Journal of Number Theory 225 (2021) 281–293

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Explicit result on equivalence of rational quadratic forms avoiding primes

Wai Kiu Chan [a,*], Haochen Gao [b], Han Li [a]

[a] *Department of Mathematics and Computer Science, Wesleyan University, Middletown, CT, 06459, USA*
[b] *WesBox 91800, Wesleyan University, Middletown, CT, 06459, USA*

ARTICLE INFO

Article history:
Received 30 July 2020
Received in revised form 11 January 2021
Accepted 21 February 2021
Available online 17 March 2021
Communicated by F. Pellarin

MSC:
11E12

Keywords:
Equivalence of quadratic forms

ABSTRACT

Given a pair of regular quadratic forms over $\mathbb{Q}$ which are in the same genus and a finite set of primes P, we show that there is an effective way to determine a rational equivalence between these two quadratic forms which are integral over every prime in P. This answers one of the principal questions posed by Conway and Sloane (1999) [3, page 402],.

1. Introduction

A fundamental question in the arithmetic theory of quadratic forms is to decide when two given rational quadratic forms are integrally equivalent. For the sake of convenience, we will identify each quadratic form with its Gram matrix. Given a pair of n-ary regular quadratic forms F and G over $\mathbb{Q}$, the question is to decide whether there is a matrix $\tau \in \mathrm{GL}_n(\mathbb{Z})$ such that

* Corresponding author.
E-mail addresses: wkchan@wesleyan.edu (W.K. Chan), hgao@wesleyan.edu (H. Gao), hli03@wesleyan.edu (H. Li).

https://doi.org/10.1016/j.jnt.2021.02.006
0022-314X/

$$\tau' F \tau = G, \tag{1.1}$$

where τ' denotes the transpose of τ. Gauss' reduction theory provides a quite satisfactory solution to this question when $n = 2$. Therefore in the subsequent discussion we will focus mainly on the case when $n \geq 3$, although many results mentioned later also hold for the binary case. When F and G are positive definite, one can deduce from (1.1) explicit upper bounds on the height of τ in terms of the heights of F and G (the height of a matrix, denoted by H, and other height functions will be defined later in Section 2). Hence, in principle, we could perform an exhaustive search for τ, and a fortiori provide an effective solution to the question in this case.

When F and G are indefinite, (1.1) has infinitely many solutions and an exhaustive search for τ is not possible. However, Siegel [11] showed that there exists a function $C(n, F, G)$ such that if (1.1) has a solution then it must have one whose height is less than $C(n, F, G)$. Although Siegel did not give an explicit upper bound for $C(n, F, G)$, his method is effective. Indeed, by following Siegel's argument Straumann [12] showed that

$$C(n, F, G) \leq \exp\left(k_n (H(F)H(G))^{\delta_n}\right)$$

where δ_n is an explicit polynomial in n and k_n is a constant depending only on n. Masser [7, page 252] conjectured that (for $n \geq 3$)

$$C(n, F, G) \ll_n (H(F) + H(G))^{\lambda_n}$$

where λ_n is a constant depending only on n. This conjecture has been confirmed by Dietmann [4] for $n = 3$ (and for $n \geq 4$ when $\det(F)$ is cube-free), and by the third author and Margulis [5, Theorem 1] for all $n \geq 3$ who also show that λ_n can be taken to be a polynomial of n. Thus, in principle, there is a deterministic algorithm to decide if F and G are equivalent over $\mathbb{Z}$ and, if they are, to exhibit an explicit integral equivalence τ satisfying (1.1).

Another approach is appealing to the theory of spinor genus. Before checking whether F and G are equivalent over $\mathbb{Z}$, we could check first if they are in the same genus, that is, if they are equivalent over $\mathbb{R}$ and over $\mathbb{Z}_p$ for every prime p. Over $\mathbb{R}$ this is straightforward; by Sylvester's Law of Inertia we just need to make sure that F and G have the same numbers (counted with multiplicity) of positive as well as negative eigenvalues. Over $\mathbb{Z}_p$, this can be done effectively by using the invariants deriving from the Jordan decompositions of F and G; see [8, Chapter IX] or [2, Chapter 8]. When $n \geq 3$, the spinor genus and the class of an indefinite quadratic form coincide [8, 104:5]. Therefore, the question is now reduced to deciding if F and G are in the same spinor genus, assuming that F and G are already in the same genus. There are effective algorithms to do just that; see [1] or [3, Chapter 13, Section 9]. These algorithms usually require a rational matrix τ which satisfies (1.1) and is invertible over the ring $\mathbb{Z}^P := \bigcap_{p \in P} (\mathbb{Z}_p \cap \mathbb{Q})$,

where P is the set of prime divisors of $2\det(F)$. Finding such an explicit τ is one of the principal questions posed by Conway and Sloane in [3, Page 402, Question (G4)]:

