用一个引理进行设计，而我们使用有限单群分类定理（有限单群分类）证明了该引理。

关键词： 紧凑数据结构 · 空间高效表示 · 有限群 · 单群 · 有限单群分类定理

相关版本： 本文的初步版本发表于第39届理论计算机科学前沿国际研讨会（STACS 2022）的论文集。

1 引言

阶为 n 的群的凯莱表是一个二维表，其中第 (i, j) 个表项是该群第 i 个元素与第 j 个元素的乘积。在字 RAM 模型中，虽然存储阶为 n 的群的凯莱表需要 $O(n^2)$ 个字，但通过访问表中的相应位置，可以在常数时间内回答乘法查询。

* 由 CSIR-UGC NET JRF 奖学金资助。

在群论中的许多计算问题里，输入群由其凯莱表给出。这些问题包括最小生成集问题、性质测试中的各种问题、群分解问题以及群同构问题 [20,2,17,21]。其中，群同构问题或许最为突出，因为尽管多年来已有大量研究，其复杂度仍未解决 [5,15,3,6,22,16]。

凯莱表在查询处理方面非常快速，但存储一个群需要二次空间。一个有趣的问题是：我们能否使用 $o(n^2)$ space[3] 为有限群设计一种数据结构，使其仍能在常数时间内回答乘法查询。我们注意到，尽管拟群和半群也可以使用凯莱表存储，但不可能使用 $o(n^2)$ space 存储拟群和半群。这仅仅是因为拟群和半群的数量太大 [28,19]，信息论下界为 $\Omega(n^2 \log n)$ 位或 $\Omega(n^2)$ 个字。

Das 等人 [11] 证明，对于任意阶为 n 的有限群 G，以及任意 $\delta \in [1/\log n, 1]$，都可以为 G 构造一种数据结构，该结构使用 $O(n^{1+\delta}/\delta)$ 空间，并在 $O(1/\delta)$ 时间内回答乘法查询。他们的结果意味着，存在用于阶为 n 的有限群的常数查询时间数据结构，这些结构使用 $O(n^{1.01})$ 空间。然而，即使允许使用 $\Theta(n.\mathrm{polylog}(n))$ 空间，该结果也无法用于设计常数查询时间数据结构。

本文设计了用于有限群的常数查询时间数据结构，可用 $O(n)$ 个字存储，其中 n 是群的阶。Farzan 和 Munro 的信息论论证表明，存储一个阶为 n 的群至少需要 $\Omega(n\log\ n)$ 位，即 $\Omega(n)$ 个字 [13]。我们的数据结构达到了这一下界，因此是最优的。渐近地达到信息论最优下界的数据结构称为紧凑数据结构。因此，我们的数据结构是用于有限群的常数查询时间紧凑数据结构。值得注意的是，针对某些受限的群类（例如阿贝尔群和 Dedekind 群），已有紧凑查询时间数据结构 [10]。

在设计该数据结构的过程中，我们首先证明了两个结果，并将其称为扩张定理：当我们已经拥有给定群的某个子群的数据结构时，如何构造该群的数据结构。其中一个结果中新构造的数据结构所需的额外空间取决于该子群的指数；另一个结果则取决于该子群的结构[4]。这表明，寻找群的合适子群可能会有所帮助。

Jordan-Hölder 定理为我们提供了一系列子群，即合成列。在我们的过程中，我们试图从给定群的合成列中挑选一些合适的子群。然而，挑选

[3] 本文采用字 RAM 模型。数据结构或算法所使用的空间是指其使用的字数量。[4] 该子群需要是正规的，且商群需要是循环的。

合适的群并非总是可行。正如我们将在第 4 节中看到的，当合成列的某个位置上存在一个“较大”的合成因子时，就会出现这种情况。合成因子都是单群。从某种意义上说，构造数据结构时的难点在于单群。

单群有时被视为有限群的构造基块。有限单群分类定理（有限单群分类）是群论中最重要的定理之一。简单来说，该定理将有限单群分为循环群、交错群、某些李型群，以及 26 个散在单群。该定理的精确表述可在第 5 节中查到。除 26 个散在单群外，其他群类都是无限的。我们利用有限单群分类证明一个关键引理，从而能够处理非阿贝尔单群的情形。

我们注意到，对于可解群，数据结构的设计独立于有限单群分类。可解群的合成因子都是素数阶循环群。这类情形采用第 3 节中证明的某个扩张定理处理。

相关工作：Farzan 和 Munro [13] 为有限阿贝尔群在一种特定计算模型下给出了简洁表示。在他们的模型中，压缩算法首先为每个群元素生成标签。查询由查询处理单元 处理，该单元类似于字 RAM 模型。不过，除了常见的算术、逻辑和比较运算外，查询处理单元还可以在常数时间内执行位反转。用户发出查询时，会向查询处理单元提供压缩算法生成的两个群元素的标签，查询处理单元随后返回这两个元素乘积的标签。

Das 等人 [11] 以及 Das 和 Sharma [10] 利用 Erdös-Rényi 立方体生成序列、Remak-Krull-Schmidt 分解和不可分解群的结构，设计了空间和查询时间高效的数据结构。我们的方法截然不同：我们利用扩张定理（第 3 节）和有限单群分类定理来设计数据结构。

备注：除了凯莱表表示之外，还有多种表示有限群的方法。置换群表示、多循环表示和生成元-关系表示都是常见的群表示。这些表示通常彼此不可比较。例如，在生成元-关系表示中，我们可以表示无限群。然而，许多问题（例如成员判定，以及判断一个群是否有限）在生成元-关系表示中都变得不可判定（参见 [27]）。在置换群表示中，成员判定所需时间相对于表示的次数呈超线性增长，而相对于群的阶则呈多对数增长 [26,25,14]。与此相比，在凯莱表表示中，由于元素是已知的，且已用作凯莱表的行索引和列索引，因此可以在常数时间内完成成员判定。在凯莱表表示中，用户明确知道每个群元素的标签或名称，并可直接访问每个元素。

元素的标签通常取为 1、2、……、 n，其中 n 是群的阶。对于置换群表示、多循环表示或生成元-关系表示，情况则截然不同。在这些情况下，用户并没有每个元素的显式表示。

2 预备知识

本节回顾本文所用的一些定义和记号。本文只考虑有限群。群 G 中元素的个数称为的阶，记作 $|G|$。若群 G 满足对所有 g_1、 $g_2 \in G$都有 $g_1 g_2 = g_2 g_1$，则称其为阿贝尔群。对于子群 H、群 G 以及 $g \in G$，集合 $gH = \{gh \mid h \in H\}$称为左陪集。类似地，我们可以定义 G的右陪集。 G 中 H 的左（或右）陪集的个数称为在中的指数，记作 $[G : H]$。 G 中 H 的左遍历是一个集合，其中恰好包含每个左陪集中的一个元素；类似地，我们可以定义右遍历。左（右）遍历的大小与指数 $[G : H]$相同。对于 $g \in G$，集合 $gHg^{-1} = \{gag^{-1} \mid a \in H\}$ 称为子群 H的一个共轭子群。若群 G 的子群 H 满足对所有 $g \in G$都有 $gHg^{-1} = H$，则称其在 G 中是正规的（记作 $H \trianglelefteq G$）。我们将 G中 H的正规化子定义为集合 $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$。注意， $N_G(H)$ 是 G 中最大的、以 H 为正规子群的子群。

若群 G 没有非平凡正规子群，则称其为单群 。有限单群分类定理指出，所有有限单群可分为以下五类：(1) 素数阶循环群，(2) 交错群，(3) 经典群，(4) 李型例外群，以及 (5) 26 个散在单群。

我们将在第 5 节的单群分类定理中列出有限单群的所有类别。若 G 是定义在 $\mathbb{F}_q$ 上的李型有限单群，其中 q 是某个素数 p 的幂，则 G 的 Borel 子群 B 定义为 G 的 Sylow p-子群与极大分裂环面 T 的半直积。Borel 子群也是该有限单群的 Sylow p-子群的正规化子（见 [8], [29]）。

对于本文而言，了解单群中某些子群的阶 的一些结果或许就足够了。读者可以选择跳过这些群的结构细节。我们会在需要时说明所关注的子群类型，以及有关这些子群阶的结果。有兴趣的读者可参阅 Carter [8],、Wilson [29]，或 Aschbacher [4] 的著作，了解更多详情。

定义 1（例如参见 [12]）。群 G 的次正规列是子群链

$$1 = G_k \leqslant G_{k-1} \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$$

使得 $G_i \trianglelefteq G_{i-1}$，对所有 i。

定义 2（参见例如 [12]）。在群 G 中，一个子群序列

$$1 = G_k \leqslant G_{k-1} \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$$

若对所有 $i \in [k]$，$G_i \trianglelefteq G_{i-1}$ 和 G_{i-1}/G_i 都是单群，则称其为合成列 。其中，k 是 G的合成长度 。

定理 1（Jordan-Hölder 定理，参见例如 [12]）。设 G 是一个有限群，且 $G \neq 1$。那么

(i) G 有一个合成列。

(ii) 合成列中的合成因子是唯一的，即，若 $1 = N_r \leqslant N_{r-1} \leqslant \cdots \leqslant N_1 \leqslant N_0 = G$ 和 $1 = M_s \leqslant M_{s-1} \leqslant \cdots \leqslant M_1 \leqslant M_0 = G$是 G 的两个合成列，则 $r = s$，且存在 $\{1, 2, ..., r\}$ 的一个置换 π，使得：

$$\frac{M_{\pi(i)}}{M_{\pi(i)+1}} \cong \frac{N_i}{N_{i+1}}, for\ 1 \leqslant i \leqslant r.$$

定理 2（对应定理，参见例如 [23]）。设 $K \trianglelefteq G$，且令 $\nu : G \longrightarrow G/K$ 为典范映射，即对所有 g，$\nu(g) = Kg$。那么，$S \mapsto \nu(S) = S/K$是从 G 中所有包含 K 的子群 S 构成的集合到 G/K 的所有子群构成的集合的一个双射。

计算模型：本文采用一种称为字 RAM 模型的抽象计算模型。在该模型中，数据存储在寄存器和存储单元中。每个存储单元和寄存器都可以存储 $O(\log n)$ 位，其中 n 是输入的大小。存储单位称为字。字 RAM 模型中的机器可以访问一个字，并在常数时间内执行常见的算术、逻辑和比较运算。就本文而言，输入大小是群的阶。不失一般性，我们可以假设群的元素为 1、2、3、...、n。因此，每个群元素都可以存储在一个字中，并且可以在常数时间内访问。

数据结构的构建分为两个阶段：预处理阶段和查询阶段。在预处理阶段，假设给定一个由凯莱表表示的有限群。利用凯莱表，我们构建一个由若干数组和表组成的数据结构。在查询阶段，我们处理乘法查询。对于一次乘法查询，用户给出两个群元素 g_1 和 g_2。任务是求出 g_1 和 g_2 的乘积。在这一阶段，我们访问预处理阶段构建的数据结构来回答查询。回答单次查询所需的时间称为查询时间。

通常不考虑构建数据结构的预处理阶段所耗费的时间和空间。不过，我们证明，在我们的情形中，数据结构可以在多项式时间内计算出来。我们主要关注的是

所构建的数据结构占用的空间，以及回答群元素相乘查询所需的时间。

定义 3. 设 G 是一个群，s 和 t 是两个正实数。如果 G 具有一个 (s,t)-数据结构，也就是说，G 可以存储在一个数据结构中，该结构使用的空间至多为 s，并且能够在至多 t 的时间内回答乘法查询。

定义 4. 设 $\mathcal{G}$ 是一个群类，且 s，$t : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ 是两个函数。如果对于每个阶为 n 的群 $G \in \mathcal{G}$，都存在一个使用 $O(s(n))$ 空间存储 G 的数据结构，并且能够在至多 $O(t(n))$ 的时间内回答乘法查询，那么我们称 $\mathcal{G}$ 具有一个 $(O(s(n)), O(t(n)))$-数据结构。

3 扩张定理

本节讨论如何利用子群的数据结构，为包含这些子群的群构建新的数据结构。

定理 3. 存在正常数 c 和 d，使得对于任意群 G 及其子群 H，如果 H 具有某个 (s,t)-数据结构，其中 s 和 t，那么 G 就具有一个 $(s + c([G : H]^2 + |G|), 2t + d)$-数据结构。

证明。首先，我们固定 G 中 H 的一个左遍历 L 和一个右遍历 R。每个 $g \in G$都可以唯一地写成 $g = hr$，其中 $h \in H$ 且 $r \in R$。因此，我们可以定义函数 $s_R : G \longrightarrow H$和 $c_R : G \longrightarrow R$，使得 $g = s_R(g)c_R(g)$。类似地，我们可以定义 $c_L : G \longrightarrow L$ 和 $s_L : G \longrightarrow H$，使得 $g = c_L(g)s_L(g)$。我们可以将这四个函数存储在四个长度均为 $|G|$ 的数组中。

