Matrix Multiplication via Matrix Groups

Jonah Blasiak
Department of Mathematics, Drexel University, Philadelphia, PA, USA

Henry Cohn
Microsoft Research New England, One Memorial Drive, Cambridge, MA, USA

Joshua A. Grochow
Departments of Computer Science and Mathematics, University of Colorado Boulder, CO, USA

Kevin Pratt
School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA

Chris Umans
Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA, USA

Abstract

In 2003, Cohn and Umans proposed a group-theoretic approach to bounding the exponent of matrix multiplication. Previous work within this approach ruled out certain families of groups as a route to obtaining $\omega = 2$, while other families of groups remain potentially viable. In this paper we turn our attention to matrix groups, whose usefulness within this framework was relatively unexplored.

We first show that groups of Lie type cannot prove $\omega = 2$ within the group-theoretic approach. This is based on a representation-theoretic argument that identifies the second-smallest dimension of an irreducible representation of a group as a key parameter that determines its viability in this framework. Our proof builds on Gowers' result concerning product-free sets in quasirandom groups. We then give another barrier that rules out certain natural matrix group constructions that make use of subgroups that are far from being self-normalizing.

Our barrier results leave open several natural paths to obtain $\omega = 2$ via matrix groups. To explore these routes we propose working in the continuous setting of Lie groups, in which we develop an analogous theory. Obtaining the analogue of $\omega = 2$ in this potentially easier setting is a key challenge that represents an intermediate goal short of actually proving $\omega = 2$. We give two constructions in the continuous setting, each of which evades one of our two barriers.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Fast matrix multiplication, representation theory, matrix groups

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.19

Funding We thank the American Institute of Mathematics for a SQuaRE grant.
Jonah Blasiak: NSF grant DMS-1855784.
Joshua A. Grochow: NSF CAREER award CISE-2047756.
Chris Umans: NSF grant CCF-1815607 and a Simons Foundation Investigator award.

1 Introduction

The exponent of matrix multiplication is the smallest number ω such that for each $\varepsilon > 0$, there exists an algorithm for multiplying two $n \times n$ matrices using $O(n^{\omega+\varepsilon})$ field operations. It is clear that $\omega \geq 2$, and a long line of work has led to the best upper bound currently known of $\omega < 2.37286$ from [3]. It is a longstanding and well-known open problem to resolve the conjecture that $\omega = 2$.

In [11] a group-theoretic approach to bounding ω was proposed. Given any finite group G and three subsets of G satisfying a certain condition (the *triple product property*), this approach yields an upper bound on ω by reducing an instance of matrix multiplication

14th Innovations in Theoretical Computer Science Conference (ITCS 2023).
Editor: Yael Tauman Kalai; Article No. 19; pp. 19:1–19:16
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

to multiplication in the group algebra of G. This approach can capture the Coppersmith–Winograd family of algorithms [10], which includes the current record bound. While some barriers are known for the group-theoretic approach, for instance that abelian groups cannot not prove $\omega < 3$ (see [11, Lemma 3.1]) or that certain generalizations of the constructions in [10] cannot achieve $\omega = 2$ [6, 7, 18], the possibility that one could show $\omega = 2$ using a suitable family of nonabelian groups remains wide open.[1]

Previous work on the group-theoretic approach has focused mainly on families of very *non-simple* groups, i.e., groups built up from simple groups through repeated group extension. For example, the best bounds known on ω can be obtained using a semidirect product of the symmetric groups with direct products of abelian groups. At the same time, the aforementioned barriers rule out these kinds of constructions and certain generalizations [6, 7, 18]. But this has left the simple groups – in some sense the opposite end of the spectrum of finite groups – largely unexplored.

In this paper we address this gap in knowledge by studying *finite groups of Lie type*[2] in the framework of [11]. This is an important class of groups that contains all of the finite simple groups except alternating or cyclic groups and finitely many sporadic groups. Some good examples to keep in mind are the classical matrix groups such as the group $\mathrm{SL}(n, q)$ of determinant 1 matrices over the finite field $\mathbb{F}_q$ or the group of $n \times n$ orthogonal matrices over $\mathbb{F}_q$ with respect to a quadratic form.

1.1 Results

We start by showing that triple product property[3] constructions (see Definition 2.1) in groups of Lie type cannot prove any bound on ω better than $2 + \varepsilon$ for some absolute constant $\varepsilon > 0$ (Corollary 3.5). This resolves a question asked in [11]. Our proof combines a representation-theoretic argument with known bounds on the dimension and number of irreducible representations in groups of Lie type [15, 12]. More broadly, we identify the second-smallest dimension of an irreducible representation as a key parameter of a group that determines its viability for the approach of [11]: Theorem 3.2 shows that groups where this quantity is large cannot yield good bounds on ω. For example, any family of groups for which the second-smallest dimension of an irreducible representation grows as a power of the size of the group cannot yield $\omega = 2$. It had been known since [11] that the largest dimension played a key role in the quality of the bound, but small dimensions were not previously understood to be relevant.

This first barrier builds on Gowers' theorem on product-free sets in quasirandom groups [13]. We note that whereas Gowers' result involves the minimum dimension of a *nontrivial* representation, the additional structure of our problem allows us to consider the second-smallest dimension of an irreducible representation (in other words, we can skip any other representations of dimension 1). This gives us lower bounds in groups where Gowers'

[1] Other barrier results rule out different generalizations of the Coppersmith–Winograd approach, such as [4, 2, 1, 9], but it remains unclear the extent of the implications those barriers have for the group-theoretic approach.

[2] Specifically, by a group of Lie type we mean any one of the (possibly twisted) Chevalley groups, including the Suzuki and Ree groups, or the quotient of such a group by its center. A Chevalley group is the fixed points of a Steinberg endomorphism in a semisimple algebraic group over a finite field (see Definition 21.6 and Table 22.1 in [17]). Among others, this list includes $\mathrm{SL}(n, q)$, $\mathrm{SU}(n, q)$, $\mathrm{SO}(2n + 1, q)$, $\mathrm{Sp}(2n, q)$, $\mathrm{SO}^+(2n, q)$, and $\mathrm{SO}^-(2n, q)$. Obtaining simple groups can require taking the quotient by the center, but that does not change our conclusions, such as Corollary 3.5.

[3] We note in Remark 3.3 that similar barriers hold for simultaneous triple product property constructions, as defined in [10, Definition 5.1].

result does not apply, such as $\mathrm{SL}(n,q)$. It is interesting that while triple product property constructions in abelian groups cannot yield nontrivial bounds on ω, this barrier shows that *highly nonabelian* groups also have significant limitations.

Next we show in Theorem 3.7 that subgroups with large normalizers cannot be used in a triple product property construction to obtain $\omega = 2$. This barrier is particularly effective in the setting of matrix groups. For example, one cannot obtain $\omega = 2$ via a triple product property construction using three subgroups inside $\mathrm{GL}(n,q)$ for varying q and any fixed n, or even inside products of such groups.

