Canad. J. Math. 2024, pp. 1–28
http://dx.doi.org/10.4153/S0008414X24000713

Uniform bounded elementary generation of Chevalley groups

Boris Kunyavskiĭ, Eugene Plotkin, and Nikolai Vavilov

Abstract. In this paper, we establish a definitive result which almost completely closes the problem of bounded elementary generation for Chevalley groups of rank ≥ 2 over arbitrary Dedekind rings R of arithmetic type, with uniform bounds. Namely, we show that for every reduced irreducible root system Φ of rank ≥ 2, there exists a universal bound $L = L(\Phi)$ such that the simply connected Chevalley groups $G(\Phi, R)$ have elementary width $\leq L$ for all Dedekind rings of arithmetic type R.

Introduction and State of Art

In the present paper, we consider Chevalley groups $G = G(\Phi, R)$ and their elementary subgroups $E(\Phi, R)$ over Dedekind rings of arithmetic type. Usually, it is more convenient to speak of the simply connected group $G_{\mathrm{sc}}(\Phi, R)$. In most of the cases we are interested in, it coincides with the elementary group $E_{\mathrm{sc}}(\Phi, R)$. When there is no danger of confusion, we drop any indication of the weight lattice.

Our ring R is an arbitrary Dedekind ring of arithmetic type, which means that throughout the paper, one has to distinguish the corresponding number and function cases.

We occupy ourselves with the classical problem of estimating the width of $E(\Phi, R)$ with respect to the elementary generators $x_\alpha(\xi)$, $\alpha \in \Phi$, $\xi \in R$. We consider the subset $E^L(\Phi, R)$ consisting of products of $\leq L$ such elementary generators. The **elementary width** is defined as the smallest L such that each element of $E(\Phi, R)$ can be represented as a product of $\leq L$ elementary generators $x_\alpha(\xi)$; in other words,

$$E(\Phi, R) = E^L(\Phi, R).$$

If there is no such L, we say that the width is infinite. If the width is finite, we say that G is **boundedly elementarily generated**.

Received by the editors February 11, 2024; revised July 15, 2024; accepted July 22, 2024.

Research of Boris Kunyavskiĭ and Eugene Plotkin was supported by the ISF grant 1994/20. Nikolai Vavilov was supported by the "Basis" Foundation grant N. 20-7-1-27-1 "Higher symbols in algebraic K-theory." A part of this research was accomplished when Boris Kunyavskiĭ was visiting the IHES (Bures-sur-Yvette). Support of these institutions is gratefully acknowledged.

Nikolai Vavilov suddenly passed away on September 14, 2023. It was he who initiated this research. Everybody who had a privilege to work with Nikolai and who had been touched by his mathematical vision and intuition, comprehensive and profound erudition, and generous personality will never forget him. He will be deeply missed. Let the memory of our friend be blessed. *B.K., E.P.*

AMS subject classification: **20G07**.

Kywords: Chevalley groups, Dedekind rings, bounded generation.

Let us start with a short review of early works on the topic. Most of them, and many papers even today, only treat the special case of $\mathrm{SL}(n, R)$. The pioneering 1975 paper by George Cooke and Peter Weinberger [CW] showed that, with the exception of $\mathrm{SL}(2, R)$ over very meagre rings, such as $R = \mathbb{Z}, \mathbb{F}_q[t]$, or other arithmetic rings with the finite multiplicative group, the problem of bounded elementary generation admits a positive **uniform** solution. In other words, in this case, there exists a bound $L = L(\Phi)$ depending solely on Φ such that the elementary width of $G(\Phi, R)$ over all Dedekind rings R of arithmetic type does not exceed L.

However, their actual proofs were *conditional*; they depended on a very strong form of the **GRH** = Generalized Riemann Hypothesis. The most important early contributions toward obtaining *unconditional* proofs of such results over *number rings* are due to David Carter and Gordon Keller, 1983–1985.

• The arithmetic proofs for $\mathrm{SL}(n, R)$, $n \geq 3$, with *explicit* bounds depending not only on Φ but also on some arithmetic invariants of R, were obtained in [CK1, CK2],

• For the model theoretic proofs in the number case, which yield the *existence* of bounds $L = L(\Phi, d)$ depending on Φ and the degree $d = [K : \mathbb{Q}]$, non-constructive, without presenting any actual bounds, see, for instance, the truly remarkable [but unfortunately still unpublished] preprint by Carter and Keller with Eugene Paige [CKP], and its re-exposition by Dave Morris [Mo].

• Around 1990, Oleg Tavgen [Ta1, Ta2, Ta3] succeeded in generalizing these results to all Chevalley groups of normal types, and to most twisted Chevalley groups. With this end, he invented a very slick reduction trick, which reduced the study of bounded generation to rank 2 cases, essentially to $\mathrm{SL}(3, R)$ and $\mathrm{Sp}(4, R)$, and was able to solve the cases of $\mathrm{Sp}(4, R)$ and $G(\mathsf{G}_2, R)$ by direct matrix computations imitating the arithmetic proof by Carter and Keller. As the Carter–Keller bounds, Tavgen's ones depended on arithmetic invariants of R.

• The only published result for the function case until rather recently was the very early 1975 paper by Clifford Queen [Qu], who established *the best possible* absolute bound $L = 5$, but only for *some* function rings with infinite multiplicative group subject to further arithmetic conditions. Even the case of $R = \mathbb{F}_q[t]$ remained open at that stage.

Such was the state of art around 1990, and the results listed above remained almost unrivaled for about two more decades. There were some interesting attempts to come up with explicit bounds (compare, for instance, [Li, LM, Mu]), but the resulting bounds always depended on some further arithmetic invariants and/or worked only under some severe restrictions on R.

However, there were many reasons which eventually led to a new surge of activity in this direction starting around 2010.[1] Let us mention relations with the congruence subgroup property, Kazhdan property T, Waring-type problems for groups, model theoretic applications, and so on.

[1]We ourselves learned about the status of this problem as unsolved from Sury; see [VSS]. In particular, it is proved in [VSS] that the only rings for which one has $G = UU^-UU^-$ are rings with stable range 1, so that $L = 5$ is the best possible bound for SL_2 over arithmetic rings with stable range $1\frac{1}{2}$.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

An important initial breakthrough, the first *unconditional* proof of the bounded generation of $\mathrm{SL}\left(2,\mathbb{Z}\left[\frac{1}{p}\right]\right)$ with an *explicit* bound, and at that the best possible one, $L=5$, was achieved by Maxim Vsemirnov [Vs].

Let us list the key contributions of the last five years which together essentially amount to the complete solution of the problem.

• For the *number case*, when R^* is infinite, there is a definitive result for $\mathrm{SL}(2,R)$ by Morgan, Rapinchuk, and Sury [MRS] in 2018, with a small uniform bound $L\le 9$, which can be improved [and was improved!] in some cases. Thus, Bruce Jordan and Yevgeny Zaytman [JZ] improved it to $L\le 8$ (and further improved to $L\le 7$ or $L\le 6$ in the presence of finite or real valuations in S).

• In the same 2018, Bogdan Nica [Ni] has finally established bounded elementary generation of $\mathrm{SL}(n,\mathbb{F}_q[t])$, $n\ge 3$. He proposed a slight variation of Carter–Keller's approach, replacing the full multiplicativity of Mennicke symbol by a weaker form, "swindling lemma." This is where we jumped in. In [KPV], we developed reductions of all non-symplectic Chevalley groups to $\mathrm{SL}(3,\mathbb{F}_q[t])$ and devised a similar proof for $\mathrm{Sp}(4,\mathbb{F}_q[t])$.

• The decisive contributions in the function case are due to Alexander Trost [Tr1, Tr2], who succeeded in proving versions of all necessary arithmetic lemmas in the function case. Actually, his versions are *better* than the corresponding results in the number case.[2] In particular, he gave an *explicit uniform* bound for the bounded elementary generation of $\mathrm{SL}(n,R)$, $n\ge 3$, which does not depend on the degree $d=[K:\mathbb{F}_q(t)]$.

• Finally, the recent paper by Kunyavskii, Morris, and Rapinchuk [KMR] improves the uniform bound for $\mathrm{SL}(2,R)$ for rings R with infinite multiplicative group R^* to $L\le 7$ in the number case and establishes a similar result with the bound $L\le 8$ in the *function case*.

Thus, the results of [CKP, Mo, MRS, Tr2, KMR] *completely* solve the problem of the uniform bounded elementary generation for the special linear groups $\mathrm{SL}(n,R)$, $n\ge 3$ – and when R^* is infinite, even for $\mathrm{SL}(2,R)$.

The methods of our previous paper [KPV] completely reduce the proof of a similar result for almost all other Chevalley groups, including even the *symplectic* groups $\mathrm{Sp}(2l,R)$, $l\ge 3$ to the case of $\Phi=\mathsf{A}_2$. *The only* case that does not follow right away by combining results of the above papers is that of $\mathrm{Sp}(4,R)$.

Here, we solve the remaining case of $\mathrm{Sp}(4,R)$ and thus come up with a complete solution of uniform bounded generation for Chevalley groups in the general case.

Theorem A *Let Φ be a reduced irreducible root system of rank $l\ge 2$. Then there exists a constant $L=L(\Phi)$, depending on Φ alone, such that for any Dedekind ring of arithmetic type R, any element in $G_{\mathrm{sc}}(\Phi,R)$ is a product of at most L elementary root unipotents,*

$$G_{\mathrm{sc}}(\Phi,\ R)=E^L(\Phi,R).$$

[2] One of the reasons is that adjoining roots of unity in the number case, one gets a cyclotomic extension which may have nontrivial ramification, whereas in the function case, one gets a constant extension, which is not ramified.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Remark 0.1 The bounds obtained in Theorem A are *uniform* with respect to R, both in the number and function cases. What is important – and unexpected! – is that in the function case, they are *explicit*.

Remark 0.2 In the number case, explicit bounds are only available when R^* is infinite.

Remark 0.3 Theorem A was already announced in [KLPV], with a sketch of proof. However, since [KLPV] is focused on bounded generation for the Steinberg groups, it would be unreasonable to provide their tedious computational aspects of the proof for Chevalley groups. Therefore, the most tricky case of $\mathrm{Sp}(4,R)$ was skipped there; in several cases not needed for the treatment of Steinberg groups, the arguments were only briefly sketched, and no care of explicit numerical bounds was taken. Here, we supply all the details for the case of $\mathrm{Sp}(4,R)$. Moreover, we redo the case $\mathrm{SL}(3,R)$ for the function rings, which was already solved in [Tr2]. However, we do it in the style of [Ni] rather than [CK1], which allows us to improve the estimate for L from $L \leq 65$ to $L \leq 44$. This improvement then gives slightly better bounds in all explicit estimates for all other Chevalley groups in the function case.

Remark 0.4 Note that uniform estimates, being interesting in their own right, are indispensable for some applications – for example, for estimating Kazhdan constants of arithmetic groups; see [Ha].

Roughly, the ingredients of the proof are as follows.

• We consider the case where R^* is infinite separately and prove the following statement.

Theorem B *For any Dedekind ring of arithmetic type R with the infinite multiplicative group R^*, any element in $G_{\mathrm{sc}}(\Phi,R)$ is a product of at most $L = 7N$ elementary unipotents in the number case or $L = 8N$ elementary unipotents in the function case, where $N = |\Phi^+|$ is the number of positive roots of Φ.*

The proof of Theorem B is cheap modulo deep results for rank 1 case and requires Tavgen's reduction trick. This is done in Section 3. Thus, in the proof of Theorem A, we may assume that R^* is finite. This is important in the number case.