假设我们需要求 g_1 和 g_2的乘积。注意，

$$g_1 g_2 = c_L(g_1)s_L(g_1)s_R(g_2)c_R(g_2).$$

由于 $s_L(g_1)$、$s_R(g_2) \in H$，我们可以使用用于 H 的数据结构，在 t 时间内找到 $s_L(g_1)s_R(g_2)$。令 $h_1 = s_L(g_1)s_R(g_2)$。因此，我们可以写出 $g_1g_2 = c_L(g_1)h_1c_R(g_2)$。给定 $l \in L$ 和 $h \in H$，我们知道存在唯一的元素 $h' \in H$ 和$r \in R$，使得 $lh = h'r$。因此，我们可以定义两个函数 $Flip_H : L \times H \longrightarrow H$和 $Flip_R : L \times H \longrightarrow R$，使得 $lh = Flip_H(l,h)Flip_R(l,h)$。我们可以将 $Flip_H$ 和 $Flip_R$ 存储在两个二维数组中，所需空间与 $|H \times L| = |G|$呈线性关系。借助这些函数，我们可以写出

$$g_1 g_2 = Flip_H(c_L(g_1), h_1)Flip_R(c_L(g_1), h_1)c_R(g_2) = h_2 r_1 r_2$$

其中 $h_2 = Flip_H(c_L(g_1), h_1)$、$r_1 = Flip_R(c_L(g_1), h_1)$ 和 $r_2 = c_R(g_2)$。

再次利用这样一个事实：任意 G 中的元素 g 都可以唯一地写成 $g = hr$，其中 $h \in H$ 且 $r \in R$，从而定义函数 $Cross_H : R \times R \longrightarrow H$ 和 $Cross_R : R \times R \longrightarrow R$，使得对于所有 r、$r' \in R$，都有 $rr' = Cross_H(r,r')Cross_R(r,r')$。

注意，我们可以将这些函数存储在两个二维数组中，每个数组所需空间与 $|R \times R| = (|G|/|H|)^2$ 成线性关系。借助这些函数，我们可以写出

$$g_1 g_2 = h_2 \mathrm{Cross}_H(r_1, r_2)\mathrm{Cross}_R(r_1, r_2) = h_2 h_3 r_3$$

其中 $\mathrm{Cross}_H(r_1, r_2) = h_3$ 和 $r_3 = \mathrm{Cross}_R(r_1, r_2)$。

同样，我们可以使用用于 H 的数据结构，在时间 t内计算乘积 $h_4 = h_2 h_3$。因此，$g_1 g_2 = h_4 r_3$。最后，我们将函数 $\mathrm{Fuse} : H \times R \longrightarrow G$简单地定义为：对所有 $h \in H$ 和 $r \in R$，$\mathrm{Fuse} : H \times R \longrightarrow G$均为 $\mathrm{Fuse}(h, r) = hr$。显然，用于存储 Fuse的二维数组需要与 $|H \times R| = |G|$成线性关系的空间。因此，要得到最终结果，我们只需返回 $g_1 g_2 = \mathrm{Fuse}(h_4, r_3)$。

除 Cross_R 和 Cross_H 之外的所有函数所需空间均与 $|G|$成线性关系，而 Cross_R 和 Cross_H 所需空间均与 $(|G|/|H|)^2$成线性关系。用于 H 的数据结构至多需要 s的空间。因此，所需总空间与 $|G|+(|G|/|H|)^2$成线性关系。注意，在此证明中定义的每个函数都恰好查询一次。因此，查询全部九个函数所需的时间有一个常数上界 d。此外，查询用于 H 的数据结构所需时间至多为 $2t$。因此，我们得到了用于 G的所需数据结构。

注释 *1.* 我们注意到，如果给定 H 的 (s, t)-数据结构，那么上述用于 G 的数据结构也可以在多项式时间内计算出来。

上述定理的一个直接推论如下。

推论 1. 设 $0 < c_1 \leqslant c_2$ 为两个常数。设 $\mathcal{G}_{c_1,c_2}$ 为群类 G，其中的群具有一个满足 $c_1\sqrt{|G|} \leqslant |H| \leqslant c_2\sqrt{|G|}$ 的子群 H。那么 $\mathcal{G}_{c_1,c_2}$ 具有 $(O(n), O(1))$-数据结构。

证明. H 的凯莱表大小至多为 $c_2^2|G|$，并且能在常数时间内回答查询。由于 $|G|/|H| \leqslant (1/c_1)\sqrt{|G|}$，我们有 $(|G|/|H|)^2 \leqslant (1/c_1)^2|G|$。因此结论由定理 3 得出。

在下一个定理中，我们将说明如何利用群的正规子群的数据结构来构造该群的数据结构，其中商群为循环群。

定理 4. 存在正常数 c 和 d，使得对于每个群 G 及其任意正规子群 N，若 G/N 是循环群，且 N 具有某个 s 和 t对应的 (s, t)-数据结构，则 G 具有 $(s + c|G|, 2t + d)$-数据结构。

证明。由于 G/N 是循环群，它由元素 g_0N 生成，其中 $g_0 \in G$。N 在 G 中的陪集为 N、g_0N、g_0^2N，……，$g_0^{k-1}N$，其中 k是群G/N的阶，即 $k = [G : N]$。显然，$k \leqslant |G|$。令 $S = \{0, 1, \ldots\ldots k-1\}$。

集合 $\{g_0^0, g_0^1, \ldots, g_0^{k-1}\}$ 是 G中 N 的左遍历和右遍历。因此，任意元素 g 都可以唯一地写成 $g = g_0^r n = n' g_0^r$，其中 $r \in S$，并且

$n, n' \in N$。这使我们能够定义函数 $e : G \longrightarrow S$, $s_R : G \longrightarrow N$ 和 $s_L : G \longrightarrow N$，使得对于所有 $g \in G$

$$g = g_0^{e(g)} s_R(g) = s_L(g) g_0^{e(g)}.$$

这三个函数可以分别存储在大小为 $|G|$ 的数组中。为了计算 g_1 和 g_2 的乘积，我们首先注意到 $g_1 g_2 = g_0^{e(g_1)} s_R(g_1) s_L(g_2) g_0^{e(g_2)}$。这些表达式可以通过分别查询每个函数一次来获得。乘积 $n_1 = s_R(g_1) s_L(g_2)$ 可以使用 N 的数据结构在 t 的查询时间内获得。因此 $g_1 g_2 = g_0^{\alpha} n_1 g_0^{\beta}$，其中 $\alpha = e(g_1)$ 和 $\beta = e(g_2)$。

接下来，我们定义一个函数 $Flip : N \times S \longrightarrow N$，使得对于所有 $n \in N$ 和 $i \in S$，都有 $n g_0^i = g_0^i Flip(n, i)$。换句话说，$Flip(n, i)$ 就是 $g_0^{-i} n g_0^i$。这个函数可以存储在线性于 $|N \times S| = |G|$ 的空间中。现在我们可以写成 $g_1 g_2 = g_0^{\alpha} g_0^{\beta} Flip(n_1, \beta) = g_0^{\alpha+\beta} n_2$，其中 $n_2 = Flip(n_1, \beta)$。
接下来我们计算 $g_0^{\alpha} g_0^{\beta} = g_0^{\alpha+\beta}$。注意，$\alpha + \beta \in \{0, 1, 。。。。。。, 2k-2\}$。我们定义两个函数 $red_e : \{0, 1, 。。。。。。, 2k-2\} \longrightarrow S$ 和 $red_N : \{0, 1, 。。。。。。, 2k-2\} \longrightarrow N$，使得对于所有 $\ell \in \{0, 。。。。。。, 2k-2\}$，都有 $g_0^{\ell} = g_0^{red_e(\ell)} red_N(\ell)$。注意，对于 $\ell < k$，$red_e(\ell) = \ell$ 和 $red_N(\ell) = id$。这两个函数可以用关于 k 线性空间的空间存储。由于 $k \leqslant |G|$，所需空间至多与 G 线性相关。

因此，

$$g_1 g_2 = g_0^{\alpha+\beta} n_2 = g_0^{red_e(\alpha+\beta)} red_N(\alpha+\beta) n_2.$$

和之前一样，$red_N(\alpha+\beta)$ 与 n_2 的乘积 n_3 可以使用针对 N的数据结构求得。设 $red_e(\alpha+\beta) = \gamma$。因此，$g_1 g_2 = g_0^{\gamma} n_3$。
最后，我们将函数 $Fuse : S \times N \longrightarrow G$ 定义为：对所有 $i \in S$ 和 $n \in N$，$Fuse : S \times N \longrightarrow G$ 为 $Fuse(i, n) = g_0^i n$。显然，函数 $Fuse$ 可以用关于 $|G|$ 呈线性关系的空间存储。

乘积 $g_1 g_2$ 就是 $Fuse(\gamma, n_3)$。

此证明中定义的每个函数都占用关于 $|G|$ 呈线性关系的空间，而用于 N的数据结构最多占用 s。每个函数都恰好查询一次，用于 N 的数据结构则查询两次。由此证明该定理。

注释 *2.* 这与注释 1 类似。在这种情况下，如果给定定理 4 中用于 H 的数据结构，那么可以在多项式时间内计算出用于 G 的数据结构。

4 有限群的紧凑数据结构

设 G 是一个阶为 n的群。我们的目标是为 G 设计一种常数查询时间数据结构，其大小与 n呈线性关系。我们首先考虑 G的一个合成列 $1 = G_k \lhd ... G_1 \lhd G_0 = G$。如果合成列中存在一个大小与 $\sqrt{n}$相差至多一个常数因子的子群 G_i，我们就可以应用推论 1，为 G获得一个 $(O(n), O(1))$-数据结构。否则，我们考虑最小的

阶大于 $\sqrt{n}$的子群 G_i。注意，此处 $|G_{i+1}|$ 至多为 $\sqrt{n}$，因此 G_{i+1} 的凯莱表大小至多为 n。利用该凯莱表，可以在常数时间内回答涉及 G_{i+1} 中元素的乘法查询。

现在我们考虑合成因子 G_i/G_{i+1}。这个商群是一个单群。如果它是阿贝尔群，那么它必定是循环群（具有素数阶），我们可以利用定理 4 为 G_i构造一个数据结构。然后，对 G 及其子群 G_i 应用定理 3，将为 G提供所需的数据结构。

非平凡情形是 G_i/G_{i+1} 为非阿贝尔群的情况。这正是我们使用有限单群分类定理的地方。分类定理使我们能够将非阿贝尔情形划分为各种子情形。在每个子情形中，我们证明可以插入两个子群 G_{i_2} 和 G_{i_1}，使得 $G_{i+1} \lhd G_{i_2} < G_{i_1} < G_i$，并以这种方式使指标 $[G_{i_2} : G_{i+1}]$、$[G_{i_1} : G_{i_2}]$ 和$[G_i : G_{i_1}]$ 都“较小”。由于 G_{i+1} 已经具有一个大小关于 n呈线性的常数查询时间数据结构（即其凯莱表），因此我们可以依次对群和子群对 (G_{i_2}, G_{i+1})、(G_{i_1}, G_{i_2})以及(G_i, G_{i_1}) 应用定理 3，从而得到一个大小关于n呈线性的 G_i 常数查询时间数据结构。最后，再次对 G 及其子群 G_i 应用定理 3，将为 G提供所需的数据结构。

4.1 可解有限群

在本小节中，我们考虑有限可解群这一类。我们先讨论这种情形，再转向所有有限群这一类的一般情形，因为前者不依赖有限单群分类定理。

定理 5. 这一类具有常数查询时间数据结构。

证明。 设为一个群，且.....是的合成列。设。

情形 *1*：存在使得。我们只需应用推论 1，即可得到所需的数据结构。

情形 *2*： 不存在使得。设为满足的最大指数。我们将有。的凯莱表至多有个条目。由于是可解群，是素数阶循环群。因此，我们可以应用定理 4，为得到线性于的常数查询时间数据结构。接下来注意到至多为。若将定理 3 应用于及其子群，就能得到所需的的数据结构。

由于群的合成列可以在多项式时间内计算，因此很容易验证定理 5 中的数据结构可以在多项式时间内构造。

4.2 一般情形

在考虑一般有限群的情形之前，我们需要非阿贝尔单群的以下结果。

引理 1. 存在正常数 b_1 和 b_2，使得对于任意非阿贝尔单群 H，都存在子群 H_1 和 H_2，使得 $1 \leqslant H_2 \leqslant H_1 \leqslant H$ 和$|H_2| \leqslant \sqrt{|H|}$、$[H : H_1] \leqslant b_1\sqrt{|H|}$ 以及 $[H_1 : H_2] \leqslant b_2\sqrt{|H|}$。