Our first barrier result rules out obtaining exponent 2 from finite groups of Lie type, but still leaves open the possibility that such groups could serve as building blocks in efficient algorithms for matrix multiplication. For example, the *direct product* of such groups escapes the barrier entirely, since the second-smallest dimension of an irreducible representation of a direct product equals the second-smallest dimension among the irreducible representations of the factors. Similarly, our normalizer barrier suggests that constructions should aim to use subgroups that are *self-normalizing*. We therefore view our barriers as giving us useful information about what a possible construction using finite groups of Lie type must look like, if it is to give $\omega = 2$.

In the second part of the paper, we give constructions that naturally use a direct product in a critical way (Theorem 4.9), and constructions that use self-normalizing subgroups (Theorem 4.10). It is important to note that we know of *no* constructions in *finite* groups of Lie type that even meet a certain "packing bound" (Definition 2.3), a prerequisite for obtaining $\omega = 2$. This remains an important challenge. In lieu of such constructions, we direct our efforts at obtaining constructions in *continuous* Lie groups, which seems easier and mathematically cleaner to work in, and where we can ask direct analogues of the main questions. Here we have constructions that meet the packing bound. Moreover, we give examples that use direct products and self-normalizing subgroups, desiderata by the barrier results.

Our constructions do not achieve the Lie analogue of beating exponent 3, and we suggest improving them and finding other examples as key challenges highlighted by this work.

1.2 Outline

In the next section we review the group-theoretic approach to bounding ω. In Section 3 we give our barriers. We then introduce the Lie exponent in Section 4 and give our constructions. We conclude with some questions in Section 5.

2 Background

In this section we review the approach of [11] to bounding ω. For a finite group G, let $\mathrm{Irr}(G)$ denote the set of equivalence classes of irreducible complex representations of G, and for $X \subseteq G$, let $Q(X) = \{xx'^{-1} : x, x' \in X\}$ be the quotient set of X and $X^{-1} = \{x^{-1} : x \in X\}$ be its collection of inverses.

▶ **Definition 2.1** ([11, Definition 2.1]). *We say that subsets S, T, and U of a group G satisfy the* triple product property *if for all $s \in Q(S)$, $t \in Q(T)$, and $u \in Q(U)$,*

$$stu = 1 \implies s = t = u = 1.$$

The simplest case is when the three subsets of G are subgroups, in which case we do not need to take their quotient sets since $Q(H) = H$ for every subgroup H. However, the known constructions that achieve nontrivial upper bounds for ω do not use subgroups [10].

Given three subsets of G that satisfy the triple product property, [11] shows how to reduce a matrix multiplication problem to convolution of functions on G (in other words, multiplication in the group algebra $\mathbb{C}[G]$). This reduction yields the following inequality for the exponent of matrix multiplication ω:

▶ **Theorem 2.2** ([11, Theorem 4.1]). *If S, T, and U satisfy the triple product property in G, then*

$$(|S|\,|T|\,|U|)^{\omega/3} \le \sum_i d_i^{\omega},$$

where $d_i \in \mathbb{N}$ are the dimensions of the irreducible representations of G.

If $|S|$, $|T|$, and $|U|$ are large and the dimensions d_i are not too large, then this inequality yields an upper bound for ω. For example, if

$$|S|\,|T|\,|U| > \sum_i d_i^3,$$

then it proves that $\omega < 3$. Using Theorem 2.2, it was shown in [10] that $\omega < 2.41$. In fact, this framework is powerful enough to capture the Coppersmith–Winograd family of algorithms, including the latest record of $\omega < 2.37286$ from [3].

In the notation of Theorem 2.2, we always have $\sum_i d_i^{\omega} \ge \sum_i d_i^2 = |G|$. Thus, the inequality in the theorem never implies a better bound on ω than $(|S|\,|T|\,|U|)^{\omega/3} \le |G|$ would. This inequality is always consistent with $\omega = 2$, because the multiplication maps from $S \times T$, $T \times U$, and $S \times U$ to G must be injective to satisfy the triple product property, and therefore $|S|\,|T|\,|U| \le |G|^{3/2}$. This gives us a necessary condition for proving that $\omega = 2$ via Theorem 2.2:

▶ **Definition 2.3.** *We say a sequence $G_1, G_2, \ldots$ of finite groups* meets the packing bound *if there exist subsets S_i, T_i, and U_i of G_i satisfying the triple product property such that*

$$|S_i|\,|T_i|\,|U_i| = |G_i|^{3/2-o(1)}$$

as $i \to \infty$.

Several families of groups meeting the packing bound were constructed in [11]. In the terminology of [11], meeting the packing bound means the pseudo-exponent of G_i converges to 2 as $i \to \infty$. A simple argument [11, Lemma 3.1] shows that this can happen only if $|G_i| \to \infty$.

Meeting the packing bound is a necessary condition for Theorem 2.2 to yield $\omega = 2$: if a family of groups contains no sequence meeting the packing bound, then there is a constant $\varepsilon > 0$ such that no group in the family can prove an upper bound on ω better than $2 + \varepsilon$ via Theorem 2.2. However, meeting the packing bound is not in itself sufficient to achieve $\omega = 2$, or even $\omega < 3$.

3 Barriers for matrix groups

In this section we explain the two barriers mentioned in the introduction. Each of them is based on an idea that is particularly relevant for matrix groups, although we formulate the bounds in greater generality.

3.1 A representation-theoretic barrier

We begin by proving our representation-theoretic barrier, which we then apply to groups of Lie type. Our proof of Theorem 3.2 follows the Fourier-analytic proof of Gowers' theorem on mixing in quasirandom groups (see, for example, [8, Lemma 2.2]). Our barrier is a function of the second-smallest dimension of an irreducible representation of G. Because we use this parameter frequently, we introduce notation for it:

▶ **Definition 3.1.** *For a finite nonabelian group G, let $n(G) := \min_{\pi \in \mathrm{Irr}(G):\ \dim \pi > 1} \dim \pi$ be the smallest dimension of an irreducible representation of G of dimension greater than* 1.

▶ **Theorem 3.2.** *If subsets S, T, and U satisfy the triple product property in a finite nonabelian group G, then*

$$|S|\,|T|\,|U| \le \frac{|G|^{3/2}}{n(G)^{1/2}} + |G|.$$

Proof. Let 1_X denote the indicator function of a subset $X \subseteq G$. For brevity, given $X \subseteq G$ and $\pi \in \mathrm{Irr}(G)$, we will write $\pi(X) := \sum_{x \in X} \pi(x)$ and $d_\pi := \dim \pi$.

