拟本原几乎难以捉摸群

EMILY V. HALL

arXiv:2301.05569v1 [math.GR] 13 Jan 2023

Abstract. 设 G 是有限集 Ω 上的非平凡传递置换群，并回忆一下，若 G 的某个元素没有不动点，则称它为错排。根据若尔当的一条经典定理，错排总是存在的；但有些所谓的隐晦群不含任何素数阶错排。在近期的一篇论文中，Burness 与作者提出了几乎难以捉摸群这一类群，它们恰含一个素数阶错排共轭类。本文完成了拟本原几乎难以捉摸群的分类。

1. 引言

设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个传递置换群，其中 $|\Omega| \geqslant 2$，点稳定子为 H。若尔当在1872年提出的一条经典定理 [27] 是轨道计数引理的一个简单推论，它表明 G 总是含有在 Ω 上无不动点作用的元素。我们称这类元素为错排。近年来，错排受到广泛研究，并自然地出现在若干不同的研究背景中。例如，Serre [42]探讨了若尔当定理在许多不同数学领域中的一些有趣应用。

这一领域研究的一个重要重点，是探讨具有特定性质的错排是否存在。例如，Fein、Kantor 和 Schacher [20] 于1981年给出的 Jordan 定理扩展表明，G 总是包含一个素数幂阶的错排。[20] 中的证明需要用到有限单群分类，这与 Jordan 定理的初等证明形成了鲜明对比。有趣的是，尽管我们可以确定素数幂阶的错排必然存在，但这并不总意味着我们能找到素数阶的错排。例如，散在群 M_{11}在12个点上的本原作用（即它在极大子群 $\mathrm{PSL}_2(11)$ 的右陪集上的作用）不包含素数阶的错排（但确实包含阶为4和8的错排）。沿用 [11], 的说法，若一个传递群不包含素数阶错排，就称它为隐晦群。尽管目前还无法完整分类隐晦群，但 Giudici [22]对其中一大类例子进行了分类。他的主要定理指出，若 G 是一个具有传递极小正规子群的隐晦群，那么 $G = \mathrm{M}_{11} \wr K$ 在 Δ^k上的积作用，其中 $|\Delta| = 12$，k 是一个正整数，且 $K \leqslant S_k$ 是传递的。

注意，G 中的错排集合是一个正规子集，因此它是若干共轭类的并集。因此，考察错排共轭类的数量是很自然的。Burness 和 Tong-Viet 在 [8] 中证明，本原置换群 G 的点稳定子 H 满足该群恰有一个错排共轭类，当且仅当它是锐 2-传递的，或为 $(G, H) = (A_5, D_{10})$ 或 $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$。此后，Guralnick 在 [24], 中推广了这一结果，证明一个传递群若恰有一个错排共轭类，则它必为本原群。

受 Burness、Tong-Viet 和 Guralnick 工作的启发，文献 [7] 中引入了无逃逸性的一个自然扩展。若一个传递置换群恰好有一个素数阶错排共轭类，我们就称它为几乎难以捉摸的。例如，若 n 是素数幂，则对称群 S_n 在其对 n 个点的自然作用下是几乎难以捉摸的。若 G 是有限群，且 H 是无核子群，那么

称 (G, H) 几乎难以捉摸会比较方便，若 G 在 H 的陪集上的自然传递作用是几乎难以捉摸的。

回顾一下，若一个置换群的每个非平凡正规子群都具有传递性，则称该群为拟本原群。例如，若 G 是一个以 G_0 为底群、以H 为点稳定子的几乎单群，那么当且仅当 $G = G_0H$时， G 是拟本原群。注意，每个本原群都是拟本原群。在 [7, 中，借助 Praeger [41], 提出的拟本原群 O'Nan-Scott 定理的一个版本，定理 1], 证明了每个拟本原几乎难以捉摸群要么是几乎单群，要么是二重传递仿射群。此外，在 [7] 中，研究了底群为交错群、散在群或李型一秩群的本原几乎单群；其余经典群则在 [25]中得到了处理。因此，要完成对本原几乎难以捉摸群的分类，还需考察李型例外群和 2-传递仿射群。

我们的第一个主要结果是定理 1。在定理陈述中，鉴于同构关系 $G_2(2)' \cong \mathrm{U}_3(3)$ 和 ${}^2G_2(3)' \cong \mathrm{L}_2(8)$，我们排除了底群为 $G_2(2)'$ 和 ${}^2G_2(3)'$ 的群。关于定理 1 中出现的情形，读者可参阅第 6 节的表 A2 和注 6.2。

定理 1. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个几乎单本原置换群，其点稳定子为 H ，底群为 G_0，且 G_0 是李型例外群。那么，当且仅当 (G, H) 属于以下情形之一时， G 几乎难以捉摸

$$(G_2(4).2, \mathrm{J}_2{:}2),\ ({}^2F_4(2)', \mathrm{L}_2(25)),\ ({}^2F_4(2), \mathrm{L}_2(25).2_3)\ \ or\ ({}^2F_4(2), 5^2{:}4S_4).$$

接下来，设 $G = V{:}H \leqslant \mathrm{AGL}(V)$ 是一个底群为 $V = (\mathbb{F}_p)^d$、点稳定子为 $H \leqslant \mathrm{GL}_d(p)$ 的二重传递仿射群，其中 p 是素数，且 $d \geqslant 1$。这里， G 的 2-传递性蕴含 H 在 V 的非零向量上传递作用。这些群由 Hering [26] 分类，这也是我们证明定理 2 的关键要素。定理 2 的 (iii) 部分中，我们用 $\mathcal{P}(n, i)$ 表示 Magma [2] 的本原群数据库中次数为 n 的 i^{th} 本原群。例如， $\mathcal{P}(2^4, 17) = 2^4{:}\mathrm{Sp}_4(2)'$。此外，我们用 $\Gamma\mathrm{L}_m(q)$ 表示 $\mathbb{F}_q$ 上维数为 m 的一般半线性群，其中 q 是一个 p 次幂。

定理 2. 设 $G = V{:}H$ 是一个二重传递仿射群，满足 $|V| = n = p^d$，其中 p为素数，且 $d \geqslant 1$。那么， G 几乎难以捉摸，当且仅当以下条件之一成立
(i) $H \leqslant \Gamma\mathrm{L}_1(p^d)$. (ii) $\mathrm{SL}_2(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_2(q)$，其中 $p = 2$， d 为偶数，且 $q = 2^{d/2}$。(iii) $G = \mathcal{P}(n, i)$，其中 (n, i) 包含于表1中。

n	i	n	i
2^4	17, 19	11^2	36, 38, 42, 43, 44
3^4	44, 68, 69, 70, 90, 99	19^2	73, 80
3^6	145, 198, 239, 240, 366	23^2	49, 51
5^2	12, 14, 17, 19	29^2	97, 103, 104
7^2	22, 23, 29	59^2	79, 84

表1：几乎难以捉摸的仿射群 $G = \mathcal{P}(n, i)$

结合定理1和定理2以及 [7, 25], 中的主要结果，我们现在完成对几乎难以捉摸的本原群的分类（表A1和表A2见第 6 节）。

定理 3. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个有限本原置换群，其点稳定子为 H。那么， G 几乎难以捉摸，当且仅当以下条件之一成立：(i) G 是几乎单群，且 (G, H) 属于表 A1 或 A2；或 (ii) $G = V{:}H$ 是定理 2 中所述的二重传递仿射群。

现在，我们将定理 3 中的分类从本原群扩展到拟本原群。为此，我们需要确定这些对 (G, H)：其中 G 是一个底群为 G_0 的几乎单群，H 是 G 的一个核自由非极大子群，满足 $G = G_0H$，并且 G 关于 G 在 H 的陪集上的自然作用几乎难以捉摸。相关表格请参阅第 6 节。

定理 4. 设 G 是一个底群为 G_0 的几乎单群，并且 H 是 G 的无核非极大子群，满足 $G = G_0H$。则 (G, H) 几乎难以捉摸，当且仅当以下情形之一成立：

(i) $G_0 = \mathrm{U}_n(q)$，且 H 稳定自然模的一个一维非退化子空间，其中 q 为偶数，且 $n \geqslant 5$ 是 $q + 1$ 的一个素因子。(ii) $G_0 = \mathrm{L}_2(p)$，其中 $p \geqslant 5$ 为素数，且 (G, H) 见表 B1。(iii) (G, H) 见表 B2。

注 1. 这里我们对定理 4 作一些说明。

(a) 假设 (G, H) 属于定理 4 的情形 (i)，并记 $H < M$，其中 M 是自然模的一个一维非退化子空间的稳定子。则 (G, M) 属于表 A1 的情形 U1，其中关于 n 和 q 的相关条件见注 6.2(b)。正如我们在第 5 节 5.2 中讨论的，我们预计此情形不会出现真正的几乎难以捉摸的例子（即不满足所有数论约束的例子），这将使我们能够删去定理 4 中的情形 (i)。关于此情形下的拟本原群，更多信息请参见注 4.9。(b) 对于 (ii)，若 (G, H) 是表 B1 所列的情形，则对于任意同构于 H 的 G 的子群 K，(G, K) 都几乎难以捉摸。更多详情见注 4.11 和注 4.15。(c) 设 (G, H) 是表 B2 所列的任意情形。则 G 有一个子群 K，满足 $H \cong K$，使得 (G, K) 几乎难以捉摸。表中记录了满足 $G = G_0H$ 且同构于 H 的子群的 G-共轭类总数，以及其中产生几乎难以捉摸例子的 G-共轭类数量。关于表 B2 的更多信息，请参见注 6.3。

设 $G \leqslant \mathrm{Sym}(\Omega)$ 为一个拟本原置换群，其点稳定子为 H。假设 G 是一个底群为 G_0 的几乎单群，其中 G_0 为交错群或散在群，并且 G 并非难以捉摸（即 $(G, n) \neq (\mathrm{M}_{11}, 12)$）。令 r 表示$|\Omega|$的最大素因子。在 [5, 推论 1 中，2], Burness、Giudici 和 Wilson 证明了：若 G 是本原的，则 G 包含一个阶为 r 的错排。通过考察定理 3 和 4 中出现的各种情形，我们可以建立以下扩展。与定理 4 一样，$G_0 = \mathrm{U}_n(q)$ 且 H 稳定自然模的一个一维非退化子空间的情形，在推论 5 中作为特殊情形出现。证明见第 5 节。

推论 5. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 为一个拟本原几乎难以捉摸的置换群，其底群为 G_0，点稳定子为 H。假设 G 具有素数阶为 s 的错排。那么，要么 s 是 $|\Omega|$ 的最大素因子，要么下列情形之一成立

(i) G 是本原的，$(s, r) = (2, 3)$，且$(G, H) = ({}^2F_4(2)', \mathrm{L}_2(25))$或$({}^2F_4(2), \mathrm{L}_2(25).2_3)$。(ii) G是非本原的，且以下情形之一成立：(a) $G_0 = \mathrm{U}_n(q)$，并且 H 恰当地包含于自然模的某个一维非退化子空间的稳定子中，其中 q 是偶数，$n \geqslant 5$ 是 $q + 1$的一个素因子。(b) $s = 2$，且(G, H)与表 B1 中情形 II 或 III 相同。(c) $s = 3$，且$(G, H) = (\mathrm{L}_2(p)\ C_p{:}C_d)$与表 B1 中情形 IV 相同，使得$(p-1)\ d$ 可被一个奇素数整除。

设 G 是一个以 G_0 为底群的几乎单群，并设 H 是 G 的无核子群，使得 $G = G_0H$ 且 (G, H) 几乎难以捉摸。我们将 H 的深度记作

$d_G(H)$，定义为子群链的最长可能长度

$$G > L_1 > \cdots > L_{\ell-1} > L_\ell = H, \tag{1}$$

使得对于所有 $1 \leqslant i \leqslant \ell$，$(G, L_i)$ 都是几乎难以捉摸的。这里我们将 ℓ 称为 (1) 中链的长度。我们将 G 的几乎难以捉摸深度定义为

$$D_G = \max d_G(H)$$

其中，我们在 G 的所有满足 $G = G_0H$ 且 (G, H) 几乎难以捉摸的核自由子群 H 中取最大值。在下面的推论中，我们分别用 $\omega(n)$ 和 $\pi(n)$ 表示正整数n的素因子总数和不同素因子个数。证明见第 5 节；关于出现的群，更多信息请参阅注 6.3。

推论6. 设 G 是底群为 G_0 的几乎单群，并令 $k = |G : G_0|$。若$D_G \geqslant 2$，则以下结论之一成立：

(i) $G_0 = \mathrm{U}_n(q)$，其中 q 为偶数，且 $n \geqslant 5$ 是 $q+1$的一个素因子。(ii) $D_G = \omega(k(p-1)/2) - \pi(k(p-1)/2) + 1$ 且 $G_0 = \mathrm{L}_2(p)$，其中 $p = 2^m - 1$ 是素数。(iii) $D_G = \omega((p-1)/2) - \pi((p-1)/2) + 1$ 且 $G = \mathrm{L}_2(p)$，其中 $p = 2.3^a - 1$ 是满足 $a \geqslant 2$的素数。(iv) $D_G = \omega(p+1) - \pi(p+1) + 1$ 且 $G = \mathrm{PGL}_2(p)$，其中 $p = 2^m + 1$ 是素数。(v) $D_G = 2$ 且 $G =$ 为 M10、A_9、S_9、$\mathrm{L}_2(8).3$、$\mathrm{U}_5(2).2$ 或 $\mathrm{PSp}_6(2)$。(vi) $D_G = 3$ 且 $G =$ 为 $\mathrm{L}_2(49).2_3$。(vii) $D_G = 4$ 且 $G =$ 为 $\mathrm{U}_4(2)$、$\mathrm{U}_4(2).2$ 或 $\mathrm{U}_3(3).2$。

注2. 此处我们对推论6作一些说明。

(a) 若要使一个群在情形(i)中出现，且满足 $D_G \geqslant 1$，则 G 必须如表 A1中的情形 U1所示。也就是说，$G = G_0.[2f]$，其中 $q = 2^f$，并且满足所有相关的数论条件。如上所述，我们预计不会有任何群在此情形中出现（例如参见注 6.2(b)）。不过，我们注意到，如果$G = G_0.C_{2f}$是情形U1中的一个真实例子，那么 $D_G \geqslant \omega(2f) - 1$。(b) 我们不知道 D_G 能否任意大，这似乎取决于数论中一些极其困难的未决问题。但我们已通过计算验证，如果 $G_0 = \mathrm{L}_2(p)$，且 $p < 2^{1020}$ 是所需形式的素数，那么 $D_G \leqslant 10$。

作为引言的结束，我们简要介绍本文的结构。在第 2 节中，我们通过证明定理 1 完成对几乎难以捉摸的几乎单群本原群的分类。其中，G 是一个底群为 G_0 的几乎单群李型例外群，而 H 是 G 的无核极大子群。我们首先给出若干具有数论性质的初步结果，并简要讨论例外群的子群结构。我们还给出定理 2.12，该定理对满足 $\pi(G_0) - \pi(H_0) \leqslant 1$ 的对 (G_0, H) 进行了分类，其中 $H_0 = H \cap G_0$ 和 $\pi(X)$ 表示 $|X|$ 的不同素因子个数。这是 [34, 推论 5], 的一个扩展，也是[25, 定理 2], 的类比，后者针对经典群进行了陈述。由于当且仅当$\pi(G_0) - \pi(H_0) \leqslant 1$ 时，G才是几乎难以捉摸的，因此这一关键结果大幅减少了我们在定理 1 的证明中需要考虑的情形数量。

接下来，在第 3 节中，我们证明关于 2-传递仿射群的定理 2，从而完成对本原几乎难以捉摸群的分类。在此，我们应用 Hering 定理 [26], ，该定理将 2-传递仿射群划分为若干无限族以及少数散在情形。对于出现的散在情形，我们在 Magma[2] 中采用计算方法；而无限族则逐一处理。

在第 4 节中，我们将本原分类推广到所有拟本原群。我们很容易将问题归结为这样的情形：G 是底群为 G_0 的几乎单群，且点稳定子H包含于一个无核极大子群 M中，使得(G, M)几乎难以捉摸。

这使我们能够利用定理 3 考察由此产生的各种可能性。对于表 A2 中的群对(G, M)，我们可以在 Magma中使用计算方法。对于表 A1 中的无限族，我们可以采用与本原群类似的技术。例如，我们可以将问题归结为满足 $\pi(M \cap G_0) = \pi(H \cap G_0)$的情形（见引理 4.4）。最后，我们在第 5 节中给出推论 5 和 6 的证明，并在第 6 节中列出定理 3 和 4 的陈述中提及的相关表格。

记号。我们采用相当标准的群论记号。设 A 和 B 是群，n是正整数。我们用 C_n 或 n 表示阶为 n 的循环群，用 $[n]$ 表示阶为 n的某个未指明的可解群。此外，我们用 D_n 表示阶为 n的二面体群。A 被 B 扩张的某个未指明扩张记作 $A.B$；若该扩张分裂，有时记作 $A{:}B$ 。对于单群，我们采用 Kleidman 和 Liebeck 的记号 [30]。例如，

$$\mathrm{PSL}_n(q) = \mathrm{L}_n(q) = \mathrm{L}_n^+(q), \ \ \mathrm{PSU}_n(q) = \mathrm{U}_n(q) = \mathrm{L}_n^-(q)$$