• In the **function** case, our proofs in this paper have almost zero arithmetic components. Namely, all arithmetic results we need are taken essentially as is from the paper by Trost [Tr2, Lemma 3.1 and Lemma 3.3]. After that, the rest of the proof is a pure theory of algebraic groups and some stability theorems from algebraic K-theory.

More precisely, we show – this part is indeed essentially contained already in [KPV] – that for all non-symplectic Chevalley groups, bounded generation is reduced to that for $\mathrm{SL}(3,R)$. What has been overlooked in [KPV], though, is that bounded generation of $\mathrm{Sp}(2l,R)$, $l \geq 3$, also reduces to $\mathrm{SL}(3,R)$, with the help of the symplectic lemmas on switching long and short roots [KPV]. Only after rediscovering this trick ourselves in March 2023, we noticed that a similar approach has been used by Kairat Zakiryanov [Za], and this reference should have been included in [KPV].

For the only remaining case $\mathrm{Sp}(4,R)$, we can also obtain an *explicit uniform* bound by combining the arithmetic lemmas of Trost [Tr2] with our Sp_4-lemmas from [KPV], in *exactly* the same style as in [KPV, Section 6], and that is by far the most difficult part of the proof. Namely, Trost's Lemma 3.1 is essentially a generalization of our Lemma 6.4; we only have to supplement it slightly in characteristic 2. Trost's Lemma 3.3 shows that – unlike for the number fields! – the case of a general function ring R is not much different from the case when R is a PID (and, in particular, there is no dependence on degree or other invariants).

Note that in a more recent preprint, Trost established the uniformly bounded generation in the symplectic case (with weaker estimates); see [Tr3, Corollary 3.11].

• The **number** case is very different. Our general strategy is similar to the proof of [Tr2, Theorem 4.1]. Namely, we use very deep arithmetic results of [MRS] (or any of their improvements in [JZ, KMR]) pertaining to $\mathrm{SL}(2,R)$ to prove Theorem B asserting that there is an explicit uniform bound when R^* is infinite. *Some* such bounds can be easily derived by a version of the Tavgen's trick [Ta2, Theorem 1], as described and generalized in [VSS, SSV] and [KPV].

We are left with the rings of integers of the imaginary quadratic fields K, and thus with a single degree $d = 2$. Since this class is contained in a class defined by the first-order conditions and sharing uniform estimates of the congruence kernel, using nonstandard models (alias ultrafilters, alias compactness theorem in the first-order logic, alias…), one can then prove the following: if all $\mathrm{SL}(3,R)$ are boundedly elementarily generated, they are *uniformly* boundedly elementarily generated. This argument was devised by Carter–Keller–Paige [CKP] and then rephrased slightly differently by Morris [Mo] (see also the discussion in [Tr1, Tr2]).

Since all other cases, except $\mathrm{Sp}(4,R)$, are reduced to $\mathrm{SL}(3,R)$ by the standard tricks collected in [KPV], we are again left with $\mathrm{Sp}(4,R)$ alone. Of course, in the *number case*, the bound given for $\mathrm{Sp}(4,R)$ by Tavgen [Ta2] is not uniform; it depends on the degree *and* the discriminant of the number field K. However, since $\mathrm{Sp}(4,R)$ and its elementary generators are described by first order relations, we can again use exactly the same argument of [CKP, Mo] to conclude that there exists an absolute constant as an upper bound for the width of all $\mathrm{Sp}(4,R)$, where R is the ring of integers of an imaginary quadratic number field. Of course, now we know only that *some* such constant exists; it is by no means explicit.

Remark 0.5 As the reader may have noticed, there is a significant overlap between our research and the recent works of Alexander Trost. Below, for the reader's convenience, following the referee's suggestion, we present a brief summary of the main common points. Some more detailed explanations can be found in the relevant parts of the paper.

• In the number field case, our general strategy is based on focusing on the case of imaginary quadratic fields. This approach, in the setup of elementary bounded generation problems, was first applied by Trost; see [Tr2, Theorem 4.1].[3]

• Arithmetical lemmas, indispensable for the proofs, can be viewed as variations on the Carter–Keller theme; see [CK1]. All such variations use some generalized form of Dirichlet's theorem on primes in an arithmetic progression (see [BMS]) along with certain specific arguments (see, for example, [MRS]). In the present paper, our main arithmetic tools in the function field case are Trost's Lemmas 3.1 and 3.3 from [Tr2].

[3] This idea goes back to Serre who applied it in the close context of the congruence subgroups problem; see the first page of his seminal paper [Se].

Lemma 3.1 provides an explicit procedure for extracting $(q-1)^{\text{th}}$ roots of Mennicke symbols, generalizing the main content of our Lemma 6.4 from [KPV]. The latter lemma also contains a treatment of square roots of Mennicke symbols requiring a separate argument in characteristic 2. This is used in the present paper and in the proof of Claim 3 in [Tr3].

• Uniform bounds for the symplectic groups in the function field case were obtained by Trost in [Tr3, Corollary 3.11], generalizing our earlier results in [KPV]. In the present paper, we achieve better constants with the help of the swindling method.

• Our proof of the uniform boundedness of Sp_4 in the number case, given in Section 8 of the present paper, and Trost's proof in [Tr1] are essentially of the same model-theoretic nature, as the prototypical proof for SL_n of Carter–Keller–Paige (and Morris). More precisely, Trost's arguments, based on a quite technical Theorem 3.16 from [Tr1], use the compactness theorem of the first-order logic, whereas ours employ nonstandard models.

The paper is organized as follows. In Section 1, we recall notation and collect some preliminary results. In Section 2, we recall some important arithmetic lemmas. In Section 3, we prove Theorem B and also the cases of Theorem A corresponding to the simply laced root systems Φ and $\Phi = \mathsf{F}_4$ (we collect these cases in Theorem C). Section 4 deals with surjective stability of K_1-functor and consequences. In Section 5, we prove a swindling lemma for the groups $\mathrm{SL}(3,R)$ and $\mathrm{Sp}(4,R)$. In Section 6 and 7, we establish new bounds for the width of $\mathrm{SL}(3,R)$ and $\mathrm{Sp}(4,R)$ in the function case. Section 8 is devoted to $\mathrm{Sp}(4,R)$ in the number case. Finally, Section 9 contains some concluding remarks and open problems.

1 Notation and preliminaries

In this section, we briefly recall the notation, mainly taken from [KLPV], that will be used throughout the paper and some background facts. For more details on Chevalley groups over rings, see [Va1] or [VP], where one can find many further references.

1.1 Chevalley groups

Given a reduced root system Φ (usually assumed irreducible), we denote by Φ^+, Φ^-, and $\Pi = \{\alpha_1, \dots, \alpha_l\}$ the sets of positive, negative, and fundamental roots with respect to a chosen order. Throughout, we denote $N = |\Phi^+|$.

For a lattice $\mathcal{P}$ intermediate between the root lattice $\mathcal{Q}(\Phi)$ and the weight lattice $\mathcal{P}(\Phi)$ and any commutative unital ring R with the multiplicative group R^*, we denote by $G = G_{\mathcal{P}}(\Phi, R)$ the Chevalley group of type $(\Phi, \mathcal{P})$ over R. In the case $\mathcal{P} = \mathcal{P}(\Phi)$, the group G is called simply connected and is denoted by $G_{\mathrm{sc}}(\Phi, R)$. In another extreme case $\mathcal{P} = \mathcal{Q}(\Phi)$, the group G is called adjoint and is denoted by $G_{\mathrm{ad}}(\Phi, R)$.

Many results do not depend on the lattice $\mathcal{P}$, and we often omit any reference to $\mathcal{P}$ in the notation and denote by $G(\Phi, R)$ *any* Chevalley group of type Φ over R. Usually, by default, we assume that $G(\Phi, R)$ is simply connected, but in some cases, it is convenient to work with the adjoint group, which is then reflected in the notation.

Fixing a split maximal torus $T = T(\Phi, R)$ in $G = G(\Phi, R)$ and identifying Φ with $\Phi(G, T)$, we denote by X_α, $\alpha \in \Phi$, the unipotent root subgroups in G, elementary

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

with respect to T. We fix maps $x_\alpha\colon R \mapsto X_\alpha$, so that $X_\alpha = \{x_\alpha(\xi) \mid \xi \in R\}$, and require that these parametrizations are interrelated by the Chevalley commutator formula with integer coefficients; see [Ca], [Steinb]. The above unipotent elements $x_\alpha(\xi)$, where $\alpha \in \Phi$, $\xi \in R$, elementary with respect to $T(\Phi, R)$, are also called [elementary] unipotent root elements or, for short, simply root unipotents.

Further,

$$E(\Phi, R) = \langle x_\alpha(\xi),\ \alpha \in \Phi,\ \xi \in R\rangle$$

denotes the *absolute* elementary subgroup of $G(\Phi, R)$, spanned by all elementary root unipotents, or, what is the same, by all [elementary] root subgroups X_α, $\alpha \in \Phi$. For $\varepsilon \in \{+, -\}$, denote

$$U^\varepsilon(\Phi, R) = \langle x_\alpha(\xi) \mid \alpha \in \Phi^\varepsilon,\ \xi \in R\rangle \le \mathrm{E}_{\mathrm{sc}}(\Phi, R).$$

1.2 Relative groups

Let $\mathfrak{q} \trianglelefteq R$ be an ideal of R, and let $\rho_\mathfrak{q}\colon R \longrightarrow R/\mathfrak{q}$ be the reduction modulo $\mathfrak{q}$. By functoriality, it defines the reduction homomorphism of Chevalley groups $\rho_\mathfrak{q}\colon G(\Phi, R) \longrightarrow G(\Phi, R/\mathfrak{q})$. The kernel of $\rho_\mathfrak{q}$ is denoted by $G(\Phi, R, \mathfrak{q})$ and is called the principal congruence subgroup of $G(\Phi, R)$ of level $\mathfrak{q}$. We denote by $X_\alpha(\mathfrak{q})$ the intersection of X_α with the principal congruence subgroup $G(\Phi, R, \mathfrak{q})$. Clearly, $X_\alpha(\mathfrak{q})$ consists of all elementary root elements $x_\alpha(\xi)$, $\alpha \in \Phi$, $\xi \in \mathfrak{q}$, of level $\mathfrak{q}$:

$$X_\alpha(\mathfrak{q}) = \{x_\alpha(\xi) \mid \xi \in \mathfrak{q}\}.$$

By definition, $E(\Phi, \mathfrak{q})$ is generated by $X_\alpha(\mathfrak{q})$, for all roots $\alpha \in \Phi$. The same subgroups generate $E(\Phi, R, \mathfrak{q})$ as a *normal* subgroup of the absolute elementary group $E(\Phi, R)$.

The classical Suslin–Kopeiko–Taddei theorem asserts that for $\mathrm{rk}(\Phi) \ge 2$, one has $E(\Phi, R, \mathfrak{q}) \trianglelefteq G(\Phi, R)$. The quotient

$$\mathrm{K}_1(\Phi, R, \mathfrak{q}) = G_{\mathrm{sc}}(\Phi, R, \mathfrak{q})/E_{\mathrm{sc}}(\Phi, R, \mathfrak{q})$$

is called the [relative] K_1-functor. The absolute case corresponds to $\mathfrak{q} = R$,

$$\mathrm{K}_1(\Phi, R) = G_{\mathrm{sc}}(\Phi, R)/E_{\mathrm{sc}}(\Phi, R).$$

Observe

$$\mathrm{K}_1(\mathsf{A}_l, R, \mathfrak{q}) = \mathrm{SK}_1(l+1, R, \mathfrak{q}),$$

so that our K_1-functor corresponds rather to the SK_1 of the classical theory.