Suppose that S, T, U satisfy the triple product property. Equivalently, the value at the identity in the 6-fold convolution $1_S * 1_{S^{-1}} * 1_T * 1_{T^{-1}} * 1_U * 1_{U^{-1}}$ equals $|S|\,|T|\,|U|$. The Fourier inversion formula says that a function $f\colon G \to \mathbb{C}$ can be reconstructed using the inner product $\langle X, Y\rangle = \mathrm{Tr}(X\overline{Y}^\top)$ (where $\overline{Y}$ denotes the entry-wise complex conjugate) as

$$f(g) = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} d_\pi \left\langle \sum_{h \in G} f(h)\pi(h), \pi(g) \right\rangle.$$

Applying this formula to $f = 1_S * 1_{S^{-1}} * 1_T * 1_{T^{-1}} * 1_U * 1_{U^{-1}}$ and $g = 1$ yields

$$|G|\,|S|\,|T|\,|U| = \sum_{\pi \in \mathrm{Irr}(G)} d_\pi \mathrm{Tr}(\pi(S)\pi(S^{-1})\pi(T)\pi(T^{-1})\pi(U)\pi(U^{-1})).$$

When $d_\pi = 1$,

$$\pi(S)\pi(S^{-1}) = \sum_{s \in S} \pi(s) \sum_{s \in S} \overline{\pi(s)} = |\pi(S)|^2,$$

which is a nonnegative real number, and $\pi(S)\pi(S^{-1}) = |S|^2$ if π is the trivial representation. Thus,

$$\begin{aligned} |G|\,|S|\,|T|\,|U| &\ge (|S|\,|T|\,|U|)^2 + \sum_{\pi:\ d_\pi > 1} d_\pi \mathrm{Tr}(\pi(S)\pi(S^{-1})\pi(T)\pi(T^{-1})\pi(U)\pi(U^{-1})) \\ &= (|S|\,|T|\,|U|)^2 + \sum_{\pi:\ d_\pi > 1} d_\pi \mathrm{Tr}(\pi(S^{-1})\pi(T)\pi(T^{-1})\pi(U)\pi(U^{-1})\pi(S)). \end{aligned}$$

By the Cauchy–Schwarz inequality,

$$|G|\,|S|\,|T|\,|U| \ge (|S|\,|T|\,|U|)^2 - \sum_{\pi:\ d_\pi > 1} d_\pi \|\pi(S^{-1}T)\| \cdot \|\pi(T^{-1}U)\| \cdot \|\pi(U^{-1}S)\|,$$

where $\|\cdot\|$ denotes the Frobenius norm of a matrix (i.e., $\|M\|^2 = \mathrm{Tr}(M\overline{M}^\top)$).

Fourier inversion implies a nonabelian version of Parseval's identity, which states that for any function $f\colon G \to \mathbb{C}$,

$$\sum_{g \in G} |f(g)|^2 = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} d_\pi \left\| \sum_{g \in G} f(g)\pi(g) \right\|^2.$$

Applying this formula with $f = 1_{S^{-1}} * 1_T$, which is equal to the indicator function of $S^{-1}T$ by the triple product property, we obtain

$$|S|\,|T|\,|G| = \sum_{\pi \in \mathrm{Irr}(G)} d_\pi \|\pi(S^{-1}T)\|^2,$$

and thus for each $\pi \in \mathrm{Irr}(G)$ with $d_\pi > 1$,

$$\|\pi(S^{-1}T)\| \leq \sqrt{|S|\,|T|\,|G|/n(G)}.$$

Using this bound and the Cauchy–Schwarz inequality, we find that

$$\begin{aligned}|G|\,|S|\,|T|\,|U| &\geq (|S|\,|T|\,|U|)^2 - \sqrt{|S|\,|T|\,|G|/n(G)} \sum_{\pi\colon\, d_\pi > 1} d_\pi \|\pi(T^{-1}U)\| \cdot \|\pi(U^{-1}S)\| \\ &\geq (|S|\,|T|\,|U|)^2 \\ &\qquad - \sqrt{|S|\,|T|\,|G|/n(G)} \sqrt{\sum_{\pi\colon\, d_\pi > 1} d_\pi \|\pi(T^{-1}U)\|^2} \sqrt{\sum_{\pi\colon\, d_\pi > 1} d_\pi \|\pi(U^{-1}S)\|^2},\end{aligned}$$

and so by Parseval's identity,

$$\begin{aligned}|G|\,|S|\,|T|\,|U| &\geq (|S|\,|T|\,|U|)^2 - \sqrt{|S|\,|T|\,|G|/n(G)} \sqrt{|G|\,|T|\,|U|} \sqrt{|G|\,|S|\,|U|} \\ &= (|S|\,|T|\,|U|)^2 - |S|\,|T|\,|U|\,|G|^{3/2}/n(G)^{1/2}.\end{aligned}$$

We conclude that

$$|S|\,|T|\,|U| \leq \frac{|G|^{3/2}}{n(G)^{1/2}} + |G|,$$

as desired. ◀

▶ Remark 3.3. One can show a similar bound for sets S_i, T_i, U_i satisfy the *simultaneous* triple product property [6, Definition 2.2]. The proof proceeds by examining the coefficient of the identity in $f * g * h$, where $f = \sum_i 1_{S_i} * 1_{T_i^{-1}}$, $g = \sum_i 1_{T_i} * 1_{U_i^{-1}}$, and $h = \sum_i 1_{U_i} * 1_{S_i^{-1}}$. If the simultaneous triple product property is satisfied, then this coefficient equals $\sum_i |S_i|\,|T_i|\,|U_i|$, and $\|f\|^2 = \sum_i |S_i|\,|T_i|$, $\|g\|^2 = \sum_i |T_i|\,|U_i|$, and $\|h\|^2 = \sum_i |U_i|\,|S_i|$. When π is the trivial representation, $\pi(f * g * h) = (\sum_i |S_i|\,|T_i|)(\sum_i |T_i|\,|U_i|)(\sum_i |U_i|\,|S_i|)$. Combining these facts as before, we find that

$$\Big(\sum\nolimits_i |S_i|\,|T_i|\Big)^{1/2} \Big(\sum\nolimits_i |T_i|\,|U_i|\Big)^{1/2} \Big(\sum\nolimits_i |U_i|\,|S_i|\Big)^{1/2} \leq \frac{|G|^{3/2}}{n(G)} + |G|.$$

We immediately obtain the following corollary from Theorem 3.2:

▶ **Corollary 3.4.** *No sequence $G_1, G_2, \ldots$ of finite groups satisfying $n(G_i) \geq \Omega(|G_i|^\delta)$ with $\delta > 0$ can meet the packing bound.*

▶ **Corollary 3.5.** *There exists a constant $\varepsilon > 0$ such that no triple product property construction in a group of Lie type can yield an upper bound on ω better than $2 + \varepsilon$.*

This corollary is more subtle than the previous one, since it does not simply amount to a failure to meeting the packing bound.

Proof. First, we deal with the case of groups of Lie type of bounded rank. Such groups G satisfy $n(G) \geq \Omega(|G|^{\delta})$ for some constant $\delta > 0$, as one can check from the bounds given in [15], and this condition suffices by Corollary 3.4.