此外，设 G 是有限群，H 是无核子群。对于置换群的一种性质 X ，如果 G 在 G 对 H的陪集的自然作用下具有性质 X，我们就称 (G, H) 具有性质 X 。例如，如果 G 在 G对 H的陪集的自然作用下几乎难以捉摸，我们就称 (G, H) 几乎难以捉摸。我们用 $\pi(A)$ 和 $\pi(n)$ 分别表示 $|A|$ 和 n的不同素因子的个数，用 $\alpha(A)$ 和 $\alpha(n)$ 分别表示 $|A|$ 和 n的不同素因子集合。对于正整数 a 和 b ，我们用 (a, b) 表示 a 和 b的最大公因数。

致谢。我谨向我的博士生导师 Tim Burness 教授致谢，感谢他的指导和宝贵意见。我还要感谢英国工程与自然科学研究委员会以及海尔布隆数学研究所提供的经费支持。

2. Exceptional Groups

本节中我们证明定理 1。在本节中，令 G 表示一个底群为 G_0的几乎单置换群，其中 G_0是定义在 $\mathbb{F}_q$上的李型例外群，并令H 表示 G中的一个点稳定子。此外，本节中我们记 $q = p^f$，其中 p 为素数，且 $f \geqslant 1$。我们注意到，具有

$$G_0 \in \{{}^2F_4(2)', G_2(2)', {}^2G_2(3)'\} \tag{2}$$

的群非常适合采用简单的计算方法来证明定理 1。具体而言，对于定理 1，底群属于 (2) 中的群 G 已在[7, 命题 4.4、4.12 和 5.1] 中处理；此处的几乎难以捉摸情形见表 A2。注意，底群为 $G_2(2)' \cong \mathrm{U}_3(3)$ 或 ${}^2G_2(3)' \cong \mathrm{L}_2(8)$ 的群，在表 A2 中分别记为 $\mathrm{U}_3(3)$ 或 $\mathrm{L}_2(8)$，以避免因同构而重复。因此，在本节余下部分中，我们假设 G_0 不是 (2) 中的群之一。

2.1. 预备结果。

本节将给出一些在证明定理 1 时有用的预备结果。我们将讨论例外群的子群结构，以及某些素数阶元素的共轭类。不过，我们将先讨论文献中关于本原素因子的一些有用数论结果。设 n 为正整数。若 $q^n - 1$ 的一个素因子对于所有 $1 \leqslant i < n$ 都不整除 $q^i - 1$ ，则称其为本原素因子。我们定义

$$P_q^n = \{r \mid r \text{ is a primitive prime divisor of } q^n - 1\}$$

并注意到 $P_p^{nf} \subseteq P_q^n$。以下结果是 Zsigmondy [49] 在19世纪90年代提出的一个著名定理，涉及本原素因子的存在性。

定理 2.1. 集合 P_q^n非空，除非 $(n, q) = (1, 2)$、$(6, 2)$，或者 $n = 2$ 和$q = p$ 是梅森素数。

引理 2.2. 假设 $r \in P_q^n$ 是奇素数，且令 m 为正整数。那么 r整除 $q^m - 1$ 当且仅当 n 整除 m。此外，对于某个 $d \geqslant 1$， $r = nd + 1$ 。
证明。第一部分的证明例如可见于 [4, 引理 A.1] ，而第二部分则是费马小定理的一个简单推论。
□

在本文中，我们经常会关注这样的情形：对于 n 的某些取值， $|P_q^n| = 1$ 且 $q = p^f$。然而，一般来说，很难给出关于n、 p 和 f 的精确条件，使得 $|P_q^n| = 1$。这部分是由于在尝试解决该问题时出现的丢番图方程十分复杂。例如，假设 $P_q^n = \{r\}$，并且 n 是一个不整除 $q - 1$的奇素数。那么（q， n， r）必然是下列方程的一个解

$$\frac{q^n - 1}{q - 1} = r^l$$

目前，该丢番图方程的所有可能整数解尚不为人所知。然而，下述结果对 n 可被 3 整除时的可能解提供了一些限制；在大多数情形下，这已足以满足我们的需要。

命题 2.3. 设 x、 y 和 b 为整数，满足 $|x|$、 $|y| > 1$ 和 $b \geqslant 2$。假设 (x, y, b) 是下列方程的一个解：

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1 = y^b.$$

那么 $(x, y, b) = (18, 7, 3)$ 或 $(-19, 7, 3)$。

证明. 这是 [1, 命题 1] 的一个特例。 □

虽然我们无法给出关于 n、 p 和 f 的精确条件以使得 $|P_q^n| = 1$，但 [25,引理 2.4] 给出了关于 f 的必要条件。例如，若 $n \geqslant 7$，则 $|P_q^n| = 1$ 当且仅当 $\alpha(f) \subseteq \alpha(n)$，其中 $\alpha(x)$ 表示正整数 x 的素因子集合。此外，若假设 $P_q^n = \{dn + 1\}$，那么对于 n 的某些取值，我们可以给出关于正整数 d 的条件，例如参见 [25, 引理 2.5、2.9、2.11 和 2.12] 。特别地，[25, 引理 2.9] 讨论了在某个 $a \geqslant 0$ 下，情形 $n = 2^a 3$ 时 d 的可能取值。这里我们将这一结果推广到 $n = 3$ 和 6。

引理 2.4. 假设 $n \in \{3, 6\}$ 和 $P_q^n = \{r\}$。那么，要么 $r \geqslant 8nf + 1$，要么 $r = dnf + 1$，且下列情况之一成立：

(i) $d = 1$ 和 $(n, q) = (3,4)$、$(6,3)$、$(6, 4)$、$(6, 5)$、$(6, 8)$ 或 $(6, 19)$。(ii) $d = 2$ 和 $(n, q) = (3,2)$ 或 $(6, 23)$。(iii) $d = 4$ 和 $(n, q) = (3,3)$。(iv) $d = 6$ 和 $(n, q) = (3,7)$、$(6,9)$ 或 $(6, 11)$。
(v) $d = 7$ 和 $(n, q) = (6,7)$。

在开始讨论例外群及其子群结构之前，我们先陈述以下初等观察，这是 [9, 引理 2.2] 的一个应用。为完整起见，我们给出详细证明。注意，当且仅当 $x^G \cap H = \emptyset$ 时， $x \in G$ 是一个错排，其中 x^G 表示 x 的共轭类。

引理 2.5. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个底群为 G_0、点稳定子为 H 的几乎单拟本原置换群。定义 $H_0 = H \cap G_0$。设 r 是 $|\Omega|$的一个素因子，并分别以 a_r 和 b_r 表示阶为 r的元素的 G_0-类和 H_0-类的数量。假设 $a_r > b_r$。那么 G中存在一个阶为 r 的错排。

证明。由于我们假设了 $a_r > b_r$，存在一个阶为 r 的元素 $y \in G_0$ ，使得$y^{G_0} \cap H_0 = \emptyset$。反设在 G中不存在阶为 r 的错排。于是特别有 $y^G \cap H \neq \emptyset$，例如对某个 $g \in G$，有 $y^g \in H$。注意到 $G = G_0 H$，因为 G 是拟本原的，所以我们可以写成 $g = uh$ ，其中 $u \in G_0$ 且 $h \in H$。因此$(y^u)^h \in H$，这意味着 $y^u \in H^{h^{-1}} = H$。然而 $y^u \in G_0$，这与 $y^{G_0} \cap H_0 = \emptyset$ 这一事实矛盾。因此， y 是在 G中阶为 r 的一个错排。□

许多李型例外群的极大子群结构及其共轭分类已有详尽记载。对于底群为$G_2(q)$的群，Kleidman [29] 确定了q 为奇数时的极大子群的共轭类，而 Cooperstein [13] 确定了 q 为偶数时的极大子群的共轭类（另见 [3, 表 8.30、8.41 和 8.42]）。底群为 ${}^2F_4(q)$和 ${}^3D_4(q)$的群的极大子群，分别由 [39] 和[28] 确定。最后，关于底群为 ${}^2G_2(q)$和 ${}^2B_2(q)$的群的极大子群，可参见 [3, 表 8.43 和 8.16], ；这些内容分别转载自 [29] 和[45] 。此外，底群为$F_4(q)$、 $E_6(q)$和 ${}^2E_6(q)$的群的极大子群，最近已由 Craven 在 [17]中完成共轭分类。对于其余的例外群，即 $G_0 \in \{E_7(q)\ E_8(q)\}$的那些群，我们给出以下定理。在本定理及本节余下部分中，我们记 $\bar{G} = (G_\sigma)'$，其中 G 是定义在 $\mathbb{F}_p$ 上的伴随型单李代数群，而 σ 是 G的一个适当的 Steinberg 自同态。此外，我们指出，该定理稍作调整后，对情形 $G_0 \in \{G_2(q)\ F_4(q)\ {}^2E_6(q)\ E_6(q)\}$同样成立。这是 [36, 定理 8]的一个版本。

定理 2.6. 设 G 是一个底群为 $G_0 = (G_\sigma)' \in \{E_7(q)\ E_8(q)\}$ 的几乎单群。设 H 是 G 的一个核自由极大子群，并令 $H_0 = H \cap G_0$。则以下情况之一成立：

(I) H 是一个极大抛物子群；

(II) $\bar{H} = N_{\bar{G}}(H_\sigma)$，且 H 是 G的一个 σ-稳定非抛物极大秩子群： H 的可能性见 [35, 表 5.1 和表 5.2]。

(III) $\bar{H} = N_{\bar{G}}(H_\sigma)$，其中 H 是 G的一个极大闭 σ-稳定正维子群（既非抛物子群，也非极大秩子群）。(IV) H 与 G 在 $\mathbb{F}_q$的某个子域上同型。(V) H 是一个奇异局部子群（见 [12]）。(VI) $G_0 = E_8(q)$， $p \geqslant 7$ 和 $H_0 = (A_5 \times A_6).2^2$。(VII) H 是几乎单群，且不属于 (III) 或 (IV) 型。

$G_0 = E_7(q)$ 和$E_8(q)$ 的极大抛物子群（(I) 型）的共轭类，与对应 Dynkin 图的节点一一对应。本文关注这些子群阶的素因子。要确定极大抛物子群 P 的素因子，使用 Levi 分解 $P = QL$ 会很方便，其中 Q 是 P 的幺幂根基， L 是一个 Levi 子群。从这里我们可以利用 Dynkin 图轻易读出 $|L|$ 的素因子（注意， p 是 $|Q|$ 的唯一素因子）。例如，若 $G = E_7(q)$ 且 $P = P_5$，那么 $|L|$ 的素因子必定整除 $|\mathrm{SL}_5(q)||\mathrm{SL}_3(q)|$。

根据 [35, 定理 8] ，(III) 型子群可划分为以下三种情形：

命题 2.7. 设 G 和 H 如定理 2.6 中所述，且 H 为（III）型。则以下情形之一成立：

(i) $G_0 = E_7(q)$、 $p \geqslant 3$ 和 $H_0 = (2^2 \times \mathrm{P\Omega}_8^+(q).2^2).S_3$ 或 ${}^3D_4(q)$。3；
(ii) $G_0 = E_8(q)$、 $p \geqslant 7$ 和 $H_0 = \mathrm{PGL}_2(q) \times S_5$；(iii) $(G_0, \mathrm{soc}(H_0))$ 是表 [36, 表 3]中列出的情形之一。

我们给出一个关于（VII）型子群的类似命题。注意，我们用 Lie(p) 表示定义在特征为 p 的域上的李型有限单群集合。近年来，关于 $S = \mathrm{soc}(H)$ 的可能情况已得到显著细化。结合 Craven [15, 16], 近期研究中的主要结果，我们得到如下结论：

命题 2.8. 设 G 和 H 如定理 2.6 所述，其中 H 为 (VII) 型，且 $\mathrm{soc}(H) = S$。则下列情形之一成立：

(i) $S \notin$李型(p)，且 S 的可能情况见 [37, 表 10.1–10.4]；或 (ii) $S \in$李型(p)，且以下情况之一成立：

(a) $G_0 = E_8(q)$ *and either* $S = \mathrm{L}_2(q_0)$ *with* $q_0 \leqslant (2, q-1).1312$ *or*

$$S \in \{\mathrm{L}_3^\epsilon(3), \mathrm{L}_3^\epsilon(4), \mathrm{U}_3(8), \mathrm{PSp}_4(2)', \mathrm{U}_4(2), {}^2B_2(8)\};$$

(b) $G_0 = E_7(q)$ *and* $S = \mathrm{L}_2(q_0)$ *with* $q_0 \in \{7, 8, 25\}$.

命题 2.8 的 (i) 中 S 的可能情况列表已得到进一步细化，见 Craven[14]和 Litterick [38]。不过，对于我们的工作而言， [37] 中的表格已足够。

以下关于 $G_2(q)$ 的结果将有助于分析例外群和仿射群。设 $G = G_2(q)$，其中 $q \geqslant 3$，并令 V 表示 $G_2(q)$ 的最小模（回顾一下，我们写作 $q = p^f$，其中 p 是素数， f 是正整数）。对于 $G_2(q)$ 的最小模，我们是指 V 是一个维数为 $7 - \delta_{2,\ p}$ 的不可约模，其中 $\delta_{2,\ p}$ 是克罗内克δ。我们注意到， $M =$SL$_3^\epsilon(q)$:2 是 G 的极大子群，因此 M 的指数为 2 的子群 SL$_3^\epsilon(q)$ 自然嵌入 G 中。此外，对于矩阵 A_1、……、A_n，我们使用 diag(A_1、……、A_n) 表示一个分块对角矩阵，其块为 A_1、……、A_n，并用 A_i^{-T} 表示 A_i 的逆转置。

引理 2.9. 设 $G = G_2(q)$ 且 $q \geqslant 3$，令 V 为 G的最小模。取 $x \in H =$ SL$_3^\epsilon(q)$，使得 x 在自然的 H-模上作用为矩阵 A。那么在共轭意义下， x在 V 上的作用为

$$\begin{cases} \mathrm{diag}(A, A^{-T}) & \textit{if } q \textit{ is even} \\ \mathrm{diag}(A, A^{-T}, 1) & \textit{otherwise} \end{cases}.$$

证明。我们考察代数群 $G = G_2(k)$ 和 $H =$ SL$_3(k)$，其中 $k = \mathbb{F}_{p^\circ}$ 设 $V = V \otimes k$ 表示 G 的最小模， W 表示自然的 H-模。那么 $\dim V = 7 - \delta_{2,\ p}$ 并且

$$\bar{V} \downarrow \bar{H} = \begin{cases} \bar{W} \oplus \bar{W}^* & \text{if } q \text{ is even} \\ \bar{W} \oplus \bar{W}^* \oplus 0 & \text{otherwise} \end{cases},$$

其中 W^* 表示 W 的对偶，0 表示平凡的 H-模。由于 x 在 $\bar{W}$ 上的作用为矩阵 A，因此 x 在 $\bar{W}^*$上的作用为 A^{-T}，结论立即得出。□

现在我们给出一些关于李型例外群中某些素数阶元素的共轭类的有用结果。

命题 2.10. 设 $G = G_2(q)$，其中 $q \geqslant 3$，并且对于 $i \in \{3, 6\}$，令 s_i 表示 $q^i - 1$的最大本原素因子。假设 s_i 是 $q^i - 1$的唯一本原素因子。那么 G 至少包含 $\frac{s_i - 1}{6}$ 个阶为 s_i的元素的不同共轭类。

证明。 $i = 6$ 和 $i = 3$ 的证明类似，因此我们只详细讨论$i = 6$的情形。假设 s_6 是 $q^6 - 1$ 的唯一一个本原素因子。注意，我们可以将 G 视为 GL(V) 的子群，其中 V 是 $G_2(q)$ 的最小模。令$M =$ SU$_3(q)$:2，它是 G 的一个极大子群（例如参见 [3, 表 8.30、8.41 和 8.42]）。定义 $L :=$ SU$_3(q)$ $< M$，其自然模为 W，并取 $x \in M$ 为一个阶为 s_6的元素。于是 $x \in L$，因为 s_6 不整除 $|M : L|$。 L 中半单素数阶元素的共轭类由这些元素在 L 的自然模（在适当的扩域上）上作用时的特征值集合唯一确定。根据[4, 命题 3.3， 2], 存在 $(s_6 - 1)/3$ 个不同的 L类，其元素的阶为 s_6，每一类都由一个特征值集合 $[\Lambda_j]$表示，其中 $\Lambda_j = \{\lambda_j, \lambda_j^{q^2}, \lambda_j^{q^4}\}$，且 $\lambda_j \in \mathbb{F}_{q^6}$是一个 s_6^{th}单位根（注意 $\Lambda_j \neq \Lambda_j^{-1}$）。注意， $M = L.\langle\psi\rangle$，其中 ψ 是一个作用为逆转置的自同构。因此，由 $[\Lambda_j]$ 和 $[\Lambda_j^{-1}]$ 表示的类在 M中融合。特别地，存在 $(s_6 - 1)/6$个不同的 M类，其元素的阶为 s_6。应用引理 2.9 可知，至少存在 $(s_6 - 1)/6$ 个不同的此类元素的 GL(V) 类，结论得证。□

命题 2.11。设 $G \in \{F_4(q)\ {}^3D_4(q)\}$，并假设 $q^4-q^2+1=r$ 是素数。那么，在 G中存在 $(q^4-q^2)/\alpha$ 个不同的 G类，其元素的阶为 r；当$G={}^3D_4(q)$时，$\alpha=4$；当 $G=F_4(q)$时，$\alpha=12$。