(G4) "*If two quadratic forms are in the same genus, find an explicit rational equivalence whose denominator is prime to any given number.*"

Existence of such rational equivalence can be deduced from the weak approximation property of the special orthogonal groups [8, 101:7]. Siegel [10] also demonstrated the existence by a different argument making use of the Cayley Transformation. Both approaches have not been made effective. However, a careful review of Siegel's argument suggests to us that his proof can be made effective and this is our approach to a solution to (G4). Our main result (Theorem 3.1) is an explicit upper bound on the height of a skew-symmetric matrix whose image under the Cayley transformation is the rational equivalence wanted in (G4). Thus, in principle, one of such rational equivalences can be found by an exhaustive search.

The rest of the paper is organized as follows. Throughout this paper, k, m, n are positive integers and p is always a prime number. Section 2 contains preliminary materials on estimates pertaining to the p-adic valuations and on quadratic forms. The main theorem, Theorem 3.1, will be presented in Section 3.

2. Preliminaries

For any prime number p, $|\ |_p$ is the p-adic valuation normalized so that $|p|_p = p^{-1}$. The norm $\|\ \|_p$ on any $\mathbb{Q}_p^m$ is the p-adic sup-norm, that is,

$$\|\boldsymbol{\xi}\|_p = \max_{1\le i\le n}\{|\xi_i|_p\}, \quad \boldsymbol{\xi} = (\xi_1, \dots, \xi_m) \in \mathbb{Q}_p^m.$$

Let $h_p(\boldsymbol{\xi}) := \max\{\|\boldsymbol{\xi}\|_p, 1\}$, which is often called the p-adic inhomogeneous height of $\boldsymbol{\xi}$. It is obvious that $\|\boldsymbol{\xi}\|_p \le h_p(\boldsymbol{\xi})$. For any $m \times n$ matrix A over $\mathbb{Q}_p$, $\|A\|_p$ and $h_p(A)$ are defined by viewing A as a vector in $\mathbb{Q}_p^{mn}$.

Lemma 2.1. *Let X, Y be two $n \times n$ matrices over $\mathbb{Q}_p$. Then:*

(1) $\|X + Y\|_p \le \max\{\|X\|_p, \|Y\|_p\}$.
(2) $\|XY\|_p \le \|X\|_p \|Y\|_p$.
(3) $|\det(X)|_p \le \|X\|_p^n \le h_p(X)^n$.
(4) *If X is invertible, then* $\|X^{-1}\|_p \le \frac{\|X\|_p^{n-1}}{|\det(X)|_p}$.

Proof. This is clear. □

Lemma 2.2. *Let X, Y be $n \times n$ matrices over $\mathbb{Q}_p$. If $\|Y - X\|_p < \frac{|\det(X)|_p}{h_p(X)^n}$, then $|\det(X)|_p = |\det(Y)|_p$.*

Proof. Let us write $Y = (y_{ij})$ and $X = (x_{ij})$, and let S_n be the symmetric group on $\{1, \dots, n\}$. Notice that

$$\begin{aligned} |\det(Y) - \det(X)|_p &= \left| \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} y_{i\sigma(i)} \right) - \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)} \right) \right|_p \\ &= \left| \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(\prod_{i=1}^{n} y_{i\sigma(i)} - \prod_{i=1}^{n} x_{i\sigma(i)} \right) \right|_p . \end{aligned}$$

To finish the proof, it suffices, by the ultra-triangle inequality, to show that the p-adic valuation of each term in the sum is strictly less than $|\det(X)|_p$. For the sake of brevity, we will only demonstrate the analysis for one term. The readers will find no trouble in carrying out the same argument for the other terms.

Let us consider the term $\prod_{i=1}^{n} y_{ii} - \prod_{i=1}^{n} x_{ii}$. By writing $y_{ii} = x_{ii} + \delta_i$, we see that

$$\prod_{i=1}^{n} y_{ii} - \prod_{i=1}^{n} x_{ii} = \prod_{i=1}^{n} (x_{ii} + \delta_i) - \prod_{i=1}^{n} x_{ii}$$

which is a sum of $2^n - 1$ terms, each being a product of n numbers in $\mathbb{Q}_p$ whose p-adic valuation is smaller than

$$\|X\|_p^{n-k} \, \|Y - X\|_p^k$$

for some $1 \le k \le n$. Note that $\|X-Y\|_p^k \le \|X-Y\|_p$ for any $k \ge 1$ because $\|X-Y\|_p < 1$ as a result of Lemma 2.1(3). Therefore,

$$\|X\|_p^{n-k} \|X - Y\|_p^k \le \|X - Y\|_p \, h_p(X)^n < |\det(X)|_p$$

as claimed. □

Lemma 2.3. *Let P be a finite set of primes, d be a positive integer, and $0 < \varepsilon \le 1$ be a real number. Suppose that for every $p \in P$, an $x_p \in \mathbb{Q}_p$ is given such that $dx_p \in \mathbb{Z}_p$. Then, there exists $z \in \mathbb{Z}$ such that for each $p \in P$,*

$$\left| \frac{z}{d} - x_p \right|_p < \varepsilon \quad \text{and} \quad 0 \le z < \prod_{p \in P} p^{\ell_p}$$

where $\ell_p = \left\lceil \log_p \left(\frac{d}{\varepsilon} \right) \right\rceil + 1$.