证明。 证明使用有限单群分类定理（CFSG）。证明思路见第 5 节，详细内容见附录。

接下来我们证明本文的主定理。我们注意到，以下定理证明中的情形 2 可视为为非阿贝尔单群设计线性空间和常数查询时间数据结构问题的推广版本。

定理 6. 所有有限群构成的类 $\mathcal{G}_{fin}$ 具有 $(O(n), O(1))$-数据结构。

证明。 设 G 是一个阶为 n的群。我们首先考虑一个合成列$1 = G_k \lhd$。.
$G_1 \lhd G_0 = G$ 是 G的一个合成列。
情形 *1*： 这是存在 i 使得 $\sqrt{n}/2 \leqslant |G_i| \leqslant \sqrt{n}$的情形。此情形与可解群的情形完全相同。
情形 *2*： 与之前一样，在此情形中，我们假设不存在阶大于 $\sqrt{n}/2$但小于 $\sqrt{n}$的合成列元素 G_i。设 i 是满足 $\sqrt{n} < |G_i|$的最大指数。于是有 $|G_{i+1}| < \sqrt{n}/2$。显然， G_{i+1} 的凯莱表至多有 $n/4$ 个条目。由于 $[G : G_i] < \sqrt{n}$，根据定理 3，只需为大小与 n成线性关系的 G_i 设计常数查询时间数据结构。因此，在证明的其余部分，我们将专注于为 G_i 设计一个使用 $O(n)$ 空间的常数查询时间数据结构。

如果合成因子 G_i/G_{i+1} 是阿贝尔的，那么我们又回到了可解群第二种情形中的相同情况。因此，我们假设G_i/G_{i+1} 是非阿贝尔的。

我们应用引理 1，得到子群 H_1 和 H_2，使得$1 \leqslant H_2 \leqslant H_1 \leqslant H = G_i/G_{i+1}$。根据群的对应定理，$H_1$ 和 H_2 分别将具有 G_{i_1}/G_{i+1} 和 G_{i_2}/G_{i+1} 的形式，其中某些子群 G_{i_1} 和 G_{i_2} 满足 $G_{i+1} \leqslant G_{i_2} \leqslant G_{i_1} \leqslant G_i$。由引理 1，我们有 $[H_1 : H_2] \leqslant b_2|H|$。由于 $H_1 = G_{i_1}/G_{i+1}$ 和 $H_2 = G_{i_2}/G_{i+1}$，我们有 $[G_{i_1}/G_{i+1} : G_{i_2}/G_{i+1}] \leqslant b_2\sqrt{|G_i/G_{i+1}|} \leqslant b_2\sqrt{n}$。
因此，$[G_{i_1} : G_{i_2}] \leqslant b_2\sqrt{n}$。类似地，$[G_i : G_{i_1}] \leqslant b_1\sqrt{n}$。再次根据引理 1，我们有 $H_2 \leqslant \sqrt{|H|}$。这意味着，$[G_{i_2} : G_{i+1}] \leqslant \sqrt{|G_i/G_{i+1}|} \leqslant \sqrt{n}$。
由于 G_{i+1} 有一个大小至多为 n 且 $[G_{i_2} : G_{i+1}] \leqslant \sqrt{n}$的凯莱表，我们将拥有一个针对大小至多为 G_{i_2} 的子群的常数查询时间数据结构

n，根据定理 3。由于 $[G_{i_1} : G_{i_2}] \leqslant b_2\sqrt{n}$ 且 $[G_i : G_{i_1}] \leqslant b_1\sqrt{n}$，再对群与子群对 (G_{i_1}, G_{i_2}) 和(G_i, G_{i_1}) 应用两次定理 3，即可得到一个针对 G_i 的数据结构，其大小与 n 呈线性关系，并且能够在常数时间内回答乘法查询。

关于如何在多项式时间内构造上述数据结构的讨论见第 5 节末尾。

5 引理 1 的证明概要

本节概述引理 1 背后的证明思路。我们首先陈述有限单群分类定理。

定理 7 ([29])。*(*有限单群分类定理*)*

每个有限单群都同构于以下某个群：

(i) 一个素数阶循环群 C_p；*(ii)* 一个交错群 A_m，其中 $m \geqslant 5$;

(iii) 一个经典群；

(a) 线性：$A_m(q)$(或 $PSL_{m+1}(q)$)，$m \geqslant 1$，但不包括 $PSL_2(2)$ 和 $PSL_2(3)$;
(b) 酉：${}^2A_m(q^2)$(或 $PSU_{m+1}(q)$)，$m \geqslant 2$，但不包括 $PSU_3(2)$；*(c)* 辛：$C_m(q))$(或 $PS_{p_{2m}}(q)$)，$m \geqslant 2$，但不包括 $PS_{p4}(2)$；*(d)* 正交：$B_m(q)$(或 $P\Omega_{2m+1}(q)$)，$m \geqslant 3$，q 为奇数；$D_m(q)$(或 $P\Omega^+_{2m}(q)$)，$m \geqslant 4$；${}^2D_m(q^2)$(或 $P\Omega^-_{2m}(q)$)，$m \geqslant 4$，其中 q 是某个素数的 p^α 次幂；

(iv) 一个李型例外群：

$$G_2(q), q \geqslant 3; F_4(q); E_6(q); {}^2E_6(q); {}^3D_4(q); E_7(q); E_8(q) \text{ } or$$

其中 q 是某个素数的幂；

$${}^2B_2(2^{2m+1}), m \geqslant 1; {}^2G_2(3^{2m+1}), m \geqslant 1; {}^2F_4(2^{2m+1}), m \geqslant 1$$

或 *Tits* 群 ${}^2F_4(2)'$；

(*v*) *26* 个散在单群中的一个：

(a) 五个马蒂厄群 M_{11},M_{12},M_{22},M_{23},M_{24}；*(b)* 七个利奇格子群 Co_1,Co_2,Co_3,McL, HS, Suz, J_2；*(c)* 三个菲舍尔群 Fi_{22},Fi_{23},Fi'_{24}；

(d) 怪兽群 $\mathbb{M}, \mathbb{B}$, Th, HN, He；*(e)* 六个离群群 J_1,J_2,J_4,O′N, Ly, Ru。

上述定理中提及的每一类群的定义，都可以在关于有限单群分类的标准教材中找到（例如， [8], [29], [4]）。

由于引理 1 讨论的是非阿贝尔单群，我们需要考虑定理 7 中的情形 (ii) 至 (v)。我们逐一考察这些情形下的各个子情形，并证明存在满足引理条件的子群 H_1 和 H_2。

我们注意到，情形 (v) 中列出的 26 个散在单群的阶都是常数。因此，在证明中，我们只需令 H_2 为单位子群、 H_1 为 H，便可忽略这些群。当然，若这样做，我们就需要选取一个极大的常数 b_2，因为某些散在单群的阶非常大。幸运的是，关于情形 (v) 中列出的群已有一些已知结果，这些结果有助于我们将常数 b_1 和 b_2 控制在 5 以下。

对于交错群 A_m （情形 (ii)），很容易证明， $H_1 = A_i$ 以及$H_2 = A_{i-1}$ 对某个适当选取的 $i < m$ 成立即可。详细内容见附录。

对于其余的群，在选择H_1 和 H_2时，我们使用以下两种方法。具体方法如下：

1. **方法 1：** 在此方法中，我们首先选择 H_2，使其成为给定单群 H的某个西洛子群。接下来，我们选取 H_1，使其成为 H_2 在H 中的正规化子，或者选取包含 H_2的 Borel 子群。

例： 令 H 为某个 $q > 2$ 对应的单群 $A_m(q)$，其中 $q > 2$ 出现在定理 7 的情形 (iii) 中。这里， q 是某个素数 p的幂。已知 $A_m(q)$ 的阶为 $q^{m(m+1)/2}\prod_{i=1}^{m}(q^{i+1}-1)/(q-1, m+1)$，其中 $(q-1, m+1)$ 表示 $q-1$ 和 $m+1$ 的最大公约数（参见 [4], 第 252 页）。显然， H 将具有一个阶为 $q^{m(m+1)/2}$的西洛 p-子群。我们令 H_2 为该子群。接下来，我们选取 H_1 为 H_2 在H中的正规化子。另已知 H_1 的阶为 $q^{m(m+1)/2}(q-1)^m$ （参见 [29], 第 46 页）。可以验证，结合 $b_1 = 2$ 和 $b_2 = 1$，这些选择满足引理 1 的条件（详细内容见附录）。

2. **方法 2：** 在此方法中，我们选择 H_1 作为单群 H 的极大子群，并选择 H_2 作为 H_1 的某个西洛子群。

示例：在方法 1 下的示例中，我们考虑 $A_m(q)$为 $q > 2$ 的情形。在本例中，我们取 $q = 2$ 的情形。此时， $H = A_m(q)$的阶为 $2^{m(m+1)/2}\prod_{i=1}^{m}(2^{i+1}-1)$ （见 [4], 第 252 页）。已知

H 的极大子群的阶为 $|H|/(2^m-1)$（见 [18], 第 175 页）。我们取此子群为 H_1。接下来，我们取 H_2 为 H_1的 Sylow 2-子群，其阶为 $2^{m(m+1)/2}$。容易验证， H_1 和 H_2 的这些取法连同 $b_1 = b_2 = 1$ 满足引理 1 的条件（详细信息见附录）。

表 1 列出了我们用于在相应的非阿贝尔单群中选择合适子群的方法。最后两列表示相应单群的常数因子 b_1 和 b_2（见表 1）。

对于情形 (v)，我们使用方法 2 来获得合适的子群。

情形	H	关于 q 的条件	方法	b_1	b_2
(iii)	$A_m(q)$	$q>2$	方法1 2 1		
		$q=2$	方法2 1 1		
	${}^2A_m(q^2), m>1$	$q>2$	方法1 2 1		
		$q=2; 6\nmid(m-1)$	方法 2 1 1		
		$q=2; 6\mid(m-1)$	方法 2 1 1		
	$C_m(q), m>2$	$q>2$	方法1 2 1		
		$q=2$	方法2 1 1		
	$B_m(q), m>1$	q 奇数	方法1 2 1		
	$D_m(q), m>3$	$q>2$	方法1 2 1		
		$q=2$	方法2 1 1		
	${}^2D_m(q^2), m>3$	$q>2$	方法1 3 1		
		$q=2$	方法2 1 1		
(iv)	$G_2(q)$	$q\geqslant 3$	方法1 1 1		
	$F_4(q)$	所有 q	方法2 1 1		
	$E_6(q)$	$q>2$	方法1 1 1		
		$q=2$	方法2 1 1		
	${}^2E_6(q)$	所有 q	方法1 1 1		
	${}^3D_4(q)$	所有 q	方法1 1 1		
	$E_7(q)$	$q>2$	方法1 1 1		
		$q=2$	方法2 1 1		
	$E_8(q)$	$q>2$	方法1 1 1		
		$q=2$	方法2 1 1		
	${}^2B_2(q)$	$q=2^{2t+1}, t\geqslant 1$	方法1 1 1		
	${}^2G_2(q)$	$q=3^{2t+1}, t\geqslant 1$	方法1 1 1		
	${}^2F_4(q)$	$q=2^{2t+1}, t\geqslant 1$	方法1 1 1		
	${}^2F_4(2)'$	$q=2$	方法2 1 1		

表 1. 用于选择合适子群的常数因子和方法汇总表

附录中的第6.4节包含两张综合表，列出了在有限单群分类的不同情形下用于引理 1 证明的子群的阶。

注*3*。 现在我们讨论如何在多项式时间内构造定理 6 中给出的数据结构。除了一些简单的多项式时间计算外，

可以验证，要在多项式时间内构造该数据结构，只需在多项式时间内完成以下四项任务。

1. 计算合成列；2. 计算 Sylow p-子群；3. 计算子群的正规化子；4. 计算单群的极大子群

s.