证明。我们查看 [18, 43, 44] 中相关的表。首先假设 $G={}^3D_4(q)$。通过查阅 [18, 表 2.1] 我们看到，阶为 r 的半单元素只有标记为 s_{14} 的那些。接着查看 [18, 表 4.4] 我们看到，G 恰好包含 $1\ 4(q^4-q^2)$ 个阶为 r 的不同 G-类元素。接下来假设 $G=F_4(\bar{q})$ 且 q 为偶数。那么 [43, 表 II] 显示，标记为 h_{76} 的元素是唯一阶为 r 的半单元素，并且有 $1\ 12(q^4-q^2)$ 个这样的 G-类。类似地，对于 $G=F_4(q)$ 且 q 为奇数的情形，查阅 [44, 表 8 和 9] 可知，所需元素标记为 h_{99}，结论得证。□

2.2. 一个约化定理。提醒读者，$H_0=H\cap G_0$ 和 $\pi(X)$ 表示 $|X|$的不同素因子的数量。此外，回想一下，当且仅当 $x^G\cap H=\emptyset$ 时，$x\in G$ 是一个错排。从这个定义显然可知，只有当 $\pi(G_0)-\pi(H_0)\geq 1$ 时，G 才是几乎难以捉摸的。在 Liebeck、Praeger 和 Saxl 的工作中，描述了单群 G 的满足 $\pi(G)=\pi(M)$ 的子群 M。这里我们给出这一结果的一个扩张，它是经典群的 [25, 定理 2] 的类比。这个结果是定理 1 证明中的一个关键工具。

定理 2.12. 设 $G\leqslant \mathrm{Sym}(\Omega)$ 是一个几乎单本原置换群，其点稳定子为 H，底群为 G_0，且 G_0 是定义在 $\mathbb{F}_q$ 上的李型例外群。那么 $\pi(G_0)-\pi(H_0)\geq 1$ 当且仅当以下条件之一成立：

(i) $\pi(G_0)=\pi(H_0)$，且 $(G_0,H_0)=(G_2(2)',\mathrm{L}_2(7))$、$(G_2(3),\mathrm{L}_2(13))$ 或 $({}^2F_4(2)',\mathrm{L}_2(25))$。(ii) $\pi(G_0)=\pi(H_0)+1$，且 (G_0,H_0) 见表 2。

注记 2.13. 表 2 中标为 i 的列表示一个附加条件，即存在 q^i-1 的唯一一个本原素因子 r_i。标为 r 的列表示整除 $|G_0|$ 但不整除 $|H_0|$ 的唯一素数。若 i 列中有条目，则 r 恰为 q^i-1 的唯一一个本原素因子。特别地，我们注意到，若 $i=6$ 且 $q\neq 19$，则 $r=q^2-q+1$；若 $i=12$，则 $r=q^4-q^2+1$（这可利用命题 2.3 证明）。

定理 2.12 的证明。通过直接比较 $|G_0|$的阶（见 [40, 第 208] 页）和 $|H_0|$ 的阶（相关参考文献见第 2.1 节）即可证明。大多数情形下的分析都类似，因此我们只详细说明少数几种情形：

(a) $G_0={}^2F_4(q)$ 和 $H_0=a^{\pm}$:12，其中 $a^{\pm}=(q^2\pm\sqrt{2q^3}+q\pm\sqrt{2q}+1)$；(b) $G_0=E_6(q)$ 和 $H_0=E_6(q_0)$。((3, $q-1$) k)，其中 $q=q_0^k$，且 k 为素数；(c) $G_0={}^3D_4(q)$ 和 $H_0=G_2(q)$；(d) $G_0=E_7(q)$ 和 H 是一个 P_7 抛物子群；(e) $G_0=E_8(q)$ 和 soc$(H)=S=\mathrm{L}_2(q_0)\in$ 李型(p)，其中 $q_0\leqslant(2,q-1)$1312。

首先考虑情形 (a)，并注意到 $|G_0|=q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$。容易证明，$a^+$ 和 a^- 都整除 $q^{12}+1$。因此，$|H_0|$ 的所有素因子都整除 $6(q^{12}+1)$。令 s_4和 s_{12}分别为 q^4-1和 $q^{12}-1$的最大本原素因子（根据定理 2.1，这两者都存在；并且注意到 s_{12} 整除 q^6+1）。由引理 2.2，存在某些正整数 d_i，使得 $s_4=4d_4+1$ 和 $s_{12}=12d_{12}+1$ 成立，因此 $s_4,s_{12}\geqslant 5$。此外，由引理 2.2，s_4 和 s_{12} 都是 $q^{12}-1$的素因子。因此，s_4 和 s_{12} 都不整除 $|H_0|$，这意味着 $\pi(G_0)-\pi(H_0)\geqslant 2$。

现在假设我们处于情形 (b)。此处有 $|G_0|=\frac{1}{d}q_0^{36k}\prod_{i\in I}(q_0^{ik}-1)$，其中 $I=\{2,5,6,8,9,12\}$，且 $d=(3,q-1)$ 的每个素因子都必须整除$q_0\cdot\prod_{j\in J}(q_0^j-1)$，其中 $J=\{5,9,12\}$。显然，$q_0^{12k}-1$和 $q_0^{9k}-1$ 的本原素因子整除 $|G_0|$，但不整除 $|H_0|$，因为 $12k,9k\geqslant 18$。

Case	G_0	H_0	条件	i	r
R1	${}^2G_2(q)$	$2\times \mathrm{L}_2(q)$		6	7
R1′	${}^2G_2(3)'$	$2^3{:}7$			3
R2′		D_{14}			3
R3′		D_{18}		6	7
G1	$G_2(q)$	J_1	$q=11$	6	37
G2		J_2	$q=4$	6	13
G3		$\mathrm{L}_2(13)$	$q=4$	2	5
G4		$2^3.\mathrm{L}_3(2)$	$q=3$	3	13
G5		$\mathrm{SL}_3(q){:}2$		6	r
G6		$\mathrm{SU}_3(q){:}2$		3	r
G7		${}^2G_2(q)$	$q=3^f, f$为奇数	3	r
G1′	$G_2(2)'$	$[3^{1+2}]{:}(3^2-1)$		3	7
G2′		$4.\mathrm{PGU}_2(3)$		3	7
G3′		$4^2{:}S_3$		3	7
D1	${}^3D_4(q)$	$[q^9]{:}(\mathrm{SL}_2(q^3)\circ(q-1)).(2,q-1)$		12	r
D2		$G_2(q)$		12	r
D3		$\mathrm{L}_2(q^3)\times \mathrm{L}_2(q)$	q 偶数	12	r
D4		$(\mathrm{SL}_2(q^3)\circ \mathrm{SL}_2(q)).2$	q 奇数	12	r
D5		$[2^{11}]{:}(7\circ \mathrm{SL}_2(q))$	$q=2$	12	13
D6		$(7\circ \mathrm{SL}_3(2)).7.2$	$q=2$	12	13
D7		$7^2.\mathrm{SL}_2(3)$	$q=2$	12	13
F1	$F_4(q)$	$(2,q-1).\Omega_9(q)$		12	r
F1′	${}^2F_4(2)'$	$\mathrm{L}_3(3){:}2$		4	5
F2′		$A_6.2^2$		12	13
F3′		$5^2{:}4A_4$		12	13

表 2： $\pi(G_0)-\pi(H_0)$ 6 1 的情形

接下来考虑情形 (c)。此处

$$|G_0|=q^{12}(q^6-1)^2(q^4-q^2+1) \text{ and } |H_0|=q^6(q^2-1)(q^6-1).$$

首先注意到， r是 $q^{12}-1$的本原素因子，当且仅当 r整除 q^4-q^2+1。因此， $|G_0|$ 中不整除 $|H_0|$ 的唯一素因子是q^4-q^2+1的素因子。因此，对于某个奇素数 r 和某个正整数 l， $\pi(G_0)-\pi(H_0)=1$ 当且仅当 $q^4-q^2+1=r^l$。在命题 2.3 中代入 $x=-q^2$，可推得 $l\geqslant 2$没有解。因此我们必须假设 $q^4-q^2+1=r$，这就得到表 2 中的情形D2。注意，当 r 为素数时，方程 $q^4-q^2+1=r$有解。例如，可以取 $q\in\{2,3,4,9\}$。

接下来假设我们处于情形 (d)。在此情形下， $|G_0|=\frac{1}{d}q^{63}\prod_{i\in I}(q^i-1)$，其中 $I=\{2,6,8,10,12,14,18\}$，且 $d=(2,q-1)$，并且 $H_0=QL$，其中 Q 是一个 p-群，而 $|L|$ 的素因子整除 $|E_6(q)|$。因此， $|H_0|$ 的所有素因子都整除 $q(q^5-1)(q^8-1)(q^9-1)(q^{12}-1)$。所以， $q^{14}-1$ 和 $q^{18}-1$ 的本原素因子整除$|G_0|$，而不整除 $|H_0|$。

最后假设我们处于情形 (e)，并令 $q_0=p^t$。此处

$$|G_0|=p^{120f}\prod_{i\in I}(p^{if}-1) \text{ and } |S|=\frac{1}{d}p^t(p^{2t}-1),$$

其中 $I=\{2,8,12,14,18,20,24,30\}$ 和 $d=(2,p^t-1)$。注意到 $|H_0|$ 整除 $|S|dt$。小于 $(2,q-1)$ 1312 的 2 和 3 的最大幂分别为 2^{10} 和 3^8。因此我们可以假设 $t\leqslant 10$，于是 $2t<24f,30f$。因此， $p^{24f}-1$ 的本原素因子以及$p^{30f}-1$ 的本原素因子整除 $|G_0|$ 而不整除 $|H_0|$。□

2.3. 定理 1 的证明。现在我们可以证明定理 1 了。首先注意，满足 $G_0 = {}^2G_2(q)$、 ${}^2G_2(3)'$、 ${}^2B_2(q)$、 $G_2(2)'$ 和 ${}^2F_4(2)'$ 的情形，先前已在 [7, 命题 4.4、4.12、5.1 以及第 4.3 和 4.4]节中处理。因此，在本节余下部分，我们可以假设 G_0 不是这些群之一。我们先借助 MAGMA [2]处理一些小群。

命题 2.14. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个几乎单本原置换群，其点稳定子为 H，底群为 $G_0 = G_2(3)$ $G_2(4)$ $G_2(5)$ 或 ${}^3D_4(2)$。那么，当且仅当 $(G, H) = (G_2(4).2, J_2.2)$ 时， G 几乎难以捉摸。

证明. 在 MAGMA [2] 中，我们使用 AutomorphismGroupSimpleGroup 命令得到群 $\mathrm{Aut}(G_0)$，将其表示为置换群（但不一定作用在 Ω 上）。使用 LowIndexSubgroups，我们可以构造满足 $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ 的群 G。对于每个群 G，我们调用 MaximalSubgroups，它会返回 G 中极大子群的共轭类集合。然后，对于这些极大子群中的每一个 H，我们使用 Core 命令检查它是否核自由。我们还可以通过检查阶和结构来识别 H，例如使用 GroupName 和 NormalSubgroups 等命令。接着，我们可以使用内置的 MAGMA 函数 Classes 和 IsConjugate 构造一个函数，以判定群 G 作用在子群 H 的陪集上时是否几乎难以捉摸。为此，我们使用 Classes 命令计算 G 和 H 中素数阶元素的共轭类。最后，我们反复使用 IsConjugate 来确定 G 中 H-类的融合，从而输出素数阶错排的共轭类。如果输出的此类共轭类唯一，则我们得出结论：(G, H) 几乎难以捉摸。□

在本节余下部分，我们将证明几乎难以捉摸群没有其他例子。回顾一下，(G, H) 几乎难以捉摸，当且仅当 $\pi(G_0) - \pi(H_0) \geq 1$。因此，定理 2.12 将定理 1 的证明归结为表 2 中的情形 G1-G7、D1-D7 和 F1。此外，我们指出，情形 G2-G4 和 D5-D7 已在命题 2.14 中处理。

在下述命题中，我们将证明表 2 中情形 G1、G5-G7 的定理 1。首先，我们说明在 $\mathrm{GL}(V) = \mathrm{GL}_n(q)$ 中幺幂元的记号，其中 $q = p^f$。取 $M = \mathrm{GL}_n(q)$，并设 $x \in M$ 为一个阶为 p 的元素。x 在 V 上的若尔当标准形记作

$$x = [J_p^{a_p}, \ldots, J_1^{a_1}],$$

一个分块对角矩阵，其中 J_k 表示一个大小为 k 的标准幂零 Jordan 块， a_k 表示其重数（注意 $n = \sum_{i=1}^{p} i a_i$）。特别地，若 x、$y \in M$，则 x 和 y 在 M 中共轭，当且仅当它们在 V 上具有相同的若尔当标准形（例如参见 [4, 引理 3.1。14] ）。

命题 2.15. 设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个几乎单本原置换群，其点稳定子为 H，底群 G_0 如表 2 中情形 G1、G5、G6 或 G7 所示。则 G 不是几乎难以捉摸的。

证明. 令 V 表示最小的 G_0-模。这里 $G_0 = G_2(q)$，根据命题 2.14，我们可以假设 $q \geqslant 7$。注意，在所有情形中都存在唯一的本原素因子 r_i，它是 $q^i - 1$ 的本原素因子；对于情形 G1 和 G5，有 $i = 6$，对于情形 G6 和 G7，有 $i = 3$。我们注意到， r_i 也是 $p^{fi} - 1$ 的本原素因子，因此根据引理 2.2，我们可以写成 $r_i = ifd_i + 1$，其中 d_i 是一个正整数。此外，我们注意到，G_0 中每个阶为 r_i 的元素都是一个错排。

由命题 2.10， G_0 至少包含 $ifd_i/6$ 个阶为 r_i 的错列共轭类。注意， $|\mathrm{Out}(G_0) : G_0| = (1 + \delta_{(3,p)})f$。因此， G 至少包含 β 个阶为 r_i 的不同错列共轭类，其中

$$\beta := \begin{cases} id_i/12 & \text{if } p = 3 \\ id_i/6 & \text{otherwise.} \end{cases}$$

由引理 2.4，$\beta \geqslant 2$ 当且仅当 $(q,i) \neq$ (8,6),(19,6)。因此我们得出结论：对于情形 G1、G6、G7，以及满足 $q \neq 8$,19 的情形 G5，G 并非几乎难以捉摸。对于 G5 的最后几种情形，即 $H_0 = \mathrm{SL}_3(q)$:2 且 $q = 8$ 或 19，仍需处理。

首先假设 $q = 19$。设 $x \in H_0$ 是一个阶为 19 的元素。那么，自然三维模上的 q 中的 $_3$ SL $x \in$ 必须具有若尔当标准形 $[J_2, J_1]$ 或 $[J_3]$ 。因此，根据引理 2.9，x在 V 上分别具有若尔当标准形 $[J_2^2, J_1^3]$或 $[J_3^2, J_1]$。通过查阅 ˜表 1], 可知，G_0 中阶为 19 的元素属于标记为 A_1 的共轭类，并且在 V 上具有若尔当标准形$[J_3, J_2^2]$。因此，存在阶为 19 的错排。

最后假设 $q = 8$，因此 3 是 $q^2 - 1$的唯一一个本原素因子。根据 [4,命题 3.2，H_0 中存在唯一一个阶为 3 的元素类。利用 Magma 很容易验证，G_0中存在两个不同的阶为 3 的共轭类。因此，根据引理 2.5，G_0 包含阶为 3 的错排。□

命题 2.16. 设 $G \leqslant$Sym(Ω) 是一个几乎单本原置换群，其点稳定子为 H，底群为 G_0，且属于表 2 中的情形 D1–D4。那么 G 并非几乎难以捉摸。

证明. 根据命题 2.14，我们不妨假设 $q \geqslant 3$。这里我们假设 $q^4 - q^2 + 1 = r$ 是素数，并且在所有情形下，G_0 中任何阶为 r 的元素都是错排（因为 r 整除 $|G_0|$，但不整除 $|H_0|$）。根据命题 2.11，在 G_0 中，存在 $(q^4-q^2)/4$ 个不同的 G_0 共轭类，其元素是阶为 r 的错排。由于 $|\mathrm{Aut}(G_0) : G_0| = 3f$，其中 $q = p^f$，因此至少存在 $(q^4-q^2)/12f$ 个不同的 G 共轭类，其元素是阶为 r 的错排。容易验证，对所有 $q \geqslant 3$，均有 $(q^4 - q^2)/12f \geqslant 2$。□

命题 2.17. 设 $G \leqslant$Sym(Ω) 是一个几乎单本原置换群，其点稳定子为 H，底群为 G_0，对应于表 2 中的情形 F1。则 G 并非几乎难以捉摸。

证明. 这里 $H_0 = (2, q-1).\Omega_9(q)$，并且注意到，根据 [35]，我们可以假设 G 不包含图自同构（另见表 7.1 和 7.2]）。对于 $q = 2$，我们按照命题 2.14 的证明进行，因此可以假设 $q \geqslant 3$。在此情形下，$q^4 - q^2 + 1 = r$ 是一个素数，且 G_0 中任何阶为 r 的元素都是错排。根据命题 2.11，G_0中有 $(q^4 - q^2)/12$ 个不同的 G_0 类，其元素的阶为 r。由于 $|G : G_0| \leqslant f$，至少有 $(q^4 - q^2)/12f \geqslant 2$ 个不同的 G 类错排。结论成立。□