1.3 Arithmetic case

For a global field K and a finite nonempty set S of places of K (containing all archimedean places when K is a number field), let

$$R = \{x \in K \mid v(x) \ge 0\ \forall v \notin S\}.$$

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

It is a Dedekind domain whose maximal ideals can be canonically identified with the places outside S. Following [BMS], we say that R is *the Dedekind ring of arithmetic type* defined by the set S (or, for short, an arithmetic ring).

For the arithmetic rings Bass, Milnor, and Serre [BMS] have explicitly calculated $K_1(\Phi, R, \mathfrak{q})$, $\Phi = \mathsf{A}_l, \mathsf{C}_l$, $l \geq 2$, in terms of Mennicke symbols. Namely, they have proven that $\mathrm{K}_1(\mathsf{A}_l, R, \mathfrak{q}) \cong C(\mathfrak{q})$ and $\mathrm{K}_1(\mathsf{C}_l, R, \mathfrak{q}) \cong \mathrm{Cp}(\mathfrak{q})$ (the universal Mennicke groups), which in turn are then identified via reciprocity laws with certain groups of roots of 1 in R.

The [almost] positive solution of the congruence subgroup problem for these groups amounts to the fact that the **congruence kernel**

$$C(G) := \varprojlim C(\mathfrak{q})$$

taken over all nonzero ideals $\mathfrak{q} \trianglelefteq R$ is finite. Actually, it is trivial, apart from the case when R is the ring of integers $\mathcal{O}_K$ in a purely imaginary number field K, when $C(G) \cong \mu(K)$ is the group of all roots of 1 in K.

Later, their results were generalized to all Chevalley groups by Hideya Matsumoto [Ma]. The following special case of his results [Ma, Théorème 12.7] explains why we usually prefer to work with simply connected groups.

Lemma 1.1 *Let R be a Dedekind ring of arithmetic type and Φ a reduced irreducible root system of rank at least* 2. *Then*

$$\mathrm{E}_{\mathrm{sc}}(\Phi, R) = G_{\mathrm{sc}}(\Phi, R).$$

2 Supporting statements

2.1 Reduction to the ring of integers

The following result is a combination of [BMS, Lemma 2.1] and [BMS, Lemma 5.3]. The same proof, with several successful deteriorations, is reproduced on page 685 of [CK1].

Lemma 2.1 *Let R be a Dedekind ring, $s \in R$, $s \neq 0$. Then*

$$\mathrm{SL}\Big(2, R\Big[\frac{1}{s}\Big]\Big) = \mathrm{SL}(2, R)E^3\Big(2, R\Big[\frac{1}{s}\Big]\Big).$$

In other words, every 2×2 matrix with entries in $R\big[\frac{1}{s}\big]$ can be reduced to a matrix with entries in R by ≤ 3 elementary moves with parameters in $R\big[\frac{1}{s}\big]$. Since the number of elementary moves during the rank reduction does not depend on the ring R, and the only such dependence occurs at the base of induction, we immediately get the following corollary.

Lemma 2.2 *Let R be a Dedekind ring such that any element of $\mathrm{G}_{\mathrm{sc}}(\Phi, R)$ is a product of L elementary root unipotents. Then for any $s \in R$, $s \neq 0$, any element of $\mathrm{G}_{\mathrm{sc}}(\Phi, R\big[\frac{1}{s}\big])$ is a product of at most $L + 3$ elementary root unipotents.*

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

2.2 Arithmetic lemmas

The following lemma is the arithmetic heart of the whole proof. In the number case, it is [CK1, Lemma 1], and in the function case, it was first proven in full generality in [Tr2, Lemma 3.1] (before that, only a special case $R = \mathbb{F}_q[t]$ was established as [KPV, Lemma 6.4]).

Lemma 2.3 *Let $\mathcal{O}_K$ be the ring of integers of a global field K, and let $x \in \mathrm{SL}(2, \mathcal{O}_K)$. Let m be the number of roots of 1 in K in the number case, respectively $m = q - 1$, where $\mathbb{F}_q$ is the field of constants of K in the function case. Then for any matrix $A \in \mathrm{SL}(2, \mathcal{O}_K)$, there exist nonzero elements $a, b \in \mathcal{O}_K$ with the following properties:*

- *$b\mathcal{O}_K$ is a prime ideal, and, moreover, in the number case, $b\mathcal{O}_K$ is unramified in $K/\mathbb{Q}$ and does not contain m.*
- *A can be transformed to a matrix with the first row (a^m, b) by means of not more than 4 elementary moves in the number case, or 3 elementary moves in the function case.*

Remark 2.4 In the function case, in addition to Lemma 2.3, we shall need its version with $m = 2$ to be able to extract square roots of Mennicke symbols. If q is odd, such a version follows automatically because we then have $a^{q-1} = (a^{(q-1)/2})^2$. If q is even, to adjust the proof of Lemma 2.3 to the case $m = 2$, an additional argument is needed. Similar to Trost's proof of [Tr3, Claim 3], we apply our argument from the end of the proof of [KPV, Lemma 6.4]. Namely, if K is a global function field of characteristic 2 and $f \in \mathcal{O}_K$ is such that the principal ideal $f\mathcal{O}_K$ is prime, any $g \in \mathcal{O}_K$ is a square modulo $f\mathcal{O}_K$ because its image $\bar{g}$ in the residue field $\mathcal{O}_K/(f)$ of characteristic 2 is a square, as any other element of a finite field of characteristic 2. This makes the argument significantly shorter: one only has to take care of the primality of the ideals $a_2\mathcal{O}$ and $b_2\mathcal{O}$ (in the notation of [Tr2, Lemma 3.1]), which is achieved by applying the Dirichlet theorem.

For a global function field K with the field of constants $\mathbb{F}_q$ and $b \in \mathcal{O}_K$, $b \neq 0$, we denote by $\varepsilon(b)$ the exponent of the [finite] multiplicative group $(\mathcal{O}_K/b\mathcal{O}_K)^*$ and set $\delta(b) = \varepsilon(b)/(q-1)$. The following result is due to Trost [Tr2, Lemma 3.3].

Lemma 2.5 *Let K be a global function field with the field of constants $\mathbb{F}_q$, $a, b \in \mathcal{O}_K \backslash \{0\}$, such that $b\mathcal{O}_K$ is prime and a and b are comaximal, $a\mathcal{O}_K + b\mathcal{O}_K = \mathcal{O}_K$. Then for every unit $u \in \mathcal{O}_K^*$, there exists $c \in \mathcal{O}_K$ such that*

- *$bc \equiv u \pmod{a}$,*
- *$\delta(b)$ and $\delta(c)$ are coprime.*

3 Tavgen rank reduction theorem and applications

3.1 Tavgen rank reduction theorem

In this section, we prove Theorem B and establish some other useful consequences of Tavgen's reduction theorem.

The following trick allowing one to reduce the rank of a root system under consideration was invented by Tavgen [Ta2] (and then generalized in [VSS] and [SSV]). The following final form is proven in [KPV, Theorem 4.2].

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Lemma 3.1 *Let Φ be a reduced irreducible root system of rank $l \geq 2$, and R be a commutative ring. Let $\Delta_1, \dots, \Delta_t$ be some subsystems of Φ, whose union contains all fundamental roots of Φ. Suppose that for all Δ_i, the elementary Chevalley group $\mathrm{E}_{\mathrm{sc}}(\Delta_i, R)$ admits a unitriangular factorization*

$$\mathrm{E}_{\mathrm{sc}}(\Delta_i, R) = U^+(\Delta_i, R)\, U^-(\Delta_i, R)\, U^+(\Delta_i, R) \dots U^{\pm}(\Delta_i, R)$$

of length N (not depending on i). Then the elementary group $\mathrm{E}_{\mathrm{sc}}(\Phi, R)$ itself admits unitriangular factorization

$$\mathrm{E}_{\mathrm{sc}}(\Phi, R) = U^+(\Phi, R)\, U^-(\Phi, R)\, U^+(\Phi, R) \dots U^{\pm}(\Phi, R)$$

of the same length N.

It is used below in two cases, when all Δ_i's are A_1, and when all of them are A_2.

3.2 The case when R^* is infinite

The case where a Dedekind ring R of arithmetic type has infinitely many units is now *completely* solved, with very small *absolute* constant. Here is a brief account of main steps along this route. Vsemirnov [Vs] established a first unconditional result of this sort, not depending on the GRH; Morgan, Rapinchuk, and Sury [MRS] proved that $\mathrm{SL}(2, R)$ is boundedly elementarily generated in number case for an arbitrary R with infinite R^*. The absolute bound obtained in their paper is $L = 9$.

In the paper presently under way, the first author, Morris, and Rapinchuk [KMR] improved the bound to $L = 7$ in the number case (which we believe is the best possible and cannot be further improved, in general). A similar result holds in the function case, with the bound $L = 8$ (which, we believe, can be further improved to $L = 7$).

Lemma 3.2 [KMR] *For any Dedekind ring of arithmetic type R with the infinite multiplicative group R^*, any element in* $\mathrm{SL}(2, R)$ *is a product of at most* 7 *elementary transvections in the number case or at most* 8 *elementary transvections in the function case.*

Together with Lemma 3.1, this immediately implies Theorem B: it covers the case $\Delta = \mathsf{A}_1$, and all higher rank cases are reduced to rank one by putting $\Delta_i = \mathsf{A}_1$ in Lemma 3.1.

Thus, the condition $|R^*| = \infty$ makes a huge relief. Essentially, no extra work is needed to treat the general case with not the best possible but still rather plausible bounds (anyway, asymptotically, L cannot be smaller than something like $3N$ to $4N$).

So, if we are not interested in actual bounds, but just in uniform boundedness, the rest of the exposition is formally dedicated to the Dedekind rings of arithmetic type with *finite* multiplicative groups. Thus, in the number case, we restrict our attention to the rings of integers in imaginary quadratic number fields (since $\mathbb{Z}$ is already covered). In the function case, as discovered by Trost [Tr2], for ranks ≥ 2, we do not have to distinguish between rings with finite and infinite multiplicative group, so that the rest of this section does not depend on [KMR] (but does depend on [MRS]).

3.3 The simply laced case and $\Phi = \mathsf{F}_4$

In this section, we prove the statement of Theorem A for the simply laced root systems and also for $\Phi = \mathsf{F}_4$.

By a theorem of Carter–Keller–Paige (see [CKP], (2.4)) (rewritten and explained by Morris [Mo]), bounded generation for groups of type A_l, $l \geq 2$, holds for all Dedekind rings R in number fields K, with a bound depending on l and also on the degree d of K. But since for all degrees $d \geq 3$ the existence of uniform bound already follows from Theorem B, we only need to take maximum of that, and the universal bound for $d = 2$.

Combining this result with the subsequent work of Trost [Tr2] on the function field case, one obtains the following result; see [Tr2, Theorem 4.1].

Lemma 3.3 [Tr2] *For each $l \geq 2$, there exists a constant $L = L(l) \in \mathbb{N}$ such that for any Dedekind ring of arithmetic type R, any element in $\mathrm{G}_{\mathrm{sc}}(\mathsf{A}_l, R)$ is a product of at most L elementary root unipotents.*

In fact, in the sequel, we only need the special case of the above result pertaining to $\mathrm{SL}(3, R)$, which corresponds to A_2. Indeed, by stability arguments, one has $L(l) \leq L(l-1) + 3l + 1$ for all $l \geq 2$, so that all $L(l)$, $l \geq 3$ can be expressed in terms of the constant $L(2)$. In the function case, Trost [Tr2] gave the estimate $L(2) \leq 65$. No such explicit estimate is available in the number case because the uniform boundedness was established by model-theoretic arguments.

