BOUNDED GENERATION OF S-ARITHMETIC SUBGROUPS OF ISOTROPIC ORTHOGONAL GROUPS OVER NUMBER FIELDS

IGOR V. EROVENKO AND ANDREI S. RAPINCHUK

In memory of Professor Gordon E. Keller

ABSTRACT. Let f be a nondegenerate quadratic form in $n \geqslant 5$ variables over a number field K and let S be a finite set of valuations of K containing all Archimedean ones. We prove that if the Witt index of f is $\geqslant 2$ or it is 1 and S contains a non-Archimedean valuation, then the S-arithmetic subgroups of $\mathbf{SO}_n(f)$ have bounded generation. These groups provide a series of examples of boundedly generated S-arithmetic groups in isotropic, but not quasi-split, algebraic groups.

1. INTRODUCTION

An abstract group Γ is said to have *bounded generation* (abbreviated (BG)) if there exist elements $\gamma_1, \ldots, \gamma_t \in \Gamma$ such that $\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_t \rangle$, where $\langle \gamma_i \rangle$ is the cyclic subgroup generated by γ_i. Such groups are known to have a number of remarkable properties: the pro-p completion $\hat{\Gamma}^{(p)}$ is a p-adic analytic group for every prime p [8, 12]; if Γ in addition satisfies condition (Fab)[1] then it has only finitely many inequivalent completely reducible representations in every dimension n over any field (see [14, 23, 25] for representations in characteristic zero, and [1] for arbitrary characteristic); if Γ is an S-arithmetic subgroup of an absolutely simple simply connected algebraic group over a number field, then Γ has the congruence subgroup property [15, 20]. There are reasons to believe that the class of groups having (BG) is sufficiently broad, in particular it most probably contains all higher rank lattices in characteristic zero (note that there are also *simple,* hence nonlinear, infinite boundedly generated groups [16]). Unfortunately, bounded generation of lattices is known only in very few cases. First, it was noted that the results on factoring a unimodular matrix over an arithmetic ring as a product of a bounded number of elementary matrices [6, 7, 13, 17, 31] imply bounded generation of the corresponding unimodular groups (notice, however, that the results on "bounded factorization" do not extend to "nonarithmetic" Dedekind rings [29]). Later, Tavgen [28] showed that every S-arithmetic subgroup of a split or quasi-split algebraic group over a number field K of K-rank $\geqslant 2$ is boundedly generated. However, until recently there were no examples of boundedly generated S-arithmetic groups in algebraic groups that are not split or quasi-split. The goal of this paper is to establish bounded generation of a large family of S-arithmetic subgroups in isotropic orthogonal groups.

The first-named author would like to acknowledge partial financial support from the UNCG New Faculty Grant. The second-named author would like to acknowledge partial financial support from the NSF grant DMS-0138315, the BSF grant #2000171 and the Humboldt Foundation (Bonn, Germany).

[1] We recall that condition (Fab) for Γ means that every subgroup of finite index Γ_1 of Γ has finite abelianization $\Gamma_1^{ab} = \Gamma_1/[\Gamma_1, \Gamma_1]$.

Main Theorem *Let f be a nondegenerate quadratic form over a number field K in $n \geqslant 5$ variables, S be a finite set of valuations of K containing all Archimedean ones. Assume that either the Witt index of f is $\geqslant 2$ or it is one and S contains a non-Archimedean valuation. Then any S-arithmetic subgroup of $\mathbf{SO}_n(f)$ has bounded generation.*

This result was announced with a sketch of proof in [9] for the case where the Witt index of f is $\geqslant 2$. The argument in [9] boiled down to reducing the general case to $n = 5$ where the group is split, so one can use the result of Tavgen [28]. Unfortunately, this argument does not immediately extend to the situation where the Witt index is one due to some technical problems, but mainly because of the fact that the resulting special orthogonal group in dimension $n = 5$ is no longer split and bounded generation of its S-arithmetic subgroups has not been previously established. At the same time, the method used in [9] does not allow one to reduce $n = 5$ to $n = 4$ where the orthogonal group has type $A_1 \times A_1$ so one can apply the known results for SL_2. In the present paper, the method of [9] is modified in order to to overcome the difficulties noted above. Our primary objective was to treat the case $n = 5$, but it turned out that the resulting argument applies in all dimensions and in fact simplifies the proof given in [9].

Now, we explain briefly how the proof of the Main Theorem goes. To facilitate the use of strong approximation, we will argue for the spin group $G = \mathbf{Spin}_n(f)$ rather than for the special orthogonal group $\mathbf{SO}_n(f)$; notice that (BG) of S-arithmetic subgroups in one of them implies the same property for the other — see Proposition 6.2. We consider the standard representation of G on the n-dimensional quadratic space and, after choosing appropriately two anisotropic orthogonal vectors a, $b \in K^n$, analyze the product map

$$P := G(a) \times G(b) \times G(a) \times G(b) \xrightarrow{\mu} G,$$

where $G(a)$ and $G(b)$ denote the stabilizers of a and b, respectively. The proof of (BG) is reduced from dimension n to dimension $n-1$ by proving that either $\mu(P_{\mathcal{O}(S)})$ or a product of its several copies contains a subset of $G_{\mathcal{O}(S)}$ open with respect to the topology defined by a certain finite set of valuations (see §6 for precise formulations). To achieve this, we construct an auxiliary variety Z and factor μ as a product of two regular maps $\phi\colon P \to Z$ and $\psi\colon Z \to G$, see §2. We then establish a local-global principle for the fibers of ϕ (see §3), and finally make sure that the relevant local conditions are satisfied. Eventually, this process enables us to descend either to a 5-dimensional form of Witt index two or to a 4-dimensional isotropic form. So, to complete the argument it remains to observe that (BG) of S-arithmetic subgroups is a result of Tavgen [28] in the first case, and follows from the known results for SL_2 [7, 13, 17, 31] in the second case. It appears that some parts of the argument, particularly the entire method of factoring a sizable set of S-integral transformations of a quadratic lattice as a product of transformations of sublattices having smaller rank, are of independent interest and may have other applications.

2. Preliminaries

In this section, K will denote an arbitrary field of characteristic $\neq 2$. Let f be a nondegenerate quadratic form over K of dimension $n \geqslant 5$. Given an extension E/K, we let $i_E(f)$ denote the Witt index of f over E, and we will write $i_v(f)$ instead of

$i_{K_v}(f)$ if K is a number field and v is a valuation of K. Throughout the paper, we will assume that $i_K(f) \geqslant 1$, i.e., f is K-isotropic. We realize f on an n-dimensional vector space W over K and let $(\cdot \mid \cdot)$ denote the associated bilinear form. We also fix a basis $e_1, e_2, \ldots, e_n$ of W in which f looks as follows:

$$f(x_1, \ldots, x_n) = x_1 x_2 + \alpha_3 x_3^2 + \cdots + \alpha_n x_n^2, \tag{1}$$

and set $a = e_n$, $b = e_{n-1}$.

Next, we need to introduce some algebraic varieties and morphisms between them. Consider $\mathbf{W} = W \otimes_K \Omega$, where Ω is a "universal domain", and extend f and $(\cdot \mid \cdot)$ to $\mathbf{W}$. Let G denote the spin group $\mathbf{Spin}_n(f)$ associated with $\mathbf{W}$, regarded as an algebraic K-group (naturally) acting on $\mathbf{W}$. For a vector $w \in \mathbf{W}$, $G(w)$ will denote its stabilizer, and we will write $G(w_1, w_2)$ for $G(w_1) \cap G(w_2)$ etc. We will be working with the following algebraic K-varieties:

$$\begin{aligned}
P &= G(a) \times G(b) \times G(a) \times G(b), \\
X &= \{s \in \mathbf{W} \mid f(s) = f(a)\}, \\
Y &= \{(g, s) \in G \times X \mid (s|g(b)) = 0\}, \\
Z &= \{(g, s, t) \in Y \times \mathbf{W} \mid (t|a) = 0,\ f(t) = f(b),\ (s|t) = 0\},
\end{aligned}$$

and the following morphisms:

$$\begin{aligned}
\mu &: P \to G, & \mu(x, y, z, u) &= xyzu, \\
\phi &: P \to Z, & \phi(x, y, z, u) &= (xyzu,\ xy(a),\ xy(b)), \\
\varepsilon &: Z \to Y, & \varepsilon(g, s, t) &= (g, s), \\
\nu &: Z \to X, & \nu(g, s, t) &= s.
\end{aligned}$$

We notice that the image of ϕ is indeed contained in Z as

$$(xy(a)|xyzu(b)) = (a|zu(b)) = (z^{-1}(a)|b) = (a|b) = 0,$$

hence $(xyzu, xy(a)) \in Y$, and also

$$(xy(b)|a) = (b|x^{-1}(a)) = (b|a) = 0.$$

The proof of the Main Theorem hinges on the fact that the product morphism $\mu: P \to G$ can be factored as $\mu = \psi \circ \phi$, where

$$\psi: Z \to G, \quad \psi(g, s, t) = g.$$

Proposition 2.1

(i) *For every* $g \in G_K$, $\psi^{-1}(g)_K \neq \varnothing$.

(ii) *For every* $\zeta \in Z_K$, $\phi^{-1}(\zeta)_K \neq \varnothing$.

Consequently, $\mu(P_K) = G_K$.

Proof. (i) If $g(b) = \pm b$, one easily verifies that $(g, a, b) \in \psi^{-1}(g)_K$. So, we may assume that $g(b) \neq \pm b$. Set

$$u' = \frac{(g(b)|b)}{f(b)}\, b.$$

Being isotropic, the space $\langle a, b\rangle^{\perp}$ contains a nonzero vector u'' such that $f(u'') = f(b) - f(u')$. Then the vector $u := u' + u''$ satisfies the following conditions:

$$(u|a) = 0, \quad (u|b) = (g(b)|b), \quad \text{and} \quad f(u) = f(b).$$

Since $g(b) \neq \pm b$, the last two conditions imply that $\langle u, b\rangle$ and $\langle g(b), b\rangle$ are isometric 2-dimensional subspaces of W, so by Witt's theorem there exists $\sigma \in \mathrm{O}_n(f)$ such that $\sigma(u) = g(b)$ and $\sigma(b) = b$. Then

$$(\sigma(a)|b) = (a|b) = 0$$

and

$$(\sigma(a)|g(b)) = (a|\sigma^{-1}(g(b))) = (a|u) = 0,$$

implying that $(g, \sigma(a), b) \in \psi^{-1}(g)_K$.

(ii) Suppose that $\zeta = (g, s, t) \in Z_K$. Since $(t|a) = 0$, the vectors t and a are linearly independent. As $f(t) = f(b)$, by Witt's theorem there exists $\rho \in \mathrm{O}_n(f)$ such that

$$\rho(b) = t \quad \text{and} \quad \rho(a) = a. \tag{2}$$

In fact, one can always find such a ρ in $\mathrm{O}'_n(f)$, the kernel of the spinor norm θ on $\mathrm{SO}_n(f)$. Indeed, if $\det \rho = -1$, we can pick an anisotropic $c \in W$ orthogonal to both a and b, and replace ρ with $\rho\tau_c$, where τ_c is the reflection associated with c, which allows us to assume that $\rho \in \mathrm{SO}_n(f)$. Furthermore, since the space $\langle a, b\rangle^{\perp}$ is isotropic, there exists $\delta \in \mathrm{SO}_n(f)(a, b)$ such that $\theta(\delta) = \theta(\rho)$ (see [2, Thm. 5.18]). Then we can replace ρ with $\rho\delta^{-1} \in \mathrm{O}'_n(f)$.