众所周知，即使对于置换群，任务（1）、（2）和（3）也可以在多项式时间内完成（例如参见 [24]）。对于（4），我们注意到，单群的任意极大子群至多由 4 个元素生成 [7]。因此，事实上，给定单群的凯莱表，我们可以在多项式时间内枚举出其所有极大子群。

还有一个更加微妙的问题：我们如何确定应当应用哪种方法（方法 1 还是方法 2），以获得引理 11 和定理 12 所要求的正确子群？有两种方式可以处理这一问题。a) 我们直接同时应用两种方法。根据引理 11，其中一种方法必然会产生所需大小的子群。b) 我们可以通过进行同构测试来确定该单群的类型。注意，由于任意单群都只由两个元素生成，因此单群之间的同构性可以在多项式时间内进行测试。我们还需要使用一个众所周知的事实：对于任意给定的阶，至多存在 2 个单群。

参考文献

1. N. Ahanjideh 和 A. Iranmanesh. 一些经典单群的 Sylow 正规化子。《马来西亚数学科学学会通报》*(2)*，35(2):459–467，2012年。2. Vikraman Arvind 和 Jacobo Torán. 拟群同构与最小生成集问题的复杂性。载于国际算法与计算研讨会，第 233–242 页。施普林格，2006年。3. Vikraman Arvind 和 Jacobo Torán. 可解群同构（几乎）属于 NP∩ coNP。《*ACM* 计算理论汇刊》，2(2):4:1–4:22，2011年。4. M. Aschbacher. 有限群论。剑桥高等数学研究丛书。剑桥大学出版社，第 2 版，2000年。5. László Babai、Paolo Codenotti 和 Youming Qiao. 对不含阿贝尔正规子群的群进行多项式时间同构判定。载于国际自动机、语言与编程研讨会，第 51–62 页。施普林格，2012年。6. László Babai 和 Youming Qiao. 对具有阿贝尔 Sylow 塔的群进行多项式时间同构判定。载于*STACS'12*（第 *29* 届计算机科学理论方面研讨会），第 14 卷，第 453–464 页。LIPIcs，2012年。7. Timothy C Burness、Martin W Liebeck 和 Aner Shalev. 生成与随机生成：从单群到极大子群。数学进展，248:59–95，2013年。8. Roger W. Carter. 李型有限群。Wiley 经典丛书。约翰·威立父子出版公司，奇切斯特，1993年。共轭类与复特征标，1985年原版重印，Wiley-Interscience 出版物。

9. J. H. Conway、R. T. Curtis、S. P. Norton、R. A. Parker 和 R. A. Wilson. 有限群图谱。牛津大学出版社，Eynsham，1985年。单群的极大子群与普通特征标，在 J. G. Thackray 的计算协助下完成。10. Bireswar Das 和 Shivdutt Sharma. Dedekind 群和有限环的紧凑数据结构。载于*WALCOM*，第 90–102 页，2021年。11. Bireswar Das、Shivdutt Sharma 和 P. R. Vaidyanathan. 有限群的空间高效表示。《计算机与系统科学杂志》，114:137–146，2020年。12. David S. Dummit 和 Richard M. Foote. 抽象代数。约翰·威立父子出版公司，新泽西州霍博肯，第 3 版，2004年。13. Arash Farzan 和 J. Ian Munro. 有限阿贝尔群的简洁表示。载于*ISSAC 2006*，第 87–92 页。ACM，纽约，2006年。14. Merrick Furst、John Hopcroft 和 Eugene Luks. 置换群的多项式时间算法。载于第*21*届计算机科学基础年会（*sfcs 1980*），第 36–41 页。IEEE，1980年。15. Francois Le Gall. 一类群扩张的高效同构判定。*arXiv* 预印本 *arXiv:0812.2298*，2008年。16. T. Kavitha. 阿贝尔群同构及相关问题的线性时间算法。《计算机系统科学杂志》，73(6):986–996，2007年。17. Neeraj Kayal 和 Timur Nezhmetdinov. 高效分解群。载于国际自动机、语言与编程研讨会，第 585–596 页。施普林格，2009年。18. Peter B. Kleidman 和 Martin W. Liebeck. 有限经典群的子群结构。伦敦数学会讲义系列。剑桥大学出版社，1990年。19. Daniel J. Kleitman、Bruce R. Rothschild 和 Joel H. Spencer. 阶为 n 的半群数量。《美国数学会会刊》，55(1):227–232，1976年。20. S Ravi Kumar 和 Ronitt Rubinfeld. 阿贝尔群运算的性质测试，1998年。21. Gary L. Miller. 关于 $n^{\log n}$ 同构技术：初步报告。载于 Richard J. Lipton、Walter A. Burkhard、Walter J. Savitch、Emily P. Friedman 和 Alfred V. Aho（编），第十届 *ACM* 计算理论年会论文集，*1978*年*5*月*1*日至*3*日，美国加利福尼亚州圣迭戈，第 51–58 页。ACM，1978年。22. Youming Qiao、Jayalal Sarma 和 Bangsheng Tang. 关于具有正规霍尔子群的群的同构判定。《计算机科学与技术学报》，27(4):687–701，2012年。23. Joseph J. Rotman. 群论导论，数学研究生教材第 148 卷。施普林格出版社，纽约，第 4 版，1995年。24. Ákos Seress. 置换群算法，剑桥数学丛书第 152 卷。剑桥大学出版社，剑桥，2003年。25. Charles C. Sims. 置换群研究中的计算方法。载于 John Leech（编），抽象代数中的计算问题，第 169–183 页。Pergamon，1970年。26. Charles C Sims. 置换群计算。载于第二届 *ACM* 符号与代数运算研讨会论文集，第 23–28 页，1971年。27. Charles C. Sims. 有限表示群的计算，数学及其应用百科全书第 48 卷。剑桥大学出版社，剑桥，1994年。28. J. H. van Lint 和 R. M. Wilson. 组合学教程。剑桥大学出版社，剑桥，1992年。29. Robert A. Wilson. 有限单群，数学研究生教材第 251 卷。施普林格伦敦有限公司，伦敦，2009年。

16 B. Das、A. Kumar、S. Sharma 和 D. Thakkar

30. Robert A. Wilson。散在群的极大子群。载于有限单群：图谱三十年及其后，第 694 卷当代数学，第 57–72 页。美国数学会，罗得岛州普罗维登斯，2017。

附录

6 引理 1 的证明

本节将详细证明引理 1。我们按照《有限单群分类定理》中提到的顺序给出详细计算，即定理 7。正如第 2 节所述，我们只需用到一些关于单群某些子群的阶 的已知结果。为证明之目的，可以略去对这些群的详细描述。证明中用到的结果涉及有限单群的阶、单群的极大子群的阶，以及单群中某些类型的西洛子群的正规化子。这些单群的阶的信息可从 [4] 中获取（见第 252 页）。

在定理 7 的情形 (ii) 中， H 是一个交错群。任意集合的稳定子在自然作用下都是交错群的子群。子群 H_1 和 H_2 是从给定交错群 H 中适当选取的稳定子子群。

对于定理 7 的情形 (iii) 和 (iv)，我们使用方法 1 和方法 2 来获得引理 1 所要求的子群。在这些情形中，有限单群 H 是李型的，并定义在有限域 $\mathbb{F}_q$ 上，其中 q 是某个素数 p 的幂。在方法 1 中，我们取 H_2 为 H 的某个西洛 p 子群。这种 H_2 的存在性由众所周知的西洛定理得出。对于 H_1 的存在性，我们取 H_2 的正规化子或 Borel 子群。关于正规化子阶的信息可从（见 [8]，第 76, [29]，页，第 46 页）获得。

对于使用方法 2 的群，我们将 H 的极大子群视为 H_1，并将 H_2 视为 H_1 的某个西洛 p-子群。极大子群的指数（因此其阶）可由 [18]，第 175 页和 [29]，第 156 页得出。

对于情形 (v) 中的单群，我们使用方法 2，极大子群的阶的信息（H_1）可由 [30] 得出。此外，在选择 H_2 时，我们选择 H_1 的某个西洛子群。

备注

以下两条备注中的不等式在计算中多次用到。为求完整起见，我们给出这些不等式的证明。

注*4*。 对于所有整数 $q > 2$，都有 $\frac{q}{(q-1)^2} < 1$。

证明。

$$\begin{aligned}1-\frac{q}{(q-1)^2} =& \frac{(q-1)^2-q}{(q-1)^2}\\ =& \frac{q^2-3q+1}{(q-1)^2}\\ =& \frac{(q-\frac{3+\sqrt{5}}{2})(q-\frac{3-\sqrt{5}}{2})}{(q-1)^2}\\ >& 0.\end{aligned}$$

因此，$\frac{q}{(q-1)^2}<1$，对于 $q>2$

注 *5*。

$$\prod_{i=1}^{i=m}(q^{i+1}-(-1)^{i+1})<q^{\sum_{i=1}^{i=m}(i+1)}$$

.

证明。 我们可以观察到，1 的符号会交替变化。当 i 为偶数时，1 的符号为负；当 i 为奇数时，1 的符号为正。

Now,

$$(q^{2j-1}-(-1)^{2j-1})(q^{2j}-(-1)^{2j})=(q^{4j-1}-1-q^{2j}+q^{2j-1})<q^{4j-1}\,(j\geqslant 1).$$

如果 m 为偶数，那么很容易看出，我们可以将连续的奇数项和偶数项两两配对，这些项的乘积小于 q 的幂之和。如果 m 为奇数，那么未配对的项是 q^m-1。注意，$(q^m-1)<q^m$。因此，在这种情况下，所有项的乘积也小于 q 的幂之和。

注 *6*。 两个非零自然数 m 和 n 的最大公约数（最大公约数）记作 (m,n)。

6.1 交错群

交错群 A_m 是有限集上的所有偶置换构成的群。众所周知，当 $m\geqslant 5$ 时，A_m 是单群。注意，对于自然作用，点 α 或集合 $S\subset[m]$ 的稳定子是 A_m 的子群。特别地，集合 $\{i+1,...、m\}$ 的稳定子是 A_m 的子群，并且与 A_i 同构。

因此，存在 K_j，它是 A_m 的子群，使得 $K_j\cong A_j, \forall\, j$ 和 $|K_j|=j!\,2$。令 $k\in\mathbb{Z}$，使得 $\frac{k!}{2}\leqslant\sqrt{\frac{m!}{2}}<\frac{(k+1)!}{2}$，且

$$H_2\cong A_k \text{ amd } H_1\cong A_{k+1}.$$

因此， A_k 是 A_{k+1} 的子群，因为 A_k 是稳定子，它固定点 $k+1$ 和 $H_2 \leqslant H_1$。注意，

$$|H_2|^2 = \left(\frac{k!}{2}\right)^2 \leqslant \frac{m!}{2}.$$

现在，考虑

$$\begin{aligned}\frac{m!}{2} &< \left(\frac{(k+1)!}{2}\right)^2 \\ \frac{(k+2)(k+3)\cdots m}{2} &< \frac{1\cdot 2\cdots k+1}{4} \\ (k+2)(k+3)\cdots m &< 3\cdot 4\cdots k+1.\end{aligned}$$

注意，右边的每一项都小于左边的每一项。因此，左边的项数必定严格少于右边的项数，这意味着

$$\begin{aligned}m-(k+1) &< (k+1)-2 \\ m-2k &< 0 \\ \frac{m}{2} &< k.\end{aligned}$$

因此，$k > \frac{m}{2}$，而且很容易找到这样的 k。
考虑，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 = \left(\frac{\frac{(k+1)!}{2}}{\frac{k!}{2}}\right)^2 = (k+1)^2.$$

现在，当 $m = 5$、$k = 3$ 和 $m = 6$、$k = 4$ 时，我们可以看到以下不等式成立：

$$(k+1)^2 < \frac{m!}{2}.$$

考虑一下， $m \geqslant 7$ 和 $k \geqslant 4$，那么，

$$\begin{aligned}\frac{k!}{2} &\leqslant \sqrt{\frac{m!}{2}} \\ \left(\frac{k!}{2}\right)^2 &\leqslant \frac{m!}{2} \\ \frac{k^2(k-1)^2(k-2)^2}{4} &\leqslant \left(\frac{k!}{2}\right)^2 \leqslant \frac{m!}{2}.\end{aligned}$$

Let,

$$\begin{aligned}\frac{4(k+1)^2}{k^2(k-1)^2(k-2)^2} &= \frac{4(1+\frac{1}{k})^2}{(k-1)^2(k-2)^2} \\ &< \frac{4}{4\cdot 9}\frac{25}{16} \\ &< 1\end{aligned}$$

$$(k+1)^2 < \frac{k^2(k-1)^2(k-2)^2}{4} \leqslant \left(\frac{k!}{2}\right)^2 \leqslant \frac{m!}{2}.$$

因此，这意味着，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 = (k+1)^2 \leqslant \frac{m!}{2}.$$

显然，

$$\left(\frac{|H|}{|H_1|}\right)^2 = \left(\frac{\frac{(m)!}{2}}{\frac{(k+1)!}{2}}\right)^2 < \left(\frac{\frac{m!}{2}}{\sqrt{\frac{m!}{2}}}\right)^2 = \frac{m!}{2}.$$

6.2 经典群

在本节中，我们将 H 视为定理 7 的情形 (iii) 中所述的经典单群。设 q 为某个素数 p的幂。如前所述，我们使用方法 1 和方法 2 来证明单群 H存在子群 H_2 和 H_1。