Now we are in a position to get a particular case of Theorem A.

Theorem C *Let Φ be simply laced of rank ≥ 2 or $\Phi = \mathsf{F}_4$, and R be any Dedekind ring of arithmetic type. Then $G_{\mathrm{sc}}(\Phi, R)$ is a product of at most $L = L(2)N$ elementary unipotents.*

Proof Since the fundamental root systems of the simply laced systems and F_4 are covered by copies of A_2, one can take $\Delta_i = \mathsf{A}_2$ in Lemma 3.1 and then apply Lemma 3.3 to the A_2 case. ∎

Thus, in addition to Theorem B, we obtain another stronger form of Theorem A, now without the assumption that R^* is infinite, but only in the special case of simply laced systems of rank ≥ 2 and F_4. The bound here is very rough, since $L(2)$ is the number of *elementary* factors; the number of unitriangular ones can be much smaller. Also, the use of stability arguments allows one to get much better bounds, of the type $L = L(2) + M$, with $3N \leq M \leq 4N$, where some multiple of N occurs as a summand, not as a factor.

4 Stability of K_1-functor and flipping long and short roots

Another way to reduce bounded generation of $G(\Phi, R)$ to bounded generation of $G(\Delta, R)$, where $\Delta \subset \Phi$, is called surjective stability of K_1-functor. Recall that $\mathrm{K}_1(\Phi, R) = G(\Phi, R)/E(\Phi, R)$. Let the root embedding $\Delta \subset \Phi$ be given. Surjective stability of K_1-functor tells us that $G(\Phi, R) = E(\Phi, R)G(\Delta, R)$; see, for example, [St], [Pl]. Moreover, it provides a reduction from $G(\Phi, R)$ to $G(\Delta, R)$ by a bounded number of steps, with a bound depending on R and the root embedding. Here is the main observation we use (see [KPV]).

Lemma 4.1 *Let R be a Dedekind ring of arithmetic type. Then (uniform) bounded generation of the groups $G(\Phi, R)$, $\Phi \neq \mathsf{C}_2$, follows from (uniform) bounded generation of the group $G(\mathsf{A}_2, R)$.*

We illustrate Lemma 4.1 by two examples of the Chevalley groups of types $\Phi = \mathsf{B}_l$, $l \geq 3$, and $\Phi = \mathsf{G}_2$ with explicit bounds for reduction. Of course, by stability arguments, one can assume that $G(\mathsf{B}_l, R)$ is already reduced to $G(\mathsf{B}_3, R)$.

Proposition 4.2 *Let R be a Dedekind ring and assume that any element of $\mathrm{G}(\mathsf{A}_2, R)$ is a product of at most L elementary root unipotents. Then any element of $\mathrm{G}(\mathsf{G}_2, R)$ is a product of at most $L + 20$ elementary root unipotents.*

Proof From [KPV, Proposition 5.3], we obtain the universal bound $L(2) + 20$ for the elementary generation of $\mathrm{E}_{\mathrm{sc}}(\mathsf{G}_2, R)$ over all Dedekind rings of arithmetic type. ∎

Proposition 4.3 *Let R be a Dedekind ring and assume that any element of $\mathrm{G}_{\mathrm{sc}}(\mathsf{A}_2, R)$ is a product of L elementary root unipotents. Then any element of $\mathrm{E}_{\mathrm{ad}}(\mathsf{B}_3, R)$ is a product of at most $L + 31$ elementary root unipotents.*

Proof First, observe that [KPV, Lemmas 7.3 and 6.1] are valid for any Dedekind ring R (although they are formally stated under the assumption $R = \mathbb{F}_q[t]$).

By [KPV, Lemma 7.3], each element $x \in \mathrm{E}_{\mathrm{ad}}(\mathsf{B}_3, R)$ is a product of an image of $y \in \mathrm{G}_{\mathrm{ad}}(\mathsf{B}_2, R)$ and at most 21 elementary root unipotents. However, since the image of y in $\mathrm{G}_{\mathrm{ad}}(\mathsf{B}_3, R)$ is elementary and, in particular, lies in the kernel of the spinor norm, we conclude that y itself lies in the kernel of the spinor norm [Ba, Proposition 3.4.1], and therefore, y is the image of some $z \in \mathrm{G}_{\mathrm{sc}}(\mathsf{B}_2, R)$ [Ba, (3.3.4)].

Next, by [KPV, Lemma 6.1], z is equal to a product of the image of some $w \in \mathrm{G}_{\mathrm{sc}}(\mathsf{A}_1, R)$ and at most 10 elementary root unipotents (where $\mathsf{A}_1 \subset \mathsf{B}_2$ is the inclusion on long roots). Therefore, x is the product of the image of w in $\mathrm{G}_{\mathrm{ad}}(\mathsf{B}_3, R)$ and at most 31 elementary root unipotents.

However, since the inclusion $\mathsf{A}_1 \subset \mathsf{B}_3$ factors through A_2, we conclude that x is a product of an image of some element from $\mathrm{G}_{\mathrm{sc}}(\mathsf{A}_2, R)$ and at most 31 elementary root unipotents. The claim follows. ∎

Corollary 4.4 *For any Dedekind ring of arithmetic type R, any element of $\mathrm{G}_{\mathrm{sc}}(\mathsf{B}_3, R)$ is a product of at most $L(2) + 41$ elementary root unipotents.*

Proof Any element of $\mathrm{G}_{\mathrm{sc}}(\mathsf{B}_3, R)$ is elementary by Lemma 1.1, and therefore, its image in $\mathrm{G}_{\mathrm{ad}}(\mathsf{B}_3, R)$ is a product of at most $L(2) + 31$ elementary root unipotents by Proposition 4.3. However, $\mathrm{G}_{\mathrm{sc}}(\mathsf{B}_3, R)$ is a central extension of $\mathrm{G}_{\mathrm{ad}}(\mathsf{B}_3, R)$ with the kernel cyclic of order 2. The generator of the kernel comes from $\mathrm{G}_{\mathrm{sc}}(\mathsf{D}_3, R)$ [Ba, (3.4)], where it can be expressed as a product of at most 10 elementary root unipotents by [HO, Theorem 7.2.12]. ∎

4.1 The case of $\mathrm{Sp}(2l, R)$, $l \geq 3$

Thus, we are left with the analysis of the the symplectic groups $\mathrm{Sp}(2l, R)$, $l \geq 2$. Quite amazingly, the results of [KPV] and [Tr2] allow to reduce $\mathrm{Sp}(6, R)$ to $\mathrm{SL}(3, R)$ as well. As mentioned in [KLPV], the idea of such a reduction was contained already in Zakiryanov's thesis; see [Za]. Of course, as above, the case $\Phi = \mathsf{C}_l$, $l \geq 3$ is immediately reduced to $\Phi = \mathsf{C}_3$ by stability.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Proposition 4.5 *Let R be a Dedekind ring and assume that any element of* $G_{sc}(A_2, R)$ *is a product of L elementary root unipotents. Then any element of* $E_{sc}(C_3, R)$ *is a product of at most* $L + 40$ *elementary root unipotents.*

Proof As in the case of $\Phi = B_3$, we first invoke [KPV, Lemma 7.1] to reduce a matrix from $Sp(6, R)$ to a matrix from $Sp(4, R)$ by 16 elementary transformations. Then we invoke [KPV, Lemma 6.1] to reduce a matrix from $Sp(4, R)$ to a matrix from $Sp(2, R) = SL(2, R)$ in *long* root position by 10 elementary transformations. After that, we invoke Lemma 2.3 to get a square in the nondiagonal position by 4 elementary transformations in the number case or to do the same in the function case by 3 elementary transformations. Now, we can invoke [KPV, Lemma 6.15] to move such a matrix in the long root fundamental position to a matrix in the short root fundamental position by 10 elementary transformations. At this stage, we can apply Lemma 3.3 to the *short* root $\widetilde{A}_2 \le C_3$, which gives us $\le 16 + 10 + 4 + 10 + L$ elementary moves in all cases. ∎

So, we have two remaining tasks. First of all, we have to prove Theorem A in the $C_2 = Sp(4, R)$ case, which is not covered by our previous considerations. Second, we want to make the number $L(2)$, which is a crucial constituent in all estimates, as small as we can.

5 Swindling lemma

We concentrate now on minimizing estimates for bounded generation. As we know, this problem depends severely on the number of moves which are necessary in order to move any matrix from $SL(3, R)$, where R is a Dedekind ring of arithmetic type, to the identity matrix.

In this section, we establish what Nica [Ni] calls "swindling lemma," which is essentially a very weak form of multiplicativity of Mennicke symbols, sufficient for our purposes and cheaper than the form used in [CK1] in terms of the number of elementary moves. For the symplectic case, such a lemma in full generality is already contained in [KPV]. Here, we come up with a reverse engineering version of Nica's lemma [Ni, Lemma 4] in the linear case. The proof itself is organized in the same style as the proofs in [KPV, Section 6.3].

5.1 Swindling lemma for $SL(3, R)$

The following result is essentially [Ni, Lemma 4]. Of course, formally Nica assumes that R is a PID, to conclude that *all s* have the desired factorizations. But calculations with Mennicke symbols [BMS] show that his result holds [at least] for all Dedekind rings. Below, we extract the rationale behind his proof to apply it in the only situation we need. Namely, we stipulate that the desired factorization of s does exist.

Lemma 5.1 *Let R be any commutative ring. Assume that*

$$A = \begin{pmatrix} a & b & 0 \\ sc & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL(3, R),$$

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

where s admits factorization $s = s_1 s_2$ such that

$$a \equiv d \equiv 1 \pmod{s_1}, \qquad a \equiv d \equiv -1 \pmod{s_2}.$$

Then A can be transformed to

$$A = \begin{pmatrix} \pm a & -sb & 0 \\ c & \mp d & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SL}(3, R)$$

by ≤ 11 elementary moves.

Proof Let $t_1, t_2 \in R$ be such that

$$a = 1 + s_1 t_1 = -1 + s_2 t_2.$$

Below, we use programmers' notation style to describe elementary moves, keeping the letter A to denote all matrices appearing along the way.

- **Step 1**

$$A = At_{31}(s_1) = \begin{pmatrix} a & b & 0 \\ sc & d & 0 \\ s_1 & 0 & 1 \end{pmatrix}.$$

- **Step 2+3**

$$A = t_{13}(-t_1)t_{23}(-s_2 c)A = \begin{pmatrix} 1 & b & -t_1 \\ 0 & d & -s_2 c \\ s_1 & 0 & 1 \end{pmatrix}.$$

- **Step 4**

$$A = t_{31}(-s_1)A = \begin{pmatrix} 1 & b & -t_1 \\ 0 & d & -s_2 c \\ 0 & -s_1 b & a \end{pmatrix}.$$

At this stage, we have rolled s_1 over the diagonal by simultaneously moving the 2×2 matrix from the NW-corner to the SE-corner. Now we have to roll over s_2 by simultaneously returning our 2×2 matrix back to the NW-corner.

- **Step 5+6**

$$A = At_{12}(-b)t_{13}(t_1 + s_2) = \begin{pmatrix} 1 & 0 & s_2 \\ 0 & d & -s_2 c \\ 0 & -s_1 b & a \end{pmatrix}.$$

Now we are in exactly the same position as we were after the first move and can start rolling back.