Arguing similarly, we find $\eta \in \mathrm{O}'_n(f)$ such that

$$\eta(a) = s \quad \text{and} \quad \eta(b) = t \tag{3}$$

and $\sigma \in \mathrm{O}'_n(f)$ such that

$$\sigma(a) = s \quad \text{and} \quad \sigma(b) = g(b). \tag{4}$$

Since the elements ρ, η, and σ have spinor norm one, they are images under the canonical isogeny $\pi\colon \mathbf{Spin}_n(f) \to \mathbf{SO}_n(f)$ of suitable elements $\tilde{\rho}$, $\tilde{\eta}$, $\tilde{\sigma} \in G_K = \mathrm{Spin}_n(f)$. Set $x = \tilde{\rho}$, $y = \tilde{\rho}^{-1}\tilde{\eta}$, $z = \tilde{\eta}^{-1}\tilde{\sigma}$, and $u = (xyz)^{-1}g$. Then $(x, y, z, u) \in P_K$ and $xyzu = g$. Moreover, $xy(a) = s$ and $xy(b) = t$, which shows that $\phi(x, y, z, u) = \zeta$, as required. $\square$

Remark. It follows from Proposition 2.1 that $G_K = G(a)_K G(b)_K G(a)_K G(b)_K$. For classical groups, decompositions of this kind were introduced by M. Borovoi [4]. Our proof of the Main Theorem is based on the analysis of the Borovoi decomposition for the group of S-integral points. In [9] we used the Borovoi decomposition involving three factors, $G(a)$, $G(b)$, and $G(a)$, but as we will see, the decomposition with four factors allows one to bypass some technical difficulties and eventually leads to a more general result.

The following properties of the morphisms introduced above will be used in the sequel.

Lemma 2.2 *The morphisms $\phi\colon P \to Z$ and $\varepsilon\colon Z \to Y$ are surjective. Consequently, if* $\operatorname{char} K = 0$, *there exists a Zariski K-open set $P_0 \subseteq P$ such that for $h \in P_0$, the points $\phi(h)$ and $(\varepsilon \circ \phi)(h)$ are simple on Z and Y respectively, and the differentials $d_h\phi\colon T(P)_h \to T(Z)_{\phi(h)}$, $d_{\phi(h)}\varepsilon\colon T(Z)_{\phi(h)} \to T(Y)_{(\varepsilon\circ\phi)(h)}$, and $d_h\mu\colon T(P)_h \to T(G)_{\mu(h)}$ are surjective.*

Proof. It follows from Proposition 2.1 that $\phi\colon P \to Z$ and $\mu\colon P \to G$ are surjective. Now, given $(g,s) \in Y$, over an algebraically closed field one can always find $t \in \langle a,s\rangle^{\perp}$ such that $f(t)=f(b)$, whence the surjectivity of $\varepsilon\colon Z \to Y$. The rest of the lemma follows from a well-known result about dominant separable morphisms (see, for example, [3, Ch. AG, Thm. 17.3]) and the irreducibility of P. □

Lemma 2.3 *Set $\eta = \nu \circ \phi$. Then $\eta(P_E) = X_E$ for any extension E/K.*

Proof. It is enough to show that $\phi(P_E) = Z_E$ and $\nu(Z_E) = X_E$, the first assertion being part (ii) of Proposition 2.1 in which K is replaced with E. For the second assertion, let $s \in X_E$. Then by Witt's theorem there exists $g \in \mathbf{SO}_n(f)_E$ such that $g(a) = s$. Since the orthogonal complement to a in $W \otimes_K E$ is isotropic, arguing as in the proof of part (ii) of Proposition 2.1, we see that g can be chosen to be of the form $g = \pi(\tilde{g})$ for some $\tilde{g} \in G_E$. If $s = \pm a$, then one immediately verifies that $(\tilde{g}, s, b) \in \nu^{-1}(s)_E$. Otherwise, the space $\langle a,s\rangle$ is 2-dimensional. Since the orthogonal complement to $\langle a,b\rangle$ in $W \otimes_K E$ is isotropic, we can argue as in the proof of part (i) of Proposition 2.1 to find $w \in W \otimes_K E$, $w \notin \langle a,b\rangle$, satisfying

$$(w|b) = 0, \quad (w|a) = (s|a), \quad \text{and} \quad f(w) = f(a).$$

By Witt's theorem, it follows from the last two conditions that there exists $\sigma \in \mathbf{SO}_n(f)_E$ such that $\sigma(w) = s$ and $\sigma(a) = a$. Set $t = \sigma(b) \in W \otimes_K E$. Then

$$(t|a) = (\sigma(b)|\sigma(a)) = (b|a) = 0$$

and

$$(t|s) = (\sigma(b)|g(a)) = (b|\sigma^{-1}g(a)) = (b|w) = 0$$

whence $(g,s,t) \in \nu^{-1}(s)_K$, as required. □

3. Fibers of the morphism ϕ

From now on, K will denote a number field. We let V^K, V_∞^K, and V_f^K denote the set of all inequivalent valuations of K, the subsets of Archimedean, and non-Archimedean valuations, respectively. As usual, for $v \in V^K$, K_v denotes the completion of K with respect to v, and for $v \in V_f^K$, $\mathcal{O}_v$ denotes the ring of integers in K_v (by convention, $\mathcal{O}_v = K_v$ for $v \in V_\infty^K$). Given a finite subset S of V^K containing V_∞^K, we let $\mathcal{O}(S)$ denote the ring of S-integers in K, i.e.,

$$\mathcal{O}(S) = \{x \in K \mid x \in \mathcal{O}_v \text{ for all } v \notin S\}.$$

Finally, $A_{K,S}$ will denote the ring of S-adeles of K (adeles without the components corresponding to the valuations in S), and $A_{K,S}(S) := \prod_{v \notin S} \mathcal{O}_v$ will be the ring of S-integral S-adeles.

Now, suppose that f is a quadratic form as in §2. For a real $v \in V_\infty^K$, we let (n_v^+, n_v^-) denote the signature of f over $K_v = \mathbb{R}$. By scaling f (which does not affect the orthogonal group), we can achieve that $n_v^+ \geqslant n_v^-$ (and consequently $n_v^+ \geqslant 3$ as $n \geqslant 5$) for all real $v \in V_\infty^K$. Then one can choose a basis $e_1, \ldots, e_n$ of $W = K^n$ so that in the corresponding expression (1) for f, the coefficients α_i belong to $\mathcal{O}(S)$ for all $i = 3, \ldots, n$, and, in addition, α_{n-1}, $\alpha_n > 0$ in $K_v = \mathbb{R}$ for all real $v \in V_\infty^K$ (these conventions will be kept throughout the rest of the paper).

As we mentioned in the previous section, our goal is to find a version of the Borovoi decomposition for the group of S-integral points. Towards this end, in this section we will develop some conditions on $\zeta \in Z_{\mathscr{O}(S)}$ which ensure that $\phi^{-1}(\zeta)_{\mathscr{O}(S)} \neq \varnothing$. To avoid any ambiguity, we would like to stipulate that S-integral points in the space $\mathbf{W}$ and its (closed) subvarieties will be understood relative to the fixed basis $e_1, \ldots, e_n$, and $G_{\mathscr{O}(S)}$ by definition consists of those $g \in G_K$ for which $\pi(g) \in \mathrm{SO}_n(f)$ is represented in the fixed basis by a matrix with entries in $\mathscr{O}(S)$ (of course, it is possible to realize $G_{\mathscr{O}(S)}$ as the group of S-integral points in the usual sense with respect to some faithful representation of G, but we will not need this realization). The same conventions apply to $\mathscr{O}_v$-points for $v \notin S$.

The following set of valuations plays a prominent role in our argument:

$$V_0 = \left(\cup_{i=3}^n V(\alpha_i)\right) \cup V(2),$$

where for $\alpha \in K^\times$, we set $V(\alpha) = \{v \in V^K \setminus S \mid v(\alpha) \neq 0\}$.

Theorem 3.1 *Let $\zeta \in Z_{\mathscr{O}(S)}$. Suppose that $\phi^{-1}(\zeta)_{\mathscr{O}_v} \neq \varnothing$ for all $v \in V_0$. Then $\phi^{-1}(\zeta)_{\mathscr{O}(S)} \neq \varnothing$.*

We begin by establishing the following local-global principle for the fibers of ϕ.

Lemma 3.2 *Let $\zeta \in Z_{\mathscr{O}(S)}$. Suppose that $\phi^{-1}(\zeta)_K \neq \varnothing$ and $\phi^{-1}(\zeta)_{\mathscr{O}_v} \neq \varnothing$ for all $v \notin S$. Then $\phi^{-1}(\zeta)_{\mathscr{O}(S)} \neq \varnothing$.*

Proof. Let $\zeta = (g, s, t)$ and $H = G(a, b)$. Being the spinor group of the space $\langle a, b\rangle^\perp$, which is K-isotropic and has dimension $\geqslant 3$, the group H has the property of strong approximation with respect to S, i.e., (diagonally embedded) H_K is dense in $H_{\mathbb{A}_{K,S}}$ (see [18, 104:4], [21, Thm. 7.12]). We now observe that $\phi^{-1}(\zeta)$ is a principal homogeneous space of the group $H \times H \times H$. More precisely, the equation

$$(h_1, h_2, h_3) \cdot (x, y, z, u) = (x h_1^{-1}, h_1 y h_2^{-1}, h_2 z h_3^{-1}, h_3 u) \tag{5}$$

defines a simply transitive action of $H \times H \times H$ on $\phi^{-1}(\zeta)$. Indeed, one immediately verifies that for any $(x, y, z, u) \in \phi^{-1}(\zeta)$ and any $(h_1, h_2, h_3) \in H \times H \times H$, the right-hand side of (5) belongs to $\phi^{-1}(\zeta)$, and that (5) defines an action. Now, suppose that $(x_i, y_i, z_i, u_i) \in \phi^{-1}(\zeta)$, where $i = 1, 2$. Set

$$h_1 = x_2^{-1} x_1, \quad h_2 = (x_2 y_2)^{-1}(x_1 y_1), \quad h_3 = (x_2 y_2 z_2)^{-1}(x_1 y_1 z_1).$$

Then the conditions $x_i(a) = a$ and $x_i(b) = t$ for $i = 1, 2$ imply that $h_1 \in H$. Similarly, from $(x_i y_i)(a) = s$ and $(x_i y_i)(b) = t$ we derive that $h_2 \in H$, and from $(x_i y_i z_i)(a) = s$ and $(x_i y_i z_i)(b) = g(b)$ that $h_3 \in H$. In view of our construction, to prove that

$$(x, y, z, u) := (h_1, h_2, h_3) \cdot (x_1, y_1, z_1, u_1)$$

coincides with (x_2, y_2, z_2, u_2), it remains to observe that

$$u = h_3 u_1 = (x_2 y_2 z_2)^{-1}(x_1 y_1 z_1) u_1 = (x_2 y_2 z_2)^{-1} g = u_2,$$

so our claim follows.

Now, fix $(x, y, z, u) \in \phi^{-1}(\zeta)_K$. Then

$$\Sigma = \{(h_1, h_2, h_3) \in H_{\mathbb{A}_{K,S}} \times H_{\mathbb{A}_{K,S}} \times H_{\mathbb{A}_{K,S}} \mid (h_1, h_2, h_3) \cdot (x, y, z, u) \in \phi^{-1}(\zeta)_{\mathbb{A}_{K,S}(S)}\}$$

is a nonempty open subset of $H_{A_{K,S}} \times H_{A_{K,S}} \times H_{A_{K,S}}$. By strong approximation for H, there exists $(h_1, h_2, h_3) \in (H_K \times H_K \times H_K) \cap \Sigma$, and then

$$(h_1, h_2, h_3) \cdot (x, y, z, u) \in \phi^{-1}(\zeta)_K \cap \phi^{-1}(\zeta)_{A_{K,S}(S)} = \phi^{-1}(\zeta)_{\mathcal{O}(S)}$$

is a required S-integral point. □

To finish the proof of Theorem 3.1 it now remains to prove the following.