Now let G be a group of Lie type of rank r and dimension d over $\mathbb{F}_q$. Then $|G| = \Theta(q^d)$ (see, for example, [17, Table 24.1]), and the lower bound $n(G) \geq \Omega(q^r)$ holds by [15]. Hence by Theorem 3.2,

$$|S|\,|T|\,|U| \leq |G|^{3/2}/\sqrt{n(G)} + |G| = O(q^{3d/2-r/2}).$$

By [12, Theorem 1.1], there are $O(q^r)$ conjugacy classes in G. Let $d_1, \dots, d_m$ be the dimensions of the irreducible representations of G, where m is the number of conjugacy classes of G. We have $\sum_i d_i^2 = |G| = \Theta(q^d)$, and

$$\frac{\sum_i d_i^\omega}{m} \geq \left(\frac{\sum_i d_i^2}{m}\right)^{\omega/2}$$

since $x \mapsto x^{\omega/2}$ is a convex function. Hence $\sum_i d_i^\omega \geq \Omega(q^{r+\omega(d-r)/2})$, and therefore Theorem 2.2 cannot yield an upper bound on ω better than

$$\omega \leq 3\left(\frac{r + \log_q C}{r}\right)$$

for some absolute constant $C > 0$. If r is large enough, then this bound cannot approach 2, and the case of bounded r was dealt with above. ◀

Note that this corollary holds not just for groups of Lie type, but also for simple groups that are quotients of groups of Lie type by their centers. In particular, the second part of argument depends on only two bounds, namely a lower bound for $n(G)$ and an upper bound for the number of conjugacy classes in G. Both of these bounds are preserved by taking the quotient: a quotient group always has at most as many conjugacy classes as the original group, and every irreducible representation of the quotient yields an irreducible representation of the original group.

Another consequence of Theorem 3.2 is a slightly sharper estimate for how close $|S|\,|T|\,|U|$ can come to $|G|^{3/2}$ when S, T, and U satisfy the triple product property in G. It follows from [11, Lemma 3.1] that $|S|\,|T|\,|U| < |G|^{3/2}$, but this inequality does not rule out the possibility that $|S|$, $|T|$, and $|U|$ might be a large as $\lfloor |G|^{1/2} - 1 \rfloor$. The following corollary shows that this cannot happen when $|G|$ is sufficiently large.

▶ **Corollary 3.6.** *If subsets S, T, and U satisfy the triple product property in a finite group G, then $|S|\,|T|\,|U| \leq |G|^{3/2}/\sqrt{2} + |G|$.*

Proof. If G is abelian, then $|S|\,|T|\,|U| \leq |G|$ by [11, Lemma 3.1]. Otherwise $n(G) \geq 2$ and the conclusion follows from Theorem 3.2. ◀

3.2 A barrier for subgroups that are not self-normalizing

In contrast to the previous barrier, which follows from properties of the containing group, we now give a barrier in terms of the three subsets used in a triple product property construction. It will apply only to the case of three subgroups, as opposed to arbitrary subsets.

For $X \subseteq G$, let $N(X) = \{g \in G : gXg^{-1} = X\}$ denote the normalizer of X in G, and let $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$ denote the center of G.

▶ **Theorem 3.7.** *Suppose that subgroups H_1, H_2, and H_3 satisfy the triple product property in a finite group G, and let $s_i = |N(H_i)|/|H_i|$. Then*

$$|H_1|\,|H_2|\,|H_3| \le \frac{|G|^{3/2}}{(s_1 s_2 s_3)^{1/4}}.$$

Proof. The main observation in this proof is that $|H_1|\,|N(H_1) \cap H_2|\,|H_3| \le |G|$ (and the analogous inequality for any permutation of H_1, H_2, and H_3). To prove this inequality, we will show that the map

$$(h_1, h_2, h_3) \mapsto h_1 h_2 h_3$$

is injective on $H_1 \times (N(H_1) \cap H_2) \times H_3$. If not, then there exist $(h_1, h_2, h_3) \neq (h_1', h_2', h_3')$ for which

$$h_1 h_2 h_3 = h_1' h_2' h_3',$$

which implies that

$$h_2'^{-1} h_1'^{-1} h_1 h_2 h_3 h_3'^{-1} = 1.$$

However, $h_2'^{-1}(h_1'^{-1}h_1)h_2'$ is another element $h_1'' \in H_1$ (not equal to 1 if $h_1' \neq h_1$), since h_2' is in the normalizer of H_1. We thus have $h_1''(h_2'^{-1}h_2)(h_3 h_3'^{-1}) = 1$ with not all three factors equal to 1, which contradicts the triple product property for H_1, H_2, and H_3.

Now this inequality implies that

$$|G| \ge |H_1|\,|N(H_1) \cap H_2|\,|H_3| = |H_1|\frac{|N(H_1)|\,|H_2|}{|N(H_1)H_2|}|H_3| \ge |H_1|\frac{|N(H_1)|\,|H_2|}{|G|}|H_3|.$$

The inequality in the theorem statement follows by repeating this argument with H_2, H_3 and then H_3, H_1 in place of H_1 and H_2 and taking the product. ◀

▶ Remark 3.8. The same proof in fact works for subsets S, T, U satisfying the triple product property, not just subgroups, and leads to the conclusion that

$$|S|\,|T|\,|U| \le \left(\frac{|G|^3}{|N(Q(S)) \cap T|\,|N(Q(T)) \cap U|\,|N(Q(U)) \cap S|}\right)^{1/2}.$$

The following corollary shows that triple product property constructions using subgroups of groups G satisfying $|Z(G)| = \Omega(|G|^{\delta})$ with $\delta > 0$ cannot meet the packing bound. For example, this shows that triples of subgroups in $\mathrm{GL}(n, q)$ with fixed n cannot meet the packing bound.[4]

▶ **Corollary 3.9.** *If subgroups H_1, H_2, and H_3 satisfy the triple product property in a finite group G, then*

$$|H_1|\,|H_2|\,|H_3| \le \frac{|G|^{3/2}}{|Z(G)|^{1/2}}.$$

[4] More generally, arbitrary subsets cannot meet the packing bound, because intersecting random translates of the subsets with $\mathrm{SL}(n, q)$ would give subsets of $\mathrm{SL}(n, q)$ meeting the packing bound in expectation, and we have seen that this is impossible since $\mathrm{SL}(n, q)$ a group of Lie type of bounded rank when n is fixed.

Proof. Because $H_1 \cap Z(G)$, $H_2 \cap Z(G)$, and $H_3 \cap Z(G)$ satisfy the triple product property in the abelian group $Z(G)$,

$$|Z(G)| \geq |H_1 \cap Z(G)|\,|H_2 \cap Z(G)|\,|H_3 \cap Z(G)|$$

by [11, Lemma 3.1]. Combining this inequality with $Z(G) \subseteq N(H_i)$ shows that

$$\begin{aligned} |Z(G)| &\geq |H_1 \cap Z(G)|\,|H_2 \cap Z(G)|\,|H_3 \cap Z(G)| \\ &= |H_1|\,|H_2|\,|H_3|\,|Z(G)|^3/(|H_1 Z(G)|\,|H_2 Z(G)|\,|H_3 Z(G)|) \\ &\geq |H_1|\,|H_2|\,|H_3|\,|Z(G)|^3/(|H_1 N(H_1)|\,|H_2 N(H_2)|\,|H_3 N(H_3)|) \\ &= |H_1|\,|H_2|\,|H_3|\,|Z(G)|^3/(|N(H_1)|\,|N(H_2)|\,|N(H_3)|), \end{aligned}$$

and therefore $|N(H_1)|\,|N(H_2)|\,|N(H_3)|/(|H_1|\,|H_2|\,|H_3|) \geq |Z(G)|^2$. The conclusion now follows by Theorem 3.7. ◀