Proof. Since $\mathbb{Z}$ is dense in each $\mathbb{Z}_p$, there exists $z_p \in \mathbb{Z}$ such that

$$|dx_p - z_p|_p < \frac{\varepsilon}{d}, \qquad \forall\, p \in P.$$

By the Chinese Remainder Theorem, there exists an integer z such that for each $p \in P$,

$$z \equiv z_p \mod p^{\ell_p}, \qquad \text{and} \qquad 0 \le z < \prod_{p \in P} p^{\ell_p}.$$

Moreover, since $p^{\ell_p} \frac{\varepsilon}{d} > 1$,

$$\begin{aligned} |z - dx_p|_p &= |z - z_p + z_p - dx_p|_p \\ &\le \max\{|z - z_p|_p, |z_p - dx_p|_p\} \\ &< \frac{\varepsilon}{d}. \end{aligned}$$

Then, since $d|d|_p \ge 1$, $\left|\frac{z}{d} - x_p\right|_p < \varepsilon$ as claimed. □

The following lemma is essentially [10, Lemma 15] but we draw a different conclusion at the end of its proof.

Lemma 2.4. *Let $A \in \mathrm{GL}_n(\mathbb{Q}_p)$. There exists at least one diagonal matrix E whose diagonal entries are 1 or -1 such that*

$$|\det(A - E)|_p \ge |2^n \cdot \det(A)|_p.$$

Proof. Let D be the diagonal matrix with indeterminate diagonal entries $\lambda_1, \lambda_2, \cdots, \lambda_n$. The determinant $\det(A - D)$ is a linear function of any of the $\lambda_k (k = 1, 2..., n)$ and the same holds for the function

$$T(\lambda_1, \lambda_2, \cdots, \lambda_n) := \sum_{\Lambda \in \mathcal{E}} \det(A - \Lambda D), \tag{2.1}$$

where $\mathcal{E}$ is the group of $n \times n$ diagonal matrices with ± 1 as the diagonal entries. If D is replaced by ΛD, for any $\Lambda \in \mathcal{E}$, the function T is not changed. Consequently T is an even function of any of the variables $\lambda_k (k = 1, 2..., n)$. This proves that T is a constant. By taking in particular $D = I_n$ and $\mathbf{0}$ in (2.1), we obtain

$$\left| \sum_{\Lambda \in \mathcal{E}} \det(A - \Lambda) \right|_p = |2^n \cdot \det(A)|_p .$$

Therefore, there must be at least one $E \in \mathcal{E}$ such that $|\det(A - E)|_p \ge |2^n \cdot \det(A)|_p$. □

For any $\boldsymbol{\xi} \in \mathbb{Q}^m$, the homogeneous height of $\boldsymbol{\xi}$ is

$$H(\boldsymbol{\xi}) := \|\boldsymbol{\xi}\| \prod_p \|\boldsymbol{\xi}\|_p$$

where $\|\boldsymbol{\xi}\|$ is the sup-norm of $\boldsymbol{\xi}$. The inhomogeneous height of $\boldsymbol{\xi}$ is defined as

$$h(\boldsymbol{\xi}) := H((1, \boldsymbol{\xi})) = \|(\boldsymbol{\xi}, 1)\| \prod_p h_p(\boldsymbol{\xi}).$$

It is not hard to see that for any positive number C, there are only finitely many $\boldsymbol{\xi} \in \mathbb{Q}^m$ such that $h(\boldsymbol{\xi}) \leq C$ (the Northcott Property). For any $m \times n$ matrix A over $\mathbb{Q}$, $H(A)$ and $h(A)$ are defined by viewing A as a vector in $\mathbb{Q}^{mn}$.

Let F and G be two n-ary regular quadratic forms over $\mathbb{Q}$. There are two matrices determined by F and G that will be taken as input data in Theorem 3.1:

(i) A matrix $\Sigma \in \mathrm{GL}_n(\mathbb{Q})$ such that $\Sigma' F \Sigma$ is diagonal.
The columns $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ of Σ form an orthogonal basis of $\mathbb{Q}^n$ with respect to the bilinear form induced by F. Finding such an orthogonal basis is the well-known Gram-Schmidt process. We first pick a vector $\boldsymbol{x}_1$ such that $F(\boldsymbol{x}_1) \neq 0$. The second vector $\boldsymbol{x}_2$ must be in the orthogonal complement of $\boldsymbol{x}_1$ and hence it is in the solution space of the homogeneous system $\boldsymbol{x}' F \boldsymbol{x}_1 = \boldsymbol{0}$. We may continue this process to find the other $\boldsymbol{x}_i$.