A 线性型经典群：

1.1 $H = A_m(q);\ \ m \geqslant 1,\ \ q > 2$ （方法 1）

有限单群 $A_m(q)$ 同构于射影特殊线性群 $PSL_{m+1}(q)$，其中 $PSL_{m+1}(q)$ 是通过取特殊线性群 $SL_{m+1}(q)$ 并将其中心取商群得到的群，即 $A_m(q) \cong \frac{SL_{m+1}(q)}{Z(SL_{m+1}(q))}$（见 [29], 第 44 页）。已知（见 [4], 第 252 页）其阶为:

$$|H| = \frac{q^{\frac{m(m+1)}{2}} \prod_{i=1}^{m}(q^{i+1}-1)}{(q-1,m+1)}.$$

设 H_2 为 $A_m(q)$的 Sylow p-子群，则 $|H_2| = q^{\frac{m(m+1)}{2}}$。注意，$|H_2|^2 \leqslant |H|$。考虑 H的 Borel 子群 H_1，其阶为（见 [29], 第 46 页）：

$$|H_1| = \frac{q^{\frac{m(m+1)}{2}}}{(q-1,m+1)}(q-1)^m.$$

考虑,

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{\frac{q^{\frac{m(m+1)}{2}}}{(q-1,m+1)}(q-1)^m}{q^{m(m+1)}} \\ &= \frac{1}{(q-1,m+1)}\frac{(q-1)^m}{q^{\frac{m(m+1)}{2}}} \\ &< \frac{1}{(q-1,m+1)}\frac{q^m}{q^{\frac{m(m+1)}{2}}} \\ &< \frac{q^m}{q^{1+2+3+\ldots+m}}\end{aligned}$$

$$< 1.$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

此外,

$$\begin{aligned}
\frac{|H|}{|H_1|^2} &= \frac{\frac{q^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(q^{i+1}-1)}{(q-1,m+1)}}{(\frac{q^{\frac{m(m+1)}{2}}}{(q-1,m+1)}(q-1)^m)^2} \\
&= \frac{(q-1,m+1)\prod_{i=1}^{m}(q^{i+1}-1)}{q^{\frac{m(m+1)}{2}}(q-1)^{2m}} \\
&< \frac{q^{1+2+\ldots+m}q^{m+1}}{q^{\frac{m(m+1)}{2}}(q-1)^{2m}} \\
&= \frac{q^{m+1}}{(q-1)^{m+1}(q-1)^{m-1}} \\
&= \frac{1}{(1-\frac{1}{q})^{m+1}(q-1)^{m-1}} \\
&= \frac{1}{(1-\frac{1}{q})^{2}(1-\frac{1}{q})^{m-1}(q-1)^{m-1}} \\
&= \frac{1}{(1-\frac{1}{q})^{2}(q-2+\frac{1}{q})^{m-1}} \\
&< 3.
\end{aligned}$$

因此,

$$\left(\frac{|H|}{|H_1|}\right)^2 < 3\,|H| \implies \frac{|H|}{|H_1|} < 2\sqrt{|H|}.$$

1.2 $A_m(q)$; $m \geqslant 1, q = 2$ （方法 2）

有限单群 $A_m(2)$ 的阶为 $2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1)/(q-1,m+1)$，且同构于射影特殊线性群 $PSL_{m+1}(2)$ 或 $L_{m+1}(2)$。它有一个指数为 $(2^{m+1}-1)$ 的极大子群（见 [18], 第 175 页）。令 H_1 为 $A_m(2)$ 的一个这样的极大子群。那么,

$$\begin{aligned}
|H_1| &= \frac{|A_m(2)|}{(2^{m+1}-1)} \\
&= \frac{2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1)}{(2^{m+1}-1)}.
\end{aligned}$$

令 H_2 为 H_1 的 Sylow 2-子群。那么， H_2 的阶为 $2^{\frac{m(m+1)}{2}}$ ，且 $|H_2|^2 < |A_m(2)|$。这意味着

$$\frac{|H_1|}{|H_2|} = \prod_{i=1}^{m-1}(2^{i+1}-1).$$

考虑,

$$\begin{aligned}\frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|A_m(2)|} &= \frac{\left(\prod_{i=1}^{m-1}(2^{i+1}-1)\right)^2}{2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1)} \\ &= \frac{\prod_{i=1}^{m-1}(2^{i+1}-1)}{2^{\frac{m(m+1)}{2}}(2^{m+1}-1)} \\ &< \frac{2^{\frac{m(m+1)}{2}-1}}{2^{\frac{m(m+1)}{2}}(2^{m+1}-1)} \\ &< 1.\end{aligned}$$

因此，我们得到

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |A_m(2)|.$$

Now,

$$\begin{aligned}\left(\frac{|A_m(2)|}{|H_1|}\right)^2 &= (2^{m+1}-1)^2 \\ &< 2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1) \\ &= |A_m(q)|.\end{aligned}$$

酉型经典群：

1.1 $H = {}^2A_m(q^2)$; $m \geqslant 2, q > 2$ (方法 1)

有限单群 ${}^2A_m(q^2)$ 同构于射影特殊酉群 $PSU_{m+1}(q)$。群 $PSU_{m+1}(q)$ 是通过将特殊酉群 $SU_{m+1}(q)$ 对其中心取商得到的群，即 ${}^2A_m(q^2) \cong SU_{m+1}(q)/Z(SU_{m+1}(q))$ （参见 [29], 第 66 页）。已知（参见 [4], 第 252 页），${}^2A_m(q^2)$ 的阶为,

$$|H| = \frac{q^{\frac{m(m+1)}{2}}}{(q+1, m+1)}\prod_{i=1}^{m}(q^{i+1}-(-1)^{i+1}).$$

设 H_2 为 ${}^2A_m(q^2)$ 的 Sylow p 子群，则 $|H_2| = q^{\frac{m(m+1)}{2}}$ 和 $|H_2|^2 \leqslant |H|$。设 H_1 为 H 的 Borel 子群，其阶为（参见 [29], [8]），

$$|H_1| = \frac{q^{\frac{m(m+1)}{2}}}{(q+1,m+1)}(q-1)^{\lfloor m/2 \rfloor}(q+1)^{\lceil \frac{m-1}{2} \rceil}.$$

考虑,

$$\begin{aligned}\left(\frac{|H_1|}{|H_2|}\right)^2 &= \left(\frac{(q-1)^{\lfloor m/2 \rfloor}(q+1)^{\lceil \frac{m-1}{2} \rceil}}{(q+1,m+1)}\right)^2 \\ &\leqslant \frac{(q-1)^m(q+1)^m}{(q+1,m+1)^2} \\ &= \frac{(q^2-1)^m}{(q+1,m+1)^2} \\ &\leqslant |H_1|.\end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 \leqslant |H_1| < |H|.$$

此外,

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{\frac{q^{\frac{m(m+1)}{2}}}{(q+1,m+1)}\prod_{i=1}^{m}(q^{i+1}-(-1)^{i+1})}{\left(\frac{(q-1)^{\lfloor m/2 \rfloor}(q+1)^{\lceil \frac{m-1}{2} \rceil}q^{\frac{m(m+1)}{2}}}{(q+1,m+1)}\right)^2} \\ &= \frac{(q+1,m+1)\prod_{i=1}^{m}(q^{i+1}-(-1)^{i+1})}{(q-1)^m(q+1)^{m-1}q^{\frac{m(m+1)}{2}}} \\ &< \frac{(q+1,m+1)q^{\frac{(m+1)(m+2)}{2}-1}}{(q-1)^m(q+1)^{m-1}q^{\frac{m^2+m}{2}}} \qquad \text{(by Remark 5)} \\ &= \frac{(q+1,m+1)q^{\frac{(m+1)(m+2)}{2}-1}}{(q-1)(q^2-1)^{m-1}q^{\frac{m^2+m}{2}}} \\ &= \frac{(q+1,m+1)q^m}{(q-1)(q^2-1)^{m-1}} \\ &< 2\,\frac{q}{\left(q-\frac{1}{q}\right)^{m-1}} \\ &< 4.\end{aligned}$$

因此,

$$\left(\frac{|H|}{|H_1|}\right)^2 \leqslant 4|H| \implies \frac{|H|}{|H_1|} \leqslant 2\sqrt{|H|}$$

1.2 $H = {}^2A_m(q^2)$; $m \geqslant 2$, $q = 2$ （方法 2）

有限单群 ${}^2A_m(2^2)$ 的阶为 $2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})/(3,m+1)$, 且同构于射影特殊酉群$\mathrm{PSU}_{m+1}(2)$ 或 $U_{m+1}(q)$。群 $U_{m+1}(q)$ 有一个指数为 $\frac{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}{3}$ 的极大子群

当 $6 \nmid (m-1)$ 时，且指数为 $\frac{2^m(2^{m+1}-1)}{3}$ 时，当 $6 \mid (m-1)$ 时（见 [18]，第 175 页）。

（情形 1） $6 \nmid (m-1)$

设 H_1 是 ${}^2A_m(2^2)$ 的对应极大子群，其指数为

$$\frac{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}{3}$$

${}^2A_m(2^2)$ 中。因此， H_1 的阶为，

$$\begin{aligned}|H_1| &= \frac{|\,{}^2A_m(2^2)|}{\frac{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}{3}} \\ &= \frac{3}{(3,m+1)}\frac{2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})}{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}.\end{aligned}$$

设 H_2 是 H_1 的 Sylow 2-子群。那么， $|H_2| = 2^{\frac{m(m+1)}{2}}$ 和 $|H_2|^2 < |\,{}^2A_m(2^2)|$。此外，

$$\frac{|H_1|}{|H_2|} = \frac{3}{(3,m+1)}\frac{\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})}{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}.$$

考虑，

$$\begin{aligned}\frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|\,{}^2A_m(2^2)|} &= \frac{\left(\frac{3}{(3,m+1)}\frac{\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})}{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}\right)^2}{\frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)}\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})} \\ &= \frac{9}{(3,m+1)}\frac{\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})}{2^{\frac{m(m+1)}{2}}((2^{m+1}-(-1)^{m+1})(2^m-(-1)^m))^2} \\ &< \frac{9}{(3,m+1)}\frac{2^{\frac{(m+1)(m+2)}{2}-1}}{2^{\frac{m(m+1)}{2}}((2^{m+1}-(-1)^{m+1})(2^m-(-1)^m))^2} \qquad \text{(根据注释 5)} \\ &= \frac{9}{(3,m+1)}\frac{2^m}{((2^{m+1}-(-1)^{m+1})(2^m-(-1)^m))^2} \\ &< \frac{9}{(3,m+1)}\frac{1}{\left(\left(2^{\lfloor\frac{m+1}{2}\rfloor}-\frac{(-1)^{m+1}}{2^{\lfloor\frac{m}{2}+1\rfloor}}\right)(2^m-(-1)^m)\right)^2} \\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |\,{}^2A_m(2^2)|$$

Now,

$$\left(\frac{|\,{}^2A_m(2^2)|}{|H_1|}\right)^2 = \left(\frac{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}{3}\right)^2$$

$$< \frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)} \prod_{i=1}^{m} (2^{i+1} - (-1)^{i+1}) = |{}^2A_m(2^2)|.$$

（情形 2） $6|(m-1)$（即 $m \geqslant 7$）

在这种情况下，我们知道群 ${}^2A_m(q^2)$ 有一个指数为 $\frac{2^m(2^{m+1}-1)}{3}$ 的极大子群。设 H_1 是这样一个极大子群。那么，

$$\begin{aligned} |H_1| &= \frac{|{}^2A_m(2^2)|}{\frac{2^m(2^{m+1}-1)}{3}} \\ &= \frac{\frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)} \prod_{i=1}^{m} (2^{i+1} - (-1)^{i+1})}{\frac{2^m(2^{m+1}-1)}{3}} \\ &= \frac{3}{(3,m+1)} 2^{\frac{m(m-1)}{2}} \prod_{i=1}^{m-1} (2^{i+1} - (-1)^{i+1}). \end{aligned}$$

设 H_2 是 H_1 的 Sylow 2-子群，则 H_2 的阶为 $2^{\frac{m(m-1)}{2}}$，且 $|H_2|^2 < |{}^2A_m(2^2)|$。此外，

$$\frac{|H_1|}{|H_2|} = \frac{3}{(3,m+1)} \prod_{i=1}^{m-1} (2^{i+1} - (-1)^{i+1}).$$

考虑，

$$\begin{aligned} \frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|{}^2A_m(2^2)|} &= \frac{\left(\frac{3}{(3,m+1)} \prod_{i=1}^{m-1} (2^{i+1} - (-1)^{i+1})\right)^2}{\frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)} \prod_{i=1}^{m} (2^{i+1} - (-1)^{i+1})} \\ &= \frac{9}{(3,m+1)} \frac{\prod_{i=1}^{m-1} (2^{i+1} - (-1)^{i+1})}{2^{\frac{m(m+1)}{2}} (2^{m+1} - (-1)^{m+1})} \\ &< \frac{9}{(3,m+1)} \frac{2^{\frac{m^2+m-2}{2}}}{2^{\frac{m^2+m}{2}} (2^{m+1} - (-1)^{m+1})} \qquad \text{(by Remark 5)} \\ &= \frac{9}{(3,m+1)} \frac{1}{2\,(2^{m+1} - (-1)^{m+1})} \\ &< 1. \qquad \text{(，因为 } m \geqslant 7) \end{aligned}$$

这意味着，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |{}^2A_m(2^2)|.$$

Now,

$$\left(\frac{|{}^2A_m(2^2)|}{|H_1|}\right)^2 = \left(\frac{2^m(2^{m+1}-1)}{3}\right)^2$$

$$
\begin{aligned}
&= \frac{2^{2m}(2^{m+1}-1)^2}{9} \\
&< \frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)} \prod_{i=1}^{m} (2^{i+1}-(-1)^{i+1}) \\
&= |{}^2A_m(2^2)|.
\end{aligned}
$$

辛线性型经典群：

1.1 $H = C_m(q)$; $m \geqslant 2$, $q > 2$ (方法 1)