4 Constructions in Lie groups

In this section, we study triple product property constructions in Lie groups (i.e., groups that are also smooth manifolds). All Lie groups will be assumed to be positive-dimensional. We define the Lie exponent of a Lie group G in terms of the rank $r(G)$, which we take to be the real dimension of a Cartan subalgebra of the Lie algebra.[5]

▶ **Definition 4.1.** *The* Lie exponent $\omega(G)$ *of a Lie group G of rank $r(G)$ is the infimum of the quantity*

$$\frac{r(G)}{(\dim M_1 + \dim M_2 + \dim M_3)/3 - (\dim G - r(G))/2}$$

over all submanifolds M_1, M_2, and M_3 of G satisfying the triple product property and $(\dim M_1 + \dim M_2 + \dim M_3)/3 > (\dim G - r(G))/2$. (Recall that the infimum of the empty set is $+\infty$.) The Lie exponent of a family of groups is the infimum of $\omega(G)$ over G in the family.

We primarily have in mind semisimple Lie groups, or more generally reductive groups, and it is unclear how relevant the Lie exponent is for other groups. Note that if G is abelian, then $r(G) = \dim_{\mathbb{R}} G$.

Definition 4.1 is motivated by the following analogy with the finite field setting. The finite groups of Lie type fall into families of Chevalley groups defined over $\mathbb{F}_q$ as q varies, with the families corresponding to the classification of simple Lie groups (as well as some complications such as twisting). For example, $\mathrm{SL}(n, q)$ is analogous to $\mathrm{SL}(n, \mathbb{R})$ or $\mathrm{SL}(n, \mathbb{C})$. Suppose we have triple product property constructions with subsets of sizes $q^{m_1+o(1)}$, $q^{m_2+o(1)}$, and $q^{m_3+o(1)}$ in such a family of simple groups G_q as $q \to \infty$. This is a finite analogue of having submanifolds of dimensions m_1, m_2, and m_3. It follows from [16, Theorem 1.3] that the largest irreducible representation of G_q has dimension $q^{(d-r)/2+o(1)}$ as $q \to \infty$, where d and r are the dimension and rank of the corresponding Lie group.[6] If the dimensions of the irreducible representations of G_q are $d_1, \dots, d_k$, then by Theorem 2.2,

[5] Note that this differs from the usual convention for complex Lie groups of using the complex dimension. For example, this is why Table 4.1 shows that $r(\mathrm{GL}(n, \mathbb{C})) = 2n$.

[6] To deduce this result from [16, Theorem 1.3], note that the Steinberg representation has dimension $q^{(d-r)/2}$. See also [16, Theorems 5.1–5.3] for some classical groups that are not quite simple.

$$\begin{aligned}
q^{(m_1+m_2+m_3+o(1))\omega/3} &\le \sum_i d_i^\omega \\
&\le \sum_i d_i^2 \max_j d_j^{\omega-2} \\
&= |G| \max_j d_j^{\omega-2} \\
&= q^{d+(\omega-2)(d-r)/2+o(1)},
\end{aligned}$$

and taking the limit as $q \to \infty$ shows that

$$\omega \le \frac{r}{(m_1+m_2+m_3)/3-(d-r)/2}$$

if the denominator is positive. In other words, Definition 4.1 is exactly the bound on ω one would get if the construction had an analogue in the corresponding finite groups of Lie type. We note that we know of no general reason why such an analogue should exist; indeed, we do not know of any finite analogues of the Lie group constructions given later in this section. We pose the following question:

▶ **Question 4.2.** *Is it true that for every Lie group G, the exponent of matrix multiplication is at most $\omega(G)$?*

By Proposition 4.3 below, the answer must be yes if $\omega = 2$. A direct proof would be of considerable interest. Even without such a proof, we view $\omega(G)$ as a model for what groups can do in the continuous setting, which allows for geometric constructions that may not work over finite fields, but that we might hope give inspiration for related constructions in the finite setting.

▶ **Proposition 4.3.** *Every Lie group G has $\omega(G) > 2$.*

Proof. If M_1, M_2, and M_3 satisfy the triple product property in G, then the map $(m_1, m_2) \mapsto m_1^{-1}m_2$ from $M_1 \times M_2$ to G is injective, and so $\dim M_1 + \dim M_2 \le \dim G$. Similarly, $\dim M_2 + \dim M_3 \le \dim G$ and $\dim M_1 + \dim M_3 \le \dim G$. Averaging these inequalities shows that $(\dim M_1 + \dim M_2 + \dim M_3)/3 \le (\dim G)/2$, and therefore the bound we obtain for $\omega(G)$ is at least

$$\frac{r(G)}{(\dim G)/2 - (\dim G - r(G))/2} = 2.$$

Equality could hold only if $\dim M_i = (\dim G)/2$ for all i. In that case, every continuous, injective function from $M_1 \times M_2$ to G must be open by invariance of domain, and therefore has an open image. In particular, for $m_1' \in M_1$ and $m_2' \in M_2$ consider the map sending $(m_1, m_2) \in M_1 \times M_2$ to $m_1' m_1^{-1} m_2 m_2'^{-1}$. Its image contains a neighborhood of 1, but by the triple product property it intersects the quotient set $Q(M_3) = M_3 M_3^{-1}$ only at 1, which is impossible since $Q(M_3)$ contains a submanifold $M_3 m_3^{-1}$ (for fixed $m_3 \in M_3$) of dimension $(\dim G)/2$ that contains 1. ◀

Note that in the notation of Definition 4.1, if $\dim M_1 + \dim M_2 + \dim M_3 \le \dim G$, then they cannot prove any better upper bound for $\omega(G)$ than 3. This conclusion is immediate if $r(G) = \dim G$, and one can check that it follows from $r(G) \le \dim G$. In fact, the best upper bound we know on the Lie exponent is 3, which holds for abelian groups:

▶ **Proposition 4.4.** *If G is abelian, then $\omega(G) = 3$.*

Proof. Let $H_1 = G$ and $H_2 = H_3 = \{1\}$. Then H_1, H_2, and H_3 satisfy the triple product property in G. Since $r(G) = \dim G$ and $\dim H_1 + \dim H_2 + \dim H_3 = \dim G$, it follows that $\omega(G) \leq 3$.

For the other direction, note that if G is abelian, then the product map $M_1 \times M_2 \times M_3 \to G$ must be injective or else the triple product property fails. If the map is injective, then $\dim M_1 + \dim M_2 + \dim M_3 \leq \dim G$ and hence $\omega(G) \geq 3$. ◀

There is also a Lie analogue of the packing bound from Definition 2.3.