这就完成了定理 1 的证明。此外，鉴于 [7] 和 [25],，这也完成了本原几乎单、几乎无逃逸群的分类。

3. Affine Groups

本节证明定理 2，该定理对本原几乎难以捉摸仿射群进行了分类。设 p 为一个素数，并令 $V =(\mathbb{F}_p)^d$ 为定义在 $\mathbb{F}_p$上的 d 维向量空间。V 上的仿射变换是一个映射 $t_{h,v} : V \longrightarrow V$，其中 $h \in$ 属于 GL(V)，且 $v \in V$ 满足 $t_{h,v}(u) := hu + v$。这些仿射变换构成仿射一般线性群，记作 AGL(V) 或 AGL$_d$(p)，我们可以将其视为作用在 V上的置换群。AGL(V)的底群可视为 V 上的加法群，它同构于 $(C_p)^d$；若 G 是作用在 V 上的仿射群，则

$$V \trianglelefteq G = V{:}H \leqslant \mathrm{AGL}(V),$$

其中，GL(V)中的 $H \leqslant$是 V中零向量的稳定子。此外，仿射群G 是本原的，当且仅当 H 是 GL(V)的不可约子群。本节余下部分中，我们假设 $G = V{:}H \leqslant$ AGL(V)是一个本原仿射群，并用 (v, h) 表示 G 的元素，其中 $v \in V$且 $h \in H$。

3.1. 预备结果。本节中始终设 $V^* = V \setminus \{0\}$。我们首先讨论仿射群中的素数阶无不动点置换。注意，$|V| = p^d$，因此每个素数阶无不动点置换的阶都是 p。任何形如 $(v, 1) \in G$ 且满足 $v \in V^*$ 的元素，都是阶为 p 的错排，因为它在 V 上的作用是平移 v。此外，每个

	n	H	条件
I	p^d	$H \leqslant \Gamma\mathrm{L}_1(p^d)$	
II	q^a	$\mathrm{SL}_a(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_a(q)$	$a \geqslant 2$
III	q^a	$\mathrm{Sp}_a(q) \trianglelefteqslant H$	$a \geqslant 4$ 偶
IV	q^6	$\mathrm{G}_2(q)' \trianglelefteqslant H$	q 偶
V	$5^2, 7^2, 11^2, 23^2$	$\mathrm{SL}_2(3) \trianglelefteqslant H$	
VI	3^4	$2^{1+4} \trianglelefteqslant H$	
VII	3^4 11^2 19^2 29^2 59^2	$\mathrm{SL}_2(5) \trianglelefteqslant H$	
VIII	2^4 „ „	A_6, A_7	
IX	3^6	$\mathrm{SL}_2(13)$	

表 3：Hering 定理中出现的群。

属于 H 的元素都有不动点。事实上，我们可以精确判定 G 中的元素何时是素数阶错列。

引理 3.1. 元素 $(v,h) \in G$ 是一个阶为 p 的错排，当且仅当满足以下所有条件：

(i) $h^p = 1$, (ii) $v \in \ker(h^{p-1} + \cdots + h + 1)$, (iii) $v \notin \mathrm{im}(h-1)$。

证明. 设 $g = (v,h)$ 是 G 中的一个非平凡元素。由于 G 通过仿射变换作用于 V，容易看出，g 是一个错排，当且仅当对所有 $u \in V$，$u \neq hu + v$。也就是说，$v \notin \mathrm{im}(h-1)$。现在，$g^p = (v + hv + h^2v + \cdots + h^{p-1}v, h^p)$，因此 g 的阶为 p，当且仅当 $h^p = 1$ 且 $(h^{p-1} + \cdots + h + 1)(v) = 0$，其中 $h^{p-1} + \cdots + h + 1 \in \mathrm{Hom}(V,V)$。也就是说，$v \in \ker(h^{p-1} + \cdots + h + 1)$。结论得证。□

根据 [7, 定理 1],，每个本原几乎难以捉摸的仿射群都是 2-传递的。为完整起见，我们给出这一简单观察的证明。

引理 3.2. G 几乎难以捉摸，当且仅当 G 是 2-传递的。

证明。假设 G 几乎难以捉摸。回顾一下，G 中任何形如 $(v, 1)$ 的元素，只要 $v \in V^*$ 是一个阶为 p 的错排，也就是说，V 的每个非平凡元素都是阶为 p的错排。由于 G 几乎难以捉摸，这种形式的元素必定在 G 中共轭，即对于所有 $v \in V^*$，都有 $V^* = v^G$。此外，由于 $G = VH$ 且 V是阿贝尔群，因此对于所有 $v \in V^*$，都有 $v^G = v^{VH} = v^H$。这意味着 H 在V^*上递移作用，也就是说，G 是 2-传递的。□

Hering [26] 已确定了 2-传递仿射群。关于这一结果，其他便于查阅的资料来源有 [33, 附录 1] 和 [10, 第 7 节。3]。

定理 3.3（Hering 定理）。设 $G = V{:}H$ 是一个次数为 $n = p^d$ 的 2-传递仿射群。那么 (n, H) 是表 3 中的情形之一。

在第 3.1 节余下部分，我们将建立一些关于 H 中阶为 p 的元素的若尔当标准形的结果。请注意，我们将使用与第 2.3 节所述相同的若尔当标准形记法。当 H 属于 Hering 定理中的某个无限族时，这些结果尤其有用（见表 3 中的情形 I–IV）。对于这些无限族，我们证明 Hering 定理情形 III 和 IV 中不存在几乎难以捉摸的例子（见命题 3.15 和 3.16），但情形 I 和 II 中确实存在几乎难以捉摸的群（见命题 3.13 和 3.14）。注意，表 3 中情形 II 出现的每个子群都是 2-传递的（见 [19, 第 55] 页），而关于情形 I 中 2-传递群具体结构的详细信息可见 [21, 第 15] 节。

此外，对于情形 V–IX 中的群，我们在 MAGMA 中使用计算方法，见命题 3.12。

命题 3.4。设 $h \in H$是一个阶为 p、在V上的若尔当标准形为$[J_p^{a_p}, \dots, J_1^{a_1}]$的元素。那么，存在一个元素 $v \in V^*$，使得 $(v,h) \in G$ 是一个阶为 p的错排，当且仅当对于某个 $1 \leqslant i \leqslant p-1$，有 $a_i > 0$。

证明。取一个 V的 $\mathbb{F}_p$-基 $\{v_1, \dots, v_d\}$，使得 $h = [J_p^{a_p}, \dots, J_1^{a_1}]$。由引理 3.1，存在一个 $v \in V^*$，使得 $(v,h) \in G$ 是一个阶为 p 的错排，当且仅当存在一个 $v \in V^*$，使得 $v \in \ker(h^{p-1} + \cdots + h + 1)$ 且 $v \notin \mathrm{im}(h-1)$。

注意到，任意的 $v \in V^*$ 都可以写成 $v = c_1 v_1 + \cdots + c_d v_d$，其中 $c_1, \dots, c_d \in \mathbb{F}_p$，并且 $h^i = [(J_p^i)^{a_p}, \dots, (J_1^i)^{a_1}]$，其中

$$J_k^i = \begin{pmatrix} 1 & \binom{i}{1} & \binom{i}{2} & \dots & \binom{i}{k-1} \\ 0 & 1 & \binom{i}{1} & \dots & \binom{i}{k-2} \\ 0 & 0 & 1 & \dots & \binom{i}{k-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

其中，当 $a < b$ 或 $b \leqslant 0$时，我们取 $\binom{a}{b} = 0$。

由于对于所有 $1 \leqslant t \leqslant p-2$，$\sum_{i=t}^{p-1} \binom{i}{t} = \binom{p}{t+1}$ 都能被 p 整除，因此容易证明，$v \in$ 属于 $\ker(h^{p-1} + \cdots + h + 1)$ 当且仅当 $a_p = 0$，或者对于所有 $1 \leqslant k \leqslant a_p$，$c_{kp} = 0$。类似地，$v \in$ 属于 $\mathrm{im}(h-1)$ 当且仅当对于所有 $1 \leqslant i \leqslant p$，$a_i = 0$，或者对于所有$1 \leqslant k \leqslant a_i$，$c_{ki+t} = 0$，其中

$$t = \begin{cases} \sum_{j=i+1}^{p} a_j j & \text{if } i < p \\ 0 & \text{if } i = p \end{cases}.$$

因此显然可知 $\ker(h^{p-1} + \cdots + h + 1) \geqslant \mathrm{im}(h-1)$，且当且仅当$a_i = 0$对所有 $1 \leqslant i \leqslant p-1$成立时取等号。也就是说，存在 $v \in V^*$使得 $v \in \ker(h^{p-1} + \cdots + h + 1)$ 且 $v \notin \mathrm{im}(h-1)$，当且仅当对某个 $1 \leqslant i \leqslant p-1$有 $a_i > 0$。因此结论得证。□

推论 3.5. 设 $G = V{:}H$ 是一个次数为 p^d 的 2-传递仿射群。那么 G 几乎难以捉摸，当且仅当以下条件之一成立：

(i) $|H|$ 不能被 p 整除；或 (ii) $|H|$ 和 d 均能被 p 整除，且每个阶为 p 的 $h \in H$ 在 V 上的若尔当标准形为$[J_p^{d/p}]$。

接下来，我们简要讨论 $\mathrm{GL}_{d/k}(q^k)$ 到 $\mathrm{GL}_d(q)$ 的嵌入，其中 $k \geqslant 1$ 是 d 的一个因子。设 $V_\#$ 是 $\mathbb{F}_{q^k}$ 上的一个 d/k 维向量空间。于是，我们可以将 $V_\#$ 视为 $\mathbb{F}_q$ 上的一个 d 维向量空间 V。此外，$V_\#$ 的任意 $\mathbb{F}_{q^k}$-线性变换也是 V 的一个 $\mathbb{F}_q$-线性变换，这就给出了 $\mathrm{GL}_{d/k}(q^k)$ 到 $\mathrm{GL}_d(q)$ 的嵌入。我们陈述以下引理，它是正规基定理的直接推论（例如参见 [32,定理 2.35]）。

引理 3.6。设 d 和 k 为正整数，且 k 整除 d。考虑向量空间 $V = (\mathbb{F}_q)^d$ 和 $V_\# = (\mathbb{F}_{q^k})^{d/k}$，其中 $q = p^f$ 为素数且 $f \geqslant 1$。Fix 一个 $\mathbb{F}_{q^k}$-基 $\{v_1, \dots, v_{d/k}\}$，它是 $V_\#$ 的基。则存在一个标量 $\lambda \in \mathbb{F}_{q^k} \setminus \mathbb{F}_q$，使得

$$\{\lambda v_1, \lambda^q v_1, \dots\dots, \lambda^{q^{k-1}} v_1, \dots, \lambda v_{d/k}, \lambda^q v_{d/k}, \dots, \lambda^{q^{k-1}} v_{d/k}\}$$

是 V 的一个 $\mathbb{F}_q$-基。

下面的结果是 [4, 引理 5.32]。

引理 3.7. 设 d 和 k 为正整数，且 k 整除 d。设 $h \in \mathrm{GL}_{d/k}(p^k)$ 是一个阶为 p、在 $V_\# = (\mathbb{F}_{p^k})^{d/k}$ 上具有若尔当标准形 $[J_p^{a_p}, \dots, J_1^{a_1}]$ 的元素。则 h 在 $V = (\mathbb{F}_p)^d$ 上具有若尔当标准形 $[J_p^{ka_p}, \dots, J_1^{ka_1}]$。

证明. 固定 $V_{\#}$ 的一个 $\mathbb{F}_{p^k}$-基 $\{v_1,\dots,v_{d/k}\}$，使得 $h=[J_p^{a_p},\dots,J_1^{a_1}]\in \mathrm{GL}_{d/k}(p^k)$。于是根据引理 3.6，存在 V 的一个 $\mathbb{F}_p$-基，

$$\beta=\{\lambda v_1,\lambda^p v_1,\dots\dots,\lambda^{p^{k-1}}v_1,\dots,\lambda v_{d/k},\lambda^p v_{d/k},\dots,\lambda^{p^{k-1}}v_{d/k}\},$$

使得 $\lambda\in\mathbb{F}_{p^k}\setminus\mathbb{F}_p$。由于我们知道 h 在 $\{v_1,\dots,v_{d/k}\}$的基向量上的作用，且 h 是关于 $\mathbb{F}_{p^k}$的线性映射，因此很容易看出 h 在 β的基向量上的作用。于是，按照基 β的适当排列，我们得到所需的 $h=[J_p^{ka_p},\dots,J_1^{ka_1}]$。□

本节最后的结果涉及一般半线性群，我们先回顾该群的结构。设 d 和 k 为正整数，并固定一个素数p。设 $\{u_1,\dots,u_d\}$ 是 $\mathrm{GL}_d(p^k)$ 的自然模 $U=(\mathbb{F}_{p^k})^d$ 的一组基。我们可以定义映射 $\gamma:U\mapsto U$，其中

$$\gamma:\sum_i \lambda u_i\mapsto\sum_i\lambda^p u_i.$$

于是 γ诱导出一个域自同构 ϕ: $\mathrm{GL}_d(p^k)\mapsto\mathrm{GL}_d(p^k)$，其中对于所有 $(a_{ij})\in\mathrm{GL}_d(p^k)$，都有 $(a_{ij})^\phi=(a_{ij}^p)$。一般半线性群定义为 $\Gamma\mathrm{L}_d(p^k)=\mathrm{GL}_d(p^k):\langle\phi\rangle$，我们将 $\Gamma\mathrm{L}_d(p^k)$ 的元素写作 (g,ϕ^l)，其中 $g\in\mathrm{GL}_d(p^k)$ 且 $\phi^l\in\langle\phi\rangle$。我们称映射 ϕ 为 $\mathrm{GL}_d(p^k)$ 中阶为 k 的标准域自同构。一般而言，我们称 $\Gamma\mathrm{L}_d(p^k)\backslash\mathrm{GL}_d(p^k)$ 中的元素为域自同构，并注意到它们具有如下形式：(g,ϕ^l)，使得 $1\leqslant l\leqslant k-1$。此外，我们回顾一下，若 k 整除 d，则 $\mathrm{GL}_{d/k}(p^k)$ 嵌入 $\mathrm{GL}_d(p)$。因此，由于映射 γ 是一个 $\mathbb{F}_p$- 线性映射，$\Gamma\mathrm{L}_{d/k}(p^k)$ 嵌入 $\mathrm{GL}_d(p)$。

引理 3.8. 设 $G=\Gamma\mathrm{L}_{d/k}(p^k)$，其中 p 是素数，且对于某个 $f\geqslant 1$，有 $k=pf$。设$x=(1,\psi)\in G$是一个阶为 p的元素。那么 x在 V上的若尔当标准形为 $[J_p^{d/p}]$。

证明. 我们先注意到，标准域自同构 ϕ 的阶为 $k=pf$，因此对于某个 $1\leqslant i\leqslant p-1$，有 $\psi=\phi^{if}$。取一个 $\mathbb{F}_{p^k}$- 基 $\{v_1,\dots,v_{d/k}\}$，使其为 $V_{\#}=(\mathbb{F}_{p^k})^{d/k}$ 的基，并如上文所述与 ϕ 相容。由引理 3.6，存在一个 $\mathbb{F}_p$-基 V，

$$\beta=\{\lambda v_1,\lambda^p v_1,\dots\lambda^{p^{k-1}}v_1,\dots,\lambda v_{d/k},\lambda^p v_{d/k},\dots\lambda^{p^{k-1}}v_{d/k}\}$$

使得 $\lambda\in\mathbb{F}_{p^k}\backslash\mathbb{F}_p$。注意，$\psi$对 β中的向量的作用如下：$\psi(\lambda^{p^l}v_m)=\lambda^{p^{l+if}}v_m$，对所有 $0\leqslant l\leqslant k-1$ 和 $1\leqslant m\leqslant d/k$均成立。我们可以将集合 β 划分为 d/k 个大小为k的集合，即集合 $\{\lambda v_1,\lambda^p v_1,\dots\lambda^{p^{k-1}}v_1\}$，.....，$\{\lambda v_{d/k},\lambda^p v_{d/k},\dots\lambda^{p^{k-1}}v_{d/k}\}$。在这些 d/k 集合上，ψ 的作用是 f 个互不相交的 p-循环。例如，在第一个集合上，这样一个 p-循环的例子是（λv_1，$\lambda^{p^{if}}v_1$，.....，$\lambda^{p^{(p-1)if}}v_1$）。因此，ψ在 β上的作用是 d/p 个互不相交的p-循环的乘积。由此可得，$(1,\psi)$ 在 V 上的若尔当标准形为 $[J_p^{d/p}]$。□

现在我们可以陈述关于一般半线性群 $\Gamma\mathrm{L}_{d/k}(p^k)$ 中阶为 p 的域自同构的若尔当标准形的结果。首先，我们陈述一个著名的数论结果。提醒读者，对于正整数 a 和 b，我们用记号（a，b）表示 a 和 b 的最大公因数。

引理 3.9。设 a、b、k、n、$m\in\mathbb{Z}$ 满足 k、$m\neq 0$ 且（k，m）$=d$。那么 $ka\equiv kb$（模 m）当且仅当 $a\equiv b$（模 $\frac{m}{d}$）。此外，线性同余 $kx\equiv n$（模 m）有解当且仅当 d 整除 n。而且，如果 d 整除 n，则模 m 恰有 d 个解。

引理 3.10. 设 d 为正整数，且 p 是 d的素因子。设 $x\in\Gamma\mathrm{L}_1(p^d)$ 是一个阶为 p的域自同构。那么 x 在 $V=(\mathbb{F}_p)^d$上的若尔当标准形为 $[J_p^{d/p}]$。

证明. 回顾 $H = \Gamma\mathrm{L}_1(p^d) = \mathrm{GL}_1(p^d){:}\langle\phi\rangle$，其中 ϕ 是阶为 d的标准域自同构。我们将 $x = (a, \psi)$ 写作，其中 $a \in \mathrm{GL}_1(p^d)$，且 $\psi = \phi^j$ 对某个整数 $1 \leqslant j < d$成立。此外，我们将 $d = pk$ 写作，其中 $k \geqslant 1$为某个值。由于 x 的阶为 p，这意味着 ψ 的阶为 p，且 $a\psi(a)\dots\psi^{p-1}(a) = 1$。特别地，$j = ik$，其中 $1 \leqslant i \leqslant p-1$。