有限单群 $C_m(q)$ 的阶可在（参见 [4], 第 252 页）中查到，它为,

$$|H| = \frac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{(2,q-1)}.$$

设 H_2 是 H的 Sylow p-子群，则 $|H_2| = q^{m^2}$ 且 $|H_2|^2 \leqslant |H|$。设H_1 是 H 中 H_2 的正规化子，则 H_1 的阶（参见 [1], 第 3 页）为,

$$|H_1| = \frac{q^{m^2}}{(2,q-1)}(q-1)^m.$$

考虑,

$$
\begin{aligned}
\frac{|H_1|}{|H_2|^2} &= \frac{\frac{q^{m^2}}{(2,q-1)}(q-1)^m}{q^{2m^2}} \\
&= \frac{1}{(2,q-1)}\frac{(q-1)^m}{q^{m^2}} \\
&< \frac{1}{(2,q-1)}\frac{q^m}{q^{m^2}} \\
&< 1.
\end{aligned}
$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

此外,

$$
\begin{aligned}
\frac{|H|}{|H_1|^2} &= \frac{\frac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{(2,q-1)}}{(\frac{q^{m^2}}{(2,q-1)}(q-1)^m)^2} \\
&= \frac{(2,q-1)\prod_{i=1}^{m}(q^{2i}-1)}{q^{m^2}(q-1)^{2m}} \\
&< \frac{(2,q-1)}{q^{m^2}}\frac{\prod_{i=1}^{m}q^{2i}}{(q-1)^{2m}}
\end{aligned}
$$

$$
\begin{aligned}
&= (2, q-1)\frac{q^{m+m^2}}{q^{m^2}(q-1)^{2m}} \\
&= (2, q-1)(\frac{q}{(q-1)^2})^m \\
&\leqslant 2 \qquad \text{(by Remark 4)}
\end{aligned}
$$

因此,

$$
\left(\frac{|H|}{|H_1|}\right)^2 \leqslant 2\,|H| \implies \frac{|H|}{|H_1|} < 2\sqrt{|H|}.
$$

1.2 $H = C_m(q)$; $m \geqslant 2$, $q = 2$ （方法 2）

单群 $C_m(q)$ （或 $PSp_{2m}(q)$）的阶为 $2^{m^2}\prod_{i=1}^{m}(2^{2i}-1)$。已知群 $PSp_{2m}(q)$ 有一个指数为 $2^{m-1}(2^m-1)$ 的极大子群（见 [18], 第 175 页）。设 H_1 是这样一个子群，则 H_1 的阶为:

$$
\begin{aligned}
|H_1| &= \frac{|C_m(2)|}{2^{m-1}(2^m-1)} \\
&= \frac{2^{m^2}\prod_{i=1}^{m}(2^{2i}-1)}{2^{m-1}(2^m-1)} \\
&= \frac{2^{m^2-m+1}(2^{2m}-1)\prod_{i=1}^{m-1}(2^{2i}-1)}{(2^m-1)} \\
&= 2^{m^2-m+1}(2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1).
\end{aligned}
$$

设 H_2 是 H_1的 Sylow 2-子群。那么， H_2 的阶为 2^{m^2-m+1}。注意到 $|H_2|^2 < |C_m(2)|$。因此,

$$
\frac{|H_1|}{|H_2|} = (2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1).
$$

考虑,

$$
\begin{aligned}
\frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|C_m(2)|} &= \frac{((2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1))^2}{2^{m^2}\prod_{i=1}^{m}(2^{2i}-1)} \\
&= \frac{(2^m+1)^2(\prod_{i=1}^{m-1}(2^{2i}-1))^2}{2^{m^2}(2^{2m}-1)\prod_{i=1}^{m-1}(2^{2i}-1)} \\
&= \frac{(2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1)}{2^{m^2}(2^m-1)} \\
&< \frac{(2^m+1)\prod_{i=1}^{m-1}2^{2i}}{2^{m^2}(2^m-1)}
\end{aligned}
$$

$$\begin{aligned}&= \frac{(2^m+1)2^{m(m-1)}}{2^{m^2}(2^m-1)}\\ &= \frac{(1+2^{-m})}{(2^m-1)}\\ &< 1.\end{aligned}$$

因此,

$$\Big(\frac{|H_1|}{|H_2|}\Big)^2 < |C_m(2)|.$$

Now,

$$\begin{aligned}\Big(\frac{|C_m(2)|}{|H_1|}\Big)^2 &= (2^{m-1}(2^m-1))^2\\ &= 2^{2m-2}(2^m-1)^2\\ &< 2^{m^2}(2^m-1)(2^m+1)\\ &< 2^{m^2}\prod_{i=1}^{m}(2^{2i}-1)\\ &= |C_m(2)|.\end{aligned}$$

正交型经典群:

1.1 $H = B_m(q)$; $m \geqslant 3$ 和 q 为奇数（方法 1）

有限单群 $B_m(q)$ 的阶为（见 [4], 第 252 页）,

$$|H| = \tfrac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{(2,q-1)}.$$

设 H_2 是 H的 Sylow p子群，则 $|H_2| = q^{m^2}$ 且 $|H_2|^2 \leqslant |H|$。设H_1 是 H 中 H_1 的正规化子，则其阶为（见 [1], 第 3 页）,

$$|H_1| = \frac{q^{m^2}}{(2,q-1)}(q-1)^m.$$

由于 $|B_m(q)| = |C_m(q)|$ ，且在两个群中 H_1 的正规化子的阶也相等，因此所有计算对 $B_m(q)$也适用。

2.1 $H = D_m(q)$; $m \geqslant 4$, $q > 2$ （方法 1）

有限单群 $D_m(q)$ 的阶可在（见 [4]，第 252 页）中找到，且它是,

$$|H| = \tfrac{q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{(4,q^m-1)}.$$

设 H_2 为 $D_m(q)$ 的 Sylow p 子群，则 $|H_2| = q^{m(m-1)}$ 和 $|H_2|^2 \trianglelefteqslant H|$。设 H_1 为 H 的 Borel 子群。其阶为（见 [29], [8]），

$$|H_1| = \frac{q^{m(m-1)}}{(4, q^m - 1)}(q-1)^m.$$

考虑，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{\frac{q^{m(m-1)}}{(4,q^m-1)}(q-1)^m}{q^{2m(m-1)}} \\ &= \frac{1}{(4, q^m-1)}\frac{(q-1)^m}{q^{m(m-1)}} \\ &< \frac{1}{(4, q^m-1)}\frac{q^m}{q^{m(m-1)}} \\ &< 1.\end{aligned}$$

因此，

$$\Big(\frac{|H_1|}{|H_2|}\Big)^2 < |H_1| < |H|$$

此外，

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{\frac{q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{(4,q^m-1)}}{(\frac{q^{m(m-1)}}{(4,q^m-1)}(q-1)^m)^2} \\ &= \frac{(4, q^m-1)(q^m-1)\prod_{i=1}^{m}(q^{2i}-1)}{q^{m(m-1)}(q-1)^{2m}} \\ &< \frac{(4, q^m-1)(q^m-1)}{q^{m(m-1)}}\frac{\prod_{i=1}^{m-1} q^{2i}}{(q-1)^{2m}} \\ &< \frac{(4, q^m-1)q^m}{q^{m(m-1)}}\frac{q^{m(m-1)}}{(q-1)^{2m}} \\ &= (4, q^m-1)\Big(\frac{q}{(q-1)^2}\Big)^m \\ &\leqslant 4. \qquad \text{(by Remark 4)}\end{aligned}$$

因此，

$$\Big(\frac{|H|}{|H_1|}\Big)^2 \leqslant 4|H| \implies \frac{|H|}{|H_1|} \leqslant 2\sqrt{|H|}.$$

2.2 $H = D_m(q)$; $m \geqslant 4$, $q = 2$ （方法 2）

单群 $D_m(q)$ （或 $P\Omega^+_{2m}(q)$）的阶为 $2^{m(m-1)}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1)$。群 $P\Omega^+_{2m}(2)$ 有一个指数为 $2^{m-1}(2^m-1)$ 的极大子群（见

[18], 第 175 页）。设 H_1 是 $D_m(2)$ 的一个对应极大子群，其指数为 $2^{m-1}(2^m-1)$。则 H_1 的阶为,

$$\begin{aligned}|H_1| &= \frac{|D_m(2)|}{2^{m-1}(2^m-1)} \\ &= \frac{2^{m(m-1)}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1)}{2^{m-1}(2^m-1)} \\ &= 2^{m^2-2m+1}\prod_{i=1}^{m-1}(2^{2i}-1).\end{aligned}$$

设 H_2 为 H_1 的 Sylow 2-子群，则 H_2 的阶为 2^{m^2-2m+1} 和 $|H_2|^2 < |D_m(2)|$。此外,

$$\frac{|H_1|}{|H_2|} = \prod_{i=1}^{m-1}(2^{2i}-1).$$

考虑,

$$\begin{aligned}\frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|D_m(2)|} &= \frac{(\prod_{i=1}^{m-1}(2^{2i}-1))^2}{2^{m(m-1)}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1)} \\ &= \frac{\prod_{i=1}^{m-1}(2^{2i}-1)}{2^{m(m-1)}(2^m-1)} \\ &< \frac{\prod_{i=1}^{m-1}2^{2i}}{2^{m(m-1)}(2^m-1)} \\ &= \frac{2^{m(m-1)}}{2^{m(m-1)}(2^m-1)} \\ &= \frac{1}{(2^m-1)} \\ &< 1\end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |D_m(2)|.$$

Now,

$$\begin{aligned}\left(\frac{|D_m(2)|}{|H_1|}\right)^2 &= 2^{2(m-2)}(2^m-1)^2 \\ &< 2^{m(m-1)}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1) \\ &= |D_m(2)|.\end{aligned}$$

3.1 $H = {}^2D_m(q^2)$; $m \geqslant 4$, $q > 2$ (方法 1)

有限单群 ${}^2\mathrm{D}_m(q^2)$ 的阶可在（参见 [4]，第 252 页）中找到，它是，

$$|H| = \frac{q^{m(m-1)}(q^m+1)}{(4,q^m+1)} \prod_{i=1}^{m-1}(q^{2i}-1).$$

令 H_2 为 ${}^2\mathrm{D}_m(q^2)$ 的 Sylow p 子群，则 $|H_2| = q^{m(m-1)}$ 且 $|H_2|^2 \leqslant |H|$。令 H_1 为 H 的 Borel 子群。H_1 的阶为（见 [29], [8]）。因此，

$$|B| = \frac{q^{m(m-1)}}{(4,q^n+1)}(q-1)^m.$$

考虑，

$$\begin{aligned}
\frac{|H_1|}{|H_2|^2} &= \frac{\frac{q^{m(m-1)}}{(4,q^n+1)}(q-1)^m}{q^{2m(m-1)}} \\
&= \frac{1}{(4,q^n+1)} \frac{(q-1)^m}{q^{m(m-1)}} \\
&< \frac{1}{(4,q^n+1)} \frac{q^m}{q^{m(m-1)}} \\
&\leqslant 1.
\end{aligned}$$

因此，我们有

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

此外，

$$\begin{aligned}
\frac{|H|}{|H_1|^2} &= \frac{\frac{q^{m(m-1)}(q^m+1)}{(4,q^m+1)} \prod_{i=1}^{m-1}(q^{2i}-1)}{(\frac{q^{m(m-1)}}{(4,q^m+1)}(q-1)^m)^2} \\
&= \frac{(4,q^m+1)(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1)}{q^{m(m-1)}(q-1)^{2m}} \\
&< \frac{(4,q^m+1)(q^m+1)}{q^{m(m-1)}} \frac{\prod_{i=1}^{m-1} q^{2i}}{(q-1)^{2m}} \\
&= (4,q^m+1)(q^m+1)\frac{q^{m(m-1)}}{q^{m(m-1)}(q-1)^{2m}} \\
&< \frac{4(2q^m)}{(q-1)^{2m}} \\
&< 8 \qquad \text{(by Remark 4)}
\end{aligned}$$

这意味着，

$$\left(\frac{|H|}{|H_1|}\right)^2 < 8\,|H| \implies \frac{|H|}{|H_1|} < 3\sqrt{|H|}.$$

3.2 $H = {}^2\mathrm{D}_m(q^2)$; $m \geqslant 4$, $q = 2$ （方法 2）

我们知道，群 ${}^2\mathrm{D}_m(2^2)$（或 $\mathrm{P}\Omega^-_{2m}(2)$）的阶为 $2^{m(m-1)}(2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1)/(4,2^m+1)$。群 $\mathrm{P}\Omega^-_{2m}(2)$ 有一个指数为 $(2^m+1)(2^{m-1}-1)$ 的极大子群（见 [18], 第 175 页）。设 H_1 为这样一个子群，则其阶为,

$$\begin{aligned}|H_1| &= \frac{|\,{}^2\mathrm{D}_m(2^2)|}{(2^m+1)(2^{m-1}-1)}\\ &= \frac{\frac{2^{m(m-1)}(2^m+1)}{(4,2^m+1)}\prod_{i=1}^{m-1}(2^{2i}-1)}{(2^m+1)(2^{m-1}-1)}\\ &= 2^{m(m-1)}(2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1).\end{aligned}$$

设 H_2 为 H_1 的 Sylow 2-子群，则 $|H_2| = 2^{m(m-1)}$ 和 $|H_2|^2 \lhd {}^2\mathrm{D}_m(2^2)|$。因此,

$$\frac{|H_1|}{|H_2|} = (2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1).$$