- **Step 7+8**

$$A = t_{21}(c)t_{31}(-t_2)A = \begin{pmatrix} 1 & 0 & s_2 \\ c & d & 0 \\ -t_2 & -s_1 b & -1 \end{pmatrix}.$$

- **Step 9**

$$A = t_{13}(s_2)A = \begin{pmatrix} -a & -sb & 0 \\ c & d & 0 \\ -t_2 & -s_1 b & -1 \end{pmatrix}.$$

- **Step 10+11**

$$A = At_{31}(-t_2)t_{32}(-s_1 b) = \begin{pmatrix} -a & -sb & 0 \\ c & d & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

For the other choice of signs, one should start rolling over the other way, say, with moving A to $At_{32}(s_2)$. ∎

Remark 5.2 Below, we state a *stronger* form of the swindling lemma for *short* roots in $\mathrm{Sp}(4, R)$, Lemma 5.3 = [KPV, Proposition 6.10], where an *arbitrary* s is rolled over from c to b. One could ask, how is it possible that the symplectic result is more general than the linear one? The answer is very easy. What we do here is the linear prototype of the swindling lemma for *long* roots in $\mathrm{Sp}(4, R)$, Lemma 5.4 = [KPV, Lemma 6.7], where a *square* s^2 is rolled over from c to b. Of course, we could do the same here, but then to apply it, we would have to use the deep arithmetic Lemma 2.3 on the extraction of square roots of Mennicke symbols, which would increase the number of elementary moves.

5.2 Swindling lemma for $\mathrm{Sp}(4, R)$

In what concerns $\mathrm{Sp}(4, R)$, we keep the notation and conventions of [KPV, Section 6]. In particular, $\mathrm{Sp}(4, R)$ preserves the symplectic form with Gram matrix

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Further, α and β are fundamental roots of C_2, and the corresponding root unipotents are

$$x_\alpha(\xi) = \begin{pmatrix} 1 & \xi & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\xi \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad x_\beta(\xi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \xi & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

while $x_{-\alpha}(\xi)$ and $x_{-\beta}(\xi)$ are their transposes. Together, they generate the elementary symplectic group $\mathrm{Ep}(4, R)$ which for Dedekind rings of arithmetic type coincides with $\mathrm{Sp}(4, R)$.

There are two natural embeddings of $\mathrm{SL}(2, R)$ into $\mathrm{Sp}(4, R)$, the *short root* embedding ϕ_α

$$\phi_\alpha\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} = x_\alpha(\xi), \qquad \phi_\alpha\begin{pmatrix} 1 & 0 \\ \xi & 1 \end{pmatrix} = x_{-\alpha}(\xi),$$

and the *long root* embedding ϕ_β

$$\phi_\beta\begin{pmatrix}1 & \xi\\ 0 & 1\end{pmatrix} = x_\beta(\xi), \qquad \phi_\beta\begin{pmatrix}1 & 0\\ \xi & 1\end{pmatrix} = x_{-\beta}(\xi),$$

and unlike groups of other types in the symplectic case, they behave very differently.

The following swindling lemma for the short root embedding that we use in the sequel seems to be stronger than the linear swindling lemma. But this is because, morally, the Mennicke symbol constructed via ϕ_α is the square root of the Mennicke symbol constructed via ϕ_β. At the same time, stability reduction (see, for instance, [KPV, Lemma 6.1]) reduces a symplectic matrix to an element of $\mathrm{SL}(2,R)$ in the *long* root embedding. Thus, to be able to use this [seemingly] stronger form of swindling, we should be able to extract square roots of Mennicke symbols anyway.

Lemma 5.3 [KPV] *Let $a,b,c,d,s \in R$, $ad - bcs = 1$, and, moreover, $a \equiv d \pmod{s}$. Then*

$$\phi_\alpha\begin{pmatrix}a & b\\ cs & d\end{pmatrix} = \begin{pmatrix}a & b & 0 & 0\\ cs & d & 0 & 0\\ 0 & 0 & a & -b\\ 0 & 0 & -cs & d\end{pmatrix}$$

can be moved to

$$\phi_\alpha\begin{pmatrix}d & c\\ bs & a\end{pmatrix} = \begin{pmatrix}d & c & 0 & 0\\ bs & a & 0 & 0\\ 0 & 0 & d & -c\\ 0 & 0 & -bs & a\end{pmatrix}$$

by ≤ 26 elementary transformations.

We do not use it here, but to put things in the right prospective, let us reproduce the swindling lemma for long roots [KPV, Lemma 6.7], on which the proof of Lemma 5.3 hinges, and which is a true analogue of Lemma 5.1 valid for all commutative rings. The number of moves in Lemma 5.4 *seems* to be smaller than in Lemma 5.1. The reason is that we do not return the element of $\mathrm{SL}(2,R)$ to the initial position, corresponding to the long root β, but leave it in another embedding, corresponding to another long root $2\alpha+\beta$. This "half-swindling" in the long root embedding was followed by returning to the embedding φ_α corresponding to the short root α (see [KPV, Lemma 6.9]). This was sufficient for the proof of the key Proposition 6.10 in [KPV]

Lemma 5.4 [KPV, Lemma 6.7] *Let $a,b,c,d,s \in R$, $ad - bcs^2 = 1$, and, moreover, $a \equiv d \equiv 1 \pmod{s}$. Then*

$$\phi_\beta\begin{pmatrix}a & b\\ cs^2 & d\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & a & b & 0\\ 0 & cs^2 & d & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

can be moved to

$$\phi_{2\alpha+\beta}\begin{pmatrix} d & -c \\ -bs^2 & a \end{pmatrix} = \begin{pmatrix} d & 0 & 0 & -c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -bs^2 & 0 & 0 & a \end{pmatrix}$$

by ≤ 8 *elementary transformations.*

6 SL$(3, R)$: function case

Here, we prove that in the function case $L(2) \leq 44$. This allows us to calculate *explicit* uniform bounds for the width of all Chevalley groups of rank ≥ 2, with the sole exception of Sp$(4, R)$. This last case cannot be reduced to SL$(3, R)$ but can be treated similarly – and, in fact, *nominally*[4] easier, since there we have swindling lemma for short roots in full generality, Lemma 5.3 = [KPV, Proposition 6.10].

With the bound $L \leq 65$, the following result was already established by Trost [Tr2, Theorem 1.3]. We use his arithmetic lemmas, but to derive the bounded generation, we adopt the strategy of Nica [Ni], with some improvements suggested in our previous paper [KPV].

Lemma 6.1 *For any Dedekind ring of arithmetic type R in a global function field K, any element in* SL$(3, R)$ *is a product of* $L \leq 44$ *elementary root unipotents.*

Proof Let, as always, K be a global function field with the field of constants $\mathbb{F}_q$ and $R = \mathcal{O}_{K,S}$ be any ring of arithmetic type with the quotient field K.

• We start with any matrix $A \in \mathrm{SL}(3, R)$ and reduce it to a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, R) \leq \mathrm{SL}(3, R)$$

by ≤ 7 elementary moves.

• Now by Lemma 2.1, any matrix in $A \in \mathrm{SL}(2, \mathcal{O}_{K,S})$ can be reduced to a matrix $A \in \mathrm{SL}(2, \mathcal{O}_K)$ at the cost of ≤ 3 elementary moves. Thus, we can from the very start assume that $A \in \mathrm{SL}(2, \mathcal{O}_K)$ – in other words, that $R = \mathcal{O}_K$ is precisely the ring of integers of K.

• Using a version of Dirichlet theorem (= Kornblum–Landau–Artin theorem in the function case) on primes in arithmetic progressions, we can assume that bR is a prime ideal at the cost of 1 elementary move.

Now Lemma 2.5 implies that there exists $c \in R$ such that $bc \equiv -1 \pmod a$ and $\delta(b)$ and $\delta(c)$ are coprime. The first of these conditions guarantees the existence of $d \in R$ such that $ad - bc = 1$. Since modulo the root subgroup $X_{21} = \{t_{21}(\xi),\ \xi \in R\}$ a matrix $A \in \mathrm{SL}(2, R)$ only depends on its first row, by another 1 elementary move, we can assume that the entries of our A themselves have this last property. At this step, we have used 2 elementary moves.

[4] Of course, the difference comes from the fact that there we use extraction of square roots of Mennicke symbols. We *could* do the same here, getting a slightly shorter proof, with slightly worse bounds.

- Let $u, v \in \mathbb{N}$ be such that $u\delta(b) - v\delta(c) = 1$. It follows that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{u\delta(b)} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-v\delta(c)},$$

and we reduce the factors independently.

With this end, we proceed exactly as Carter and Keller do in [CK1], and as everybody after them. Namely, we invoke the Cayley–Hamilton theorem, which asserts that $A^2 = \mathrm{tr}(A)A - I$ so that

$$A^m = X(\mathrm{tr}(A))I + Y(\mathrm{tr}(A))A,$$

where I stands for the identity matrix and X, Y are polynomials in $\mathbb{Z}[t]$.

It is well known that X divides $Y^2 - 1$ or, what is the same, Y divides $X^2 - 1$; see the proof of [CK1, Lemma 1]. Since $\mathbb{Z}[t]$ is a unique factorization domain, there exists a factorization

$$Y = Y_1 Y_2, \qquad X \equiv 1 \pmod{Y_1}, \quad X \equiv -1 \pmod{Y_2}.$$

Remark 6.2 In fact, X and Y are explicitly known; *morally*, they are the values of two consecutive Chebyshev polynomials U_{m-1} and U_m at $\mathrm{tr}(A)/2 = (a+d)/2$, which allows one to argue inductively, *without swindling*. This is essentially the approach taken by Sergei Adian and Jens Mennicke [AM], only that they are not aware these are Chebyshev polynomials and have to establish their properties from scratch. We do not follow this path here since it would require considerably more elementary moves. ∎

- Thus, for an arbitrary m, one has

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^m = x\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + y\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} x+ya & yb \\ yc & x+yd \end{pmatrix},$$

where $x = X(a+d)$, $y = X(a+d)$. An explicit calculation shows that

$$x + ya \equiv a^m \pmod{b} \qquad \text{and} \qquad x + ya \equiv a^m \pmod{c}.$$

Substituting $a + d$ into the decomposition $Y = Y_1 Y_2$, we get

$$y = y_1 y_2, \qquad \text{where} \quad y_1 = Y_1(a+d), \quad y_2 = Y_2(a+d).$$

By the very definition of y_1 and y_2, one has

$$x \equiv 1 \pmod{y_1}, \qquad x \equiv -1 \pmod{y_2},$$

now as congruences in R. Thus,

$$x + ya \equiv x + yd \equiv 1 \pmod{y_1}, \qquad x + ya \equiv x + yd \equiv -1 \pmod{y_2},$$

and we are in a position to apply swindling, as stated in Lemma 5.1.

- Now, applying Lemma 5.1 we reduce

$$A^m = \begin{pmatrix} x+ya & yb \\ yc & x+yd \end{pmatrix}$$

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

to either

$$B = \begin{pmatrix} x + ya & y^2 b \\ c & x + yd \end{pmatrix}$$

or

$$C = \begin{pmatrix} x + ya & b \\ y^2 c & x + yd \end{pmatrix}$$

depending on whether we argue modulo c or modulo b, both in ≤ 11 elementary moves.

• In the first case, A^m, $m = -v\delta(c)$, by one appropriate row transformation, we get

$$t_{12}(*)B = \begin{pmatrix} \left(a^{\delta(c)}\right)^{-v} & * \\ c & x + yd \end{pmatrix},$$

where $a^{\delta(c)}$, and hence, $\left(a^{\delta(c)}\right)^{-v}$, is congruent to an element of $\mathbb{F}_q$ modulo c. Thus, changing the parameter of the elementary move, we may from the very start assume that

$$t_{12}(*)B = \begin{pmatrix} e & * \\ c & x + yd \end{pmatrix},$$

with $f \in \mathbb{F}_q^*$. Two more moves make this matrix diagonal

$$t_{21}(-cf^{-1})t_{12}(*)Bt_{12}(*) = h_{12}(f).$$

Altogether, we have spent $\leq 14 = 11 + 3$ elementary moves to reduce A^m to a semisimple root element in this case.