我们断言，x 与 $(1, \psi)$ 是 H-共轭的，因此结论由引理 3.8 得出。为证明这一断言，我们首先注意到，元素 $(b, \phi^t) \in H$与 $(1, \psi)$ 是 H-共轭的，当且仅当 $\phi^t = \psi$。因此，我们接下来证明，$|(1, \psi)^H|$ 等于 H 中形如 (b, ψ) 的阶为p 的元素个数。

我们回顾一下，$(b, \psi) \in H$ 的阶为 p，当且仅当

$$b\psi(b)\dots\psi^{p-1}(b) = b\phi^{ik}(b)\dots\phi^{(p-1)ik}(b) = 1.$$

利用引理 3.9，我们可以证明，对每个 $1 \leqslant z \leqslant p-1$，都存在唯一的$1 \leqslant y \leqslant p-1$使得 $zik \equiv yk \pmod{d}$。因此，由于 ϕ 的阶为 d，上面的方程恰好等价于

$$b\phi^k(b)\dots\phi^{(p-1)k}(b) = b^{1+p^k+\dots+p^{(p-1)k}} = 1.$$

由于 $\mathrm{GL}_1(p^d)$ 是一个阶为 $p^d - 1$ 的循环群，因此有

$$(p^d - 1, 1 + p^k + \dots + p^{(p-1)k}) = 1 + p^k + \dots + p^{(p-1)k}$$

许多元素 $b \in \mathrm{GL}_1(p^d)$ 满足 (b, ψ) 的阶为 p。

元素 $(b, \phi^t) \in C_H((1, \psi))$ 当且仅当 $b = \psi(b)$，这等价于 $b^{p^{ik}-1} = 1$。恰有 $(p^d - 1, p^{ik} - 1)$ 个 $= p^k - 1$这样的元素 $b \in \mathrm{GL}_1(p^d)$。因此 $|C_H((1, \psi))| = (p^k - 1)d$，于是

$$|(1, \psi)^H| = (p^d - 1)d/(p^k - 1)d = 1 + p^k + \dots + p^{(p-1)k},$$

由此得到所述结论。现在应用引理 3.8，即可得到该结果。 □

引理 3.11. 设 p、k 和 d 为整数，使得 p 是素数，d 能被 k 整除，且$d/k \geqslant 2$；k 能被 p整除。设 $x \in \Gamma\mathrm{L}^{d/k}(p^k)$ 是阶为 p 的域自同构。那么 x 在 $V = (\mathbb{F}_p)^d$上的若尔当标准形为 $[J_p^{d/p}]$。

证明. 令 ϕ 表示 $\Gamma\mathrm{L}^{d/k}(p^k)$ 中阶为 p 的标准域自同构。注意，所有阶为 p 的域自同构都包含在某个陪集 $\mathrm{GL}^{d/k}(p^k)\phi^i$ 中，其中 $1 \leqslant i \leqslant p-1$ 满足某个条件。因此 $x \in \mathrm{GL}^{d/k}(p^k)\sigma$，其中 $\sigma = \phi^i$ 对某个 $1 \leqslant i \leqslant p-1$ 成立。根据 Shintani 下降理论（例如，更多细节见第 3 节.4]），$\mathrm{GL}^{d/k}(p^k)$ 中的 $\langle\sigma\rangle$-共轭类与陪集 $\mathrm{GL}^{d/k}(p^k)\sigma$ 中的共轭类之间存在一一对应。特别地，$\mathrm{GL}^{d/k}(p^k)\sigma$ 中阶为 p 的元素类对应于 $\mathrm{GL}^{d/k}(p^{k/p})$ 中阶为 1 的元素类（证明见引理 3.20]）。由此得出，$\Gamma\mathrm{L}^{d/k}(p^k)$ 中阶为 p 的元素只有一个 $\mathrm{GL}^{d/k}(p^k){:}\langle\sigma\rangle$-共轭类。因此不妨设 $x = (1, \sigma) = (1, \phi^i)$，于是由引理 3.8 可得该结果。□

3.2. 定理 2 的证明。现在我们转而证明定理 2。提醒读者，本节中我们将始终使用以下记号：$G = V{:}H \leqslant \mathrm{AGL}(V)$，其中$V = (\mathbb{F}_p)^d$，且 H 是 $\mathrm{GL}(V)$ 的不可约子群。此外，我们还回顾一下，可以假设 G 是 2-传递的（见引理 3.2）。因此，我们将通过考察 Hering 定理中的各个情形来展开证明（见定理 3.3 和表 3）。

命题 3.12. 对于表 3 中情形 V-IX 所示的 G，定理 2 成立。

证明。这是一个简单的计算，利用了 Magma [2] 的本原群数据库，其中记录了次数不超过 4095 的本原群。PrimitiveGroups 命令会输出次数符合我们要求的群。然后，我们可以使用 Classes 命令，获取 G 中所有素数阶元素的共轭类。对于每个 G 类，我们可以使用 Fix 命令来获取群中某个元素的不动点集合，

找出这些元素的不动点数。如果没有不动点的素数阶元素只有一个 G 类，那么我们就可以得出结论：该群几乎难以捉摸。□

现在还需处理 Hering 定理中的无限族，即表 3 中的情形 I–IV。回顾一下， V 中的非零向量构成一个阶为 p 的错排共轭类。因此，若不存在形如 $(v,h) \in G$ 的错排，其中 v 和 h 均非平凡，则 G 几乎难以捉摸。

Prop命题 3.13. 设 G 是表 3 中情形 I 所述的 2-传递群。那么 G 是几乎难以捉摸

证明。这里 $n = p^d$ 和 $H \leqslant \Gamma\mathrm{L}_1(p^d) = \mathrm{GL}_1(p^d){:}d \leqslant \mathrm{GL}_d(p)$。若 p 不整除 d，则 p 不整除 $|H|$，因此由引理 3.1 可知 G 几乎难以捉摸。现在假设 p 整除 d。 $\Gamma\mathrm{L}_1(p^d)$ 中任何阶为 p 的元素都必定是域自同构，因此由引理 3.10 和推论 3.5 得证。□

命题 3.14. 设 G 如表 3 的情形 II 所示。那么， G 几乎难以捉摸，当且仅当 $p = a = 2$。

证明. 这里 $\mathrm{SL}_a(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_a(q)$，且 $n = p^d = q^a$ 满足 $a \geqslant 2$。回顾一下， $\Gamma\mathrm{L}_a(q) = \Gamma\mathrm{L}_{d/k}(p^k) < \mathrm{GL}_d(p)$，其中 $k = d/a$。定义 $V_\# = (\mathbb{F}_q)^a$，这是 a维的 $\mathbb{F}_q$ 上的向量空间（$\mathrm{GL}_a(q)$的自然模）。首先假设 $a \geqslant 3$，并取 $h \in \mathrm{SL}_a(q) \leqslant H$为一个阶为 p、在 $V_\#$上的若尔当标准形为$[J_2, J_1^{a-2}]$ 的元素。由引理 3.7， h在 V上的若尔当标准形为 $[J_2^k, J^k{}_{(a-2)}{}_1 \quad]$。因此，推论 3.5 表明 G 并非几乎难以捉摸。最后，假设 $a = 2$。取 $h \in \mathrm{GL}_2(q)$为一个阶为 p的元素。则 h 在 $V_\#$ 上的若尔当标准形为 $[J_2]$，在 V上的若尔当标准形为 $[J_2^{d/2}]$。先设 $p \geqslant 3$。由推论 3.5， G 并非几乎难以捉摸。最后设 $p = 2$。利用引理 3.11 可知， $\Gamma\mathrm{L}_2(q)$中每个阶为 2 的元素在 V上的若尔当标准形均为 $[J_2^{d/2}]$。因此由推论 3.5 即得所述结论。□

Pro命题 3.15. 假设 G 如表 3 的情形 III 所示。那么 G 并非几乎难以捉摸 $e.$

证明. 在此情形下，$\mathrm{Sp}_a(q) \trianglelefteqslant H$ 且 $p^d = q^a$，其中 $a \geqslant 4$ 为偶数。定义 $V_\# = (\mathbb{F}_q)^{a/2}$，并令 $h \in \mathrm{Sp}_a(q)$ 为一个阶为 p、在 $V_\#$ 上具有若尔当标准形 $[J_2, J_1^{a-2}]$ 的元素。于是 h 在 V 上具有若尔当标准形 $[J_2^k, J^k{}_{(a-2)_1} \quad]$，其中 $d = ak$。因此，根据推论 3.5， G并非几乎难以捉摸。□

Pro命题 3.16. 假设 G 如表 3 的情形 IV 所示。那么 G 并非几乎难以捉摸 $e.$

证明. 此处 $p = 2$ 和 $G_2(q)' \trianglelefteqslant H$，其中 $2^d = q^6$。注意，利用命题 3.12 证明中概述的相同方法，我们可以轻松处理情形$d = 6$ e。因此，不妨假设 $d \geqslant 12$ 且 $G_2(q) \trianglelefteqslant H$。

注意，$\mathrm{SL}_3(q){:}2$ 是 $G_2(q)$ 的一个极大子群（例如参见 $[3, \text{表 } 8.30]$）。令W 表示自然的 $\mathrm{SL}_3(q)$ 模，并令 $V_\# = (\mathbb{F}_q)^6$ 表示$G_2(q)$ 在 $\mathbb{F}_q$上的最小模。取 $h \in \mathrm{SL}_3(q) \leqslant H$ 为一个阶为 2 且在 W上的若尔当标准形为 $[J_2, J_1]$的元素。由引理 2.9， h在 $V_\#$上的若尔当标准形为 $[J_2^2, J_1^2]$，因此 h在 V上的若尔当标准形为$[J_2^{d/3}, J_1^{d/3}]$。因此，推论 3.5 表明 G并非几乎难以捉摸。□

这就完成了定理 2 的证明。

4. Quasiprimitive Groups

在本节中，我们通过证明定理 4，完成对所有拟本原几乎难以捉摸群的分类证明。根据 $[7, \text{定理 } 1]$，拟本原群只有在它是几乎单群或二重传递仿射群时，才可能几乎难以捉摸。每个二重传递仿射群都是本原群，因此由定理 3 可知，我们可以假设 G 是非本原的几乎单群。

在本节余下部分，我们假设 G是一个以 G_0 为底群的有限几乎单群，并且 H 是 G 的一个核自由非极大子群，其中 $G = G_0H$。特别地，我们可以将 H 嵌入 G的一个极大子群 M 中。容易证明， M实际上必定是核自由的。

引理 4.1. H 在 G 中的每个极大扩群都是核自由的。

证明. 设 M 是 G 的一个极大子群，且满足 $H < M$。反设 M 不是核自由的。由于 G_0 是 G的唯一极小正规子群，因此 G_0 是 M 的一个子群。于是 $G_0H \leqslant M$。然而， G 是拟本原的，所以 G_0 是 G 的一个传递子群，从而 $G = G_0H$。这与 $M < G$矛盾。□

特别是，这意味着 G 在 M的右陪集集合上作本原作用。回顾一下， $x \in G$ 是一个错排，当且仅当 $x^G \cap H = \emptyset$，其中 x^G 表示 x 在 G中的共轭类。

引理 4.2. 假设(G, H)几乎难以捉摸，且 $H < M$，其中 M 在 G中是极大的。那么(G, M)几乎难以捉摸，因此属于表 A1 或 A2 中的情形之一。

证明。假设 (G, M) 既非几乎难以捉摸，也非难以捉摸。那么，在 G 中，存在两个不同的由素数阶元素构成的共轭类 x^G 和 y^G，使得 $x^G \cap M = \emptyset$ 和 $y^G \cap M = \emptyset$。由于 $H < M$，G 中至少有两个不同的素数阶错排共轭类，这就产生了矛盾。因此，(G, M) 要么是几乎难以捉摸的，因而根据定理 3 可在表 A1 或 A2 中找到；要么是难以捉摸的，因而根据 [22]，$(G, M) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$。通过在 MAGMA 中进行简单计算可知，如果 $(G, M) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$，则不存在几乎难以捉摸的情形。结论得证。□

为了完成拟本原几乎难以捉摸群的分类，现在还需处理 (G, M) 属于表 A1 或 A2 的情形。

4.1. 初步结果。本节给出证明定理 4 所需的一些初步结果。提醒读者， G 是一个以G_0 为底群的有限几乎单群，且 H 是 G 的一个无核非极大子群，使得 $G = G_0H$。此外，$H < M$，使得 M 是 G的一个无核极大子群。我们先陈述一个数论引理，即 [9,引理 2.6]。

引理 4.3. 设 r 和 s 为素数， v 和 w 为正整数。若 $r^v + 1 = s^w$，则以下情形之一成立：

(i) $(r, s, v, w) = (2,3,3,2)$。(ii) $(r, w) = (2,1)$，且
$s = 2^v + 1$ 是费马素数。(iii) $(s, v) = (2,1)$，且
$r = 2^w - 1$ 是梅森素数。

回顾一下，对于任意子群 $K < G$，我们定义 $K_0 = K \cap G_0$。此外， $\alpha(K)$ 表示 $|K|$ 的不同素因子集合，而 $\pi(K) = |\alpha(K)|$。

引理 4.4. 假设 (G, M) 几乎难以捉摸，且 $\pi(G_0) = \pi(M_0) + 1$。那么，(G, H) 几乎难以捉摸，当且仅当 $\pi(M_0) = \pi(H_0)$。

证明。假设 (G, H) 几乎难以捉摸。注意，若 r 是整除 $|G_0|$ 但不整除 $|H_0|$ 的素数，那么 G_0 中每个阶为 r 的元素都是错排。因此 $\pi(G_0) - \pi(H_0) \leqslant 1$。由此可轻易得到结论，因为 $\pi(M_0) \geqslant \pi(H_0)$。□

在陈述下一个结果之前，我们先简要描述群 $G = \mathrm{PGL}_2(q)$ 中素数阶半单元素的共轭类，其中 $q = p^f$ 是素数幂。我们先考察半单 involution（在此情形下， q 必须为奇数）。在 G 中，有 2 个由 t_1 和 t_1' 表示的不同对合共轭类，采用 [4, 第 3.2 节中的记号。2] 这与 [23, 表 4.5.1] 一致。元素t_1 在 $\mathrm{GL}_2(q)$ 中的提升是一个对合，而 t_1' 的提升是一个 4 阶不可约元素。在

特别地，我们注意到 G_0 有唯一的对合共轭类。此外，当且仅当 $q \equiv 1$（模 4）时，$t_1 \in G_0$；当且仅当 $q \equiv 3$（模 4）时，$t_1' \in G_0$。更多详情请见 [4, 第 3.2 节。2]

在接下来的讨论中，我们考察奇素数阶半单元素。注意，$x^{G_0} = x^G$，其中 $x \in G$ 是一个阶为奇素数 $r \neq p$ 的元素（见 [23,定理 4.2.2(j)]）；我们将在引理 4.5 的证明中使用此处讨论的记号。设 r 是 $|G|$ 的一个奇素因子，且满足 $r \neq p$。那么，r 要么整除 $q-1$，要么整除 $q+1$。若 r 整除 $q-1$，则定义 $k=1$；否则定义为 $k=2$。取 $x \in G$ 为一个阶为 r 的元素。那么，在相差共轭的意义下，x 可提升为 $\mathrm{GL}_2(q)$ 中的元素 $\hat{x} \in$，它在$\mathbb{F}_{q^k}$上可对角化，特征值为：当 $k=1$ 时是 $[\lambda^i, \lambda^{-i}]$，当 $k=2$ 时是 $[\lambda^i, \lambda^{qi}]$；其中 λ 是 $\mathbb{F}_{q^k}$ 中的一个非平凡 r^{th} 单位根，并且 $1 \leqslant i \leqslant (r-1)/2$。阶为 r 的元素的 G-类由这些特征值集合唯一确定。因此，对于 $k=1$ 和 2，G 中阶为 r 的元素共有 $(r-1)/2$ 个这样的 G-类。我们滥用记号，将这 $(r-1)/2$ 个不同的 G-类的代表元记为 $[\Lambda]Z$，其中当 $k=1$ 时 $\Lambda = [\lambda^i, \lambda^{-i}]$，否则为 $[\lambda^i, \lambda^{qi}]$，且 $1 \leqslant i \leqslant (r-1)/2$；$Z$ 是 $\mathrm{GL}_2(q)$ 的中心。更多细节见 [4, 第 3.2 节。1]

引理 4.5. 设 $G = \mathrm{L}_2(q)$，其中 $q = p^f \geqslant 4$ 是素数幂，且 H 是 G 的子群。假设 $r \neq p$ 是 $|H|$ 的一个奇素因子，并取 $x \in G$ 为一个阶为 r 的元素。则 $x^G \cap H \neq \emptyset$。

证明. 注意到 $|G| = {}^{q}_{(2,q-1)}(q-1)(q+1)$，因此 r 整除 $q-1$ 或 $q+1$。这两种情形非常相似，所以我们只详细证明 r 整除 $q-1$ 的情形。设 $y \in H$ 是一个阶为 r 的元素。那么不失一般性，我们可以假设$y \in ([\lambda, \lambda^{-1}]Z)^G$。这意味着对于所有 $1 \leqslant t \leqslant (r-1)/2$，都有 $y^t \in ([\lambda^t, \lambda^{-t}]Z)^G$，因此 $\langle y \rangle$ 与所有由阶为 r 的元素构成的 G-类相交。于是结果成立，因为 $\langle y \rangle \leqslant H$。□