Lemma 3.3 *Let $\zeta \in Z_{\mathcal{O}(S)}$. Then $\phi^{-1}(\zeta)_{\mathcal{O}_v} \neq \varnothing$ for all $v \notin S \cup V_0$.*

The proof of Lemma 3.3 requires a version of Witt's theorem for local lattices, which we will state now and prove in the next section. Fix $v \in V_f^K$, and let $w_1, \ldots, w_n$ be an arbitrary basis of $W_v = W \otimes_K K_v$ in which the matrix F of the quadratic form f has entries in $\mathcal{O}_v$. Consider the $\mathcal{O}_v$-lattice L_v with the basis $w_1, \ldots, w_n$, its reduction $\bar{L}^{(v)} = L_v/\mathfrak{p}_v L_v$ modulo $\mathfrak{p}_v$ (which is an n-dimensional vector space over $k_v = \mathcal{O}_v/\mathfrak{p}_v$) and the corresponding reduction map $L_v \to \bar{L}^{(v)}$, $l \mapsto \bar{l}$. We also let

$$\mathrm{O}_n(f)_{\mathcal{O}_v}^{L_v} = \{\sigma \in \mathrm{O}_n(f) \mid \sigma(L_v) = L_v\}$$

be the stabilizer of L_v.

Theorem 3.4 (Witt's theorem for local lattices) *Suppose that the systems $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_m\}$ of vectors in L_v satisfy the following properties:*

(i) *$(a_i|a_j) = (b_i|b_j)$ for all $1 \leqslant i \leqslant j \leqslant m$;*

(ii) *the systems $\{\bar{a}_1, \ldots, \bar{a}_m\}$ and $\{\bar{b}_1, \ldots, \bar{b}_m\}$ obtained by reduction modulo $\mathfrak{p}_v$ are both linearly independent over k_v.*

If $\det F \in \mathcal{O}_v^\times$ and $v(2) = 0$, then there exists $\sigma \in \mathrm{O}_n(f)_{\mathcal{O}_v}^{L_v}$ such that $\sigma(a_i) = b_i$ for all $i = 1, \ldots, m$. Moreover, if $2m + 1 \leqslant n$ then such a σ can be found in $\mathrm{SO}_n(f)_{\mathcal{O}_v}^{L_v}$.

Proof of Lemma 3.3. We mimic the proof of Proposition 2.1(ii) except that instead of the usual Witt's theorem we use Theorem 3.4. We let L denote the $\mathcal{O}(S)$-lattice with the basis $e_1, \ldots, e_n$ which was fixed earlier, and for $v \notin S$ we set $L_v = L \otimes_{\mathcal{O}(S)} \mathcal{O}_v$. We claim that for every $v \in V^K \setminus (S \cup V_0)$, each of the following three pairs $(\overline{t}^{(v)}, \overline{a}^{(v)})$, $(\overline{s}^{(v)}, \overline{t}^{(v)})$, and $(\overline{s}^{(v)}, \overline{g(b)}^{(v)})$ (where $\overline{\cdot}^{(v)}$ denotes the reduction map modulo $\mathfrak{p}_v$) is linearly independent over k_v. For this we notice that $f(s) = f(a) = \alpha_n$ and $f(t) = f(b) = \alpha_{n-1}$ (cf. (1)), and because $v \notin V_0 \cup S$, both α_{n-1} and α_n are invertible in $\mathcal{O}_v$. Now, if for example, $\overline{t}^{(v)} = \lambda \overline{a}^{(v)}$ with $\lambda \in k_v$, then the condition $(t|a) = 0$ implies that

$$\bar{0} = (\overline{t}^{(v)}|\overline{a}^{(v)}) = \lambda(\overline{a}^{(v)}|\overline{a}^{(v)}) = \lambda \bar{\alpha}_n.$$

So, $\lambda = 0$. But $\overline{t}^{(v)} \neq \bar{0}$ as $\bar{\alpha}_{n-1} \neq \bar{0}$, a contradiction. All other cases are considered similarly using the orthogonality relations in the definition of Z. Then using Theorem 3.4 we find elements ρ, η, and σ in $\mathrm{SO}_n(f)_{\mathcal{O}_v}^{L_v}$ satisfying conditions (2), (3), and (4). Since $v \notin V_0 \cup S$, the lattice L_v is unimodular, and therefore the spinor norm of all three elements belongs to $\mathcal{O}_v^\times K_v^{\times 2}$ [18, 92:5]. On the other hand, the lattice $M_v := L_v \cap \langle a, b \rangle^\perp$ (which has $e_1, \ldots, e_{n-2}$ as its $\mathcal{O}_v$-basis) is unimodular of rank $\geqslant 3$, implying that $\theta(\mathrm{SO}_n(f)(a,b)_{\mathcal{O}_v}^{M_v}) = \mathcal{O}_v^{\times} K_v^{\times 2}$ [18, 92:5]. So, arguing as in the proof of Proposition 2.1(ii), we can modify the elements ρ, η, and σ so that they all have trivial spinor norm. Then they can be lifted to elements $\tilde{\rho}$, $\tilde{\eta}$, and $\tilde{\sigma}$ in $G_{\mathcal{O}_v}$, and one easily verifies that the quadruple (x,y,z,u), where $x = \tilde{\rho}$, $y = \tilde{\rho}^{-1}\tilde{\eta}$, $z = \tilde{\eta}^{-1}\tilde{\sigma}$, and $u = (xyz)^{-1}g$, belongs to $\phi^{-1}(\zeta)_{\mathcal{O}_v}$, proving the lemma. □

The proof of Theorem 3.1 is now complete.

4. Proof of Witt's theorem for local lattices

We will prove Theorem 3.4 in a more general situation then that we dealt with in the previous section. Namely, let $\mathscr{K}$ be a field of characteristic $\neq 2$ which is complete with respect to a discrete valuation v (see a remark at the end of the section regarding generalizations to not necessarily complete discretely valued fields). We let $\mathcal{O}$, $\mathfrak{p}$, and k denote the corresponding valuation ring, the valuation ideal, and the residue field, respectively; we also pick a uniformizer $\pi \in \mathfrak{p}$ so that $\mathfrak{p} = \pi\mathcal{O}$. Furthermore, let $\mathscr{W}$ be an n-dimensional vector space over $\mathscr{K}$, and f be an *arbitrary* quadratic form on $\mathscr{W}$ (in particular, we are not assuming that f has form (1) in a suitable basis of $\mathscr{W}$) with associated symmetric bilinear form $(\cdot \mid \cdot)$. We fix a basis $w_1, \ldots, w_n$ of $\mathscr{W}$ such that $(w_i|w_j) \in \mathcal{O}$ for all $i,j = 1,\ldots,n$, and let $\mathscr{L}$ denote the $\mathcal{O}$-lattice $\mathcal{O}w_1 + \cdots + \mathcal{O}w_n$. Let $\bar{\mathscr{L}} = \mathscr{L}/\mathfrak{p}\mathscr{L}$ be the reduction of $\mathscr{L}$ modulo $\mathfrak{p}$, with the corresponding reduction map $\mathscr{L} \to \bar{\mathscr{L}}$, $l \mapsto \bar{l}$. In the sequel, matrix representations for linear transformations of $\mathscr{W}$ will be considered exclusively relative to the basis $w_1, \ldots, w_n$; in particular, the $\mathcal{O}$-points of the orthogonal group $\mathrm{O}_n(f)$ are described as follows:

$$\mathrm{O}_n(f)_{\mathcal{O}} = \{X \in \mathrm{GL}_n(\mathcal{O}) \mid {}^tXFX = F\},$$

where $F = ((w_i|w_j))$ is the Gram–Schmidt matrix of the form f. The following two assumptions will be kept throughout the section:

(i) $\mathscr{L}$ is unimodular, i.e., $\det F \in \mathcal{O}^{\times}$;

(ii) $\operatorname{char} k \neq 2$.

Under these assumptions, we will prove the following, which in particular yields Theorem 3.4:

($*$) given two systems of vectors $\{a_1, \ldots, a_m\}$ and $\{b_1, \ldots, b_m\}$ in $\mathscr{L}$ satisfying conditions (i) and (ii) of Theorem 3.4, i.e., $(a_i|a_j) = (b_i|b_j)$ for all $i,j = 1,\ldots,m$, and the reduced systems $\{\bar{a}_1, \ldots, \bar{a}_m\}$ and $\{\bar{b}_1, \ldots, \bar{b}_m\}$ are linearly independent over k, there exists $X \in \mathrm{O}_n(f)_{\mathcal{O}}$ with the property $Xa_i = b_i$ for all $i = 1,\ldots,m$, and, moreover, if $2m+1 \leqslant n$, then such an X can already be found in $\mathrm{SO}_n(f)_{\mathcal{O}}$.

The proof uses the standard approximation procedure due to Hensel, although we bypass a direct usage of Hensel's Lemma for algebraic varieties. We begin with a couple of lemmas.

Lemma 4.1 *Given an integer $l \geqslant 1$ and a matrix $X \in M_n(\mathcal{O})$ satisfying*

$$ {}^tXFX \equiv F \pmod{\mathfrak{p}^l}, \tag{6}$$

there exists $Y \in M_n(\mathscr{O})$ *such that*

$$ {}^tYFY \equiv F \pmod{\mathfrak{p}^{l+1}} \tag{7}$$

and

$$Y \equiv X \pmod{\mathfrak{p}^l}.$$

Proof. We need to find $Z \in M_n(\mathscr{O})$ for which $Y := X + \pi^l Z$ satisfies (7). According to (6), $F - {}^tXFX = \pi^l A$, for some (necessarily symmetric) matrix $A \in M_n(\mathscr{O})$. In view of the congruence

$${}^tYFY \equiv {}^tXFX + \pi_v^l({}^tZFX + {}^tXFZ) \pmod{\mathfrak{p}^{l+1}},$$

to satisfy (7) it is enough choose $Z \in M_n(\mathscr{O})$ so that

$${}^tZFX + {}^tXFZ \equiv A \pmod{\mathfrak{p}}.$$

However, it follows from our assumptions that

$$Z := \frac{{}^t(FX)^{-1}A}{2} \in M_n(\mathscr{O})$$

and moreover

$${}^tZFX + {}^tXFZ = {}^tZ(FX) + {}^t(FX)Z = {}^t\left(\frac{A}{2}\right) + \left(\frac{A}{2}\right) = A$$

as A is symmetric. Thus, Z is as required. □

Corollary 4.2 *Notations as in Lemma 4.1, there exists* $\hat{X} \in \mathrm{O}_n(f)_{\mathscr{O}}$ *satisfying* $\hat{X} \equiv X \pmod{\mathfrak{p}^l}$.