▶ **Definition 4.5.** *We say a sequence $G_1, G_2, \ldots$ of Lie groups* meets the packing bound *if there exist submanifolds $M_{1,i}$, $M_{2,i}$, and $M_{3,i}$ of G_i satisfying the triple product property such that*

$$\lim_{i\to\infty} \frac{\dim G_i}{(\dim M_{1,i} + \dim M_{2,i} + \dim M_{2,i})/3} = 2.$$

▶ **Proposition 4.6.** *If Lie groups $G_1, G_2, \ldots$ have $\lim_{i\to\infty} \omega(G_i) = 2$, then they achieve the packing bound.*

Proof. It suffices to show that for M_1, M_2, and M_3 satisfying the triple product property in a group G with $(\dim M_1 + \dim M_2 + \dim M_3)/3 > (\dim G - r(G))/2$,

$$\frac{r(G)}{(\dim M_1 + \dim M_2 + \dim M_3)/3 - (\dim G - r(G))/2} \geq \frac{\dim G}{(\dim M_1 + \dim M_2 + \dim M_3)/3}.$$

This assertion follows from the inequality $(\dim M_1 + \dim M_2 + \dim M_3)/3 \leq (\dim G)/2$ used in the proof of Proposition 4.3. ◀

It was shown in [11, Theorem 6.1] that the Lie groups $\mathrm{SL}(n, \mathbb{R})$ meet the packing bound, by taking M_1, M_2, and M_3 to be the groups of upper unitriangular, lower unitriangular, and orthogonal matrices. In this construction, the group is an algebraic group over $\mathbb{R}$, as are the subgroups M_i. In particular, they are all linear algebraic groups over $\mathbb{R}$, i.e., subgroups of $\mathrm{GL}(n, \mathbb{R})$ defined by polynomial equations. Algebraic groups are a little more general than linear algebraic groups; they are to algebraic varieties as Lie groups are to manifolds.

However, algebraic varieties over $\mathbb{C}$ (or any algebraically closed field) cannot help:

▶ **Theorem 4.7.** *Let G be an algebraic group over an algebraically closed field, and let V_1, V_2, and V_3 be subvarieties of G that satisfy the triple product property. Then*

$$\dim V_1 + \dim V_2 + \dim V_3 \leq \dim G.$$

As a consequence, subvarieties of algebraic groups over $\mathbb{C}$ cannot be used to meet the packing bound or obtain a better Lie exponent than 3.

Proof. Let v_i' be any element of V_i, and define $\varphi \colon V_1 \times V_2 \times V_3 \to G$ by

$$\varphi(v_1, v_2, v_3) = v_1 v_1'^{-1} v_2 v_2'^{-1} v_3 v_3'^{-1}.$$

By the triple product property, the only solution of $\varphi(v_1, v_2, v_3) = 1$ is (v_1', v_2', v_3'), and so the solution set is zero-dimensional since we are working over an algebraically closed field. However, the fiber dimension theorem [14, Theorem 17.24] says the dimension of the solution set must be at least $\dim V_1 + \dim V_2 + \dim V_3 - \dim G$, which yields the desired inequality. ◀

The intuitive difference between $\mathbb{R}$ and $\mathbb{C}$ here is that a variety can have fewer points over $\mathbb{R}$ than one might expect by counting degrees of freedom. For example, the equation $x_1^2 + \cdots + x_n^2 = 0$ defines an $(n-1)$-dimensional variety, which has plenty of points over $\mathbb{C}$, but over $\mathbb{R}$ it consists of just a single point. Fields that are not algebraically closed may lead to an anomalously low number of solutions, and we cannot conclude that a variety is zero-dimensional just because it has only one real point. What Theorem 4.7 indicates is that to obtain strong examples, we must either use constructions that are not defined by polynomial equations, or choose equations that have fewer solutions over $\mathbb{R}$ than they do over $\mathbb{C}$. (Note that there are many possibilities that are not defined by polynomial equations. For example, constructions that use complex conjugation generally do not define complex subvarieties.)

Theorem 4.7 does rule out one superficially attractive possibility, namely obtaining Lie exponent 2 via subvarieties of algebraic groups over $\overline{\mathbb{F}}_q$ and then transitioning to finite groups by using finite subfields of $\overline{\mathbb{F}}_q$ with sizes tending to infinity.

We now give several new constructions over $\mathbb{R}$ with parameters that improve upon the previously known construction from [11]. Our constructions make use of the following observation, which relaxes the triple product property for subgroups.

▶ **Lemma 4.8.** *Suppose that H_1, H_2, and H_3 are Lie subgroups of a Lie group G and K is a compact subgroup of G such that the equation $h_1h_2h_3 = 1$ with $h_i \in H_i$ implies that $h_1, h_2, h_3 \in K$. Then the Lie exponent of G is at most*

$$\frac{r(G)}{(\dim H_1 + \dim H_2 + \dim H_3 - 2\dim K)/3 - (\dim G - r(G))/2}.$$

We will refer to this situation as the *K-triple product property.* More generally, the same holds for submanifolds M_i such that $q_1q_2q_3 = 1$ with $q_i \in Q(M_i)$ implies $q_1, q_2, q_3 \in K$, but we will need it only for subgroups.

Proof. By the slice theorem [5, Theorem I.2.1], there exist submanifolds H_i' of H_i such that $\dim H_i' = \dim H_i - \dim K$ and no two elements $h, h' \in H_i'$ satisfy $hh'^{-1} \in K$ unless $h = h'$. Then the submanifolds H_1, H_2', and H_3' of G satisfy the triple property property and yield the asserted bound. (Note that the first submanifold is H_1, not H_1'.) ◀

4.1 Asymptotic Lie exponent 3

As mentioned above and shown in [11, Theorem 6.1], the upper unitriangular, lower unitriangular, and special orthogonal groups satisfy the triple product property in $\mathrm{SL}(n, \mathbb{R})$. Since these subgroups have dimension $n(n-1)/2$ inside a group of dimension $n^2 - 1$, the groups $\mathrm{SL}(n, \mathbb{R})$ meet the packing bound.

However, the rank of $\mathrm{SL}(n, \mathbb{R})$ is $n - 1$, and so this example does not yield any Lie exponent bound (the denominator in Definition 4.1 would vanish). In this section we modify the construction to get a bound on the Lie exponent approaching 3 for powers of $\mathrm{SL}(n, \mathbb{R})$.

▶ **Theorem 4.9.** *For $m > 1$ and $n > 1$, the Lie exponent of $\mathrm{SL}(n, \mathbb{R})^m$ is at most*

$$\frac{3m(n-1)}{m(n-1) - n}.$$

In the proof we will denote the i, j entry of a matrix M by $M_{i,j}$. To avoid ambiguity we will use superscripts to index sequences of matrices, with parentheses around the superscripts to distinguish them from exponents. Recall also that a unitriangular matrix is a triangular matrix with diagonal entries equal to 1.