推论 4.6. 设 G 为几乎单群 $\mathrm{L}_2(q)$ 或 $\mathrm{PGL}_2(q)$，其中 $q = p^f \geqslant 4$ 是素数幂。设 H 是 G 的核自由子群，并假设 $r \neq p$ 是 $|H|$ 的奇素因子。那么 (G, H) 不含阶为 r 的错排。

4.2. 定理 4 的证明。现在我们可以证明定理 4 了。回顾一下，G 是一个以 G_0 为底群的几乎单群，并且有一个非极大无核子群 H，满足 $G = G_0H$。此外，$H < M$，其中 M 是 G 的无核极大子群。由引理 4.2，我们可以假设 (G, M) 出现在表 A1 或 A2 中。本节先证明定理 4 在一些小情形下成立。为此，

$$\mathcal{A} = \{A_n, \mathrm{L}_2(q), \mathrm{L}_3^{\epsilon}(q'), \mathrm{U}_4(q'), \mathrm{PSp}_4(q'), \mathrm{U}_5(2), \mathrm{U}_6(2), \mathrm{PSp}_6(2), {}^2F_4(2)', G_2(4)\},$$

其中 $n \leqslant 20$、$q \leqslant 49$ 和 $q' \leqslant 8$。

命题 4.7。定理 4 对 $G_0 \in \mathcal{A}$ 成立。

证明。令 M 表示 G 的一个无核极大子群，满足 $H < M$。由引理 4.2，(G, M) 记录于表 A1 或 A2 中。与命题 2.14 中一样，我们可以使用 MAGMA 得到群 G 和 M，使得 (G, M) 记录于表 A1 或 A2 中。使用 MaximalSubgroups 命令，我们得到 M 的极大子群共轭类代表元列表。对于每个极大子群 L，我们首先检查 $|L||G_0|/|L \cap G_0| = |G|$，以确保 G 在 L 的陪集上作用时是拟本原的；然后使用 Core 检查 L 是否为 G 的无核子群。接着，我们使用命题 2.14 中所述的同一函数，检查 (G, L) 是否几乎难以捉摸。若 (G, L) 并非几乎难以捉摸，则将其舍弃。然而，若 (G, L) 几乎难以捉摸，我们就查看 L 的极大子群，并重复这一过程，直到不再找到几乎难以捉摸的例子。□

注 4.8。取 $G_0 \in \mathcal{A}$。如注 1 中所述，可能存在多个子群类，其代表元同构于 H，且并非所有这些

类都会产生一个几乎难以捉摸的例子。表 B2 中，对于每一对 (G, H)，都存在一个子群 $K < G$，使得 $K \cong H$，且 (G, K) 几乎难以捉摸。我们记录了 G 的子群类中代表元为 $K \cong H$ 且满足 $G = G_0K$ 的类的数量，以及其中能给出几乎难以捉摸例子的类的数量。此外，若 (G, H) 记录在表 B1 中，则对于任何满足 $K \cong H$ 的子群 $K < G$，(G, K) 都几乎难以捉摸。有关这些情形的更多细节，请参见第 6 节和注 6.3。

这涵盖了 (G, M) 出现在表 A2 中的所有情形。因此，现在我们可以假设 (G, M) 属于表 A1 和 $G_0 \notin \mathcal{A}$。我们将依次考察这些情形，并使用表 A1 中的标签来表示各情形。回顾一下，我们用 $\alpha(X)$ 表示 $|X|$ 的素因子集合，因此 $\pi(X) = |\alpha(X)|$。此外，提醒读者注意，$H_0 = H \cap G$。我们先作一条注记，讨论表 A1 中的情形 U1。

注 4.9。如注 6.2(b) 和 [25, 第 5.2 节所述，3] 我们不认为情形 U1（表 A1）中会出现任何真正的本原几乎难以捉摸群。因此，我们也不认为此情形下会有拟本原几乎难以捉摸群。不过，若确实出现了这样的本原群，我们便能构造出拟本原几乎难以捉摸群，使得点稳定子 H 是 G 的无核非极大子群。例如，假设 $G = \mathrm{U}_n(2^f).C_{2f}$，$M$ 是自然模上一维非退化子空间的稳定子，且 (G, M) 如情形 U1 所述。取 $H = M_0.C_j$，其中 $M_0 = M \cap G_0$ 且 j 整除 $2f$。那么，(G, H) 是几乎难以捉摸群，当且仅当 $\pi(j) = \pi(2f)$。

命题 4.10。对于表 A 中情形 L1 或 L2 所示的 (G, M)，定理 4 成立 *1.*

证明。在此，$G_0 = \mathrm{L}_2(p)$，且 $M = C_p{:}C_{k(p-1)/2}$ 是 G 的一个 P_1 抛物子群（即，M 是 G 的一个 Borel 子群），其中 $k = |G : G_0|$；在情形 L1 中，$p = 2^m - 1$ 是一个梅森素数，而在情形 L2 中，$p = 2.3^a - 1$ 是满足 $a \geqslant 2$ 的素数。

我们首先处理情形 L1，在此情形下 $G = G_0$ 或 $\mathrm{PGL}_2(p)$。这里我们证明，(G, H) 只有在表 B1 的情形 II 或 III 中有记录时，才是几乎难以捉摸的。置 $M_0 = M \cap G_0 = C_p{:}C_{(p-1)/2}$。注意，由于 $p \equiv 3$（模 4），$|M_0|$ 是奇数，因而 $\alpha(G_0) \setminus \alpha(M_0) = \{2\}$。因此，$G_0$ 中的每个对合都是错排，并且如第 4.1 节所述，G_0 中存在唯一的对合共轭类。假设 (G, H) 是几乎难以捉摸的。我们回顾第 4.1 节中的讨论：$\mathrm{PGL}_2(p)$ 包含两个不同的共轭类。一个共轭类由 G_0 中的对合组成，其中每一个都是错排；另一个则由 $\mathrm{PGL}_2(p) \setminus G_0$ 中的对合组成。因此我们得出结论：当 $G = \mathrm{PGL}_2(p)$ 时，$|H|$ 必须为偶数。现在根据引理 4.4，$\pi(M_0) = \pi(H_0)$，这等价于条件 $\alpha(M_0) = \alpha(H_0)$，因为 $H_0 \leqslant M_0$。因此，由于 $p \equiv 3$（模 4），且当 $k = 2$ 时 $|H|$ 为偶数，我们必须有 $H = C_p{:}C_d$，其中 d 是 $k(p-1)/2$ 的一个真因子，并且 $\alpha(d) = \alpha(k(p-1)/2)$。

最后我们讨论情形 L2，其中 $G = G_0$。这里需要证明，只有当 (G, H) 记录在表 B1 的情形 IV 中时，它才是几乎难以捉摸的。假设 (G, H) 是几乎难以捉摸的。那么如上所述，我们有 $\alpha(M_0) = \alpha(H_0)$，因此 $H = C_p{:}C_d$ 其中 d 是 $(p-1)/2$ 的一个真因子，并且 $\alpha(d) = \alpha((p-1)/2)$。结论由此得出。□

注 4.11。如注 1(b) 所述，若 (G, H) 记录在表 B1 中，则对于任何满足 $K \cong H$ 的子群 $K < G$，(G, K) 都是几乎难以捉摸的。这里我们证明表 B1 中标记为 II、III 和 IV 的情形下这一结论成立。令 (G, H) 如表 B1 中的情形 II 或 III。也就是说，$G = G_0 = \mathrm{L}_2(p)$ 或 $\mathrm{PGL}_2(p)$，其中 $p = 2^m - 1$ 是一个梅森素数，并且 $H = C_p{:}C_d$，使得 d 是 $k(p-1)/2$ 的真因子，且 $\alpha(d) = \alpha(k(p-1)/2)$，其中 $k = |G : G_0|$。那么 $|G : H| = 2^{m-1}k(p-1)/d$。根据推论 4.6，对于 $p-1$ 的任意奇素因子 r，都不存在阶为 r 的错排。由于当 $k = 2$ 时 $|H|$ 为偶数，而 $|H_0|$ 为奇数，故 G 中存在唯一一个对合错置元素类。因此 (G, H) 几乎难以捉摸。情形 IV 也可用非常相似的论证。这里 $G = \mathrm{L}_2(p)$，且 $H = C_p{:}C_d$，其中 $p = 2.3^a - 1 \geqslant 17$ 是一个素数，而 d 是 $(p-1)/2$ 的真因子

满足 $\alpha(d) = \alpha((p-1)/2)$。那么 $|G: H| = 3^q(p-1)/d$。根据推论 4.6，对于 $p-1$ 的任意奇素因子 r，都不存在阶为 r 的错排。由于 $3 \notin \alpha(H)$，且 G 中存在唯一一个阶为 3 的元素类（见 [4, 命题 3.2.1]），我们得出结论：(G, H) 几乎难以捉摸。

表 A1 中的情形 L3 附带有多种数论条件。事实上，我们能够证明，所有这些数论条件仅在 2 种情形下成立。

引理 4.12。设 (G, M) 如表 A1 的情形 L3 中所述。则 $q = 9$ 或 49。

证明。这里 $G_0 = \mathrm{L}_2(q)$，$G = G_0.f$，M 是 G 的一个 P_1 抛物子群，并且满足以下条件：

(a) $q = 2r^z - 1$，其中 $z \geqslant 1$；(b) $r = 2^m + 1$ 是一个费马素数，且 $m \geqslant 2$ 是一个 2 的幂；以及 (c) $q = p^f$，其中 p 是一个素数且 $f = 2^{m-1}$。

我们首先注意到，(a) 蕴含 $p^f + 1 = 2r^z$。令 $x = p^{f/2}$（注意 $f \geqslant 2$ 是 2 的幂）。于是方程变为

$$x^2 + 1 = 2r^z. \tag{3}$$

由 [48, 引理 2.6]，对于 $z > 2$，方程 (3) 不存在满足 r 为费马素数的解。因此，我们可以假设 $z \in \{1, 2\}$。由此只需简单计算即可得出，唯一的解为 $(x, r, z) = (3, 5, 1)$ 和 $(7, 5, 2)$。也就是说，L3 中出现的情形只有 $q = 9$ 和 $q = 49$。□

命题 4.13. 对于表 A1 中情形 L3 所示的 (G, M)，定理 4 成立。

证明. 根据引理 4.12，此情形已在命题 4.7 中处理。 □

命题 4.14. 对于表 A1 中情形 L4 或 L5 所示的 (G, M)，定理 4 成立 .

证明. 此处 $G = \mathrm{PGL}_2(p)$，其中 $p = 2^m + \epsilon$ 是素数，且 $M = D_{2(p+\epsilon)}$ 满足 $\epsilon = \pm 1$。注意到 $p + \epsilon \equiv 2$ (模 4)，并令 $M_0 = M \cap G_0 = D_{p+\epsilon}$。此外，我们注意到 $\alpha(G) \setminus \alpha(M) = \{p\}$。因此，$G$ 中每个阶为 p 的元素都是错排，并且这类元素只有一个 G-共轭类，因为 $G = \mathrm{PGL}_2(p)$（见 [4, 命题 3.2.6]）。我们需要证明，只有当 (G, H) 记录在表 B1 的情形 I 中时，它才是几乎难以捉摸的。

假设 (G, H) 几乎难以捉摸。由引理 4.4 可知，必有 $\pi(H_0) = \pi(M_0)$；由于 $H_0 \leqslant M_0$，这等价于 $\alpha(H_0) = \alpha(M_0)$。提醒读者，二面体群的每个子群不是循环群就是二面体群。因此，$H = D_{2d}$ 且 d 是 $p + \epsilon$ 的真因子，其中 $\alpha(d) = \alpha(k(p+\epsilon)/2)$；我们令 $k = 2$ 在 d 为偶数时取该值，否则取 1（注意 $H_0 = D_{2d/k}$）。若 d 为奇数，则 H 有唯一的对合共轭类；但我们记得 G 中有两个这样的共轭类，所以 d 必须为偶数。也就是说，$\alpha(d) = \alpha(p + \epsilon)$，结论得证。□

注 4.15。这里我们说明，当 (G, H) 如表 B1 的情形 I 所示时，注 1(b) 成立。这里 $G = \mathrm{PGL}_2(p)$ 且 $H = D_{2d}$，其中 $p = 2^m + \epsilon$ 是素数，d 是 $p + \epsilon$ 的真因子，并且 $\alpha(d) = \alpha(p + \epsilon)$。注意 $|G: H| = 2^{m-1}p(p + \epsilon)/d$。由推论 4.6 可知，对于 $p + \epsilon$ 的任意奇素因子 r，都不存在阶为 r 的错排。由于 d 为偶数且 $H_0 = D_d$，我们看到 $H \setminus H_0$ 含有对合，因此 G 中的每个对合都有不动点。最后，由于 $p \notin \alpha(H)$，且 G 含有唯一的阶为 p 的元素共轭类（见 [4, 命题 3.2.6]），我们得出结论：(G, H) 几乎难以捉摸。

Pro位置 4.16。对于表 A1 中情形 A1、A4 或交错群 A_5 所示的 (G, M)，定理 4 成立。

证明。这里 $(G, M) = (A_n, A_{n-1})$ 或 (S_n, S_{n-1})，其中 $n = r^a$，且 r 是素数；或者 $n = 2r^a$，且 $r \geqslant 3$ 是素数（见表 A1）。由于 (G, M) 几乎难以捉摸，且有唯一一个阶为 r 且 $H < M$ 的错排共轭类，我们得出 (G, H) 含有阶为 r的错排。注意，根据命题 4.7，我们可以假设 $n > 20$。开始分析时，我们假设 H 是 M 的极大子群（如果 (G, H) 在 G 是 M 的极大子群时并非几乎难以捉摸，那么结论已成立），并将 $=$ 视为 A_n 中 A_{n-1} 的稳定子。因此 S_n 在 S_{n-1} 上的作用要么是不传递的、非本原的，要么是本原的。

根据引理 4.4，我们可以假设 $\pi(M_0) = \pi(H_0)$，因此根据 [34,推论 5]， H 必须在 $\{1,\dots,n-1\}$ 上不传递地作用。也就是说，对于某个 $1 \leqslant k < (n-1)/2$，有 $H = (S_k \times S_{n-1-k}) \cap M$。特别地， H 是 G 中该划分的稳定子

$$\{1,\dots,k\} \cup \{k+1,\dots,n-1\} \cup \{n\}.$$

我们将证明，在每种情形下，(G,H) 也包含素数阶为 s 的错排，使得 $s \neq r$，因此 (G,H) 并非几乎难以捉摸。

首先假设 $k \geqslant 4$。结论可由检查 [7, 引理 3.8] 的证明得出。不过，为完整起见，我们给出详细证明。首先注意到 $|G : H| = n\binom{n-1}{k}$。根据 [7, 命题 3.6]， $\binom{n-1}{k}$ 可被一个素数 s 整除，使得 $s > k$，且 s 不整除 n。因此 $s \neq r$，并且对于某个 $t \in \{0,1,\dots,k-1\}$， s 整除 $n-1-t$。考虑一个循环型为 $[s^{(n-1-t)/s}, 1^{t+1}]$ 的元素 $g \in G$。由于 $t < k$，可得 $g \notin H$，所以 g 是一个错排。

接下来，假设 $k = 1$ or 2。设 s 是 $n-1$ 的一个奇素因子。那么， G 中循环型为 $[s^{(n-1)/s}, 1]$ 的每个元素都是错排。因此，我们可以假设，对于某个 $t \geqslant 5$，有 $n-1 = 2^t$（回想一下，我们假设 $n > 20$）。由引理 4.3 可知， $n = r$ 是一个费马素数，此时 $G = S_n$ 且 $M = S_{n-1}$ （见表 A1 ）。先假设 $k = 1$。那么， G 中循环型为 $[2^{(n-1)/2}, 1]$ 的任意元素都是错排。最后，假设 $k = 2$，并令 s 为 $n-2$ 的一个奇素因子。于是 $s \neq r$，且 G 中循环型为 $[s^{(n-2)/s}, 1^2]$ 的任意元素都是错排。

最后，我们假设 $k = 3$。设 $n-1$ 和 $n-2$ 分别有素因子 s_1 和 s_2，使得 s_1、$s_2 \geqslant 5$。那么， G 中循环型为 $[s_1^{(n-1)/s_1}, 1]$ 或 $[s_2^{(n-2)/s_2}, 1^2]$ 的任意元素都是错排。因此，只有当 $n-1$ 和 $n-2$ 都不能被大于 3 的素数整除时， G 才是几乎难以捉摸的。假设 $n-1$ 和 $n-2$ 都只能被素数 2 和 3 整除。那么，对于某个 $b \geqslant 3$ 和 $m \geqslant 5$ （回想一下 $n > 20$），要么 $(n-1, n-2) = (2^m, 3^b)$，要么 $(3^b, 2^m)$。因此，根据引理 4.3，这种情况绝不会发生。结论得证。□

命题 4.17. 对于表 A1 中情形 A2 或 A3 所示的 (G,M)，定理 4 成立 .