• The analysis of the second case, A^m, $m = u\delta(b)$, is similar. As above, by one appropriate column transformation, we get

$$Ct_{21}(*) = \begin{pmatrix} \left(a^{\delta(b)}\right)^{u} & b \\ * & x + yd \end{pmatrix},$$

where $a^{\delta(b)}$, and thus also $\left(a^{\delta(b)}\right)^{u}$, is congruent to an element of $\mathbb{F}_q$ modulo c. Thus, changing the parameter of the elementary move, we may from the very start assume that

$$t_{12}(*)B = \begin{pmatrix} g & b \\ * & x + yd \end{pmatrix},$$

with $g \in \mathbb{F}_q^*$. Two more moves make this matrix diagonal

$$t_{12}(*)Bt_{21}(*)t_{12}(-g^{-1}b) = h_{12}(g).$$

As above, we have spent $\leq 14 = 11 + 3$ elementary moves to reduce A^m to a semisimple root element in this case as well.

• As is classically known (see, for instance, [KPV, Corollary 2.2]), the semisimple root element $h_{12}(fg) = h_{12}(f)h_{21}(g)$ can be expressed as a product of ≤ 4 elementary transformations.

Altogether, this gives us $\leq 7 + 3 + 2 + 11 + 11 + 3 + 3 + 4 = 44$ elementary moves. A reference to Trost would give 65.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Remark 6.3 The estimate in Lemma 6.1 can eventually be slightly improved. Namely, instead of appealing to Lemma 2.1 at the second step of the proof, we could proceed as in [Tr2, Remark 2.5]. More precisely, in our setup, there exists an element $x \in K$, transcendental over $\mathbb{F}_q$, such that the integral closure of $\mathbb{F}_q[x]$ in K is isomorphic to $\mathcal{O}_{K,S}$; see [Ge, Example (ii)] or [Ro, Proposition 7]. More explicitly, according to Proposition 6 and the subsequent lemma in [Ro], if $S = \{P_1, \dots, P_s\}$ and $D = a_1P_1 + \dots a_sP_s$ is a positive divisor of sufficiently large degree, then D appears as the polar divisor D_∞ of some x, so that $\mathrm{div}(x) = D_0 - D_\infty$.

This argument allows one to justify the proof of [Tr2, Lemma 3.1] over an arbitrary $R = \mathcal{O}_{K,S}$; see [KMR]. However, we do not know whether this is enough to streamline all steps of our proof, particularly the third one where we use Lemma 2.5. If yes, this would save us three elementary moves and give the estimate $L \le 41$.

7 $\mathrm{Sp}(4,R)$: function case

Here, we prove that for the group $\mathrm{Sp}(4,R)$ in the function case, the uniform bound is ≤ 90. Modulo Lemma 2.5 = [Tr2, Lemma 3.3], it is essentially the same proof as the one given in [KPV, Section 6.4], which from the very start uses extraction of square roots of Mennicke symbols – thus, Lemma 2.3 = [Tr2, Lemma 3.1]. Since the swindling in short root position established in [KPV, Proposition 6.10] is already quite general, the *only* difference with the proof in [KPV] is the necessity to invoke Lemma 2.1 to reduce to a matrix with entries in $\mathcal{O}_K$, which costs 3 extra moves.

Lemma 7.1 *For any Dedekind ring of arithmetic type R in a global function field K, any element in* $\mathrm{Sp}(4,R)$ *is a product of $L \le 90$ elementary root unipotents.*

Proof Essentially, we argue exactly as in the proof of Lemma 6.1, but now relying on the symplectic versions of the main lemmas from [KPV, Section 6], the SL_2-part of the argument will be exactly the same, so we only indicate differences.

As above, we start with a global function field K with the field of constants $\mathbb{F}_q$, and any ring of arithmetic type $R = \mathcal{O}_{K,S}$ therein.

• We start with any matrix $A \in \mathrm{Sp}(4,R)$ and reduce it to a matrix

$$A = \phi_\beta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}^\beta(2,R) \le \mathrm{Sp}(4,R)$$

in the *long* root embedding of $\mathrm{SL}(2,R)$ by ≤ 10 elementary moves, [KPV, Lemma 6.1].

• Now by Lemma 2.1, any matrix in $A \in \mathrm{SL}^\beta(2,\mathcal{O}_{K,S})$ can be reduced to a matrix $A \in \mathrm{SL}^\beta(2,\mathcal{O}_K)$ at the cost of ≤ 3 elementary moves so that we can from the very start assume that $R = \mathcal{O}_K$ is the full ring of integers of K.

The next step does not have analogues for $\mathrm{SL}(3,R)$.

• Now, being inside $\mathrm{SL}(2,\mathcal{O}_K)$, we can invoke Lemma 2.3 to transform our A to another

$$A = \phi_\beta \begin{pmatrix} a & b^2 \\ * & * \end{pmatrix} \in \mathrm{SL}^\beta(2,R) \le \mathrm{Sp}(4,R),$$

with different a and b, at a cost of ≤ 3 elementary moves.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

• Next, we can move such an A to a matrix of the shape

$$A = \phi_\beta \begin{pmatrix} a & b^2 \\ -c^2 & * \end{pmatrix} \in \mathrm{SL}^\beta(2,R) \le \mathrm{Sp}(4,R),$$

by ≤ 1 elementary move [KPV, Lemma 6.14], which, in turn, can be moved to a short root position

$$\phi_\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & -b \\ 0 & 0 & -c & d \end{pmatrix} \in \mathrm{SL}^\alpha(2,R) \le \mathrm{Sp}(4,R),$$

at a cost of ≤ 9 elementary moves; see [KPV, Lemma 6.9]. Altogether, this gives us ≤ 10 elementary moves at this step; compare [KPV, Lemma 6.15].

At this stage, we are in the same situation as in the proof of Lemma 6.1 and can return to its third step repeating the proof from that point on *almost* verbatim. Of course, now we have a stronger and more general version of swindling, Lemma 5.3 instead of Lemma 5.1, but on the other hand, since it involves switching to long root embeddings, and then back again, it requires many more elementary moves than in the linear case. Let us list the steps to specify the number of elementary moves.

• Again, using a version of the Dirichlet theorem and Lemma 2.5 =[Tr2, Lemma 3.3], we can assume that b is prime and c is such that $\delta(b)$ and $\delta(c)$ are coprime. This requires ≤ 2 elementary moves.

• After that, it is exactly the same proof as that of Lemma 6.1, with reference to Lemma 5.3 instead of Lemma 5.1, which uses 26 elementary moves instead of 11 in the linear case.

• The last three steps are now literally the same as in the proof of Lemma 6.1, adding 3+3+4 elementary moves to reduce A to the identity matrix.

This finishes the proof of Lemma 7.1. Altogether, we have used

$$\le 10 + 3 + 3 + 10 + 2 + 26 + 26 + 3 + 3 + 4 = 90$$

elementary moves, as claimed. ∎

Remark 7.2 In the spirit of Remark 6.3, one can eventually improve the estimate in Lemma 7.1 to $L \le 87$ by circumventing the use of Lemma 2.1.

Remark 7.3 The 6 elementary moves needed to diagonalize the matrix at the end of the proof of Lemmas 6.1 and 7.1 have been forgotten in the proof of [KPV, Theorem 6.18]. This corrigendum worsens the estimate in that theorem to $w_E(\mathrm{Sp}(4,\mathbb{F}_q[t])) \le 85$.

8 $\mathrm{Sp}(4,R)$: number case

Thus, the only piece that is lacking at this point is a uniform bound for Dedekind rings R of number type with finite multiplicative group R^*. Since $G_{\mathrm{sc}}(\Phi,\mathbb{Z})$, $\mathrm{rk}(\Phi) \ge 2$, are boundedly generated [Ta2], we can henceforth assume that $R = \mathcal{O}_K$ is the ring of integers of an imaginary quadratic field K, $[K:\mathbb{Q}] = 2$.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

The existence of a uniform elementary width bound $L = L(2,2)$ for $\mathrm{SL}(3,R)$, $R = \mathcal{O}_K$, $[K:\mathbb{Q}] = 2$ was established by Carter, Keller, and Paige [CKP] in the language of model theory/nonstandard analysis[5] and then presented slightly differently, in more traditional logical terms, by Morris [Mo]. Observe, though, that their bound is uniform but *not* explicit.

As we know from Sections 2 and 3, the existence of a uniform bound for $\mathrm{SL}(3,R)$ implies the existence of uniform bounds for all $G_{\mathrm{sc}}(\Phi,\mathbb{Z})$, $\mathrm{rk}(\Phi) \geq 2$, with the sole exception of $\mathrm{Sp}(4,R)$.

However, using the results of Bass, Milnor, and Serre [BMS], the existence of a uniform bound for elementary width of $\mathrm{Sp}(4,R)$, $R = \mathcal{O}_K$, $[K:\mathbb{Q}] = 2$ can be easily derived by exactly the same methods as in [CKP], [Mo]. Below, we sketch a proof of the following result.

Lemma 8.1 *There exists a uniform bound $L = L'(2,2)$ such that the width of all groups $\mathrm{Sp}(4,R)$, where $R = \mathcal{O}_K$ is the ring of integers in a quadratic number field $[K:\mathbb{Q}] = 2$, does not exceed L.*

With this end, we have to briefly recall parts of its general context.

8.1 Bounded generation of ultrapowers

First, recall that being algebraic groups Chevalley groups themselves commute with direct products:

$$G(\Phi, \prod_{i\in I} R_i) = \prod_{i\in I} G(\Phi, R_i).$$

However, elementary groups do not, in general, commute with direct products, which is due to the lack of the uniform elementary generation. Namely, Wilberd van der Kallen noticed that the quotient

$$E(\Phi,R)^{\infty}/E(\Phi,R^{\infty})$$

(countably many copies) is precisely the obstruction to the bounded generation of $E(\Phi,R)$. This easily ensues from the following obvious observation. In the case of $\mathrm{SL}(n,R)$ the following result is [CKP, Theorem 2.8]; generalization to all Chevalley groups is immediate.

Lemma 8.2 *Let I be any index set and R_i, $i \in I$ be a family of commutative rings. Suppose all $E(\Phi,R_i)$ have elementary width $\leq L$,*

$$E(\Phi,R_i) = E^L(\Phi,R_i).$$

Then the elementary width of

$$\prod_{i\in I} E(\Phi,R_i) = E\Big(\Phi, \prod_{i\in I} R_i\Big)$$

does not exceed $2LN$. Conversely, the above equality implies that all $E(\Phi,R_i)$ are uniformly elementarily boundedly generated.

[5] In fact, they established the existence of such a uniform bound $L = L(n-1,d)$ for $\mathrm{SL}(n,R)$, $R = \mathcal{O}_K$, $[K:\mathbb{Q}] = d$ that depends on the rank $n-1$ of the group *and* the degree d of the number field.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Proof Take $g_i \in E(\Phi, R_i)$, $i \in I$, and for each $i \in I$, choose an elementary expression of g_i of length $\leq L$, say

$$g_i = x_{\beta(i)_1}(\xi(i)^1)\dots x_{\beta(i)_L}(\xi(i)^L) = \prod_{j=1}^{L} x_{\beta(i)^j}(\xi(i)_j) \in E(\Phi, R_i).$$

If an actual expression of g_i is shorter than L, just set the remaining $\beta(i)_j$ to the maximal root of Φ and $\xi(i)_j$ to 0.