(ii) A matrix $\sigma \in \mathrm{GL}_n(\mathbb{Q})$ such that $\sigma' F \sigma = G$.
By (i), we may assume that G is already diagonalized, say $G = \mathrm{diag}(b_1, \ldots, b_n)$. Since G is regular, each b_i is nonzero. Finding σ is tantamount to finding an orthogonal basis $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_n$ of $\mathbb{Q}^n$ with respect to the symmetric bilinear form induced by F such that $F(\boldsymbol{t}_i) = b_i$ for $1 \leq i \leq n$. Let F_{b_1} be the $(n+1)$-ary quadratic form $F(x_1, \ldots, x_n) - b_1 x_{n+1}^2$. A theorem of Masser [6] shows that there must be a vector $\boldsymbol{t}_1 \in \mathbb{Q}^n$ such that $F(\boldsymbol{t}_1) = b_1$ and

$$h(\boldsymbol{t}_1) \leq 3^{\frac{n+1}{2}} n^{n+1} H(F_{b_1})^{\frac{n+1}{2}}.$$

As we mentioned earlier, there are only finitely many vectors in $\mathbb{Q}^n$ whose inhomogeneous height satisfy this inequality. This gives us an effective procedure to find $\boldsymbol{t}_1$.
The second vector $\boldsymbol{t}_2$ must be in the orthogonal complement of $\boldsymbol{t}_1$, which is the solution space of the homogeneous system $\boldsymbol{x}' F \boldsymbol{t}_1 = \boldsymbol{0}$. Take a basis $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ of this subspace, and let T be the matrix whose columns are these $n-1$ vectors. We may then apply Masser's theorem to the quadratic form $T' F T$ and find an explicit search bound for the inhomogeneous height of $\boldsymbol{t}_2$. Once again we have an effective procedure to find $\boldsymbol{t}_2$. By continuing this process in the obvious manner we should be able to find the other $\boldsymbol{t}_i$.

As in the proof of Lemma 2.4, we let $\mathcal{E}$ be the group of diagonal matrices with diagonal entries 1 or -1.

Lemma 2.5. *Let F and G be n-ary regular rationally equivalent quadratic forms over $\mathbb{Q}$. Let $\sigma, \Sigma \in \mathrm{GL}_n(\mathbb{Q})$ be such that $\sigma' F \sigma = G$ and $\Sigma' F \Sigma$ is diagonal. Then,*

(1) *For any* $E \in \mathcal{E}$,

$$(\Sigma E \Sigma^{-1}\sigma)' F (\Sigma E \Sigma^{-1}\sigma) = G.$$

(2) *There exists a matrix* $\tau \in \{\Sigma E \Sigma^{-1}\sigma : E \in \mathcal{E}\}$ *satisfying the following properties. Suppose that* F *and* G *are equivalent over* $\mathbb{Z}_p$. *Then there exists a* $\tau_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ *such that* $\tau_p' F \tau_p = G$, *that* $\det(\tau - \tau_p) \neq 0$, *and that*

$$\|(\tau - \tau_p)^{-1}\|_p \leq h_p(\tau)^{n-1} \cdot \max\left\{\frac{1}{|2^n|_p}, \frac{1}{|\det(\sigma)|_p}\right\}.$$

Proof. Part (1) follows from direct computation, which we leave the detail to the readers. For part (2), let $\mathrm{Equiv}(F, G)$ denote the set of all prime numbers p for which F and G are equivalent over $\mathbb{Z}_p$, and let p_0 be the smallest element in $\mathrm{Equiv}(F, G)$. Let σ_0 be any matrix in $\mathrm{GL}_n(\mathbb{Z}_{p_0})$ satisfying

$$\sigma_0' F \sigma_0 = G.$$

Applying Lemma 2.4 to $A_0 := \Sigma^{-1}\sigma_0\sigma^{-1}\Sigma$, we get that there exists an $E_0 \in \mathcal{E}$ such that

$$|\det(A_0 - E_0)|_{p_0} \geq |2^n \cdot \det(A_0)|_{p_0}. \tag{2.2}$$

We shall prove that $\tau := \Sigma E_0 \Sigma^{-1}\sigma \in \mathrm{GL}_n(\mathbb{Q})$ satisfies our lemma.