考虑,

$$\begin{aligned}\frac{\left(\frac{|H_1|}{|H_2|}\right)^2}{|\,{}^2\mathrm{D}_m(2^2)|} &= \frac{((2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1))^2}{\frac{2^{m(m-1)}(2^m+1)}{(4,2^m+1)}\prod_{i=1}^{m-1}(2^{2i}-1)}\\ &= \frac{(2^{m-1}+1)^2\prod_{i=1}^{m-2}(2^{2i}-1)}{2^{m(m-1)}(2^{2m-2}-1)(2^m+1)}\\ &= \frac{(2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1)}{2^{m(m-1)}(2^{m-1}-1)(2^m+1)}\\ &< \frac{(2^{m-1}+1)\prod_{i=1}^{m-2}2^{2i}}{2^{m(m-1)}(2^{m-1}-1)(2^m+1)}\\ &= \frac{(2^{m-1}+1)2^{(m-2)(m-1)}}{2^{m(m-1)}(2^{m-1}-1)(2^m+1)}\\ &= \frac{(2^{m-1}+1)}{(2^{m-1}-1)(2^m+1)}\cdot\frac{2^{(m-2)(m-1)}}{2^{m(m-1)}}\\ &< 1.\end{aligned}$$

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |\,{}^2\mathrm{D}_m(2^2)|.$$

Now,

$$\left(\frac{|\,{}^2\mathrm{D}_m(2^2)|}{|H_1|}\right)^2 = ((2^m+1)(2^{m-1}-1))^2$$

$$\begin{aligned}
&< 2^{m(m-1)}(2^m+1)(2^{m-1}-1)(2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1)\\
&< 2^{m(m-1)}(2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1)\\
&= |{}^2D_m(2^2)|.
\end{aligned}$$

6.3 李型例外群

(1) $H = G_2(q)$; $q \geqslant 3$ (方法 1)

对于所有 $q \geqslant 3$, 群 $G_2(q)$ 都是单群。其阶为（见 [4], 第 252 页）,

$$|G_2(q)| = q^6(q^6-1)(q^2-1).$$

因此, $G_2(q)$ 有一个 p-Sylow 子群 H_2, 其阶为 q^6 和 $|H_2|^2 \leqslant |G_2(q)|$。此外, 它还具有阶为 $q^6(q-1)^2$ 的 Borel 子群 H_1 （见 [29], 第 124 页）。

考虑,

$$\begin{aligned}
\frac{|H_1|}{|H_2|^2} &= \frac{q^6(q-1)^2}{q^{12}}\\
&= \frac{(q-1)^2}{q^6}\\
&< 1.
\end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 \leqslant |H_1| \leqslant |H|.$$

Now,

$$\begin{aligned}
\frac{|H|}{|H_1|^2} &= \frac{q^6(q^6-1)(q^2-1)}{(q^6(q-1)^2)^2}\\
&< \frac{q^{6+2}}{q^6(q-1)^4}\\
&< \frac{q^2}{(q-1)^4}\\
&< 1 \qquad \text{(由注记 4)}
\end{aligned}$$

因此,

$$\left(\frac{|H|}{|H_1|}\right)^2 < |H|.$$

(2) $H = F_4(q)$ (方法 2)

有限单群 $F_4(q)$ 的阶为（见 [4], 第 252 页），

$$|F_4(q)| = q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1).$$

已知（见 [29], 第 156 页），群 $F_4(q)$ 有一个极大子群$q^{1+14} : Sp_6(q).C_{q-1}$，其阶为 $q^{24}(q^6-1)(q^4-1)(q^2-1)(q-1)$，记为 H_1。该子群有一个 Sylow p-子群，记为 H_2，其阶为 q^{24}，且 $|H_2|^2 \leqslant |F_4(q)|$。现在，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^{24}(q^6-1)(q^4-1)(q^2-1)(q-1)}{q^{48}} \\ &< \frac{q^{1+2+4+6}}{q^{24}} \\ &< 1.\end{aligned}$$

因此，

$$\Big(\frac{|H_1|}{|H_2|}\Big)^2 < |H_1| < |H|.$$

Now,

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)}{(q^{24}(q^6-1)(q^4-1)(q^2-1)(q-1))^2} \\ &= \frac{(q^4-1)^2(q^8+q^4+1)(q^4+1)}{q^{24}(q^6-1)(q^4-1)^2(q^2-1)(q-1)^2} \\ &= (1+\frac{1}{q^4}+\frac{1}{q^8})(1+\frac{1}{q^4})\frac{1}{q^{12}(q^6-1)(q^2-1)(q-1)^2} \\ &< 1.\end{aligned}$$

于是，我们得到

$$\Big(\frac{|H|}{|H_1|}\Big)^2 < |H|.$$

(3) $H = E_6(q)$; $q > 2$ (方法 1)

群 $E_6(q)$ 是一个有限单群。 $H = E_6(q)$ 的阶为（见 [4],第 252 页），

$$|E_6(q)| = \frac{q^{36}}{(3, q-1)}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1).$$

显然，它有一个阶为 q^{36} 且具有 $|H_2|^2 \leqslant |E_6(q)|$的 Sylow p-子群 H_2。设 H_1 为 H 的 Borel 子群，则 H_1 的阶为 $q^{36}(q-1)^6$（见 [29],[8]）。考虑，

$$\frac{|H_1|}{|H_2|^2} = \frac{q^{36}(q-1)^6}{q^{72}}$$

$$\begin{aligned} &< \frac{q^6}{q^{36}} \\ &< 1. \end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

Now,

$$\begin{aligned} \frac{|H|}{|H_1|^2} &= \frac{q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)}{(3,q-1)(q^{36}(q-1)^8)^2} \\ &< \frac{q^{12+9+8+6+5+2}}{(3,q-1)q^{36}(q-1)^{16}} \\ &= \frac{q^{42}}{(3,q-1)q^{36}(q-1)^{16}} \\ &= \frac{q^6}{(3,q-1)(q-1)^{16}} \\ &= \frac{1}{(3,q-1)(q-1)^4}\frac{q^6}{(q-1)^{12}} \\ &< \frac{q^6}{(q-1)^{12}} \\ &< 1. \qquad \text{(by Remark 4)} \end{aligned}$$

这意味着,

$$\left(\frac{|H|}{|H_1|}\right)^2 \leqslant |H|.$$

注意，群 $E_6(2)$ 的阶为常数。不过，我们可以使用方法2将常数 b_1、 b_2 降为 1。令 H_1 为阶为（见 [9]）的极大子群， $2^{36}\cdot 3^3\cdot 5\cdot 7\cdot 31$ ，并令 H_2 为其阶为 2^{36} 的 Sylow 2- 子群。

(4) $H = {}^2E_6(q)$ (Method 1)

对于所有 q ，群 ${}^2E_6(q)$ 都是单群，且其阶为（见 [4], 第 252 页），

$$|{}^2E_6(q)| = \frac{q^{36}(q^2-1)(q^5+1)(q^6-1)(q^8-1)(q^9+1)(q^{12}-1)}{(3,q+1)}.$$

群 ${}^2E_6(q)$ 有一个阶为 q^{36} 且 $|H_2|^2 \leqslant |H|$的 Sylow p 子群 H_2。众所周知, Borel 子群的阶是 Sylow p 子群的阶与极大环面的阶的乘积。 H 中的极大环面的阶为 $(q+1)^6$（见 [29], 第 173 页）。因此， H 的 Borel 子群H_1 的阶为 $q^{36}(q+1)^6$。

考虑：

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^{36}(q+1)^6}{q^{72}}\\ &< \frac{(q+1)^6}{q^{36}}\\ &< \frac{(q+q)^6}{q^{36}}\\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

此外，

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^{36}(q^2-1)(q^5+1)(q^6-1)(q^8-1)(q^9+1)(q^{12}-1)}{(q^{36}(q+1)^6)^2}\\ &< \frac{(q^5+1)(q^9+1)}{q^8(q+1)^{12}}\\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H|}{|H_1|}\right)^2 < |H|.$$

(5) $H = {}^3D_4(q)$ (方法 1)

对于所有 q，群 ${}^3D_4(q)$ 都是单群。已知群 ${}^3D_4(q)$ 的阶为（见 [4]，第 252 页），

$$|{}^3D_4(q)| = q^{12}(q^8+q^4+1)(q^6-1)(q^2-1).$$

显然，它有一个阶为 q^{12} 的 Sylow p 子群 H_2，以及一个阶为 $q^{12}(q^3-1)(q-1)$ 的 Borel 子群 H_1（见 [29]，第 141 页）。此外，注意到 $|H_2|^2 \leqslant |H|$。

考虑，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^{12}(q^3-1)(q-1)}{q^{24}}\\ &= \frac{(q^3-1)(q-1)}{q^{12}}\\ &< \frac{q^4}{q^{12}}\\ &< 1.\end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)}{(q^{12}(q^3-1)(q-1))^2}\\ &= \frac{(q^8+q^4+1)(q^3+1)(q+1)}{q^{12}(q^3-1)(q-1)}\\ &= \frac{(1+\frac{1}{q^4}+\frac{1}{q^8})(1+\frac{1}{q^3})(1+\frac{1}{q})}{(q^3-1)(q-1)}\\ &< 1.\end{aligned}$$

因此,

$$\left(\frac{|H|}{|H_1|}\right)^2 < |H|.$$

(6) $H = E_7(q),\quad q > 2$ （方法 1）

单群 $E_7(q)$ 的阶为（见 [4], 第 252 页）,

$$|E_7(q)| = \frac{q^{63}}{(2,q-1)}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1).$$

显然, 它有一个 Sylow p-子群 H_2, 其阶为 q^{63}, 并且 $|H_2|^2 \leqslant |H|$。令 H_1 为 H 的 Borel 子群, 则其阶为（见 [29], [8]）,

$$|H_1| = q^{63}(q-1)^7.$$

考虑,

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^{63}(q-1)^7}{q^{126}}\\ &< \frac{q^7}{q^{63}}\\ &< 1\end{aligned}$$

因此,

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

$$\begin{aligned}\frac{|H|}{|B|^2} &= \frac{\frac{q^{63}}{(2,q-1)}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)}{(q^{63}(q-1)^7)^2}\\ &< \frac{q^{18+14+12+10+8+6+2}}{(2,q-1)q^{63}(q-1)^{14}}\end{aligned}$$

$$
\begin{aligned}
&= \frac{q^{70}}{(2, q-1)q^{63}(q-1)^{14}} \\
&= \frac{1}{(2, q-1)} \frac{q^7}{(q-1)^{14}} \\
&< 1. \qquad\qquad (q \neq 2)。
\end{aligned}
$$

因此，

$$\left(\frac{|H|}{|H_1|}\right)^2 < |H|.$$

注意，群 $E_7(2)$ 的阶是常数。不过，我们可以使用方法2将常数 b_1、 b_2 降至 1。取 H_1 为阶为（见 [9]）的极大子群 $2^{63} \cdot 3^4 \cdot 7^2 \cdot 5$，并取 H_2 为其阶为 2^{63}的 Sylow 2-子群。

(7) $H = E_8(q)$, $q > 2$ (Method 1)

我们知道，对于所有 q，群 $E_8(q)$ 都是单群，且其阶为（见 [4], 第 252 页），

$$|H| = q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1).$$

群 $E_8(q)$ 有一个 Sylow p-子群 H_2，于是 $|H_2| = q^{120}$ 和 $|H_2|^2 \leqslant |H|$。令 H_1 为 Borel 子群，则其阶为 $|H_1| = q^{120}(q-1)^8$ （见 [29],第 176 页）。

考虑，

$$
\begin{aligned}
\frac{|H_1|}{|H_2|^2} &= \frac{q^{120}(q-1)^8}{q^{240}} \\
&< \frac{q^8}{q^{120}} \\
&< 1.
\end{aligned}
$$

因此，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

$$
\begin{aligned}
\frac{|H|}{|H_1|^2} &= \frac{q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)}{(q^{120}(q-1)^8)^2} \\
&= \frac{(q^8-1)}{(q-1)^{16}} \prod_{i \in \{2,12,14,18,20,24,30\}} (1 - \frac{1}{q^i}) \\
&\leqslant \frac{q^8}{(q-1)^{16}} \\
&\leqslant 1. \qquad\qquad (\text{by Remark } 4)
\end{aligned}
$$

这意味着，

$$\Big(\frac{|H|}{|H_1|}\Big)^2 \leqslant |H|.$$

请注意，群 $E_8(2)$ 的阶是常数。不过，我们可以使用方法2将常数 b_1、b_2 降至 1。令 H_1 为阶为（见 [9]）的极大子群，$2^{119} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$，并令 H_2 为其阶为 2^{119} 的 Sylow 2-子群。