Proof. Using Lemma 4.1, we construct a sequence of matrices $X_i \in M_n(\mathscr{O})$, $i = l, l+1, \ldots$ such that $X_l = X$, ${}^tX_iFX_i \equiv F \pmod{\mathfrak{p}^i}$, and $X_{i+1} \equiv X_i \pmod{\mathfrak{p}^i}$ for all $i \geqslant l$. Then $X_i \equiv X_j \pmod{\mathfrak{p}^j}$ for all $i \geqslant j \geqslant l$, implying that $\{X_i\}$ is a Cauchy sequence in $X + M_n(\mathfrak{p}^l) \subseteq M_n(\mathscr{K})$. As $\mathscr{K}$ is complete and $\mathfrak{p}^l$ is closed in $\mathscr{K}$, this sequence converges to some $\hat{X} \in X + M_n(\mathfrak{p}^l)$, which is as required. □

Lemma 4.3 *Given an integer* $l \geqslant 1$ *and two systems of vectors* $\{a_1, \ldots, a_m\}$ *and* $\{b_1, \ldots, b_m\}$ *in* $\mathscr{L}$ *as in* $(*)$ *satisfying*

$$a_i \equiv b_i \pmod{\mathfrak{p}^l} \quad \textit{for all } i = 1, \ldots, m,$$

there exists $X \in M_n(\mathscr{O})$ *such that*

$$X \equiv E_n \pmod{\mathfrak{p}^l},$$
$${}^tXFX \equiv F \pmod{\mathfrak{p}^{l+1}},$$

and

$$Xa_i \equiv b_i \pmod{\mathfrak{p}^{l+1}} \quad \textit{for all } i = 1, \ldots, m.$$

Proof. We have $b_i = a_i + \pi^l c_i$ for some $c_i \in \mathscr{L}$, and then the condition $(a_i|a_j) = (b_i|b_j)$ yields

$$(a_i|c_j) + (c_i|a_j) \equiv 0 \pmod{\mathfrak{p}} \quad \text{for all } i, j = 1, \ldots, m.$$

Now, suppose we can exhibit $Y \in M_n(\mathscr{O})$ such that

$$ {}^tYF + FY \equiv 0 \pmod{\mathfrak{p}} \tag{8} $$

and

$$ Ya_i \equiv c_i \pmod{\mathfrak{p}} \quad \text{for all } i = 1, \ldots, m. \tag{9} $$

Then $X := E_n + \pi^l Y$ is as required. Indeed,

$$ {}^tXFX \equiv F + \pi^l({}^tYF + FY) \equiv F \pmod{\mathfrak{p}^{l+1}} $$

and

$$ Xa_i = a_i + \pi^l Ya_i \equiv a_i + \pi^l c_i \equiv b_i \pmod{\mathfrak{p}^{l+1}}. $$

On the other hand, the existence of Y satisfying (8) and (9) follows from Lemma 4.4 below applied to the vector space $\mathscr{W} = \bar{\mathscr{L}}$ over the field $\mathscr{K} = k$, the symmetric matrix $\mathscr{F}$ obtained by reducing F modulo $\mathfrak{p}$, and the vectors $x_1 = \bar{a}_1, \ldots, x_m = \bar{a}_m$, and $y_1 = \bar{c}_1, \ldots, y_m = \bar{c}_m$ in $\mathscr{W}$. □

Lemma 4.4 *Let $\mathscr{K}$ be an arbitrary field of characteristic $\neq 2$, and $\mathscr{W} = \mathscr{K}^n$. Let $\mathscr{F}$ be a nondegenerate symmetric $n \times n$ matrix over $\mathscr{K}$, $(x|y) = {}^tx\mathscr{F}y$ be the corresponding symmetric bilinear form on $\mathscr{W}$, and*

$$ \mathscr{R} = \{Y \in M_n(\mathscr{K}) \mid {}^tY\mathscr{F} + \mathscr{F}Y = 0\} $$

be the corresponding space of skew-symmetric matrices. Suppose that $x_1, \ldots, x_m \in \mathscr{W}$ are linearly independent vectors, and set

$$ \mathscr{A} = \{(y_1, \ldots, y_m) \in \mathscr{W}^m \mid (x_i|y_j) + (x_j|y_i) = 0 \text{ for all } i, j = 1, \ldots, m\} $$

and

$$ \mathscr{B} = \{(Yx_1, \ldots, Yx_m) \mid Y \in \mathscr{R}\}. $$

Then $\mathscr{A} = \mathscr{B}$.

Proof. In the standard basis, matrices in $\mathscr{R}$ correspond to linear operators in

$$ \mathscr{S} = \{Y \in \operatorname{End}_{\mathscr{K}}(\mathscr{W}) \mid (Yx|y) + (x|Yy) = 0\}, $$

which in particular yields the inclusion $\mathscr{B} \subseteq \mathscr{A}$. So, it is enough to show that $\dim \mathscr{A} = \dim \mathscr{B}$.

Let $\mathscr{V}$ be the subspace of $\mathscr{W}$ spanned by $x_1, \ldots, x_m$. Then $\dim \mathscr{B} = \dim \mathscr{S} - \dim \mathscr{T}$, where

$$ \mathscr{T} = \{Y \in \mathscr{S} \mid Yv = 0 \text{ for all } v \in \mathscr{V}\}. $$

An elementary computation based on representing the transformation in $\mathscr{S}$ by matrices relative to a (fixed) orthogonal basis of $\mathscr{W}$ yields

$$ \dim \mathscr{S} = \frac{n(n-1)}{2}. \tag{10} $$

To calculate $\dim \mathscr{T}$, one needs to observe that $\mathscr{W}$ admits a basis $v_1, \ldots, v_n$ such that the vectors $v_1, \ldots, v_m$ form a basis of $\mathscr{V}$ and the matrix of the bilinear form $(\cdot \mid \cdot)$ has the following structure

$$ \begin{pmatrix} & & E_r \\ & D_{n-2r} & \\ E_r & & \end{pmatrix} $$

where E_r is the identity matrix of size r, and D_{n-2r} is a nondegenerate diagonal matrix of size $n-2r$ (notice that r is nothing but the dimension of the radical of $\mathscr{V}$, and in fact the vectors $v_1, \dots, v_r$ form a basis of this radical). Then, by considering the matrix representation of transformations from $\mathscr{S}$ relative to the basis $v_1, \dots, v_n$, one finds that

$$\dim \mathscr{T} = \frac{(n-m)(n-m-1)}{2}. \tag{11}$$

From (10) and (11) we conclude that

$$\dim \mathscr{B} = \frac{n(n-1)}{2} - \frac{(n-m)(n-m-1)}{2}. \tag{12}$$

To calculate $\dim \mathscr{A}$, we consider the linear functionals f_i, $i = 1, \dots, m$, on $\mathscr{W}$ given by $f_i(w) = (w|x_i)$. Since the x_i's are linearly independent and $\mathscr{W}$ is nondegenerate, the f_i's are also linearly independent, implying that the linear map $\mathscr{W} \to \mathscr{K}^m$, $w \mapsto (f_1(w), \dots, f_m(w))$, is surjective. It follows that the linear map $\Phi\colon \mathscr{W}^m \to \mathscr{K}^{m^2}$ given by

$$\Phi(w_1, \dots, w_m) = (f_1(w_1), \dots, f_m(w_1), \dots, f_1(w_m), \dots, f_m(w_m))$$

is also surjective. Let z_{ij} be the coordinate in $\mathscr{K}^{m^2}$ corresponding to $f_i(w_j)$. Then $\mathscr{A} = \Phi^{-1}(\mathscr{U})$ where $\mathscr{U}$ is the subspace of $\mathscr{K}^{m^2}$ defined by the conditions $z_{ij} + z_{ji} = 0$ for all $i, j = 1, \dots, m$. It follows that

$$\dim \mathscr{A} = mn - \operatorname{codim}_{\mathscr{K}^{m^2}} \mathscr{U} = mn - \frac{m(m+1)}{2},$$

comparing which with (12) we obtain $\dim \mathscr{A} = \dim \mathscr{B}$, completing the argument. $\square$

Proof of $(*)$. We will inductively construct a sequence of matrices $X_s \in \mathrm{O}_n(f)_{\mathscr{O}}$, $s = 1, 2, \dots$, satisfying

$$X_t \equiv X_s \pmod{\mathfrak{p}^s} \quad \text{whenever } t \geqslant s \tag{13}$$

and

$$X_s a_i \equiv b_i \pmod{\mathfrak{p}^s} \quad \text{for all } i = 1, \dots, m \text{ and any } s. \tag{14}$$

Then (13) implies that $\{X_s\}$ is a Cauchy sequence in $\mathrm{O}_n(f)_{\mathscr{O}} \subseteq M_n(\mathscr{K})$, which therefore converges to some $X \in \mathrm{O}_n(f)_{\mathscr{O}}$. As in the proof of Corollary 4.2, we conclude that $X \equiv X_s \pmod{\mathfrak{p}^s}$, so

$$X a_i \equiv X_s a_i \equiv b_i \pmod{\mathfrak{p}^s} \quad \text{for all } s,$$

implying that $X a_i = b_i$ for $i = 1, \dots, m$, as required.

To construct X_1 satisfying (13) and (14) for $s = 1$, we observe that by applying the usual Witt's theorem to the vector space $\bar{\mathscr{L}}$ over k and the reduction of f modulo $\mathfrak{p}$ (which is nondegenerate), we can find $Z_1 \in M_n(\mathscr{O})$ such that

$${}^t Z_1 F Z_1 \equiv F \pmod{\mathfrak{p}} \quad \text{and} \quad Z_1 a_i \equiv b_i \pmod{\mathfrak{p}} \quad \text{for } i = 1, \dots, m.$$

Then by Corollary 4.2, there exists $X_1 \in \mathrm{O}_n(f)_{\mathscr{O}}$ satisfying $X_1 \equiv Z_1 \pmod{\mathfrak{p}}$ and possessing thereby the required properties.

Suppose that the matrices $X_1,\dots,X_s$ have already been constructed. Then applying Lemma 4.3 to the systems of vectors $\{X_sa_1,\dots,X_sa_m\}$ and $\{b_1,\dots,b_m\}$ in $\mathscr{L}$ yields $X\in M_n(\mathscr{O})$ such that

$$X\equiv E_n \pmod{\mathfrak{p}^s},$$
$${}^tXFX\equiv F \pmod{\mathfrak{p}^{s+1}},$$

and

$$XX_sa_i\equiv b_i \pmod{\mathfrak{p}^{s+1}}.$$

Again, by Corollary 4.2 there exists $X_{s+1}\in \mathrm{O}_n(f)_{\mathscr{O}}$ with the property

$$X_{s+1}\equiv XX_s \pmod{\mathfrak{p}^{s+1}},$$

and by our construction such X_{s+1} does satisfy (13) and (14) for $s+1$, completing the proof of the first assertion in $(*)$.

For the second assertion, it is enough to show that if $2m+1\leqslant n$, then $\mathrm{O}_n(f)_{\mathscr{O}}$ contains a matrix X having determinant -1 and satisfying $Xa_i=a_i$ for all $i=1,\dots,m$. Since the reduction $\bar{\mathscr{L}}$ is nondegenerate, there exist $a_{m+1},\dots,a_{m+r}\in\mathscr{L}$, where $r\leqslant m$, such that $\bar{a}_1,\dots,\bar{a}_{m+r}$ span a nondegenerate subspace of $\bar{\mathscr{L}}$. Then the lattice $\mathscr{M}=\mathscr{O}a_1+\cdots+\mathscr{O}a_{m+r}$ is unimodular, and therefore $\mathscr{L}=\mathscr{M}\perp\mathscr{M}^{\perp}$, where $\mathscr{M}^{\perp}$ is the orthogonal complement of $\mathscr{M}$ in $\mathscr{L}$. Clearly, the lattice $\mathscr{M}^{\perp}$ is unimodular, hence contains a vector c such that $f(c)\not\equiv 0 \pmod{\mathfrak{p}}$. Then for X one can take (the matrix of) the reflection τ_c. □

One corollary of $(*)$ is worth mentioning. Given a nonzero vector $a\in\mathscr{L}$, we define its level $\lambda(a)$ (relative to $\mathscr{L}$) as follows:

$$\lambda(a)=\max\{l\geqslant 0 \mid a\in\mathfrak{p}^l\mathscr{L}\}.$$

Corollary 4.5 *Given two nonzero vectors $a,b\in\mathscr{L}$ such that $f(a)=f(b)$, a transformation $X\in\mathrm{O}_n(f)_{\mathscr{O}}$ with the property $Xa=b$ exists if and only if $\lambda(a)=\lambda(b)$.*

Proof. One implication immediately follows from the fact that a matrix in $\mathrm{GL}_n(\mathscr{O})$ preserves the level of any vector. For the other implication, we write a and b in the form $a=\pi^{\lambda}a_0$, $b=\pi^{\lambda}b_0$, where $\lambda=\lambda(a)=\lambda(b)$. Then $f(a_0)=f(b_0)$ and the reductions $\bar{a}_0$, $\bar{b}_0\in\bar{\mathscr{L}}$ are nonzero. By $(*)$, there exists $X\in\mathrm{O}_n(f)_{\mathscr{O}}$ such that $Xa_0=b_0$, and then also $Xa=b$. □