证明. 在表 A1 $G = S_n$ 的情形 A2 和 A3 中， $M = S_{n-2} \times S_2$，且要么 $n = 2^m$ 和 $n-1 = r$ 是梅森素数（情形 A2），要么 $n = 2^m + 1 = r$ 是费马素数（情形 A3）。由于 (G,M) 几乎难以捉摸，且只有一个阶为 r 和 $H < M$ 的错排共轭类，因此我们得出结论：(G,H) 含有阶为 r 的错排。我们先假设H 是 M 的极大子群（如果当 H 是 M 的极大子群时，(G,H) 并非几乎难以捉摸，那么结论便成立）。 M 的极大子群如下

(i) $(A_{n-2} \times 1).2$ (ii) S_{n-2} (iii) $L \times S_2$，其中 L 是 S_{n-2} 的极大子群。

参见 [46, 引理 1.3]。首先假设 H 如情形 (i) 所述。则在共轭意义下$H = \langle A_{n-2}, (n-3, n-2)(n-1, n)\rangle \leqslant G_0$。这是矛盾的，因为 $G = G_0 H$。

现在假设 H 如情形 (ii) 所述。此处 $H = S_{n-2}$，且 H 中的每个元素的循环型都是 $[a, 1^2]$，其中 a 是 $n-2$的一个划分。如果 $n = 2^m$，那么 G 中的任意具有循环型 $[2^{n/2}]$ 的对合都是一个错排。同样地，如果 $n = 2^m + 1$ 是一个费马素数，那么 G 中任意具有循环型 $[2^{(n-1)/2}, 1]$ 的对合都是一个错排。因此 G 包含阶为 r 以及阶为 2 的错排，所以 (G,H) 不是几乎难以捉摸的。

最后，假设 H 如情形 (iii) 所述。根据引理 4.4，我们不妨设 $\pi(M_0) = \pi(H_0)$，因此 $|H_0|$ 可被每个素数 $p \leqslant n-2$ 整除。于是， $|L|$ 必须被不超过 $n-2$ 的两个最大素数整除。因此，根据 [34, 定理 4]，要么 $L = A_{n-2}$，要么对于某个 $1 \leqslant k < (n-2)/2$ 有 $L = S_k \times S_{n-2-k}$。我们回顾一下， G 包含一个阶为 r 的错排共轭类（其中当 $n = 2^m$ 时 $r = n-1$，而当 n 时 $r = n$ 是一个

费马素数）。我们证明，在这些情形中的每一种情形下，(G,H) 还包含具有另一个素数阶的错排，因此 (G,H) 并非几乎难以捉摸。

首先，假设 $H = A_{n-2} \times S_2$。若 $n = 2^m$，则 G 中任何循环型为 $[2^{n/2}]$ 的对合都是错排（因为 $n/2$ 是偶数）。类似地，若 $n = 2^m + 1$ 是费马素数，则 G 中任何循环型为 $[2^{(n-1)/2}, 1]$ 的对合都是错排（因为 $(n-1)/2$ 是偶数）。

在证明的其余部分，我们可以假设对于某个 $1 \leqslant k \leqslant (n-2)/2$，有 $H = S_k \times S_{n-2-k} \times S_2$。在共轭意义下，$H$ 是下列划分的稳定子

$$\{1, \ldots, k\} \cup \{k+1, \ldots, n-2\} \cup \{n-1, n\}.$$

假设 $k \geqslant 4$。根据命题 3.6] ，存在一个素数 $s > k$，它整除 $\binom{n-2}{k}$，这意味着对于某个 $t \in \{0, 1, \ldots, k-1\}$，$s \neq r$ 和 s 整除 $n-2-t$。因此，G 中任何循环型为 $[s^{(n-2-t)/s}, 1^{t+2}]$ 的元素都是错排。现在假设 $k = 1$ 或 2。令 s 为 $n-2$ 的一个奇素因子。那么 G 中任何循环型为 $[s^{(n-2)/s}, 1^2]$ 的元素都是错排。最后，假设 $k = 3$。首先假设 $n = 2^m$，且 $n-1$ 是梅森素数。那么任何循环型为 $[2^{n/2}]$ 的元素都是错排。现在假设 $n = r = 2^m + 1$ 是费马素数。那么 $n - 2 = 2^m - 1$ 是奇数，并且根据引理 4.3，存在一个素数 $s \geqslant 5$，使得 s 整除 $n-2$（回忆 $n > 20$）。因此，G 中任何循环型为 $[s^{(n-2)/s}, 1^2]$ 的元素都是错排。结论得证。□

这就完成了定理 4 的证明，也完成了拟本原几乎难以捉摸群的分类。

5. Proof of Corollaries 5 and 6

本节将证明推论 5 和 6。

5.1. 推论 5 的证明。设 $G \leqslant \mathrm{Sym}(\Omega)$ 是一个以 G_0 为底群、点稳定子为 H 的拟本原几乎难以捉摸置换群。仿射群的情形显然成立。因此，根据定理 3 和 4，我们可以假设 G 是一个几乎单群，且 (G,H) 是表 A1、A2、B1 或 B2 中记录的情形之一。利用计算方法计算 G 的次数，可以轻松处理表 A2 和 B2 中的情形。因此，剩下的任务是处理表 A1 和 B1 中的情形。设 s 是唯一一个由素数阶错排构成的 G-共轭类中元素的阶。

假设 (G,H) 列于表 A1。所有情形的证明都类似，因此我们只展示情形 U1、L4 和 A2 的详细证明（注意，关于经典群的阶，我们采用 [30, 第 3 章和 4] ）。

首先，假设 (G,H) 属于表 A1 中的情形 U1。此处 $G = \mathrm{U}_n(q).[2f]$，其中 $q = 2^f$为偶数，$n \geqslant 5$ 是 $q+1$ 的一个素因子，且 $s = 2nf + 1$ 是 $q^{2n} - 1$的唯一一个本原素因子。此外，H 是自然模的一个一维非退化子空间的稳定子。由 [30, 命题 4.1.4] ，可得

$$|G_0| = \frac{1}{n} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - (-1)^i) \text{ and } |H_0| = \frac{1}{n} q^{(n-1)(n-2)/2} \prod_{i=1}^{n-1} (q^i - (-1)^i).$$

由于 s 是 $q^{2n} - 1$的唯一一个本原素因子，由 [25, 注 2.10] ，我们可推得

$$|\Omega| = q^{n-1} \frac{q^n + 1}{q+1} = q^{n-1}.n.s^l$$

对某个 $l \geqslant 1$成立。因此，结果由 $s = 2nf + 1 > n$成立而得。

接下来，假设 (G,H) 属于表 A1 中的情形 L4。则 $G = \mathrm{PGL}_2(p)$，且 $H = D_{2(p-1)}$，其中 $s = p = 2^m - 1$ 是梅森素数。这里 $|G| = 2^m p(p-1)$，且 $|H| = 2(p-1)$。因此 $|\Omega| = 2^{m-1}p$。由于 $p \geqslant 7$，结论成立。最后，假设 (G,H) 属于表 A1 中的情形 A2。则 $G = S_n$，且 $H = S_{n-2} \times S_2$，其中 $n = 2^m = s+1$。因此 $|\Omega| = (n(n-1))/2 = 2^{m-1}s$。由于 $s > 2$，结论成立。

最后，假设 (G, H) 记录在表 B1 中。首先假设 (G, H) 属于情形 II 或 III。则 $G = \mathrm{L}_2(p)$ 或 $\mathrm{PGL}_2(p)$，其中 $p = 2^m - 1$ 是梅森素数，且$H = C_p{:}C_d$，其中 d 是 $k(p-1)/2$ 的真因子，且 $\alpha(d) = \alpha(k(p-1)/2)$，其中$k = |G : G_0|$。这里 $s = 2$，且 $|\Omega| = 2^{m-1}k(p-1)/d$。因此，2 不是 $|\Omega|$ 的最大素因子，因为 $(p-1)/d$ 能被一个奇素数整除。接下来，假设 (G, H) 属于情形 I。则 $G = \mathrm{PGL}_2(p)$，其中 $s = p = 2^m + \epsilon$ 是素数，且 $\epsilon = \pm 1$。此外，$H = D_{2d}$，其中 d 是 $p + \epsilon$ 的真因子，且 $\alpha(d) = \alpha(p + \epsilon)$。因此$|\Omega| = 2^{m-1}p(p + \epsilon)/d$。由于 $p + \epsilon$ 的所有素因子都小于 p，我们得出 p 是 $|\Omega|$的最大素因子。最后，假设 (G, H) 属于情形 IV。这里$G = \mathrm{L}_2(p)$，其中 $p = 2.3^a - 1$ 是一个素数，满足 $a \geqslant 2$，且 $H = C_p{:}C_d$，其中 d 是 $(p-1)/2$ 的真因子，且 $\alpha(d) = \alpha((p-1)/2)$。这里 $s = 3$，且 $|\Omega| = 3^a.(p-1)/d$。因此显然，3 不是 $|\Omega|$ 的最大素因子，当且仅当 $(p-1)/d$ 有一个奇素因子。□

5.2. 推论6的证明。设 G 是底群为 G_0 的一个几乎单群，并假设$D_G \geqslant 2$。设 H 是一个非极大无核子群，满足 $G = G_0H$，且(G, H)几乎难以捉摸。根据定理 4，我们可以假设 G 是表 B1 或表 B2 中列出的群之一。

首先考虑表 B2 中的情形。在每种情形下，我们都可以使用 Magma精确计算 D_G，采用与命题 4.7 的证明中类似的技巧。最后，假设 G 是表 B1 中的群之一。这些情形的分析非常相似，因此我们只详细说明 $G = \mathrm{PGL}_2(p)$且 $p = 2^m - 1$ 是梅森素数的情形。在这种情形下，(G, H)几乎难以捉摸，当且仅当 $H = D_{2d}$ 或 $C_p{:}C_d$，其中 d 是$p - 1$ 的一个真因子，且 $\alpha(d) = \alpha(p-1)$。在这两种情形下，很容易看出

$$d_G(H) = \omega(p-1) - \omega(d) + 1.$$

例如，取 $H = C_p{:}C_d < M = C_p{:}C_{p-1}$，其中 M 是 G的一个 Borel 子群。我们可以通过构造一条以 M 为起点的子群链，并不断取素数指数子群，来计算 H 的深度；链中的每个子群均具有 $C_p{:}C_t$的形式，其中 t 是 $p - 1$ 的真因子，且 $\alpha(t) = \alpha(p-1)$。因此

$$D_G = \max d_G(H) = d_G(D_{2e}) = d_G(C_p{:}C_e)$$

其中 e 是 $p - 1$的不同素因子的乘积。也就是说，$\omega(e) = \pi(p-1)$，由此我们得出 $D_G = \omega(p-1) - \pi(p-1) + 1$，与推论的第 (ii) 部分相同。□

6. Tables

在最后这一节中，我们列出本文中一直提及的拟本原几乎难以捉摸群的表。首先，我们简要介绍如何阅读表A1和表A2。

注6.1。这里，$G \leqslant \mathrm{Sym}(\Omega)$ 是一个底群为 G_0、点稳定子为 H 的几乎单置换群。

(a) 两张表中都记录了 H 的类型。对于交错群，这描述了 H 的确切结构。当 G_0 是经典群时，我们还会记录包含 H 的 Aschbacher类。对于几何类（标记为 $\mathcal{C}_1$，...，$\mathcal{C}_8$ 的类），该类型给出 $H \cap \mathrm{PGL}(V)$ 的近似结构，其中 V 是 G_0 的自然模；而对于非几何类（记作 $\mathcal{S}$），H 的类型表示 H 的底群。例如，取 $G = \mathrm{L}_n(q)$，并设 H 的类型为 $\mathrm{GL}_1(q) \wr S_n$。那么 H 是 $V = V_1 \oplus \cdots \oplus V_n$ 的直和分解的稳定子，其中对所有 $1 \leqslant i \leqslant n$，$\dim V_i = 1$。此外，我们采用标准记号，用 P_i 表示极大抛物子群，它是 G 中一个 i维全奇异子空间的稳定子，该子空间属于 V。在其他所有情形下，H 的类型描述 $H \cap G_0$ 的结构。

Case	G_0	H 的类型	G	条件	x
U1	$\mathrm{U}_n(q)$ $\mathcal{C}_1$	$\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$	$G_0.J$	参见注 6.2(b)	$2nf+1$
L1	$\mathrm{L}_2(q)$ $\mathcal{C}_1$	P_1	$\mathrm{PGL}_2(q)$ G_0	$q=p=2^m-1$	2A
L2			G_0	$q=p$, $p+1=2.3^a$, $a\geqslant 2$	3
L3			$G_0.f$	参见备注 6.2(c)	r
L4	$\mathcal{C}_2$	$\mathrm{GL}_1(q)\wr S_2$	$\mathrm{PGL}_2(q)$	$q=p=2^m-1$	p
L5	$\mathcal{C}_3$	$\mathrm{GL}_1(q^2)$	$\mathrm{PGL}_2(q)$	$q=p=2^m+1$, $m\geqslant 3$	p
A1	A_n	S_{n-1}	S_n	$n=r^a$, $a\geqslant 1$	$[r^{n/r}]$
A2		$S_{n-2}\times S_2$	S_n	$n=2^m=r+1$	$[r,1]$
A3			S_n	$n=2^m+1=r$	$[r]$
A4		A_{n-1}	A_n	$n=r^a$, $a\geqslant 2$	$[r^{n/r}]$
A5			A_n	$n=2r^a$, $r\geqslant 3$, $a\geqslant 2$	$[r^{n/r}]$

表 A1：本原几乎难以捉摸的几乎单群：第一部分

(b) 标记为 G 的列记录了使 (G,H) 几乎难以捉摸的群 G 。此外，表中所列条件是对 G_0 的单性和 H 的极大性所需条件的补充（见 [30, 第 3 节.5]）。

(c) 在最后一列中，我们描述了 G 中唯一的素数阶错排共轭类。如果 G 中给定素数阶的元素只有一个 G-类，则用相应的素数表示该类。然而，如果给定素数阶的元素有多个共轭类，我们就会具体描述该类。例如，若 $G_0=\mathrm{U}_3(3)$，且 H 的类型为 $\mathrm{L}_2(7)$，则 G_0 包含两个阶为 3 的元素 G-类。如表中所示，这些错排在 V 上的若尔当标准形为 $[J_2,J_1]$，其中 J_i 表示大小为 i 的标准幺幂块。

类似地，若 $G=\mathrm{U}_4(2).2$，且 H 的类型为 $\mathrm{Sp}_4(2)$，则 G 有三个阶为 3 的元素 G- 类，分别标记为 3A 、 3C 和 3D，其中 $|3\mathrm{A}|=80$ 、 $|3\mathrm{C}|=240$ 和 $|3\mathrm{D}|=480$ ；错排属于 3A。 $G_0=\mathrm{PSp}_6(2)$ 且 H 的类型为 $\mathrm{O}_6^+(2)$，以及 $G_0={}^2F_4(2)'$ 且 H 的类型为 $\mathrm{L}_2(25)$ 的情形也类似。在表 A1 的情形 L1 中， G 内对合错排的 2A 类恰好是 G_0 中唯一的对合类。

最后，对于交错群和对称群，我们用元素的循环结构来表示共轭类。例如，在情形 (G,H) =(A_6,$\mathrm{L}_2(5)$) 中，唯一的素数阶错排共轭类中的元素具有循环型 $[3,1^3]$。

注 6.2. 这里我们对表A1和表A2中出现的情形补充一些说明。

(a) 根据以下同构关系

$$\mathrm{L}_2(4)\cong\mathrm{L}_2(5)\cong A_5,\ \mathrm{L}_2(9)\cong A_6,\ \mathrm{L}_2(7)\cong\mathrm{L}_3(2),$$

$$\mathrm{U}_4(2)\cong\mathrm{PSp}_4(3),\ G_2(2)'\cong\mathrm{U}_3(3),\ {}^2G_2(3)'\cong\mathrm{L}_2(8),$$

这些表是完整的。有关低维李型群与交错群之间同构的完整列表，参见 [30,命题 2.9.2 和定理 5.1。1]

(b) 对于表 A1 中的 U1 情形，还有一些附加条件。首先，我们注意到$G_0=\mathrm{U}_n(q)$，并满足数论限制，即 $q=2^f$ 为偶数， $n\geqslant 5$是 $q+1$ 的一个素因子，且 $2nf+1$ 是 $q^{2n}-1$的唯一一个本原素因子。此外， $G=G_0.J$ ，其中 $J\leqslant\mathrm{Out}(G_0)=\langle\ddot{\delta}\rangle{:}\langle\ddot{\phi}\rangle$， $J\cap\langle\ddot{\delta}\rangle=1$ ，且J 映射到 $\langle\phi\rangle$。这里我们用 δ 和 ϕ 分别表示 $\mathrm{Aut}(G_0)$ 中阶为 n 的对角自同构和阶为 $2f$ 的域自同构（参见 [3,