Proof. Let $H_1 = \mathrm{SO}(n,\mathbb{R})^m$, let

$$H_2 = \{(A^{(1)},\dots,A^{(m)}) \in \mathrm{SL}(n,\mathbb{R})^m : \text{each } A^{(i)} \text{ is upper unitriangular}\},$$

and let

$$H_3 = \left\{(B^{(1)},\dots,B^{(m)}) \in \mathrm{SL}(n,\mathbb{R})^m : \text{each } B^{(i)} \text{ is lower triangular} \right.$$
$$\left. \text{and } \prod_{i=1}^{m} B^{(i)}_{j,j} = 1 \text{ for all } j\right\},$$

These subgroups have dimensions $mn(n-1)/2$, $mn(n-1)/2$, and $m(n(n+1)/2-1)-n$, respectively. We claim that they satisfy the K-triple product property in $\mathrm{SL}(n.\mathbb{R})^m$, where

$$K = \{(C^{(1)},\dots,C^{(m)}) \in \mathrm{SL}(n,\mathbb{R})^m : \text{each } C^{(i)} \text{ is diagonal with } \pm 1 \text{ entries}\}.$$

Since $\dim \mathrm{SL}(n,\mathbb{R})^m = m(n^2-1)$ and the rank of $\mathrm{SL}(n,\mathbb{R})^m$ is $m(n-1)$, while $\dim K = 0$, the claimed bound on the Lie exponent will follow by Lemma 4.8.

Let $M = (M^{(1)},\dots,M^{(m)}) \in H_1$, $A = (A^{(1)},\dots,A^{(m)}) \in H_2$, $B = (B^{(1)},\dots,B^{(m)}) \in H_3$. We will show that if $MA = B$, then for each i, the matrix $M^{(i)}$ is diagonal with ± 1 diagonal entries, in which case the same follows for $A^{(i)}$ and $B^{(i)}$. We will prove by induction on j that $M^{(i)}e_j = \pm e_j$ for all i, where $e_1,\dots,e_n$ are the standard basis vectors.

Let the jth column of $A^{(i)}$ be $A^{(i)}_j$. For any i, $A^{(i)}_1 = e_1$, and so $M^{(i)}e_1 = B^{(i)}_1$. Since $M^{(i)}$ is orthogonal, $M^{(i)}e_1$ and thus also $B^{(i)}_1$ must be unit vectors. In particular, $|B^{(i)}_{1,1}| \le 1$ for all i. But since $\prod_{i=1}^m B^{(i)}_{1,1} = 1$ this forces $B^{(i)}_{1,1} = \pm 1$, which proves the claim for $j = 1$.

Now suppose $M^{(i)}e_j = \pm e_j$ for all $j < k$ and all i. For any i, $A^{(i)}_k = e_k + \sum_{j<k} A^{(i)}_{j,k} e_j$ and $B^{(i)}_k = B^{(i)}_{k,k} e_k + \sum_{j>k} B^{(i)}_{j,k} e_j$. From the induction hypothesis we deduce that

$$\begin{aligned} M^{(i)}e_k &= M^{(i)}\bigl(A^{(i)}_k - \sum_{j<k} A^{(i)}_{j,k} e_j\bigr) \\ &= B^{(i)}_{k,k} e_k + \sum_{j>k} B^{(i)}_{j,k} e_j - \sum_{j<k} A^{(i)}_{j,k}(\pm e_j). \end{aligned}$$

Since $M^{(i)}$ is orthogonal, $M^{(i)}e_k$ is a unit vector. Because $\prod_i B^{(i)}_{k,k} = 1$, it follows as above that $B^{(i)}_{k,k} = \pm 1$ for all i. Hence $M^{(i)}e_k = \pm e_k$ for all i, which proves the claim. ◀

4.2 Conjugates of rotation groups

▶ **Theorem 4.10.** *There are three conjugates of* $\mathrm{O}(n,\mathbb{R})$ *inside of* $\mathrm{GL}(n,\mathbb{R})$ *satisfying the* K*-triple product property, where* K *is the subgroup of diagonal matrices with* ± 1 *entries on the diagonal.*

This construction meets the packing bound. In particular, it evades the normalizer barrier since the normalizer of $\mathrm{O}(n,\mathbb{R})$ in $\mathrm{GL}(n,\mathbb{R})$ is $\mathbb{R}^\times \cdot \mathrm{O}(n,\mathbb{R})$. However, it does not prove a bound for $\omega(\mathrm{GL}(n,\mathbb{R}))$, because each of these subgroups has dimension $n(n-1)/2$, which equals $(\dim \mathrm{GL}(n,\mathbb{R}) - n)/2$, and $r(\mathrm{GL}(n,\mathbb{R})) = n$. Note that the center of $\mathrm{GL}(n,\mathbb{R})$ plays no role, and we could just as well have stated the theorem for conjugates of $\mathrm{SO}(n,\mathbb{R})$ inside $\mathrm{SL}(n,\mathbb{R})$. We use the slightly more general formulation since it is convenient to allow determinant -1 in the proof by induction.

Proof. Let $G = \mathrm{GL}(n, \mathbb{R})$ and $H = \mathrm{O}(n, \mathbb{R})$. To specify the conjugates of H, we take $D_1 = \mathrm{diag}(x_1, \dots, x_n)$ with $x_1 > x_2 > \cdots > x_n > 0$ and $D_2 = \mathrm{diag}(y_1, \dots, y_n)$ with $0 < y_1 < y_2 < \cdots < y_n$. Then we will show that H, $H_1 := D_1 H D_1^{-1}$, and $H_2 := D_2 H D_2^{-1}$ satisfy the K-triple product property in G, where K is the group of diagonal ±1 matrices.

In particular, we will show that for every $h_1 \in H_1$ and $h_2 \in H_2$, if $h_1^\top h_1 = h_2^\top h_2$, then $h_1, h_2 \in K$. The conclusion then follows, since if $h h_1 h_2^{-1} = I$ with $h \in H$, then $h_1 h_2^{-1} \in H$, meaning $(h_1 h_2^{-1})^\top (h_1 h_2^{-1}) = I$, and hence $h_1^\top h_1 = h_2^\top h_2$.

Suppose that $h_1 = D_1 M_1 D_1^{-1}$ and $h_2 = D_2 M_2 D_2^{-1}$, where $M_1, M_2 \in H$, and consider

$$h_1^\top h_1 = (D_1^{-1} M_1^\top D_1)(D_1 M_1 D_1^{-1}).$$

If $(a_1, a_2, \dots, a_n)$ is the first column of M_1, then the first column of $D_1 M_1 D_1^{-1}$ is

$$(a_1, x_2 x_1^{-1} a_2, \dots, x_n x_1^{-1} a_n)$$

as is the first row of $D_1^{-1} M_1^\top D_1$, so the upper-left entry of their product $h_1^\top h_1$ is

$$a_1^2 + (x_2/x_1)^2 a_2^2 + (x_3/x_1)^2 a_3^2 + \cdots + (x_n/x_1)^2 a_n^2.$$

Now, since $a_1^2 + a_2^2 + \cdots + a_n^2 = 1$, we can substitute for a_1^2 to obtain

$$1 + ((x_2/x_1)^2 - 1)a_2^2 + ((x_3/x_1)^2 - 1)a_3^2 + \cdots + ((x_n/x_1)^2 - 1)a_n^2.$$

Because $x_i > x_1$ for all $i > 1$, this quantity is at most 1, with equality exactly when $a_2^2 = a_3^2 = \cdots = a_n^2 = 0$. By an identical argument, if $(b_1, b_2, \dots, b_n)$ is the first column of M_2, then the upper-left entry of $h_2^\top h_2$ is

$$1 + ((y_2/y_1)^2 - 1)b_2^2 + ((y_3/y_1)^2 - 1)b_3^2 + \cdots + ((y_n/y_1)^2 - 1)b_n^2,$$

which is at least 1, with equality exactly when $b_2^2 = b_3^2 = \cdots = b_n^2 = 0$. So if $h_1^\top h_1 = h_2^\top h_2$, then in particular their upper-left entries are equal, and we conclude that $a_1^2 = b_1^2 = 1$, while $a_i = b_i = 0$ for all $i > 1$.