Remarks. 1. It is worth observing that with some extra work, $(*)$ can be extended to discretely valued but not necessarily complete fields $\mathscr{K}$. Indeed, let $\mathscr{K}_v$ be the completion of $\mathscr{K}$, and $\mathscr{O}_v$ be the valuation ring in $\mathscr{K}_v$. Consider the algebraic $\mathscr{K}$-group $\mathscr{G}=\mathbf{O}_n(f)$. Now, given $a_1,\dots,a_m$ and $b_1,\dots,b_m\in\mathscr{L}$ as in $(*)$, we let $\mathscr{H}$ denote the stabilizer of all the a_i's in $\mathscr{G}$. Applying respectively the usual Witt's theorem (over $\mathscr{K}$) and $(*)$, we will find $X_{\mathscr{K}}\in\mathscr{G}_{\mathscr{K}}$ and $X_v\in\mathscr{G}_{\mathscr{O}_v}$ such that

$$X_{\mathscr{K}}a_i=X_va_i=b_i \quad \text{for all } i=1,\dots,m.$$

Then $Y:=X_v^{-1}X_{\mathscr{K}}\in\mathscr{H}_{\mathscr{K}_v}$. However, $\mathscr{H}_{\mathscr{K}}$ is dense in $\mathscr{H}_{\mathscr{K}_v}$ in the topology defined by v. (If the subspace spanned by $a_1,\dots,a_m$ is nondegenerate, this is basically proved in [21, Prop. 7.4]; the general case is reduced to this one by splitting off the unipotent radical of $\mathscr{H}$.) It follows that $\mathscr{H}_{\mathscr{K}_v} = \mathscr{H}_{\mathscr{O}_v}\mathscr{H}_{\mathscr{K}}$. Writing Y in the form $Y = Z_v Z_{\mathscr{K}}^{-1}$ with $Z_v \in \mathscr{H}_{\mathscr{O}_v}$ and $Z_{\mathscr{K}} \in \mathscr{H}_{\mathscr{K}}$, we obtain

$$X := X_v Z_v = X_{\mathscr{K}} Z_{\mathscr{K}} \in \mathscr{G}_{\mathscr{O}_v} \cap \mathscr{G}_{\mathscr{K}} = \mathscr{G}_{\mathscr{O}}$$

and $Xa_i = X_{\mathscr{K}} a_i = b_i$ for all $i = 1, \ldots, m$.

2. As was pointed out by the anonymous referee of the earlier version of the paper, the result actually holds for arbitrary local rings and can be derived from [11, Satz 4.3] or [10, Thm. 1.2.2].

5. The quadric Q_s

In this section, we return to the notations and conventions introduced in §§2–3. To complete the proof of the Main Theorem in the next section, we need to figure out when for a given $g \in G_{\mathscr{O}(S)}$ one can choose $s, t \in L := \mathscr{O}(S)e_1 + \cdots + \mathscr{O}(S)e_n$ such that the triple $\zeta = (g, s, t)$ belongs to Z and satisfies the assumptions of Theorem 3.1. We notice that if s has already been chosen so that $(g, s) \in Y$ then the t's for which (g, s, t) belongs to Z lie on the following quadric

$$Q_s = \{x \in \langle s, a\rangle^{\perp} \mid f(x) = f(b)\}.$$

So, in this section we will examine some arithmetic properties of Q_s for an arbitrary $s \in W$ such that the space $\langle s, a\rangle$ is 2-dimensional and nondegenerate.

Lemma 5.1

(i) *For every $v \in V_{\infty}^K$, $(Q_s)_{K_v} \neq \varnothing$.*

(ii) *If $n \geqslant 6$, then $(Q_s)_K \neq \varnothing$.*

(iii) *Suppose that $s \in L$. Then for every $v \notin S \cup V_0$, $(Q_s)_{\mathscr{O}_v} \neq \varnothing$.*

Proof. (i) This is obvious if v is complex, so suppose that v is real. Then by our construction $n_v^+ \geqslant 3$, implying that the restriction of f to $\langle s, a\rangle^{\perp}$ has at least one positive square. Since $f(b) = \alpha_{n-1} > 0$ in $K_v = \mathbb{R}$, our assertion follows.

(ii) If $n \geqslant 6$ then $\dim\langle s, a\rangle^{\perp} \geqslant 4$. As a nondegenerate quaternary quadratic form over a (non-Archimedean) local field represents every nonzero element [18, 63:18], we conclude that $(Q_s)_{K_v} \neq \varnothing$ for all $v \in V_f^K$. Combining this with (i) and applying the Hasse–Minkowski theorem [18, 66:4], we obtain our claim.

(iii) We will show that there is a unimodular $\mathscr{O}_v$-sublattice $M \subseteq L_v := L \otimes_{\mathscr{O}(S)} \mathscr{O}_v$ of rank $\leqslant 3$ containing s and a. Then $L_v = M \perp M^{\perp}$ with $M^{\perp}$ unimodular of rank $\geqslant 2$. Since $f(b) \in \mathscr{O}_v^{\times}$, there exists $x \in M^{\perp}$ such that $f(x) = f(b)$ [18, 92:1b], and then $x \in (Q_s)_{\mathscr{O}_v}$, as required. To construct such an M, we let $(s_1, \ldots, s_n)$ denote the coordinates of s in the basis $e_1, \ldots, e_n$. Set $u = s_1e_1 + \cdots + s_{n-1}e_{n-1}$. As $u \in L$ and $u \neq 0$, we can write $u = \pi_v^d u_0$ where $\pi_v \in \mathscr{O}_v$ is a uniformizing element, $d \geqslant 0$ and $u_0 \in L_v \setminus \pi_v L_v$. If $f(u_0) \in \mathscr{O}_v^{\times}$, then in view of $u_0 \perp a$, the sublattice $M = \mathscr{O}_v a + \mathscr{O}_v u_0$ is as desired. Now, suppose that $f(u_0) \in \mathfrak{p}_v = \pi_v \mathscr{O}_v$. Since the sublattice $N = \mathscr{O}_v a$ is unimodular we have $L_v = N \perp N^{\perp}$ with $N^{\perp}$ unimodular; notice that $u_0 \in N^{\perp}$. The reduction $\overline{\left(N^{\perp}\right)}^{(v)} = N^{\perp} \otimes_{\mathscr{O}_v} k_v$ being a nondegenerate quadratic space over $k_v = \mathscr{O}_v/\mathfrak{p}_v$, one can find $u_1 \in N^{\perp}$ so that the images of u_0 and u_1 in $\overline{\left(N^{\perp}\right)}^{(v)}$ form a hyperbolic pair. Then the $\mathcal{O}_v$-sublattice M with the basis a, u_0 and u_1 is as required. $\square$

Lemma 5.2

(i) *Suppose that $n \geqslant 6$. Given $v \in S$, there exists an open set $\mathcal{U}_v \subseteq \mathbf{W}_{K_v}$ such that $\mathcal{U}_v \cap X \neq \varnothing$ and for any $s \in W \cap \mathcal{U}_v$, the quadric Q_s has strong approximation with respect to S. Moreover, if there exists $v \in V_{\infty}^K$ with the property $i_v(f) \geqslant 2$, then Q_s has strong approximation with respect to S for* any *s.*

(ii) *Suppose that $n = 5$ and $v \in S$ is non-Archimedean. There exists an open subset $\mathcal{U}_v \subseteq \mathbf{W}_{K_v}$ with the property $\mathcal{U}_v \cap X \neq \varnothing$ such that for $s \in W \cap \mathcal{U}_v$ one has $(\mathrm{Q}_s)_{K_v} \neq \varnothing$ and moreover if $(\mathrm{Q}_s)_K \neq \varnothing$ then Q_s has strong approximation with respect to S.*

Proof. (i) It follows from the theorem in the Appendix and Lemma 5.1(ii) that a necessary and sufficient condition for strong approximation in Q_s is that $(\mathrm{Q}_s)_S = \prod_{v \in S} (\mathrm{Q}_s)_{K_v}$ be noncompact. If $v \in V_{\infty}^K$ is such that $i_v(f) \geqslant 2$, then for any s the space $\langle s, a\rangle^{\perp}$ is K_v-isotropic and therefore $(\mathrm{Q}_s)_{K_v}$ is noncompact, hence our second assertion. For the first assertion, we observe that the space $\langle a, b\rangle^{\perp}$ is K-isotropic by our construction, and besides there exists $s_0 \in \langle a, b\rangle$ such that $f(s_0) = f(a)$ and $\langle a, s_0\rangle = \langle a, b\rangle$. The fact that the subgroup of squares $K_v^{\times 2}$ is open in $K_v^{\times}$ implies that there exists an open set $\mathcal{U}_v \subseteq \mathbf{W}_{K_v}$ containing s_0 such that for any $s \in \mathcal{U}_v$, the spaces $\langle s, a\rangle$ and $\langle s_0, a\rangle$ are isometric over K_v. Then it follows from Witt's theorem that the space $\langle s, a\rangle^{\perp}$ is K_v-isotropic, so the set $\mathcal{U}_v$ is as required.

(ii) Pick $c \in W$ orthogonal to a and b so that $f(c) = -f(b)$, and let U be the orthogonal complement in W to a, b, and c. Since $\dim U = 2$ and v is non-Archimedean, the set of nonzero values of f on $U \otimes_K K_v$ consists of more than one coset modulo $K_v^{\times 2}$, so there exists an anisotropic $u \in U$ such that $f(u) \notin -f(c)K_v^{\times 2}$, and then the space $\langle c, u\rangle$ is K_v-anisotropic. Pick $u' \in U$ orthogonal to u. Then the space $\langle a, u'\rangle^{\perp} = \langle b, c, u\rangle$ is K_v-isotropic (viz., $f(b+c) = 0$), but the space $\langle a, b, u'\rangle^{\perp} = \langle c, u\rangle$ is K_v-anisotropic. As in the proof of (i), we pick $s_0 \in \langle a, u'\rangle$ so that $f(s_0) = f(a)$ and $\langle a, s_0\rangle = \langle a, u'\rangle$, and then find an open subset $\mathcal{U}_v \subseteq \mathbf{W}_{K_v}$ containing s_0 such that for any $s \in \mathcal{U}_v$ the subspaces $\langle a, s\rangle$ and $\langle a, s_0\rangle$ are isometric over K_v. If now $s \in W \cap \mathcal{U}_v$, then it follows from Witt's theorem that the space $\langle a, s\rangle^{\perp}$ is K_v-isotropic, implying not only that $(\mathrm{Q}_s)_{K_v} \neq \varnothing$ but in fact also that $(\mathrm{Q}_s)_{K_v}$ is noncompact. Furthermore, if $d \in (\mathrm{Q}_s)_{K_v}$ then the space $\langle a, s, d\rangle^{\perp}$ is K_v-isometric to $\langle a, s_0, b\rangle^{\perp} = \langle a, b, u'\rangle^{\perp}$, hence K_v-anisotropic. Thus, if $(\mathrm{Q}_s)_K \neq \varnothing$, then by the theorem in the Appendix, Q_s has strong approximation with respect to S. $\square$

6. Proof of the Main Theorem

For convenience of reference we will list some elementary results about groups with bounded generation.

Lemma 6.1 *Let Γ be a group, and Δ be its subgroup.*

(i) *If $[\Gamma : \Delta] < \infty$ then bounded generation of Γ is equivalent to bounded generation of Δ.*

(ii) *If* Γ *has* (BG) *then so does any homomorphic image of* Γ.

(iii) *If* $\Delta \lhd \Gamma$ *and both* Δ *and* Γ/Δ *have* (BG) *then* Γ *also has* (BG).

Proof. All these assertions, except for the fact that in (i), (BG) of Γ implies (BG) of Δ, immediately follow from the definition. A detailed proof of the remaining implication is given, for example, in [17]. □

It follows from Lemma 6.1(i) that given two commensurable subgroups Δ_1 and Δ_2 of Γ (which means that $\Delta_1 \cap \Delta$ has finite index in both Δ_1 and Δ_2), (BG) of one of them is equivalent to (BG) of the other. In particular, if G is an algebraic group over a number field K, then (BG) of one S-arithmetic subgroup of G implies (BG) of all S-arithmetic subgroups of G. Furthermore, if $\pi\colon G_1 \to G_2$ is a K-defined isogeny of algebraic K-groups and Γ is an S-arithmetic subgroup of G_1, then (BG) of Γ is equivalent to (BG) of $\pi(\Gamma)$. Since the latter is an S-arithmetic subgroup of G_2 (see, for example, [21, Thm. 5.9]), we obtain the following.