G_0		类型： H	G	x
$\mathrm{L}_3(4)$	$\mathcal{C}_1$	$\mathrm{GL}_1(4) \oplus \mathrm{GL}_2(4)$	$G_0.2_1$, $G_0.2_3$, $G_0.2^2$	7
	$\mathcal{C}_5$	$\mathrm{GL}_3(2)$	$G_0.2_1$, $G_0.2_2$, $G_0.2^2$	5
	$\mathcal{S}$	A_6	$G_0.2_3$	7
$\mathrm{L}_2(8)$	$\mathcal{C}_1$	P_1	$G_0.3$, G_0	3
	$\mathcal{C}_2$	$\mathrm{GL}_1(q) \wr S_2$	$G_0.3$, G_0	3
	$\mathcal{C}_3$	$\mathrm{GL}_1(q^2)$	$G_0.3$	7
$\mathrm{U}_6(2)$	$\mathcal{C}_5$	$\mathrm{Sp}_6(2)$	$G_0.2$	11
	$\mathcal{S}$	$\mathrm{U}_4(3)$	$G_0.2$	11
$\mathrm{U}_5(2)$	$\mathcal{C}_1$	$\mathrm{GU}_1(2) \perp \mathrm{GU}_4(2)$	$G_0.2$	11
	$\mathcal{C}_2$	$\mathrm{GU}_1(2) \wr S_5$	$G_0.2$	11
$\mathrm{U}_4(3)$	$\mathcal{C}_1$	P_2	$G_0.2_2$	7
$\mathrm{U}_4(2)$	$\mathcal{C}_1$	P_1	$G_0.2$, G_0	5
	$\mathcal{C}_2$	$\mathrm{GU}_1(2) \wr S_4$	$G_0.2$, G_0	5
	$\mathcal{C}_5$	$\mathrm{Sp}_4(2)$	$G_0.2$	3A
$\mathrm{U}_3(3)$	$\mathcal{C}_1$	P_1	$G_0.2$	7
	$\mathcal{S}$	$\mathrm{L}_2(7)$	$G_0.2$, G_0	$[J_2, J_1]$
$\mathrm{U}_3(4)$	$\mathcal{C}_1$	$\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$	$G_0.4$	13
	$\mathcal{C}_2$	$\mathrm{GU}_1(q) \wr S_3$	$G_0.4$	13
$\mathrm{U}_3(8)$	$\mathcal{C}_1$	$\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$	$G_0.6$	19
$\mathrm{PSp}_6(2)$	$\mathcal{C}_1$	$\mathrm{Sp}_2(2) \perp \mathrm{Sp}_4(2)$	G_0	7
	$\mathcal{C}_8$	$\mathrm{O}_6^+(2)$	G_0	3B
	$\mathcal{C}_8$	$\mathrm{O}_6^-(2)$	G_0	7
$\mathrm{PSp}_4(7)$	$\mathcal{C}_1$	P_2	$G_0.2$, G_0	5
${}^2F_4(2)'$		$\mathrm{L}_2(25)$	$G_0.2$, G_0	2A
		$5^2{:}4A_4$	$G_0.2$	13
$G_2(4)$		J_2	$G_0.2$	13
A_{10}		$(S_7 \times S_3) \cap G$	G_0	$[5^2]$
A_9		$(S_7 \times S_2) \cap G$	$G_0.2$, G_0	$[3^3]$
		$(S_6 \times S_3) \cap G$	$G_0.2$, G_0	$[7, 1^2]$
A_6		$S_3 \wr S_2$	$G_0.2 = S_6$	$[5, 1]$
		$\mathrm{L}_2(5)$	G_0	$[3, 1^3]$
		D_{20}	$G_0.2 = \mathrm{PGL}_2(9)$	3
		$5{:}4$	$G_0.2 = \mathrm{M}_{10}$	3
		$3^2{:}Q_8$	$G_0.2 = \mathrm{M}_{10}$	5
A_5		D_{10}	G_0	$[3, 1^2]$

表 A2：本原几乎难以捉摸的几乎单群：第二部分

第 1 节.7])，并沿用 [30]，对于 $\mathrm{Aut}(G_0)$ 中的任意元素 $x \in$，我们用 $\ddot{x}$ 表示陪集 $G_0x \in \mathrm{Out}(G_0) = \mathrm{Aut}(G_0)/G_0$。正如 [25, 备注 1] 中所解释的，我们预计这种情形不会出现任何真正的例子。有关这种情形的详细信息，请参见 [25, 第 5.2 节.3]。

(c) 考虑表 A1 中的情形 L3。存在两个形如 $G_0.f$ 的群，分别为 $G_0.\langle\delta\phi\rangle$ 和 $G_0.\langle\phi\rangle$，其中 ϕ 是阶为 f 的域自同构，δ 是阶为 2 的对角自同构。此外，我们还要求 $q = p^f = 2r^a - 1$，其中 $r = 2^m + 1$ 是费马素数，$m \geqslant 2$ 是 2 的幂，$a \geqslant 1$ 且 $f = 2^{m-1}$。引理 4.12 证明了这些数论条件蕴含 $q = 9$ 或 49。

(d) 对于表 A2 中包含 $G_0 = \mathrm{L}_3(4)$ 的情形，标记为 G 的列中所记录的群采用 Atlas 记号 [47] 定义。也就是说，$G_0.2_1 = \mathrm{L}_3(4).\langle\iota\phi\rangle$、$G_0.2_2 = \mathrm{L}_3(4).\langle\phi\rangle$、$G_0.2_3 = \mathrm{L}_3(4).\langle\iota\rangle$ 和 $G_0.2^2 = \mathrm{L}_3(4).\langle\iota, \phi\rangle$，其中 ι 表示

Case	G	H	条件	$\alpha(d)$	x
I	$\mathrm{PGL}_2(p)$	D_{2d}	$p=2^m+\epsilon$, $m>2$	$\alpha\ (p+\epsilon)$	p
II		$C_p{:}C_d$	$p=2^m-1$	$\alpha(p-1)$	2
III	$\mathrm{L}_2(p)$	$C_p{:}C_d$	$p=2^m-1$	$\alpha(\frac{p-1}{2}\ )$	2
IV		$C_p{:}C_d$	$p=2.3^a-1$, $a\geqslant 2$	$\alpha(\frac{p-1}{2}\ )$	3

表 B1：一些拟本原几乎难以捉摸群

G	H	M	a	b	c	x
M_{10}	$3^2{:}4$	$3^2{:}Q_8$	2	2	2	5
A_9	$(A_5\times 3){:}2^\dagger$	$(A_6\times 3){:}2$	2	1	2	7
S_9	$S_5\times S_3{}^\dagger$	$S_6\times S_3$	2	1	2	7
$\mathrm{L}_2(8).3$	$S_3\times 3$	$D_{18}{:}3$	1	1	2	7
$\mathrm{L}_2(49).2_3$	$7^2{:}(3\times Q_8)$	$7^2{:}(3\times Q_{16})$	2	2	2	5
	$7^2{:}12$	$7^2{:}(3\times Q_{16})$	2	2	3	5
$\mathrm{U}_3(3).2$	$3.(S_3\wr 2)$	$(3^{1+2}{:}8).2$	1	1	2	7
	$3.S_3^2$	$(3^{1+2}{:}8).2$	1	1	3	7
	S_3^2	$(3^{1+2}{:}8).2$	1	1	4	7
$\mathrm{U}_4(2)$	$S_3^2{:}S_3$	$3^3.S_4$	1	1	2	5
	$3\times S_3^2$	$3^3.S_4$	1	1	3	5
	$6\times S_3$	$3^3.S_4$, $2^{1+4}{:}\mathrm{SU}_2(2){:}3$	1	1	4	5
	$\mathrm{SL}_2(3){:}A_4$	$2^{1+4}{:}\mathrm{SU}_2(2){:}3$	1	1	2	5
$\mathrm{U}_4(2).2$	$S_3\times(S_3\wr 2)$	$3^3{:}S_4\times 2$	1	1	2	5
	S_3^3	$3^3{:}S_4\times 2$	2	1	3	5
	$2\times S_3^2$	$3^3{:}S_4\times 2$, $2_3{:}A_4.D_{12}$	3	1	4	5
	$2^{1+4}{:}\mathrm{SU}_2(2){:}3$	$2^3{:}A_4.D_{12}$	1	1	2	5
$\mathrm{U}_5(2).2$	$S_3\times S_6$	$(3\times\mathrm{SU}_4(2)){:}2$	1	1	2	11
$\mathrm{PSp}_6(2)$	$S_5\times\mathrm{Sp}_2(2)^\dagger$	$S_6\times\mathrm{Sp}_2(2)$	2	1	2	7

表 B2：散在拟本原几乎难以捉摸群。

逆转置图自同构，而 ϕ 表示阶为 2 的域自同构。表 A2 中包含 $G_0=\mathrm{U}_4(3)$ 的情形也类似。此处 $G_0.2_2=\mathrm{U}_4(3).\langle\gamma\rangle$，其中 γ 是对合图自同构，且 $C_{G_0}(\gamma)=\mathrm{PSp}_4(3)$。最后，对于 $G={}^2F_4(2)$ 且 H 属于 $\mathrm{L}_2(25)$ 型的情形，我们注意到 $H=\mathrm{L}_2(25).2_3$。我们用 $\mathrm{L}_2(25).2_3$ 表示 $\mathrm{L}_2(25).\langle\delta\phi\rangle$，其中 δ 和 ϕ 分别是标准的对合对角自同构和域自同构（例如参见 [3, 第 1.7] 节）。

注 6.3。这里我们对表B1和表B2作一些说明。

（a）对于这两张表，在标为 G 的列中，我们记录了所关注的几乎单群。标为 H 的列记录了G 的核自由非极大子群（按同构分类），其中(G,H)是几乎难以捉摸的。此外，标为 x 的列给出了唯一的素数阶错排共轭类。请注意，该类以相应的素数 r表示，因为在所有情况下，G中阶为 r的元素都构成唯一的共轭类。

(b) 在表 B2 中，标记为 a 的列记录了 G 中满足 $G=G_0K$ 和 $H\cong K$ 的子群的 G 类的数量；b 记录了这些 G 类中满足 (G,K) 几乎难以捉摸的类的数量，而 $c=d_G(H)$ 表示 H 的深度（见推论6）。此外，在标记为 M 的列中，我们记录了

包含至少一个满足 $G = G_0K$、 $H \cong K$ 的 G 的子群 K，且 (G, K) 几乎难以捉摸的 G 的极大子群的 G 类的代表元。(c) 对于表 B1， p 表示一个素数；并提醒读者，对于正整数 t，我们用 $\alpha(t)$ 表示 t 的不同素因子的集合。(d) 在表 B2 中， † 表示 H 的相关 A_5 或 S_5 子群是对应的 A_6 或 S_6 子群的本原子群。(e) 在表 B2 中，我们写作 $G = \mathrm{L}_2(49).2_3 = \mathrm{L}_2(49).\langle\delta\phi\rangle$，其中 δ 和 ϕ 分别表示 G_0 的标准对合对角自同构和域自同构（见 [3, 第 1.7] 节）。

References

[1] M. A. Bennett 和 A. Levin, *The Nagell-Ljunggren equation via Runge's method*, Monatsh. Math. 177 (2015), 第 1 期, 15–31。[2] W. Bosma、J. Cannon 和 C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comput. 24 (1997), 235–265。[3] J. N. Bray、D. F. Holt 和 C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups* 407, , 伦敦数学学会讲义系列, 第 Cambridge University Press 卷, 剑桥, 2013。[4] T. C. Burness 和 M. Giudici, *Classical groups, derangements and primes*, 澳大利亚数学学会讲义系列, 第 25 卷, 剑桥大学出版社, 2016。[5] T. C. Burness、M. Giudici 和 R. A. Wilson, *Prime order derangements in primitive permutation groups* **341** 2011 158 178 , J. Algebra () , –。[6] T. C. Burness、R. M. Guralnick 和 S. Harper, *The spread of a finite group*, Ann. of Math. (2) 193 (2021), 第2期, 619–687。[7] T. C. Burness 和 E. V. Hall, *Almost elusive permutation groups*, J. Algebra 594 (2022), 519–543。[8] T. C. Burness 和 H. P. Tong-Viet, *Derangements in primitive permutation groups with an appli-* , , Quart. J. *cation to character theory* **66** 2015 63 96 Math. () , –。[9] T. C. Burness 和 H. P. Tong-Viet, *Primitive permutation groups and derangements of prime power order* **105** 2016 255 291 , Manuscripta Math. () , –。[10] P. J. Cameron, *Permutation groups*, 伦敦数学学会学生教材, 45, 剑桥大学出版社, 剑桥, 1999。[11] P. J. Cameron、M. Giudici、G. A. Jones、W. M. Kantor、M. H. Klin、D. Maruˇsiˇc 和 L. A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. 66 (2002), 325–333。[12] A. M. Cohen、M. W. Liebeck、J. Saxl 和 G. M. Seitz, *The local maximal subgroups of exceptional groups of Lie type* **64** 1992 21 48 , Proc. London Math. Soc. () , –。[13] B. N. Cooperstien, *Maximal subgroups of* $G_2(2^n)$, J. Algebra 70 (1981), 23–36。[14] D. A. Craven, *Alternating subgroups of exceptional groups of Lie type*, Proc. Lond. Math. Soc. 115 (2017), 449–501。[15] D. A. Craven, *On indecomposable Lie primitive and maximal subgroups of exceptional groups of Lie type* 2102 11096 , 2021 , arXiv: . . [16] D. A. Craven, *Maximal* PSL_2 *subgroups of exceptional groups of Lie type*, Mem. Amer. Math. Soc., 即将出版。[17] D. A. Craven, *The maximal subgroups of the exceptional groups* $F_4(q)$ $E_6(q)$ *and* ${}^2E_6(q)$ *and related almost simple groups* 2103 04869, 2021 () () () , arXiv: . . [18] D. I. Deriziotis 和 G. O. Michler, *Character table and blocks of finite simple triality groups* ${}^3D_4(q)$, Trans. Amer. Math. Soc. 303 (1987), 第 1 期, 39–70。[19] J. D. Dixon 和 B. Mortimer, *Permutation groups*, 数学研究生教材, 163。Springer-Verlag, 纽约, 1996。[20] B. Fein、W. M. Kantor 和 M. Schacher, *Relative Brauer groups II*, J. Reine Agnew. Math. 328 (1981), 39–57。[21] D. A. Foulser, *The flag-transitive collineation groups of the finite Desarguesian affine planes*, Canadian J. Math. 16 (1964), 443–472。[22] M. Giudici, *Quasiprimitive groups with no fixed point free elements of prime order*, J. Lond. Math. Soc. 67 (2003), 73–84。[23] D. Gorenstein, R. Lyons 和 R. Solomon, *The Classification of the Finite Simple Groups. Number 3* 40 , 数学调查与专著, 第 . 卷。美国数学会, 普罗维登斯, 罗得岛州（1998）。[24] R. M. Guralnick, *Conjugacy classes of derangements in finite transitive groups*, Proc. Steklov Inst. Math. 292 (2016), 112–117。

[25] E. V. Hall, *Almost exclusive classical groups*, 纯粹与应用代数杂志 226 (2022), 第11期, 论文编号 107086。[26] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order II* **93** 1985 151 164 , , J. Algebra（）–。[27] C. Jordan, *Recherches sur les substitutions*, 纯粹与应用数学杂志（Liouville）17 (1872), 351–367。[28] P. B. Kleidman, *The maximal subgroups of the Steinberg triality groups ${}^3D_4\ q$ and of their automorphism groups* **115** 1988 1, 182 199 （）, J. Algebra（）, 第 – 期。[29] P. B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2\ q$ with q odd the Ree groups ${}^2G_2\ q$ and their automorphism groups* **117** 1988 1, 30 71 （）, （）, J. Algebra（）, 第 – 期。[30] P. B. Kleidman 和 M. W. Liebeck, *The subgroup structure of the finite classical groups*, 伦敦数学学会讲义系列, 第 129 卷, 剑桥大学出版社, 1990。[31] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, 代数通讯 23 (1995), 第 11 期, 4125–4156。[32] R. Lidl 和 H. Niederreiter, *Finite Fields*, 数学及其应用百科全书, 20。剑桥大学出版社, 剑桥, 1997。[33] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. (3) 54 (1987), 第 3 期, 477–516。[34] M. W. Liebeck、C. E. Praeger 和 J. Saxl, *Transitive subgroups of primitive permutation groups*, J. Algebra 234 (2000), 291–361。[35] M. W. Liebeck、J. Saxl 和 G. M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type* **65** 1992 297 325 , Proc. London Math. Soc.（）, –。[36] M. W. Liebeck 和 G. M. Seitz, *A survey of maximal subgroups of exceptional groups of Lie type*, 《群、组合学与几何》（达勒姆, 2001）, 139–146, World Sci. Publ., River Edge, NJ, 2003。[37] M. W. Liebeck 和 G. M. Seitz, *On finite subgroups of exceptional algebraic groups*, J. reine angew. Math. 515 (1999), 25–72。[38] A. J. Litterick, *On non-generic finite subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. 253 (2018), 第 1207 期, v+156 页。[39] G. Malle, *The maximal subgroups of ${}^2F_4(q^2)$*, J. Algebra 139 (1991), 第 1 期, 52–69。[40] G. Malle 和 D. Testerman, *Linear algebraic groups and finite groups of Lie type*, 剑桥高等数学研究, 133。剑桥大学出版社, 剑桥, 2011。[41] C. E. Praeger, *An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs* **47** 1993 227 239 , J. London Math. Soc.（）, –。[42] J. -P. Serre, *On a theorem of Jordan*, 美国数学会通报 40 (2003), 429–440。[43] K. Shinoda, *The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic 2* **21** 1974 133 159 （）, 东京大学理学部学报 Sect. I A Math.（）, –。[44] T. Shoji, *The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic $p \neq 2$* **21** 1974 1 17 （）, 东京大学理学部学报 Sect. IA Math.（）, –。

[45] *On a class of doubly transitive groups* **75** 1962 105 145 M. Suzuki, , 数学年刊

[46] ´ *Maximal subgroups of direct products.* **198** 1997 352 361 （）, – J. Thevenaz, J. Algebra（）, –。[47] R. A. Wilson 等, *A World-Wide-Web Atlas of finite group representations*, http://brauer.maths.qmul.ac.uk/Atlas/v3/。[48] H. Zhu、M. Le 和 A. Togb´e, *On the exponential Diophantine equation $x^2 + p^{2m} = 2y^n$*, 澳大利亚数学会通报 86 (2012), 303–314。[49] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. F¨ur Math. u. Phys. 3 (1892) 265–284。

E.V. Hall, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: ky19128@布里斯托.ac.uk