Now consider any ordering of roots in $\Phi = \{\gamma_1, \dots, \gamma_{2N}\}$ and form products

$$u(i)^j = x_{\gamma_1}(\xi(i)^j_1)\dots x_{\gamma_{2N}}(\xi(i)^j_{2N}) = \prod_{h=1}^{2N} x_{\gamma_h}(\xi(i)^j_h) \in E(\Phi, R_i), \qquad 1 \leq j \leq L$$

by the following rule:

$$\xi(i)^j_h = \begin{cases} \xi(i)^j, & \text{if } \beta(i)_j = \gamma_h, \\ 0, & \text{otherwise.} \end{cases}.$$

Then clearly

$$g_i = u(i)^1 \dots u(i)^L \in E(\Phi, R_i), \qquad i \in I.$$

Thus, every element

$$g = (g_i)_{i\in I} \in \prod_{i\in I} E(\Phi, R_i)$$

can be expressed as $g = u^1 \dots u^L$, where each of the L factors

$$u^j = (u(i)^j)_{i\in I} \in E(\Phi, \prod_{i\in I} R_i), \qquad 1 \leq j \leq L$$

can be expressed as a product of $2N$ elementary generators

$$u^j = x_{\gamma_1}\Big((\xi(i)^j_1)_{i\in I}\Big)\dots x_{\gamma_{2N}}\Big((\xi(i)^j_{2N})_{i\in I}\Big)$$

with parameters in $\prod_{i\in I} R_i$.

Conversely, an element $g = (g_i)_{i\in I}$, where $g_i \in E(\Phi, R_i)$, such that the length of its components g_i is unbounded, cannot possibly belong to $E(\Phi, \prod_{i\in I} R_i)$. ∎

Since bounded generation is inherited by factors, any **ultraproduct** $R = \prod_{\mathcal{U}} R_i$ of rings R_i for which the elementary groups $E(\Phi, R_i)$ are uniformly boundedly generated enjoys the property that $E(\Phi, R)$ is boundedly generated. In particular, this applies to **ultrapowers** $^*R$, also known as nonstandard models of R. In other words, we have the following result.

Lemma 8.3 *Bounded elementary generation of the elementary group $E(\Phi, R)$ is equivalent to the equality*

$$^*E(\Phi, R) = E(\Phi, {}^*R)$$

for all nonstandard models $^*R$ of R.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Proof By the remark preceding the statement of this lemma, we only need to check the inverse implication. Denote by F the Fréchet filter on $\mathbb{N}$. Assume that $E(\Phi, R)$ is not boundedly generated, or, what is the same, there exists a sequence $g_i \in E(\Phi, R)$, $i \in \mathbb{N}$ of matrices from $E(\Phi, R)$ with infinitely growing lengths. Then the element $g = (g_1, g_2, g_3, \dots)$ has infinite length in $E(\Phi, R)^\infty$ and, by the very definition of F, also in $E(\Phi, R)^\infty/F$. In other words, $g \notin E(\Phi, R^\infty/F)$.

Since F is the intersection of all nonprincipal ultrafilters, there exists a nonprincipal ultrafilter $\mathcal{U}$ such that the image of g in the ultrapower ${}^*E(\Phi, R) = E(\Phi, R)^\infty/\mathcal{U}$ does not belong to $E(\Phi, {}^*R) = E(\Phi, R^\infty/\mathcal{U})$. Thus, for this particular $\mathcal{U}$, we have ${}^*E(\Phi, R) \neq E(\Phi, {}^*R)$. ∎

Remark 8.4 Assuming the Continuum Hypothesis, all ${}^*R$ are isomorphic and one has to require the equality ${}^*E(\Phi, R) = E(\Phi, {}^*R)$ for *one* nonstandard model. Otherwise, there are $2^{2^{\aleph_0}}$ ultrafilters that lead to non-isomorphic ${}^*R$, and to be on the safe side, one has to stipulate this equality for all of them.

8.2 Congruence subgroup problem for nonstandard models

However, Carter, Keller, and Paige [CKP] made this observation quite a bit more precise. Namely (see [CKP, 2.1] or [Mo, Lemma 2.29]), they established the following fact.

Lemma 8.5 *Bounded elementary generation of the elementary group $E(\Phi, R)$ is equivalent to the condition*

$$E(\Phi, {}^*R) \quad \textit{has a finite index in} \quad {}^*E(\Phi, R),$$

for all nonstandard models ${}^*R$ of R.

In fact, they proved that bounded elementary generation of the elementary group $E(\Phi, R)$ is equivalent to the almost positive solution of the congruence subgroup problem for all nonstandard models ${}^*R$ of R.

More precisely, [CKP, 2.3] and [Mo] apply the whole machinery not just to the bounded generation of $\mathrm{SL}(n, R)$ but also to the bounded generation of $E(n, R, \mathfrak{q})$ in terms of the conjugates of elementary generators of level $\mathfrak{q}$. They consider groups $\mathrm{SL}(n, R, \mathfrak{q})/E(n, R, \mathfrak{q})$ which are isomorphic to quotients of universal Mennicke groups $C(\mathfrak{q})$ for all nonzero ideals $\mathfrak{q} \trianglelefteq R$ and restate bounded elementary generation of $E(n, R, \mathfrak{q})$ as the almost positive solution of the congruence subgroup problem for $\mathrm{SL}(n, {}^*R)$.

Recall that we need a universal bound that depends only on the root system Φ and the degree of K. Since we reduce the problem to the congruence subgroup problem for $\mathrm{SL}(n, {}^*R)$, we are very close to that.

8.3 Universal bound

Before going to $\mathrm{Sp}(4, R)$ we shall recall one more principal invention of Carter, Keller, and Paige [CKP]. We need to pass from the ring of integers $R = \mathcal{O}_K$ in an algebraic number field to the ring ${}^*R$. The ring ${}^*R$ is a nonstandard model of R; that is, ${}^*R$ equals to an ultrapower $\prod_{\mathcal{U}} R$ along the ultrafilter $\mathcal{U}$. The good point is that thanks to Łoś's theorem [ChKe, Theorem 4.1.9] ultrapowers keep first-order properties of structures unchanged. The bad point is that other properties do not survive, and in many senses, ${}^*R$ is far away from the ring of integers R.

With this end, Carter, Keller, and Paige [CKP] introduce arithmetic conditions $\mathrm{Gen}(t,r)$ and $\mathrm{Exp}(t,s)$ on a ring R that depend on natural parameters r, s, and t, which are too technical to describe them here in full. Morally, $\mathrm{Gen}(t,r)$ allows to uniformly bound the number of generators of the abelian groups $C(\mathfrak{q})$, while $\mathrm{Exp}(t,s)$ allows to uniformly bound their exponent. Besides, [CKP] constantly used the fact that the stable rank of R is 1.5.

The importance of these conditions consists in the following pivotal observations. First of all, conditions $\mathrm{Gen}(t,r)$, $\mathrm{Exp}(t,s)$, and $\mathrm{sr}(R) = 1.5$ are stated in the first-order language of ring theory; see [CKP, 2.2] or [Mo, Sections 3A and 3B]. Hence, the characteristic property of ultraproducts imply the following:

Lemma 8.6 *A commutative ring R satisfies conditions* $\mathrm{Gen}(t,r)$ *and* $\mathrm{Exp}(t,s)$ *with specific parameters if and only if ${}^*R$ satisfies these conditions with the same parameters. Besides,* $\mathrm{sr}({}^*R)$ *is 1.5.*

Most importantly, these conditions allow to bound *uniformly* the universal Mennicke groups $C(\mathfrak{q})$ for all ideals $\mathfrak{q} \trianglelefteq R$ – and thus to get the finite congruence kernel of $G(\Phi, {}^*R)$. Indeed, the main (difficult!) step in obtaining a uniform bound in the number case is the following result; see [CKP, Theorem 1.8] or [Mo, Theorem 3.11].

Lemma 8.7 *Let r, s, t be positive integers, and let R be an integral domain subject to the conditions*

- $\mathrm{sr}(R) = 1.5$, • $\mathrm{Gen}(t,r)$, • $\mathrm{Exp}(t,s)$.

Then for all ideals $\mathfrak{q}$, the universal Mennicke group $C(\mathfrak{q})$ is finite and its order is uniformly bounded by t^r.

Finally, the rings of integers of the number fields of bounded degree $[K : \mathbb{Q}] \le d$ satisfy these conditions for some values of parameters (which depend on d and which we do not wish to specify here). This result depends on [a very strong form of] the Dirichlet theorem on primes in arithmetic progressions. The following lemma is a [weaker form of the] conjunction of [CKP, Lemmas 4.4 and 4.5] or [Mo, Corollary 3.5 and Theorem 3.9]; the proof thereof requires subtle arithmetic properties of norm maps on the groups of units that are based on the aforementioned Dirichlet theorem (see [CKP, Lemma 4.3] or [Mo, Lemma 3.8]).

Lemma 8.8 *The ring of integers $R = \mathcal{O}_K$ in an algebraic number field K satisfies* $\mathrm{Gen}(t,1)$ *for every positive integer t and* $\mathrm{Exp}(t,2)$ *for some t depending on the degree $d = [K : \mathbb{Q}]$.*

Hence, one can take $R = {}^*R$ in Lemma 8.7 and arrive at the almost positive solution of the congruence problem in $\mathrm{SL}(n, {}^*R)$, as required.

To use the above fact for $\mathrm{SL}(n, {}^*R) = \mathrm{SL}(n, \prod_{\mathcal{U}} R)$ is the same as to use the Compactness Theorem as is in [CKP] or [Mo, Theorem 2.7]. In any case (cf. [CKP, Theorem 2.4] or [Mo, Corollary 3.13]), we get bounded elementary generation of $\mathrm{SL}(n, R)$ with the bound that only depends on the root system Φ and the degree of K.

At this point, [CKP, 2.5] use a standard argument from nonstandard analysis. Since the elementary width $w(G) \in {}^*\mathbb{N}$ of $G = \mathrm{SL}(n, R)$ on this class of rings R is internally

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

defined, everywhere finite, and bounded (by any infinite natural number), it must attain maximal value, which is obviously finite (all of them are!).

The proof of the uniform bounded generation for Chevalley groups will be completed if we cover the case of symplectic groups. The standard reasoning says that it is enough to prove the fact for the rank 2 case – that is, for $\mathrm{Sp}(4, R)$. The proof basically follows the line depicted above for $G = \mathrm{SL}(n, R)$.

Passing from $\mathrm{SL}(n, R)$ to $\mathrm{Sp}(2l, R)$ ($l \geq 2$), we have to consider the group $\mathrm{Cp}(\mathfrak{q}) := \mathrm{Sp}(2l, \mathfrak{q})/\mathrm{Ep}(2l, \mathfrak{q})$ in place of $C(\mathfrak{q})$ (recall that the group $\mathrm{Cp}(\mathfrak{q})$ is well defined, finite, and independent of l; see [BMS, Theorem 12.4 and Corollary 12.5]).

The case $\mathrm{Sp}(4, R)$ is similar but much more difficult than the one of $\mathrm{SL}(3, R)$. The point is that there are two embeddings $\mathsf{A}_1 \to \mathsf{C}_2$ and $\widetilde{\mathsf{A}}_1 \to \mathsf{C}_2$, on long and short roots, respectively. This results in a more complicated structure of the universal Mennicke group (cf. [BMS, Lemma 13.3]). The decisive role is played by the following quite technical theorem proven by Trost. It serves as a symplectic analogue of Lemma 8.7.