Lemma 6.2 *Let* $\pi\colon G_1 \to G_2$ *be a* K*-defined isogeny of algebraic* K*-groups, where* K *is a number field. Then* (BG) *of one* S*-arithmetic subgroup in* G_1 *or* G_2 *implies* (BG) *of all* S*-arithmetic subgroups in* G_1 *and* G_2.

Applying this lemma to the universal cover $\mathbf{Spin}_n(f) \xrightarrow{\pi} \mathbf{SO}_n(f)$, we see that to prove the Main Theorem it is enough to show that for $G = \mathbf{Spin}_n(f)$, the group $G_{\mathcal{O}(S)}$, defined in terms of our fixed realization, is boundedly generated. Our argument will use the following simple observation.

Lemma 6.3 *Let* Γ *be a group, and* Δ *be its subgroup of finite index. If there exist* $\gamma, \gamma_1, \ldots, \gamma_s \in \Gamma$ *such that* $\gamma\Delta \subseteq \langle\gamma_1\rangle \cdots \langle\gamma_s\rangle$, *then* Γ *has* (BG).

Proof. Let $x_1, \ldots, x_n$ be a system of left coset representatives for Δ in Γ. Then

$$\Gamma = \bigcup_{i=1}^{n} x_i\Delta \subseteq \bigcup_{i=1}^{n} x_i\langle\gamma\rangle\langle\gamma_1\rangle\cdots\langle\gamma_s\rangle,$$

implying that $\Gamma = \langle x_1\rangle \cdots \langle x_n\rangle\langle\gamma\rangle\langle\gamma_1\rangle\cdots\langle\gamma_s\rangle$. □

To proceed with the proof of the Main Theorem, we need to introduce some additional notations. For $g \in G$, the fiber over g of the projection $Y \to G$ can (and will) be identified with

$$B_g = \{s \in \mathbf{W} \mid (s|g(b)) = 0,\ f(s) = f(a)\}; \tag{15}$$

notice that B_g is a quadric in an $(n-1)$-dimensional vector space ($= g(b)^{\perp}$). Furthermore, for $v \in V^K$ we denote

$$\mathscr{P}_v = \begin{cases} (P_0)_{K_v} & \text{if } v \in S, \\ (P_0)_{K_v} \cap P_{\mathcal{O}_v} & \text{if } v \notin S, \end{cases}$$

where $P_0 \subseteq P$ is the Zariski-open set introduced in Lemma 2.2, and set $\mathscr{G}_v = \mu(\mathscr{P}_v)$. It follows from the surjectivity of $d_h\mu$ at all points $h \in P_0$ (see Lemma 2.2) and the Implicit Function Theorem [27, pp. 83–85] that $\mathscr{G}_v$ is open in G_{K_v}.

Proposition 6.4 *If $n \geqslant 6$ and $i_K(f) \geqslant 2$ then*

$$G_{\mathscr{O}(S)} \cap \prod_{v \in V_0} \mathscr{G}_v \subseteq \mu(P_{\mathscr{O}(S)}).$$

Proof. Fix $g \in G_{\mathscr{O}(S)} \cap \prod_{v \in V_0} \mathscr{G}_v$. Then for each $v \in V_0$, one can we pick $h_v \in \mathscr{P}_v$ so that $\mu(h_v) = g$, hence $\phi(h_v) = (g, s_v, t_v)$. It again follows from Lemma 2.2 and the Implicit Function Theorem that the map $(\varepsilon \circ \phi)_v$ is open at h_v, implying that one can pick an open neighborhood $\Sigma_v \subseteq (B_g)_{\mathscr{O}_v}$ of s_v satisfying

$$(g, \Sigma_v) \subseteq \varepsilon(\phi(\mathscr{P}_v)). \tag{16}$$

Clearly, $g(a) \in B_g$, in particular, $(B_g)_K \neq \varnothing$. Furthermore, the orthogonal complement of $g(b)$ is isometric to the orthogonal complement of b, hence K-isotropic, so it follows from (21) that $(B_g)_S$ is noncompact. Since $n - 1 \geqslant 5$, by the theorem in the Appendix, B_g has strong approximation with respect to S, and therefore one can find

$$s \in (B_g)_{\mathscr{O}(S)} \cap \prod_{v \in V_0} \Sigma_v. \tag{17}$$

According to Lemma 5.2(i), the corresponding quadric Q_s (see §5) has strong approximation with respect to S. Taking into account that $Q_s = \{t \mid (g, s, t) \in \varepsilon^{-1}(g, s)\}$ and that according to (16) and (17) one has $\varepsilon^{-1}(g, s) \cap \phi(\mathscr{P}_v) \neq \varnothing$ for all $v \in V_0$, we conclude that there exists t such that

$$\zeta := (g, s, t) \in Z_{\mathscr{O}(S)} \cap \prod_{v \in V_0} \phi(P_{\mathscr{O}_v}). \tag{18}$$

Then it follows from Theorem 3.1 that $\phi^{-1}(\zeta)_{\mathscr{O}(S)} \neq \varnothing$, and therefore $g \in \mu(P_{\mathscr{O}(S)})$, proving the proposition. □

An analog of Proposition 6.4 for the case where $i_K(f) = 1$ requires a bit more work, especially if $n = 5$.

Proposition 6.5 *Suppose that $n \geqslant 5$, $i_K(f) = 1$, and S contains a non-Archimedean valuation. Then*

$$G_{\mathscr{O}(S)} \cap \prod_{v \in V_0} \mathscr{G}_v \subseteq \mu(P_{\mathscr{O}(S)})\mu(P_{\mathscr{O}(S)})\mu(P_{\mathscr{O}(S)})^{-1}. \tag{19}$$

Proof. By our assumption, one can pick in S an Archimedean valuation v_1 and a non-Archimedean valuation v_2. Let $\mathscr{U}_{v_2} \subseteq \mathbf{W}_{K_{v_2}}$ be an open subset with the properties described in Lemma 5.2, i.e., $\mathscr{U}_{v_2} \cap X \neq \varnothing$ and for any $s \in \mathscr{U}_{v_2} \cap X_K$, the quadric Q_s has strong approximation with respect to S if either $n \geqslant 6$ or $n = 5$ and $(Q_s)_K \neq \varnothing$; in addition, for such s one can guarantee that $(Q_s)_{K_v} \neq \varnothing$ if $n = 5$. It now follows from Lemma 2.3 that for the map η introduced therein, the set

$$\mathscr{P}'_{v_2} = \eta^{-1}(\mathscr{U}_{v_2} \cap X_{K_{v_2}}) \cap (P_0)_{K_{v_2}}$$

is a nonempty open subset of $P_{K_{v_2}}$. Then as above we conclude that $\mathscr{G}'_{v_2} := \mu(\mathscr{P}'_{v_2})$ is a nonempty open subset of $G_{K_{v_2}}$.

By strong approximation, $P_{\mathscr{O}(S)}$ is dense in $P_{S \setminus \{v_1\}} \times \prod_{v \in V_0} P_{\mathscr{O}_v}$, which in view of Proposition 2.1 implies that the closure of $\mu(P_{\mathscr{O}(S)})$ in $G_{(S \cup V_0) \setminus \{v_1\}}$ contains $G_{S \setminus \{v_1\}} \times$

$\prod_{v\in V_0}\mathscr{G}_v$. Since the $\mathscr{G}_v$'s are open, we conclude that the closure of $\mathscr{B} := \mu(P_{\mathscr{O}(S)})\mu(P_{\mathscr{O}(S)})^{-1}$ in $G_{(S\cup V_0)\setminus\{v_1\}}$ contains $G_{S\setminus\{v_1\}}\times\prod_{v\in V_0}\mathscr{E}_v$ for some open neighborhoods of the identity $\mathscr{E}_v\subseteq G_{K_v}$, $v\in V_0$. It follows that given an element g belonging to the left-hand side of the inclusion (19), there exists $h\in\mathscr{B}^{-1}$ such that

$$gh\in\left(\prod_{v\in(V_0\cup S)\setminus\{v_1,v_2\}}\mathscr{G}_v\right)\times\mathscr{G}'_{v_2}.$$

Thus, it is enough to show that

$$G_{\mathscr{O}(S)}\bigcap\left[\left(\prod_{v\in(V_0\cup S)\setminus\{v_1,v_2\}}\mathscr{G}_v\right)\times\mathscr{G}'_{v_2}\right]\subseteq\mu(P_{\mathscr{O}(S)}). \tag{20}$$

Fix a g belonging to the left-hand side of the inclusion (20). As in the proof of Proposition 6.4, we can find open sets $\Sigma_v\subseteq(B_g)_{\mathscr{O}_v}$ for $v\in(S\cup V_0)\setminus\{v_1,v_2\}$ such that

$$(g,\Sigma_v)\subseteq\varepsilon(\phi(\mathscr{P}_v))$$

and also an open set $\Sigma'_{v_2}\subseteq(B_g)_{K_{v_2}}$ such that

$$(g,\Sigma'_{v_2})\subseteq\varepsilon(\phi(\mathscr{P}'_{v_2})).$$

As in the proof of Proposition 6.4, we use the theorem in the Appendix to conclude that B_g has strong approximation with respect to $\{v_1\}$, so one can find

$$s\in(B_g)_{\mathscr{O}(S)}\bigcap\left[\left(\prod_{v\in(S\cup V_0)\setminus\{v_1,v_2\}}\Sigma_v\right)\times\Sigma'_{v_2}\right].$$

Then for each $v\in(S\cup V_0)\setminus\{v_1\}$, we have $\varepsilon^{-1}(g,s)_{K_v}\neq\varnothing$ implying that $(Q_s)_{K_v}\neq\varnothing$. Furthermore, the non-emptiness of $(Q_s)_{K_v}$ for $v=v_1$ follows from Lemma 5.1(i) as v_1 is Archimedean, and for $v\notin S\cup V_0$ — from Lemma 5.1(iii) as $s\in L$. So, by the Hasse–Minkowski theorem [18, 66:4], $(Q_s)_K\neq\varnothing$. Since $s\in\mathscr{U}_{v_2}$, by Lemma 5.2, Q_s has strong approximation with respect to S in all cases. The rest of the argument repeats verbatim the corresponding part of the proof of Proposition 6.4: we use strong approximation for Q_s to find a t for which the triple $\zeta=(g,s,t)$ satisfies (18); then by Theorem 3.1, $\phi^{-1}(\zeta)_{\mathscr{O}(S)}\neq\varnothing$. This implies that $g\in\mu(P_{\mathscr{O}(S)})$, and the proposition follows. □

Proof of the Main Theorem. As we explained in the beginning of this section, it is enough to establish bounded generation of $G_{\mathscr{O}(S)}$. For this, we will argue by induction on n. First, we will consider the case $i_K(f)\geqslant 2$. In this case we can assume without any loss of generality that the basis $e_1,\dots,e_n$ is chosen so that the space spanned by $e_1,\dots,e_4$ has Witt index two. If $n=5$, then the group G is K-split, so bounded generation of $G_{\mathscr{O}(S)}$ is a result of Tavgen [28]. For $n\geqslant 6$, it follows from Proposition 6.4 that $\mu(P_{\mathscr{O}(S)})$ contains an open subset of $G_{\mathscr{O}(S)}$, and since congruence subgroups form a base of neighborhoods of the identity, there exists a congruence subgroup $\Delta\subseteq G_{\mathscr{O}(S)}$

and an element $h \in G_{\mathcal{O}(S)}$ such that

$$h\Delta \subseteq \mu(P_{\mathcal{O}(S)}) = G(a)_{\mathcal{O}(S)} G(b)_{\mathcal{O}(S)} G(a)_{\mathcal{O}(S)} G(b)_{\mathcal{O}(S)}.$$

Since both $G(a)_{\mathcal{O}(S)}$ and $G(b)_{\mathcal{O}(S)}$ are boundedly generated by induction hypothesis and Δ has finite index in $G_{\mathcal{O}(S)}$, bounded generation of the latter follows from Lemma 6.3.