First, for $p = p_0$, we take $\tau_{p_0} = \sigma_0$. Since $\sigma_0 \in \mathrm{GL}_n(\mathbb{Z}_{p_0})$, we have $|\det(\sigma_0)|_{p_0} = 1$. This fact and (2.2) give us

$$\begin{aligned}
|\det(\tau - \sigma_0)|_{p_0} &= |\det(\Sigma(A_0 - E_0)\Sigma^{-1}\sigma)|_{p_0} \\
&= |\det(\Sigma)|_{p_0} |\det(A_0 - E_0)|_{p_0} |\det(\Sigma^{-1})|_{p_0} |\det(\sigma)|_{p_0} \\
&\geq |2^n \cdot \det(A_0)|_{p_0} |\det(\sigma)|_{p_0} \\
&= |2^n \cdot \det(\sigma) \cdot \det(\sigma_0) \cdot \det(\sigma^{-1})|_{p_0} \\
&= |2^n|_{p_0}.
\end{aligned}$$

Therefore, as $\|\sigma_0\|_{p_0} = 1$,

$$\begin{aligned}
\|(\tau - \sigma_0)^{-1}\|_{p_0} &\leq \frac{1}{|\det(\tau - \sigma_0)|_{p_0}} \|\tau - \sigma_0\|_{p_0}^{n-1} \\
&\leq \frac{h_{p_0}(\tau)^{n-1}}{|2^n|_{p_0}}.
\end{aligned}$$

This proves that $\tau_{p_0} = \sigma_0$ satisfies the lemma.

Next we consider the case for $p \in \mathrm{Equiv}(A, B)$ with $p > p_0$. Then, plainly, $p > 2$. By [2, Page 115] or [8, §92], F is equivalent to a diagonal quadratic form over $\mathbb{Z}_p$. Thus,

there exists a $\Sigma_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that $F_p := \Sigma_p' F \Sigma_p$ is diagonal. Let σ_p be any matrix in $\mathrm{GL}_n(\mathbb{Z}_p)$ which satisfies

$$\sigma_p' F \sigma_p = G.$$

By applying Lemma 2.4 to $A_p := \Sigma_p^{-1} \tau \sigma_p^{-1} \Sigma_p$, we get that there exists an $E_p \in \mathcal{E}$ such that

$$|\det(A_p - E_p)|_p \geq |2^n \cdot \det(A_p)|_p = |\det(A_p)|_p.$$

Let $\tau_p := \Sigma_p E_p \Sigma_p^{-1} \sigma_p$. Clearly, $\tau_p \in \mathrm{GL}_n(\mathbb{Z}_p)$. Since $E_p' F_p E_p = F_p$, we have $\tau_p' F \tau_p = G$. Notice that

$$\begin{aligned} |\det(\tau - \tau_p)|_p &= |\det(\Sigma_p (A_p - E_p) \Sigma_p^{-1} \sigma_p)|_p \\ &= |\det \Sigma_p|_p \, |\det(A_p - E_p)|_p \, |\det(\Sigma_p^{-1})|_p \, |\det(\sigma_p)|_p \\ &\geq |\det(A_p)|_p \\ &= |\det(\tau) \cdot \det(\sigma_p^{-1})|_p \\ &= |\det(\sigma)|_p. \end{aligned}$$

Hence we have

$$\begin{aligned} \|(\tau - \tau_p)^{-1}\|_p &\leq \frac{1}{|\det(\tau - \tau_p)|_p} \|(\tau - \tau_p)\|_p^{n-1} \\ &\leq \frac{h_p(\tau)^{n-1}}{|\det \sigma|_p}. \end{aligned}$$

This implies that our choice of τ_p satisfies the lemma. □

Let Q be an n-ary regular quadratic form over a field K of characteristic $\neq 2$. Let O_Q be the orthogonal group of Q and Skew_n be the set of $n \times n$ skew-symmetric matrices, both viewed as algebraic groups over K. Let L be an extension of K. If $U \in \mathrm{Skew}_n(L)$ such that $\det(U + Q) \neq 0$, then

$$\mu := (U + Q)^{-1}(U - Q) \tag{2.3}$$

is an element in $\mathrm{O}_Q(L)$ with $\det(I_n - \mu) \neq 0$. The map $U \longmapsto \mu$ is called the *Cayley Transformation* (or *Cayley-Dickson Parametrization*), which is a birational K-isomorphism from Skew_n to O_Q. For any μ in $\mathrm{O}_Q(L)$ with $\det(I_n - \mu) \neq 0$, the inverse of this Cayley Transformation is defined and given by $\mu \longmapsto U = 2Q(I_n - \mu)^{-1} - Q$. This U is in $\mathrm{Skew}_n(L)$ such that $\det(U + Q) \neq 0$ and (2.3) holds. The readers may consult [10, Lemma 16] and [9, Proposition 7.4] for more on these properties.