(8) $H = {}^2B_2(q)$、$q = 2^{2t+1}$ 和 $t \geqslant 1$（方法 1）

有限单群 ${}^2B_2(q)$ 的阶为（见 [4]，第 252 页），

$$|H| = q^2(q^2+1)(q-1).$$

因此，它有一个阶为 q^2 的 Sylow 2-子群 H_2，且 $|H_2|^2 \leqslant |H|$。令 H_1 为 ${}^2B_2(q)$ 的 Borel 子群，则其阶 H_1 为 $q^2(q-1)$（见 [29]，第 117 页）。

考虑，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \Big(\frac{q^2(q-1)}{q^4}\Big)\\ &< 1.\end{aligned}$$

因此，

$$\Big(\frac{|H_1|}{|H_2|}\Big)^2 < |H_1| < |H|.$$

Now,

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^2(q^2+1)(q-1)}{(q^2(q-1))^2}\\ &= \frac{(q^2+1)}{q^2(q-1)}\\ &= \frac{1+\frac{1}{q^2}}{q-1}\\ &< 1.\end{aligned}$$

因此，

$$\Big(\frac{|H|}{|H_1|}\Big)^2 < |H|.$$

（9） $H = {}^2G_2(q)$; 其中，$q = 3^{2t+1}$ 和 $t \geqslant 1$（方法 1）

群 ${}^2G_2(q)$ 的阶为（参见 [4], 第 252 页），

$$|{}^2G_2(q)| = q^3(q^3+1)(q-1).$$

因此，$^2G_2(q)$ 有一个阶为 q^3 的 Sylow 3-子群 $|H_2|^2 < |H|$。此外，$^2G_2(q)$ 有一个阶为 $q^3(q-1)$ 的 Borel 子群 H_1（参见[29], 第 137 页）。

考虑，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^3(q-1)}{q^6}\\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

Now,

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^3(q^3+1)(q-1)}{(q^3(q-1))^2}\\ &= \frac{(q^3+1)}{q^3(q-1)}\\ &= \frac{1+\frac{1}{q^3}}{q-1}\\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H|}{|H_1|}\right)^2 < |H|.$$

(10) $H = {}^2F_4(q)$、$q = 2^{2t+1}$ 和 $t \geqslant 1$（方法 1）

群 $^2F_4(q)$ 的阶为 $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$（参见 [4],第 252 页）。因此，它有一个阶为 q^{12} 的 Sylow 2-子群，并且 $|H_2|^2 < |H|$。此外，$^2F_4(q)$ 有一个阶为 $q^{12}(q-1)^2$ 的 Borel 子群 H_1（参见 [29], 第 165 页）。

考虑，

$$\begin{aligned}\frac{|H_1|}{|H_2|^2} &= \frac{q^{12}(q-1)^2}{q^{24}}\\ &< 1.\end{aligned}$$

因此，

$$\left(\frac{|H_1|}{|H_2|}\right)^2 < |H_1| < |H|.$$

$$\begin{aligned}\frac{|H|}{|H_1|^2} &= \frac{q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)}{(q^{12}(q-1)^2)^2}\\ &= \frac{(q^6+1)(q^4-1)(q^3+1)(q-1)}{q^{12}(q-1)^4}\end{aligned}$$

$$
\begin{aligned}
&= \frac{(q^6+1)(q^4-1)(q^3+1)}{q^{12}(q-1)^3} \\
&< \frac{q^4(1+\frac{1}{q^6})(1+\frac{1}{q^3})}{q^3(q-1)^3} \\
&= \frac{q(1+\frac{1}{q^6})(1+\frac{1}{q^3})}{(q-1)^3} \\
&< 1.
\end{aligned}
$$

这意味着，

$$\Big(\frac{|H)|}{|H_1|}\Big)^2 < |H|.$$

(11) $H = {}^2F_4(2)'$; (方法 2)

单群 $H = {}^2F_4(2)'$; 的阶为17971200。已知 H 有一个阶为11232的极大子群。我们令 H_1 为这个极大子群，并令 H_2 为 H_1 的 Sylow 2-子群，其阶为32。因此，我们得到$b_1 = b_2 = 1$。

6.4 表

本节将介绍散在单群（表2）的详细信息，以及定理 7 的情形 (ii)–(iv) 中所定义的所有单群的阶，这些内容列于表3和表4中。这些表还包含子群 H_2 和 H_1 的阶。表2展示了有关散在单群的子群 H_2 和 H_1 的信息。

H	H 的阶	阶 H_2	H 的阶 $_1$	b_1	b_2
M_{11}	7920	2^4	720	1	1
M_{12}	95040	2^2	660	1	1
M_{22}	443520	2^6	20160	1	1
M_{23}	10200960	2^7	443520	1	1
M_{24}	244823040	2^8	887040	1	1
Co_1	4157776806543360000	262144	42305400000000	1	1
Co_2	42305400000000	262144	908328960	1	1
Co_3	495767000000	2^7	10200960	1	1
McL	898128000	3^6	$3^6 \cdot 2^7 \cdot 7 \cdot 5$	1	1
HS	44352000	2^7	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	1	1
Suz	448345497600	2^{12}	251596800	1	1
J_2	604800	2^5	6048	1	1
Fi_{22}	64561751654400	2^{16}	$2^{16}(2^6-1)(2^5+1)(2^4-1)(2^3+1)$	1	1
Fi_{23}	4089470473293004800	2^{18}	$2^{18} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1	1
Fi'_{24}	1255205709190661721292800	2^{19}	$2^{19} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	1	1
$\mathbb{M}$	t_1	2^{42}	t_2	1	1
$\mathbb{B}$	t_3	2^{38}	t_4	1	1
Th	90745943887872000	2^{15}	319979520	1	1
HN	273030912000000	2^9	239500800	1	1
He	4030387200	2^8	$2^8 \cdot 255 \cdot 15$	1	1
J_1	175560	2^2	660	1	1
J_3	50232960	2^5	8160	1	1
J_4	86775571046077562880	2097152	57161637225	1	1
O'N	460815505920	2^6	3753792	1	1
Ly	51765179004000000	15625	5859000000	1	5
Ru	145926144000	2^{12}	35942400	1	1

表2。表示常数因子及用于选择合适子群的方法的表

在表2中，我们考虑 t_i、$i = 1$、2、3、4 的取值如下。

$t_1 = 808017424794512875886459904961710757005754368000000000$

$t_2 = 2^{42} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$

$t_3 = 4154781481226426191177580544000000$

$t_4 = 2^{38} \cdot (2^{12}-1) \cdot (2^9+1) \cdot (2^8-1) \cdot (2^6-1) \cdot (2^5+1) \cdot (2^2-1)$。在表3中，$c_{mi}$、$i = 1$、2、3、4、5 的取值如下。$c_{m1} = \frac{q^{\frac{m(m+1)}{2}}}{(q+1,m+1)}(q-1)^{\lfloor m/2 \rfloor}(q+1)^{\lceil \frac{m-1}{2} \rceil}$、

$c_{m2} = \frac{3}{(3,m+1)} \frac{2^{\frac{m(m+1)}{2}} \prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})}{(2^{m+1}-(-1)^{m+1})(2^m-(-1)^m)}$

$c_{m3} = \frac{3}{(3,m+1)} 2^{\frac{m(m-1)}{2}} \prod_{i=1}^{m-1}(2^{i+1}-(-1)^{i+1})$、

$c_{m4} = 2^{m^2-m+1}(2^m+1)\prod_{i=1}^{m-1}(2^{2i}-1)$

$c_{m5} = 2^{m(m-1)}(2^{m-1}+1)\prod_{i=1}^{m-2}(2^{2i}-1).$

H	$\lvert H\rvert$	$\lvert H_2\rvert$	$\lvert H_1\rvert$
$A_m(q)$; $q>2$	$\frac{q^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(q^{i+1}-1)}{(q-1,m+1)}$	$q^{\frac{m(m+1)}{2}}$	$\frac{q^{\frac{m(m+1)}{2}}}{(q-1,m+1)}(q-1)^m$
$A_m(2)$; $q=2$	$2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1)$	$2^{\frac{m(m+1)}{2}}$	$\frac{2^{\frac{m(m+1)}{2}}\prod_{i=1}^{m}(2^{i+1}-1)}{(2^{m+1}-1)}$
${}^2A_m(q^2)$; $q>2$, $m>1$	$\frac{q^{\frac{m(m+1)}{2}}}{(q+1,m+1)}\prod_{i=1}^{m}(q^{i+1}-(-1)^{i+1})$	$q^{\frac{m(m+1)}{2}}$	c_{m1}
${}^2A_m(2^2)$; $q=2$, $m>1$, $6\nmid(m-1)$	$\frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)}\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})$	$2^{\frac{m(m+1)}{2}}$	c_{m2}
${}^2A_m(2^2)$; $q=2$, $m>1$, $6\mid(m-1)$	$\frac{2^{\frac{m(m+1)}{2}}}{(3,m+1)}\prod_{i=1}^{m}(2^{i+1}-(-1)^{i+1})$	$2^{\frac{m(m-1)}{2}}$	c_{m3}
$C_m(q)$; $q>2$, $m>2$	$\frac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{(2,q-1)}$	q^{m^2}	$\frac{q^{m^2}}{(2,q-1)}(q-1)^m$
$C_m(2)$; $q=2$, $m>2$	$2^{m^2}\prod_{i=1}^{m}(2^{2i}-1)$	2^{m^2-m+1}	c_{m4}
$B_m(q)$; q奇数, $m>1$	$\frac{q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)}{(2,q-1)}$	q^{m^2}	$\frac{q^{m^2}}{(2,q-1)}(q-1)^m$
$D_m(q)$; $q>2$, $m>3$	$\frac{q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)}{(4,q^m-1)}$	$q^{m(m-1)}$	$\frac{q^{m(m-1)}}{(4,q^m-1)}(q-1)^m$
$D_m(2)$; $q=2$, $m>3$	$2^{m(m-1)}(2^m-1)\prod_{i=1}^{m-1}(2^{2i}-1)$	2^{m^2-2m+1}	$2^{m^2-2m+1}\prod_{i=1}^{m-1}(2^{2i}-1)$
${}^2D_m(q^2)$; $q>2$, $m>3$	$\frac{q^{m(m-1)}(q^m+1)}{(4,q^m+1)}\prod_{i=1}^{m-1}(q^{2i}-1)$	$q^{m(m-1)}$	$\frac{q^{m(m-1)}}{(4,q^n+1)}(q-1)^m$
${}^2D_m(2^2)$; $q=2$, $m>3$	$\frac{2^{m(m-1)}(2^m+1)}{(4,2^m+1)}\prod_{i=1}^{m-1}(2^{2i}-1)$	$2^{m(m-1)}$	c_{m5}

表3. 单群的阶（定理 7 的情形 (iii)）及其子群的阶H_2, H_1。

$G_2(q)$	$q^6(q^6-1)(q^2-1)$	q^6	$q^6(q-1)^2$
$F_4(q)$	$q^{24}\prod_{i\in\{2,6,8,12\}}(q^i-1)$	q^{24}	$q^{24}\prod_{i\in\{1,2,4,6\}}(q^i-1)$
$E_6(q)$, $q>2$	$\frac{q^{36}}{(3,q-1)}\prod_{i\in\{2,5,6,8,9,12\}}(q^i-1)$	q^{36}	$q^{36}(q-1)^6$
$E_6(2)$	$2^{36}\prod_{i\in\{2,5,6,8,9,12\}}(2^i-1)$	2^{36}	$2^{36}\cdot 3^3\cdot 5\cdot 7\cdot 31$
${}^2E_6(q)$	$\frac{q^{36}(q^9+1)}{(3,q+1)}\prod_{i\in\{2,5,6,8,12\}}(q^i-1)$	q^{36}	$q^{36}(q-1)^4(q+1)^2$
${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	q^{12}	$q^{12}\ (q^3-1)(q-1)$
$E_7(q)$, $q>2$	$\frac{q^{63}}{(2,q-1)}\prod_{i\in\{2,6,8,10,12,14,18\}}(q^i-1)$	q^{63}	$q^{63}(q-1)^7$
$E_7(2)$	$2^{63}\prod_{i\in\{2,6,8,10,12,14,18\}}(2^i-1)$	2^{63}	$2^{63}\cdot 3^4\cdot 7^2\cdot 5$
$E_8(q)$, $q>2$	$q^{120}\prod_{i\in\{2,8,12,14,18,20,24,30\}}(q^i-1)$	q^{120}	$q^{120}(q-1)^8$
$E_8(2)$	$2^{120}\prod_{i\in\{2,8,12,14,18,20,24,30\}}(2^i-1)$	2^{119}	$2^{119}\cdot 3^4\cdot 5\cdot 7^2\cdot 31$
${}^2B_2(q)$; $q=2^{2t+1}$, $t\geqslant 1$	$q^2(q^2+1)(q-1)$	q^2	$q^2(q-1)$
${}^2G_2(q)$; $q=3^{2t+1}$, $t\geqslant 1$	$q^3(q^3+1)(q-1)$	q^3	$q^3(q-1)$
${}^2F_4(q)$; $q=2^{2t+1}$, $t\geqslant 1$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	q^{12}	$q^{12}(q-1)^2$

表4. 单群的阶（定理 7 的情形 (iv)）及其子群的阶H_2, H_1。