Now, suppose that $i_K(f) = 1$ but S contains a non-Archimedean valuation. Here the induction starts with $n = 4$, in which case G is known to be K-isomorphic to either $\mathbf{SL}_2 \times \mathbf{SL}_2$ or $R_{E/K}(\mathbf{SL}_2)$ for a suitable quadratic extension E/K (see, for example, [2, Thms. 5.21 and 5.22]). In either case, since S contains a non-Archimedean valuation, bounded generation of $G_{\mathcal{O}(S)}$ follows from bounded generation of $\mathrm{SL}_2(A)$, where A is a ring of S-integers in a number field having infinitely many units [7, 31]. For $n \geqslant 5$, the argument is completed as above using Proposition 6.5 instead of Proposition 6.4. □

Appendix

The purpose of this appendix is to formulate and prove the result on strong approximation in quadrics that was used in the proof of the Main Theorem. Let $q = q(x_1, \ldots, x_m)$ be a nondegenerate quadratic form in $m \geqslant 3$ variables over a number field K, and Q be a quadric given by the equation $q(x_1, \ldots, x_m) = a$ where $a \in K^\times$. Fix a nonempty subset S of V^K.

Theorem *Assume that $Q_K \neq \varnothing$ and $Q_S := \prod_{v \in S} Q_{K_v}$ is noncompact.*

(i) *If $m \geqslant 4$ then Q has strong approximation with respect to S.*

(ii) *If $m = 3$ then Q has strong approximation with respect to S if and only if the following condition holds: Let $x \in Q_K$ and let g be the restriction of q to the orthogonal complement of x in K^3; then either g is K-isotropic, or g is K-anisotropic and there exists $v \in S$ for which g is K_v-anisotropic and additionally q is K_v-isotropic if v is real.*

Assertion (i) is proved, for example, in [18, 104:3], where it is then used to establish strong approximation for $\mathbf{Spin}_m(q)$. We have not found, however, a proof of assertion (ii) in the literature. As was pointed out in [22], both facts can be derived from the analysis of strong approximation in the homogeneous spaces G/H which relies on the strong approximation theorem for algebraic groups and results on Galois cohomology. Such analysis for the cases where G is a connected simply connected K-group and H is either its connected simply connected K-subgroup or a K-subtorus (which are sufficient for the proof of the theorem) was given in [22]; the case of an arbitrary reductive H was independently considered in [5]. In our exposition we will follow [24].

First, we establish the following criterion of strong approximation which easily translates into the language of Galois cohomology.

Lemma 6.6 *Let $X = G/H$, where G is a connected K-group and H is its connected K-subgroup. If G has strong approximation with respect to S then the closure of X_K in $X_{A(S)}$ coincides with $G_{A(S)} X_K = \{gx \mid g \in G_{A(S)},\ x \in X_K\}$. Thus, X has strong approximation with respect to S if and only if the map of the orbit spaces $G_K \backslash X_K \to G_{A(S)} \backslash X_{A(S)}$ is surjective.*

Proof. It follows from the Implicit Function Theorem that for every $v \in V^K$ and any $x_v \in X_{K_v}$, the orbit $G_{K_v} x_v$ is open in X_{K_v} [21, §3.1, Cor. 2]. Moreover, for almost all $v \in V_f^K$, the group $G_{\mathcal{O}_v}$ acts on $X_{\mathcal{O}_v}$ transitively (this is a consequence of Hensel's lemma and the fact that for almost all v there exist smooth (irreducible) reductions $\underline{G}^{(v)}$, $\underline{H}^{(v)}$ and $\underline{X}^{(v)} = \underline{G}^{(v)}/\underline{H}^{(v)}$, so $\underline{G}^{(v)}$ acts on $\underline{X}^{(v)}$ transitively by Lang's theorem (see, for example, [3, §16]). Thus, for any $x \in X_{A(S)}$, the orbit $G_{A(S)}x$ is open in $X_{A(S)}$. We conclude that the complement of $G_{A(S)}X_K$ in $X_{A(S)}$ is open, hence $G_{A(S)}X_K$ is a closed subset of $X_{A(S)}$ containing X_K. On the other hand, strong approximation in G implies that $X_K = G_K X_K$ is dense in $G_{A(S)}X_K$, and all our assertions follow. □

To give a cohomological interpretation, we recall that for any field extension P/K, there is a natural bijection

$$G_P \backslash X_P \simeq \mathrm{Ker}\left(H^1(P,H) \to H^1(P,G)\right)$$

(see [26] for the details and unexplained notations). In the adelic setting, for any finite Galois extension L/K, there is a bijection

$$G_{A(S)} \backslash (X_{A(S)} \cap \alpha(G_{A(S)\otimes_K L})) \simeq \mathrm{Ker}\left(H^1(L/K, H_{A(S)\otimes_K L}) \to H^1(L/K, G_{A(S)\otimes_K L})\right)$$

where $\alpha\colon G \to G/H = X$ is the canonical map. Given an algebraic K-group D, we let $H^1(K,D)_{A(S)}$ denote the direct limit of the sets $H^1(L/K, D_{A(S)\otimes_K L})$ taken over all finite Galois extensions L/K; we notice that if D is connected then for a fixed L/K the set $H^1(L_w/K_v, D_{\mathcal{O}(L_w)})$ is trivial for almost all $v \in V_f^K$, where $w|v$, so $H^1(K,D)_{A(S)}$ can be identified with the set $\prod'_{v\notin S} H^1(K_v,D)$ consisting of $(c_v) \in \prod_{v\notin S} H^1(K_v,D)$ such that c_v is trivial for almost all v (see [21, §6.2]). With these notations, there is a bijection

$$G_{A(S)} \backslash X_{A(S)} \simeq \mathrm{Ker}\left(H^1(K,H)_{A(S)} \to H^1(K,G)_{A(S)}\right)$$

Now we can reformulate Lemma 6.6 as follows.

Corollary 6.7 *Let $X = G/H$ as above. Assume that G has strong approximation with respect to S. Then X has strong approximation with respect to S if and only if the natural map*

$$\mathrm{Ker}\left(H^1(K,H) \to H^1(K,G)\right) \longrightarrow \mathrm{Ker}\left(H^1(K,H)_{A(S)} \to H^1(K,G)_{A(S)}\right)$$

is surjective.

We recall that to have strong approximation with respect to a finite S, an algebraic group G must be connected and simply connected [21, §7.4], so we will assume that this is the case in the rest of this appendix. The cohomological criterion of Corollary 6.7 immediately leads to the following.

Proposition 6.8 *Let $X = G/H$ where G has strong approximation with respect to S. If H is connected and simply connected then X also has strong approximation with respect to S.*

Proof. Since G and H are both simply connected, $H^1(K_v, G)$ and $H^1(K_v, H)$ are trivial for all $v \in V_f^K$ [21, Thm 6.4]. This means that

$$\begin{aligned}\operatorname{Ker}\left(H^1(K,H)_{A(S)} \to H^1(K,G)_{A(S)}\right) \\ = \prod_{v\in V_\infty^K \setminus (V_\infty^K \cap S)} \operatorname{Ker}\left(H^1(K_v,H) \to H^1(K_v,G)\right).\end{aligned}$$

So, the proposition follows from Corollary 6.7 and the fact that the map

$$\psi\colon \operatorname{Ker}\left(H^1(K,H) \to H^1(K,G)\right) \longrightarrow \prod_{v\in V^K} \operatorname{Ker}\left(H^1(K_v,H) \to H^1(K_v,G)\right)$$

is surjective. This is in fact true for any connected H. Indeed, we have the following commutative diagram:

$$\begin{array}{ccc} H^1(K,H) & \longrightarrow & H^1(K,G) \\ {\scriptstyle\beta}\big\downarrow & & \big\downarrow{\scriptstyle\gamma} \\ \prod_{v\in V_\infty^K} H^1(K_v,H) & \longrightarrow & \prod_{v\in V_\infty^K} H^1(K_v,G) \end{array}$$

Since β is surjective [21, Prop. 6.17] and γ is injective ("Hasse principle", [21, Thm. 6.6]), the surjectivity of ψ follows. $\square$

Proposition 6.8 readily yields assertion (i) of the theorem. Indeed, it follows from Witt's theorem that Q is a homogeneous space of $G = \mathbf{Spin}_m(q)$ so that if $x \in Q_K$ then Q can be identified with the homogeneous space $X = G/H$ where $H = G(x)$. Clearly, $H = \mathbf{Spin}_{m-1}(g)$, where g is the restriction of q to the orthogonal complement of x; in particular H is connected and simply connected for $m \geqslant 4$. Since Q_S is noncompact, G_S is also noncompact, and hence has strong approximation with respect to S. Thus, strong approximation for $Q \cong X$ follows from Proposition 6.8. If $m = 3$ then $H = \mathbf{Spin}_2(g)$ is a 1-dimensional torus, so to handle this case we need to analyze the cohomological criterion of Corollary 6.7 in the situation where $H = T$ is a K-torus.

So, let T be a K-torus of a connected simply connected K-group G. Fix a finite Galois extension L/K that splits T. It follows from Hilbert's Theorem 90 that

$$H^1(K,T) = H^1(L/K,T) \quad \text{and} \quad H^1(K,T)_{A(S)} = H^1(L/K, T_{A(S)\otimes_K L}).$$

So, the map in Corollary 6.7 reduces to the following

$$\begin{aligned}\phi\colon \operatorname{Ker}\left(H^1(L/K,T) \to H^1(L/K,G)\right) \longrightarrow \\ \operatorname{Ker}\left(H^1(L/K,T_{A(S)\otimes_K L}) \to H^1(L/K,G_{A(S)\otimes_K L})\right).\end{aligned}$$

We now let A denote the (full) adelic ring of K. It follows from the Hasse principle for G that the map γ in the following commutative diagram

$$\begin{array}{ccc} H^1(L/K,T) & \xrightarrow{\alpha} & H^1(L/K,G) \\ {\scriptstyle\beta}\big\downarrow & & \big\downarrow{\scriptstyle\gamma} \\ H^1(L/K,T_{A\otimes_K L}) & \xrightarrow{\delta} & H^1(L/K,G_{A\otimes_K L}) \end{array}$$

is injective, so

$$\beta(\operatorname{Ker}\alpha) = \operatorname{Im}\beta \cap \operatorname{Ker}\delta. \tag{21}$$

Let $C_L(T) = T_{\mathbb{A}\otimes_K L}/T_L$ denote the group of classes of adeles of T over L. The exact sequence

$$1 \longrightarrow T_L \longrightarrow T_{\mathbb{A}\otimes_K L} \longrightarrow C_L(T) \longrightarrow 1$$

gives rise to the exact cohomological sequence

$$H^1(L/K, T) \xrightarrow{\beta} H^1(L/K, T_{\mathbb{A}\otimes_K L}) \xrightarrow{\rho} H^1(L/K, C_L(T)). \tag{22}$$

Writing $\mathbb{A} = \mathbb{A}(S) \times K_S$ where $K_S = \prod_{v\in S} K_v$ and using (21) in conjunction with the exactness of (22), we obtain

$$\begin{aligned}\operatorname{Im}\phi = \{x \in \operatorname{Ker}\left(H^1(L/K, T_{\mathbb{A}(S)\otimes_K L}) \to H^1(L/K, G_{\mathbb{A}(S)\otimes_K L})\right) \mid \text{ there is}\\ y \in \operatorname{Ker}\left(H^1(L/K, T_{K_S\otimes_K L}) \to H^1(L/K, G_{K_S\otimes_K L})\right) \text{ with } \rho(x,y) = 0\}.\end{aligned} \tag{23}$$

Now we are in a position to give a criterion for strong approximation in $X = G/T$ in terms of properties of the map ρ.