3. Main theorem

Let F and G be two n-ary regular quadratic forms over $\mathbb{Q}$ which are equivalent over $\mathbb{Q}$. Let Σ and σ be the rational matrices, as constructed in Section 2, which have the properties that

$$\Sigma' F \Sigma \text{ is diagonal} \qquad \text{and} \qquad \sigma' F \sigma = G. \tag{3.1}$$

Let P be a finite set of primes. For each $p \in P$, let

$$\kappa_p := \max\{h_p(\Sigma E \Sigma^{-1}\sigma) : E \in \mathcal{E}\},$$

where $\mathcal{E}$ is the group of diagonal matrices with diagonal entries 1 or -1,

$$\alpha_p := \max\left\{\|F\|_p \, \kappa_p^n \, \max\left\{\frac{1}{|2^n|_p}, \frac{1}{|\det\sigma|_p}\right\}, 1\right\},$$

$$\beta_p := \frac{|2^n \det(F)\det(\sigma)|_p}{\kappa_p^n},$$

and

$$\varepsilon := \min_{p\in P}\left\{\frac{\beta_p}{\kappa_p \alpha_p^n}\right\}. \tag{3.2}$$

We define two positive constants, depending only on n, σ, Σ, F, and P, by

$$d = \prod_{p\in P} \alpha_p, \qquad C = \prod_{p\in P} p^{\lceil \log_p(\frac{d}{\varepsilon})\rceil + 1}. \tag{3.3}$$

Recall that $\mathbb{Z}^P$ is the ring $\bigcap_{p\in P}(\mathbb{Z}_p \cap \mathbb{Q})$.

Theorem 3.1. *Let P be a finite set of primes. Let F and G be n-ary regular quadratic forms over $\mathbb{Q}$. Suppose that F and G are equivalent over $\mathbb{Q}$ and over $\mathbb{Z}_p$ for each $p \in P$. Let $\sigma, \Sigma \in \mathrm{GL}_n(\mathbb{Q})$ be as in (3.1), and $d, C > 0$ be given by (3.3). Then there exists a matrix*

$$\hat{\tau} \in \left\{(U+F)^{-1}(U-F)\Sigma E \Sigma^{-1}\sigma : E \in \mathcal{E}, U \in \frac{1}{d}\cdot Skew_n(\mathbb{Z}), \|U\| \le \frac{C}{d}\right\}$$

such that

$$\hat{\tau} \in \mathrm{GL}_n(\mathbb{Z}^P), \qquad \hat{\tau}' F \hat{\tau} = G.$$

Proof. Let $\tau \in \mathrm{GL}_n(\mathbb{Q})$ and $\tau_p \in \mathrm{GL}_n(\mathbb{Z}_p)$, $p \in P$, be matrices satisfying Lemma 2.5. We have $\tau = \Sigma E \Sigma^{-1} \sigma$ for some $E \in \mathcal{E}$ and

$$\tau' F \tau = G, \qquad \tau_p' F \tau_p = G, \qquad \tau - \tau_p \in \mathrm{GL}_n(\mathbb{Q}_p) \tag{3.4}$$

and

$$\|(\tau - \tau_p)^{-1}\|_p \leq \kappa_p^{n-1} \max\left\{\frac{1}{|2^n|_p}, \frac{1}{|\det \sigma|_p}\right\}. \tag{3.5}$$

A straightforward computation shows that $\tau_p \tau^{-1}$ is in $\mathrm{O}_F(\mathbb{Q}_p)$. Moreover, by (3.4), $\det(I_n - \tau_p \tau^{-1}) \neq 0$. Therefore, we may apply the inverse of the Cayley Transformation to $\tau_p \tau^{-1}$ and write

$$\tau_p = (U_p + F)^{-1}(U_p - F)\tau, \tag{3.6}$$

where $U_p = 2F(I_n - \tau_p \tau^{-1})^{-1} - F \in \mathrm{Skew}_n(\mathbb{Q}_p)$.

The next step is to find a $U \in \mathrm{Skew}_n(\mathbb{Q})$ such that

$$U \in \frac{1}{d} \cdot \mathrm{Skew}_n(\mathbb{Z}), \qquad \|U\| \leq \frac{C}{d}, \qquad \det(U + F) \neq 0, \tag{3.7}$$

and that the matrix

$$\hat{\tau} := (U + F)^{-1}(U - F)\tau \in \mathrm{GL}_n(\mathbb{Q}) \tag{3.8}$$

satisfies

$$\|\hat{\tau} - \tau_p\|_p \leq 1. \tag{3.9}$$

This implies that $\hat{\tau} \in \mathrm{GL}_n(\mathbb{Z}_p)$ for all $p \in P$; hence $\hat{\tau} \in \mathrm{GL}_n(\mathbb{Z}^P)$. Moreover, since $\hat{\tau}\tau^{-1} \in \mathrm{O}_F(\mathbb{Q})$ because it is the image of U under the Cayley Transformation. Thus, $\hat{\tau}' F \hat{\tau} = G$ and this will finish the proof of the theorem.