Now h_1 has the form

$$\left(\begin{array}{c|ccc} \pm 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & h_1' & \\ 0 & & & \end{array}\right),$$

where h_1' is an element of $D_1' \, \mathrm{O}(n-1, \mathbb{R}) D_1'^{-1}$ with $D_1' = \mathrm{diag}(x_2, \dots, x_n)$, and h_2 has the form

$$\left(\begin{array}{c|ccc} \pm 1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & h_2' & \\ 0 & & & \end{array}\right),$$

where h_2' is an element of $D_2' \, \mathrm{O}(n-1, \mathbb{R}) D_2'^{-1}$ with $D_2' = \mathrm{diag}(y_2, \dots y_n)$. Finally, since $h_1 h_2^{-1} h = 1$ we find h also has the same block-diagonal form, and so $h_1'(h_2')^{-1} \in \mathrm{O}(n-1, \mathbb{R})$, and then we are done by induction on n. ◀

▶ Remark 4.11. This theorem holds when we replace G with $\mathrm{GL}(n, \mathbb{C})$ (resp., $\mathrm{GL}(n, \mathbb{H})$), H with $\mathrm{U}(n, \mathbb{C})$ (resp., $\mathrm{Sp}(n)$), and K with the group of diagonal matrices with unit complex (resp., quaternionic) numbers on the diagonal. This follows from a similar argument, where one replaces transpose with conjugate transpose and uses the positivity of the complex/quaternionic norm. The corresponding dimensions are shown in Table 4.1.

Table 4.1 Parameters for the real, complex, and quaternionic versions of Theorem 4.10.

(skew) field	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$\dim G$	n^2	$2n^2$	$4n^2$
$r(G)$	n	$2n$	$4n$
$\dim H$	$n(n-1)/2$	n^2	$n(2n+1)$
$\dim K$	0	n	$3n$
Meets packing bound as $n \to \infty$	yes	yes	yes
Lie exponent upper bound	∞	6	4

5 Open problems

The most important challenge highlighted by this paper is to find a construction proving that the Lie exponent of a family of Lie groups approaches 2, or to prove that such a construction cannot exist. Many questions can be asked along the way, including whether there is a Lie group with Lie exponent less than 3, and whether the Lie exponent of $\mathrm{SL}(n, \mathbb{R})$ is even finite.

It follows from [18] that triple product property constructions inside $\mathrm{SL}(2, q)^m$ cannot give $\omega = 2$ for fixed q and growing m, and Theorem 3.2 shows that $\mathrm{SL}(n, q)^m$ cannot give $\omega = 2$ for fixed m and growing q. The proofs of these two facts are quite different: one uses the polynomial method, and the other is Fourier analytic. Is there a common generalization of these two facts that would rule out obtaining $\omega = 2$ with m and q both growing?

Together with the fact that abelian groups cannot yield exponent less than 3, Theorem 3.2 implies that the alternating groups are the only simple groups left that could yield $\omega = 2$ via a triple product property construction. The representation-theoretic argument fails in this case, since A_n has an irreducible representation of dimension $n - 1$ but $|A_n| = n!/2$. Can an alternate argument rule out these groups?

References

1 Josh Alman. Limits on the universal method for matrix multiplication. *Theory Comput.*, 17:1, 1–30, 2021. `doi:10.4086/toc.2021.v017a001`.

2 Josh Alman and Virginia Vassilevska Williams. Limits on all known (and some unknown) approaches to matrix multiplication. In *Proceedings of the 59th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2018)*, pages 580–591. IEEE Computer Society, 2018. `doi:10.1109/FOCS.2018.00061`.

3 Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, (SODA 2021)*, pages 522–539. SIAM, 2021. `doi:10.1137/1.9781611976465.32`.

4 Andris Ambainis, Yuval Filmus, and François Le Gall. Fast matrix multiplication: limitations of the Coppersmith–Winograd method. In *Proceedings of the 2015 ACM Symposium on Theory of Computing (STOC 2015)*, pages 585–593. ACM, 2015. `doi:10.1145/2746539.2746554`.

5 Michèle Audin. *Torus actions on symplectic manifolds*, volume 93 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, revised edition, 2004. `doi:10.1007/978-3-0348-7960-6`.

6 Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans. On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Anal.*, pages 1–27 (Paper No. 3), 2017. `doi:10.19086/da.1245`.

7 Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, and Chris Umans. Which groups are amenable to proving exponent two for matrix multiplication? Preprint, 2017, arXiv:1712.02302.

8 Emmanuel Breuillard. A brief introduction to approximate groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 23–50. Cambridge Univ. Press, Cambridge, 2014.

9 Matthias Christandl, Péter Vrana, and Jeroen Zuiddam. Barriers for fast matrix multiplication from irreversibility. *Theory Comput.*, 17:2, 1–32, 2021. doi:10.4086/toc.2021.v017a002.

10 Henry Cohn, Robert Kleinberg, Balázs Szegedy, and Christopher Umans. Group-theoretic algorithms for matrix multiplication. In *Proceedings of the 46th Annual Symposium on Foundations of Computer Science (FOCS 2005)*, pages 379–388. IEEE Computer Society, 2005. doi:10.1109/SFCS.2005.39.

11 Henry Cohn and Christopher Umans. A group-theoretic approach to fast matrix multiplication. In *Proceedings of the 44th Annual Symposium on Foundations of Computer Science (FOCS 2003)*, pages 438–449. IEEE Computer Society, 2003. doi:10.1109/SFCS.2003.1238217.

12 Jason Fulman and Robert Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.*, 364(6):3023–3070, 2012. doi:10.1090/S0002-9947-2012-05427-4.

13 W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008. doi:10.1017/S0963548307008826.

14 Joe Harris. *Algebraic geometry: a first course*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. doi:10.1007/978-1-4757-2189-8.

15 Vicente Landazuri and Gary M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974. doi:10.1016/0021-8693(74)90150-1.

16 Michael Larsen, Gunter Malle, and Pham Huu Tiep. The largest irreducible representations of simple groups. *Proc. Lond. Math. Soc. (3)*, 106(1):65–96, 2013. doi:10.1112/plms/pds030.

17 Gunter Malle and Donna Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011. doi:10.1017/CBO9780511994777.

18 Will Sawin. Bounds for matchings in nonabelian groups. *Electron. J. Combin.*, 25(4):#P4.23, 1–21, 2018. doi:10.37236/7520.