Proposition 6.9 *Let $X = G/T$ where G is a simply connected K-group and T is a K-subtorus of G. Assume that G has strong approximation with respect to S. Then X has strong approximation with respect to S if and only if*

$$\rho\left(H^1(L/K, T_{\mathbb{A}(S)\otimes_K L})\right) \subseteq \rho\left(\operatorname{Ker}\left(H^1(L/K, T_{K_S\otimes_K L}) \to H^1(L/K, G_{K_S\otimes_K L})\right)\right). \tag{24}$$

Proof. It follows from (23) and Corollary 6.7 that all we need to prove is the equality

$$\begin{aligned}\rho\left(\operatorname{Ker}\left(H^1(L/K, T_{\mathbb{A}(S)\otimes_K L}) \to H^1(L/K, G_{\mathbb{A}(S)\otimes_K L})\right)\right)\\ = \rho\left(H^1(L/K, T_{\mathbb{A}(S)\otimes_K L})\right).\end{aligned} \tag{25}$$

Notice that for any $v \in V_f^K$ and its extension $w \in V_f^L$, the first cohomology

$$H^1(L/K, G_{K_v\otimes_K L}) = H^1(L_w/K_v, G_{L_w})$$

is trivial. This implies that

$$\begin{aligned}&\operatorname{Ker}\left(H^1(L/K, T_{\mathbb{A}(S)\otimes_K L}) \to H^1(L/K, G_{\mathbb{A}(S)\otimes_K L})\right) = \\ &\quad \operatorname{Ker}\left(H^1(L/K, T_{K_{S_\infty}\otimes_K L}) \to H^1(L/K, G_{K_{S_\infty}\otimes_K L})\right) \times H^1(L/K, T_{\mathbb{A}(S\cup S_\infty)\otimes_K L})\end{aligned}$$

where $S_\infty = V_\infty^K \setminus (V_\infty^K \cap S)$. Thus, to establish (25) it suffices to show that for any $v_0 \in V_\infty^K$ there exists $v \notin S \cup V_\infty^K$ such that

$$\rho(H^1(L/K, T_{K_{v_0}\otimes_K L})) = \rho(H^1(L/K, T_{K_v\otimes_K L})). \tag{26}$$

Let $X_*(T)$ be the group of cocharacters of T (i.e., $X_*(T) = \operatorname{Hom}(\mathbf{G}_m, T)$). It follows from the Nakayama–Tate Theorem [30] that one can identify

$$H^1(L/K, C_L(T)) \quad \text{with} \quad \hat{H}^{-1}(L/K, X_*(T))$$

and

$$H^1(L/K, T_{K_{v_0}\otimes_K L}) = H^1(L_{w_0}/K_{v_0}, T_{L_{w_0}}) \quad \text{with} \quad \hat{H}^{-1}(L_{w_0}/K_{v_0}, X_*(T))$$

and under these identifications the left-hand side of (26) coincides with the image of the corestriction map

$$\mathrm{Cor}^{\mathrm{Gal}(L/K)}_{\mathrm{Gal}(L_{w_0}/K_{v_0})} \colon \hat{H}^{-1}(L_{w_0}/K_{v_0}, X_*(T)) \longrightarrow \hat{H}^{-1}(L/K, X_*(T)).$$

Similarly, the right-hand side of (26) coincides with the image of

$$\mathrm{Cor}^{\mathrm{Gal}(L/K)}_{\mathrm{Gal}(L_{w}/K_{v})} \colon \hat{H}^{-1}(L_{w}/K_{v}, X_*(T)) \longrightarrow \hat{H}^{-1}(L/K, X_*(T))$$

(we fix extensions $w_0|v_0$ and $w|v$). Thus, (26) definitely holds if $\mathrm{Gal}(L_{w_0}/K_{v_0}) = \mathrm{Gal}(L_w/K_v)$. But for $v_0 \in V_\infty^K$, the Galois group $\mathrm{Gal}(L_{w_0}/K_{v_0})$ is cyclic, so the existence of $v \notin S \cup V_\infty^K$ with the same Galois group $\mathrm{Gal}(L_w/K_v)$ follows from Chebotarev Density Theorem (see, for example, [19, Ch. VII, Thm. 13.4]). □

We can now complete the proof of assertion (ii) of the theorem. As we pointed out earlier, here Q can be identified with the homogeneous space $X = G/T$, where $G = \mathbf{Spin}_3(q)$ and T is the 1-dimensional torus $\mathbf{Spin}_2(g)$ where g is the restriction of q to the orthogonal complement of a chosen point $x \in Q_K$. If g is K-isotropic then T splits over $L = K$, so (24) trivially holds, and Proposition 6.9 yields strong approximation in $Q \cong X$.

Suppose now that g is K-anisotropic. Then T splits over a quadratic extension L/K, with the nontrivial element of $\mathrm{Gal}(L/K)$ acting on $X_*(T) \cong \mathbb{Z}$ as multiplication by -1, so

$$H^1(L/K, C_L(T)) \cong \hat{H}^{-1}(L/K, X_*(T)) \cong \mathbb{Z}/2\mathbb{Z}.$$

Furthermore, by Chebotarev Density Theorem there exists $v \notin S \cup V_\infty^K$ such that L_w/K_v is a quadratic extension, and then

$$\rho\left(H^1(L_w/K_v, T)\right) = H^1(L/K, C_L(T))$$

implying that

$$\rho\left(H^1(L/K, T_{A(S)\otimes_K L})\right) = H^1(L/K, C_L(T)).$$

Thus, the condition (24) that gives a criterion for strong approximation in X boils down to the equality

$$\rho\left(\mathrm{Ker}\left(H^1(L/K, T_{K_S\otimes_K L}) \to H^1(L/K, G_{K_S\otimes_K L})\right)\right) = H^1(L/K, C_L(T)),$$

which in turn holds if and only if there is $v \in S$ such that

$$\mathrm{Ker}\left(H^1(L_w/K_v, T) \to H^1(L_w/K_v, G)\right) \neq \{1\}. \tag{27}$$

Clearly, (27) holds if L_w/K_v is a quadratic extension (i.e., g is K_v-anisotropic) and when $H^1(L_w/K_v, G) = \{1\}$ which happens if either $v \in V_f^K$ or q is K_v-isotropic (notice that in the latter case $G \cong \mathbf{SL}_2$ over K_v). This proves the presence of strong approximation in all cases listed in (ii). It remains to show that in all other situations strong approximation does not hold, i.e., (27) fails for all $v \in S$. If T splits over K_v then $H^1(L_w/K_v, T) = \{1\}$, so (27) cannot possibly hold. In the remaining case, v is real and G is K_v-anisotropic. Then $G = \mathbf{SL}_1(\mathbb{H})$ where $\mathbb{H}$ is the algebra of Hamiltonian quaternions and T corresponds to a maximal subfield of $\mathbb{H}$. A simple computation shows that the map $H^1(\mathbb{C}/\mathbb{R}, T) \to H^1(\mathbb{C}/\mathbb{R}, G)$ is a bijection, so again (27) fails.

(Thus, the 2-dimensional quadric over $\mathbb{Q}$ given by the equation $x_1^2+x_2^2-2x_3^2=1$ does not have strong approximation with respect to $S=V_\infty^{\mathbb{Q}}$.)

References

[1] M. Abért, A. Lubotzky, L. Pyber, Bounded generation and linear groups, *Inernat. J. Algebra Comput.* **13** (2003), no. 4, 401–413.

[2] E. Artin, Geometric Algebra, Interscience Publishers, Inc., Interscience Tracts in Pure and Applied Mathematics, New York, 1966.

[3] A. Borel, Linear Algebraic Groups, 2nd edition, GTM, 126, Springer–Verlag, New York, 1991.

[4] M.V. Borovoi, Abstract simplicity of some anisotropic algebraic groups over number fields, *Dokl. Acad. Sci. USSR* **283** (1985), 794–798.

[5] M.V. Borovoi, On strong approximation for homogeneous spaces, *Dokl. Akad. Nauk BSSR* **33** (1989), no. 4, 293–296.

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

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

[8] J.D. Dixon, M.P.F du Sautoy, A. Mann, Analytic pro-p Groups, London Math. Soc. Lecture Note Series, **157**, Cambridge Univ. Press, Cambridge, 1991.

[9] I.V. Erovenko and A.S. Rapinchuk, Bounded generation of some S-arithmetic orthogonal groups, *C. R. Acad. Sci. Paris Ser. I Math* **333** (2001), no. 5, 395–398.

[10] Y. Kitaoka, Arithmetic of Quadratic Forms. *Cambridge Tracts in Mathematics, 106.* Cambridge University Press, Cambridge, 1993.

[11] M. Kneser, Quadratische Formen, Springer–Verlag, Berlin, 2002.

[12] M. Lazard, Groupes analytiques p-adiques, *Inst. Hautes Études Sci. Publ. Math.* **26** (1965), 389–603.

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

[14] A. Lubotzky, Dimension function for discrete groups, *London Math. Soc. Lecture Note Ser.* **121** (1986), 254–262.

[15] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), no. 2, 267–295.

[16] A. Muranov, Diagrams with selection and method for constructing boundedly generated and boundedly simple groups, *Comm. Algebra* **33** (2005), no. 4, 1217–1258.

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

[18] O.T. O'Meara, Introduction to Quadratic Forms, Academic Press, Inc., Publishers, New York; Springer–Verlag, Berlin–Göttingen–Heidelberg, 1963.

[19] J. Neukirch, Algebraic Number Theory, Grundlehren der Mathematischen Wissenschaften, 322, Springer–Verlag, Berlin, 1999.

[20] V.P. Platonov and A.S. Rapinchuk, Abstract properties of S-arithmetic groups and the congruence problem, *Russian Acad. Sci. Izv. Math.* **40** (1993), no. 3, 455–476.

[21] V.P. Platonov and A.S. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, Boston, 1993.

[22] A.S. Rapinchuk, The congruence subgroup problem for algebraic groups and strong approximation in affine varieties, *Dokl. Akad. Nauk BSSR* **32** (1988), no. 7, 581–584.

[23] A.S. Rapinchuk, Representations of groups of finite width, *Dokl. Akad. Nauk SSSR* **315** (1990), 536–540.

[24] A.S. Rapinchuk, The congruence subgroup problem, Habilitationsschrift, Institute of Mathematics, Acad. Sci. Belarus, Minsk, 1990.

[25] A.S. Rapinchuk, On SS-rigid groups and A. Weil's criterion for local rigidity, *Manuscripta Math.* **97** (1998), no. 4, 529–543.

[26] J–P. Serre, Galois Cohomology, Springer–Verlag, Berlin, 1997.

[27] J–P. Serre, Lie Algebras and Lie Groups, Lecture Notes in Mathematics, 1500, Springer–Verlag, Berlin, 1992.

[28] O.I. Tavgen, Bounded generation of Chevalley groups over the rings of S-integers, *Izv. Akad. Nauk SSSR, Ser. Mat.* **54** (1990), 97–122.

[29] W. van der Kallen, $\mathrm{SL}_3(\mathbb{C}[x])$ does not have bounded word length, Algebraic K-theory, Part I (Oberwolfach, 1980), pp. 357–361, Lecture Notes in Math., 966, Springer, Berlin–New York, 1982.

[30] V.E. Voskresenskii, Algebraic Groups and Their Birational Invariants, Translations of Mathematical Monographs, 179, American Mathematical Society, Providence, RI, 1988.

[31] D. Witte Morris, Bounded generation of $\mathrm{SL}(n,A)$ (after D. Carter, G. Keller, and E. Paige). Preprint, 2005.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF NORTH CAROLINA AT GREENSBORO, GREENSBORO NC 27402, USA

E-mail address: igor@uncg.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE VA 22904, USA

E-mail address: asr3x@virginia.edu