To obtain (3.7), we will apply Lemma 2.2 to $X = U_p + F$ and $Y = U + F$, and Lemma 2.3 to U_p, ε and d. First of all, we obtain from (3.6) that

$$U_p + F = F(\tau + \tau_p)(\tau - \tau_p)^{-1} + F = F((\tau + \tau_p)(\tau - \tau_p)^{-1} + I_n). \tag{3.10}$$

Since $\tau_p \in \mathrm{GL}_n(\mathbb{Z}_p)$, we have $\|\tau_p\|_p = 1$. Then, by applying (3.5) to (3.10), we get that

$$\begin{aligned} \|U_p + F\|_p &\leq \|F\|_p \max\left\{\|\tau + \tau_p\|_p \|(\tau - \tau_p)^{-1}\|_p, 1\right\} \\ &\leq \|F\|_p \, h_p(\tau) \, \kappa_p^{n-1} \max\left\{\frac{1}{|2^n|_p}, \frac{1}{|\det \sigma|_p}\right\} \\ &\leq \alpha_p, \end{aligned}$$

and hence $h_p(U_p + F) \le \alpha_p$ because $1 \le \alpha_p$. Note that for the second inequality above, we have used

$$h_p(\tau)\,\kappa_p^{n-1}\,\max\left\{\frac{1}{|2^n|_p}, \frac{1}{|\det\sigma|_p}\right\} \ge 1 \cdot 1 \cdot \frac{1}{|2^n|_p} \ge 1.$$

This also implies that $\alpha_p \ge \|F\|_p$. Consequently,

$$\|U_p\|_p \le \max\{\|U_p + F\|_p, \|F\|_p\} \le \alpha_p. \tag{3.11}$$

Since $|\det(\tau - \tau_p)|_p \le h_p(\tau)^n \le \kappa_p^n$, we have

$$\begin{aligned} |\det(U_p + F)|_p &= \left|2^n \det(F)\frac{\det(\tau)}{\det(\tau - \tau_p)}\right|_p \\ &\ge \frac{|2^n \det(F)\det(\sigma)|_p}{\kappa_p^n} = \beta_p. \end{aligned}$$

As a result,

$$\frac{\beta_p}{\kappa_p\alpha_p^n} \le \frac{\beta_p}{\alpha_p^n} \le \frac{|\det(U_p + F)|_p}{h_p(U_p + F)^n} \le 1. \tag{3.12}$$

Let ε be as defined in (3.2), which is ≤ 1 by (3.12). It follows from (3.11) that $dU_p \in \mathrm{Skew}_n(\mathbb{Z}_p)$ for all $p \in P$. We may then apply Lemma 2.3 entry-wise and obtain a $U \in \frac{1}{d}\mathrm{Skew}_n(\mathbb{Z})$ such that

$$\|U\| \le \frac{C}{d} \qquad \text{and} \qquad \|U - U_p\|_p < \frac{\beta_p}{\kappa_p\alpha_p^n}, \qquad \forall\, p \in P. \tag{3.13}$$

Then, by (3.12),

$$\|U - U_p\|_p < \frac{\beta_p}{\kappa_p\alpha_p^n} \le \frac{\beta_p}{\alpha_p^n} \le \frac{|\det(U_p + F)|_p}{h_p(U_p + F)^n}.$$

Thus, by Lemma 2.2, $|\det(U+F)|_p = |\det(U_p+F)|_p \ge \beta_p$, implying that $\det(U+F) \ne 0$. Together with (3.13), we obtain (3.7).

Now we come to the proof of (3.9). It follows from (3.6) and (3.8) that

$$\hat{\tau} - \tau_p = (U + F)^{-1}(U - U_p)(\tau - \tau_p).$$

Then,

$$\begin{aligned} \|\hat{\tau} - \tau_p\|_p &\le \|(U + F)^{-1}\|_p \|\tau - \tau_p\|_p \|U - U_p\|_p \\ &\le \frac{\|U + F\|_p^{n-1}}{|\det(U + F)|_p}\, h_p(\tau)\, \|U - U_p\|_p. \end{aligned}$$

Since $\|U_p+F\|_p \le \alpha_p$ and $\|U-U_p\|_p < \frac{\beta_p}{\alpha_p^n} \le 1 \le \alpha_p$, we have $\|U+F\|_p \le \alpha_p$. Therefore,

$$\begin{aligned}\|\hat{\tau}-\tau_p\|_p &\le \frac{\alpha_p^{n-1}}{\beta_p}\,\kappa_p\,\|U-U_p\|_p \\ &\le \frac{\alpha_p^{n-1}}{\beta_p}\,\kappa_p\,\frac{\beta_p}{\kappa_p\alpha^n} \\ &= \alpha_p^{-1} \\ &\le 1.\end{aligned}$$

This finishes the proof of the theorem. □

We conclude by offering a few remarks on the size of the constants C and d in Theorem 3.1. These two constants depend on the input data Σ, σ, and F, and it may not be feasible to get precise estimates on their magnitudes. However, their definitions become a lot more manageable under some special but yet reasonable circumstances such as when F and G are primitive integral quadratic forms in the same genus. This is what we will be considering in the following discussion.