Lemma 8.9 [Tr1, Theorem 3.16] *Let s, t be positive integers, and let R be a commutative ring with 1 subject to the conditions*

- $\mathrm{sr}(R) = 1.5$, • $\mathrm{Gen}(2, 1)$, • $\mathrm{Gen}(t, 1)$, • $\mathrm{Exp}(t, s)$.

Then for all ideals $\mathfrak{q}$, the group $\mathrm{Cp}(\mathfrak{q})$ is finite and its order is uniformly bounded by $2t$.

This parallelism can now be used to conclude that $\mathrm{Sp}(4, R)$ is *uniformly* elementarily boundedly generated, with a *universal* bound that only depends on the degree of K (which is equal to 2 in the case under consideration), and is thus an *absolute* constant (see [Tr1, Theorem 3.20 and Section 3.3] for details of the proof). This concludes the proof of Lemma 8.1.

Remark 8.10 The arguments presented above can be rephrased in a more traditional logical language, in the form of the compactness theorem of the first-order logic, as was done by Morris [Mo, Proposition 1.5] and Trost [Tr1, Theorem 3.1].

9 Concluding remarks

Here, we mention a couple of eventual generalizations of our results.

• In the number case, the bounds for $L(2, 2)$ and $L'(2, 2)$ are not explicit at all. It seems that it might be quite a challenge to obtain *any* explicit bounds. Our impression is that it cannot be easily done at the level of the groups; one should invoke much more arithmetics.

• However, we do not claim that the bounds obtained in the present paper in the function case are sharp in any sense. It is another, maybe even a greater, challenge to obtain such sharp bounds. It is usually very hard to estimate width from above, but still harder to estimate it from below.

• Let $\mathfrak{q} \trianglelefteq R$ be an ideal of R. In the present paper, we addressed the *absolute* case $\mathfrak{q} = R$ alone. However, it makes sense to ask similar questions for the *relative* case; in other words, we believe there are *uniform* width bounds for the true elementary subgroup $E(\Phi, \mathfrak{q})$ and the relative elementary subgroups $E(\Phi, R, \mathfrak{q})$ of level $\mathfrak{q} \trianglelefteq R$ in terms of elementary generators, or elementary conjugates of level $\mathfrak{q}$.

There are some partial results in this direction for classical groups, but some of them use larger sets of generators. The results by Tavgen [Ta2], Sergei Sinchuk, and

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

Andrei Smolensky [SiSm] and by Pavel Gvozdevsky [Gv] use correct sets of generators (so-called Tits–Vaserstein generators), but their bounds are not uniform. Recently, the third author established the conclusive result in this direction [Va2]: Theorem B in that paper states that given a reduced irreducible root system Φ of rank ≥ 2, a Dedekind ring R of arithmetic type, and an ideal $\mathfrak{q}$ of R, there exists a constant $M = M(\Phi, R, \mathfrak{q})$ such that any element in $E_{sc}(\Phi, R, \mathfrak{q})$ is a product of at most M Tits–Vaserstein generators. Note that as in the works cited above, M depends on the ring and the ideal. In comparison, in the function case, Trost [Tr3] produced uniform bounds for all types of irreducible root systems except B_n and D_n.[6]

Acknowledgements We are grateful to Nikolai Bazhenov, Sergei Gorchinsky, Pavel Gvozdevsky, Andrei Lavrenov, Alexei Myasnikov, Denis Osipov, Ivan Panin, Victor Selivanov, and Dmitry Timashev for useful discussions of various aspects of this work [and [KLPV]]. Our special thanks go to Alexander Trost whose thoughtful comments on an earlier version of this paper allowed us to considerably improve the exposition. We thank the referee for careful reading and important remarks.

References

[AM] S. Adian and J. Mennicke, *Bounded generation of $SL(n, \mathbb{Z})$*. Intern. J. Algebra Comput. **2**(1992), 357–365.

[Ba] H. Bass, *Clifford algebras and spinor norms over a commutative ring*. Amer. J. Math. **96**(1974), 156–206.

[BMS] H. Bass, J. Milnor and J-P. Serre, *Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$*. Publ. Math. IHES **33**(1967), 59–137.

[CK1] D. Carter and G. Keller, *Bounded elementary generation of $SL_n(\mathcal{O})$*. Amer. J. Math. **105**(1983), 673–687.

[CK2] D. Carter and G. E. Keller, *Elementary expressions for unimodular matrices*. Commun. Algebra **12**(1984), 379–389.

[CKP] D. Carter, G. E. Keller and E. Paige, *Bounded expressions in $SL(n, A)$*. Preprint, 1985, Univ. Virginia, 1–46.

[Ca] R. W. Carter, *Simple groups of Lie type*, Wiley, London et al., 1972.

[ChKe] C. C. Chang and H. J. Keisler, *Model theory*, Elsevier, 1990.

[CW] G. Cooke and P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to SL_2*. Commun. Algebra **3**(1975), 481–524.

[Ge] L. J. Gerstein, *Indecomposable integral quadratic forms over global function fields*. Acta Arith. **96**(2000), 89–95.

[Gv] P. Gvozdevsky, *Width of $SL(n, O_S, I)$*. Commun. Algebra **51**(2023), 1581–1593.

[Ha] U. Hadad, *On Kazhdan constants of finite index subgroups in $SL_n(\mathbb{Z})$*. Internat. J. Algebra Comput. **22**(2012), 1250026, 18 pp.

[HO] A. Hahn and O. O'Meara, *The classical groups and K-theory*, Springer-Verlag, Berlin, 1989.

[JZ] B. W. Jordan and Y. Zaytman, *On the bounded generation of arithmetic SL_2*. Proc. Natl. Acad. Sci. USA **116**(2019), 18880–18882.

[KLPV] B. Kunyavskiĭ, A. Lavrenov, E. Plotkin and N. Vavilov, *Bounded generation of Steinberg over Dedekind rings of arithmetic type*. Preprint, 2022, arXiv:2204.10951.

[KMR] B. Kunyavskiĭ, D. W. Morris and A. S. Rapinchuk, *Bounded elementary generation of SL_2: approaching the end*. In preparation.

[KPV] B. Kunyavskiĭ, E. Plotkin and N. Vavilov, *Bounded generation and commutator width of Chevalley and Kac–Moody groups: function case*. Europ. J. Math. **9**(2023), https://doi.org/10.1007/s40879-023-00627-y.

[Li] B. Liehl, *Beschränkte Wortlänge in SL_2*. Math. Z. **186**(1984), 509–524.

[6] An unfinished project of the third author, joint with Kaisar Tulenbaev, aimed at lifting the dependence on $\mathfrak{q}$ in the number case. We do hope that his ideas will work in this case well.

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press

[LM] D. Loukanidis and V. K. Murty, *Bounded generation for* SL_n *(*$n \geq 2$*) and* Sp_n *(*$n \geq 1$*)*. Preprint, 1994.

[Ma] H. Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployés*. Ann. Sci. Éc. Norm. Sup. **2**(1969), 1–62.

[MRS] A. Morgan, A. Rapinchuk and B. Sury, *Bounded generation of* SL_2 *over rings of* S*-integers with infinitely many units*. Algebra Number Theory **12**(2018), 1949–1974.

[Mo] D. Morris, Bounded generation of $SL(n, A)$ *(after D. Carter, G. Keller, and E. Paige)*. New York J. Math. **13**(2007) 383–421.

[Mu] V. K. Murty, *Bounded and finite generation of arithmetic groups*. In Number theory (Halifax, NS, 1994), CMS Conf. Proc., Vol. 15, Amer. Math. Soc., Providence, RI, 1995, 249–261.

[Ni] B. Nica, *On bounded elementary generation for* SL_n *over polynomial rings*. Israel J. Math. **225**(2018), 403–410.

[Pl] E. Plotkin, *On the stability of the* K_1*-functor for Chevalley groups of type* E_7. J. Algebra **210**(1998), 67–85.

[Qu] C. Queen, *Some arithmetic properties of subrings of function fields over finite fields*. Arch. Math **26**(1975), 51–56.

[Ro] M. Rosen, S-units and S-class groups in algebraic function fields. J. Algebra **26**(1973), 98–108.

[Se] J-P. Serre, *Le problème des groupes de congruence pour* SL_2. Ann. Math. **92**(1970), 489–527.

[SiSm] S. Sinchuk and A. Smolensky, *Decompositions of congruence subgroups of Chevalley groups*. Intern. J. Algebra Comput. **28**(2018), 935–958.

[SSV] A. Smolensky, B. Sury and N. Vavilov, *Gauss decomposition for Chevalley groups, revisited. Intern*. J. Group Theory **1**(2011), 3–16.

[St] M. Stein, *Stability theorems for* K_1, K_2 *and related functors modeled on Chevalley groups*. Japan. J. Math **4**(1978), 77–108.

[Steinb] R. Steinberg, *Lectures on Chevalley groups*, Univ. Lecture Series, Vol. 66, Amer. Math. Soc., Providence, RI, 2016.

[Ta1] O. Tavgen, *Finite width of arithmetic subgroups of Chevalley groups of rank* ≥ 2. Sov. Math., Dokl. **41**(1990), no. 1, 136–140.

[Ta2] O. Tavgen, *Bounded generation of Chevalley groups over rings of algebraic* S*-integers*. Math. USSR Izv. **36**(1991), 101–128.

[Ta3] O. I. Tavgen, *Bounded generation of normal and twisted Chevalley groups over the rings of* S*-integers*. Contemp. Math. **131**(1992), 409–421.

[Tr1] A. A. Trost, *Bounded generation by root elements for Chevalley groups defined over rings of integers of function fields with an application in strong boundedness*. Preprint, 2021, arXiv:2108.12254.

[Tr2] A. A. Trost, *Elementary bounded generation for* SL_n for global function fields and $n \geq 3$. Bull. London Math. Soc. **56**(2024), 219–231.

[Tr3] A. A. Trost, *Stability, bounded generation and strong boundedness*. Preprint, 2023, arXiv:2305.11562.

[Va1] N. Vavilov, *Structure of Chevalley groups over commutative rings*. In Proc. conf. nonassociative algebras and related topics (Hiroshima, 1990), World Sci. Publ., London et al., 1991, 219–335.

[Va2] N. A. Vavilov, *Bounded generation of relative subgroups in Chevalley groups*. Zap. Nauchn. Semin. POMI **523**(2023), 7–18.

[VP] N. Vavilov and E. Plotkin, *Chevalley groups over commutative rings: I. Elementary calculations. Acta Applicandae Math.* **45**(1996), 73–113.

[VSS] N. A. Vavilov, A. V. Smolensky and B. Sury, *Unitriangular factorizations of Chevalley groups*. J. Math. Sci., New York **183**(2012), 584–599.

[Vs] M. Vsemirnov, *Short unitriangular factorizations of* $SL_2(\mathbb{Z}[1/p])$. Quart. J. Math. **65**(2014), 279–290.

[Za] K. Kh. Zakiryanov, *Symplectic groups over rings of algebraic integers have finite width over the elementary matrices*. Algebra and Logic **24**(1985), 436–440.

Dept. of Mathematics Bar-Ilan University, Ramat Gan, Israel
e-mail: kunyav@macs.biu.ac.il

Dept. of Mathematics Bar-Ilan University, Ramat Gan, Israel
e-mail: plotkin@macs.biu.ac.il

Dept. of Mathematics and Computer Science, St Petersburg State University, St Petersburg, Russia
e-mail: nikolai-vavilov@yandex.ru

https://doi.org/10.4153/S0008414X24000713 Published online by Cambridge University Press