Since F is a primitive integral quadratic form, $\|F\|_p = 1$ for all primes p. Also, because F and G are in the same genus, we have $\det(F) = \det(G)$ and hence $|\det(\sigma)| = 1$. For each $p \in P$ and every $E \in \mathcal{E}$, $h_p(\Sigma E\Sigma^{-1}\sigma)^n \ge |\det(\Sigma E\Sigma^{-1}\sigma)|_p = 1$ by Lemma 2.1(3). This means that $\kappa_p \ge 1$. It is unlikely that $\kappa_p = 1$ for all $p \in P$, since this would require that $\|\Sigma E\Sigma^{-1}\sigma\|_p \le 1$ for all $p \in P$ and for all $E \in \mathcal{E}$.

By definitions, we have

$$\alpha_p = |2^{-n}|_p\kappa_p^n \quad \text{and} \quad \beta_p = \frac{|\det(F)|_p}{|2^{-n}|_p\kappa_p^n}.$$

As a result,

$$\epsilon \le \frac{\beta_p}{\kappa_p\alpha_p^n} = \frac{|\det(F)|_p}{|2^{-(n^2+n)}|_p\kappa_p^{n^2+n+1}}.$$

This implies that the bound $\frac{C}{d}$ on $\|U\|$ in Theorem 3.1 is at least

$$\prod_{p\in P}|2^n|_p\kappa_p^{-n}\cdot\prod_{p\in P}\left(\frac{d}{\epsilon}\right)p \ge \prod_{p\in P}p\cdot\prod_{p\in P}|2^{-n^2-|P|n}|_p\kappa_p^{n^2+|P|n+1}\cdot\prod_{p\in P}|\det(F)|_p^{-1},$$

which is already very large for relatively small n as long as $2 \in P$ or $\kappa_p > 1$ for some $p \in P$. Indeed, in a lot of applications, P will contain all the prime divisors of $2\det(F)$ and $\frac{C}{d}$ would be at least

$$2^{n^2+|P|n}\cdot|\det(F)|\cdot\prod_{p\in P}p\cdot\prod_{p\in P}\kappa_p^{n^2+|P|n+1}.$$

Acknowledgment

The authors thank Markus Kirschmer for his comments and suggestions. Haochen Gao would like to thank the support from Wesleyan Summer Research Program during the summers of 2019 and 2020 when part of this project was carried out. Han Li acknowledges support by the NSF Grant DMS 1700109.

References

[1] J.W. Benham, J.S. Hsia, Spinor equivalence of quadratic forms, J. Number Theory 17 (3) (1983) 337–342.
[2] J.W.S. Cassels, Rational Quadratic Forms, London Mathematical Society Monographs, vol. 13, Academic Press Inc., [Harcourt Brace Jovanovich, Publishers], London, 1978.
[3] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 290, Springer-Verlag, New York, 1999.
[4] R. Dietmann, Polynomial bounds for equivalence of quadratic forms with cube-free determinant, Math. Proc. Camb. Philos. Soc. 143 (3) (2007) 521–532.
[5] H. Li, G.A. Margulis, Effective estimates on integral quadratic forms: Masser's conjecture, generators of orthogonal groups, and bounds in reduction theory, Geom. Funct. Anal. 26 (3) (2016) 874–908.
[6] D.W. Masser, How to solve a quadratic equation in rationals, Bull. Lond. Math. Soc. 30 (1) (1998) 24–28.
[7] D.W. Masser, Search bounds for Diophantine equations, in: Panorama of Number Theory or the View from Baker's Garden, Zurich, 1999, pp. 247–259.
[8] O.T. O'Meara, Introduction to Quadratic Forms, Springer Verlag, New York, 1963.
[9] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston MA, 1994.
[10] C.L. Siegel, Equivalence of quadratic forms, Am. J. Math. 63 (1941) 658–680.
[11] C.L. Siegel, Zur Theorie der quadratischen Formen, Nachr. Akad. Wiss. Gött. Math.-Phys. Kl. 2 (1972) 21–46.
[12] S. Straumann, Das Äquivalenzproblem ganzer quadratischer Formen: Einige explizite Resultate, Diplomarbeit, Universität Basel, 1999.