ADDENDUM AND ERRATUM TO AN ABSOLUTE SIEGEL'S LEMMA

Damien Roy and Jeffrey Lin Thunder

Introduction

In a previous paper [4], we proved a version of Siegel's lemma over the algebraic closure $\overline{k}$ of a global field k. The purpose of this note is to refine the constants in the main results of that paper. Since these constants are optimal when k is a function field, we shall suppose here that $k = \mathbb{Q}$. The tool that we need for this purpose is a more suitable definition of twisted heights for the graded parts of the symmetric algebra $S(\overline{\mathbb{Q}}^n)$ of $\overline{\mathbb{Q}}^n$ than that used in [4]. Section 1 below states precisely the definition of these heights and establishes some of their properties. It also corrects a mistake that invalidates parts of some auxiliary results in §§3–4 of [4]. Refinements for the constants are proved in §2 below. In particular, with the notations of [4], we prove:

Theorem 1. *For any subspace V of $\overline{\mathbb{Q}}^n$ of dimension $m > 0$ and any constant $c > e^{m(m-1)/4}$, there is a basis $\{\mathbf{x}_1, \dots, \mathbf{x}_m\}$ of V with*

$$H(\mathbf{x}_1) \cdots H(\mathbf{x}_m) \le cH(V).$$

1. Heights

Let n be a positive integer, let L be a field which is complete with respect to a discrete or archimedean absolute value $|\ |$, and let $\mathbf{e}_1, \dots, \mathbf{e}_n$ be the canonical basis of L^n. In §3 of [4], we defined a norm $\|\ \|$ on L^n to be the ℓ_∞-norm when L is ultrametric and the ℓ_2-norm when L is archimedean. For each integer $r \ge 1$, we also defined a norm on the r-th symmetric power $S^r(L^n)$ of L^n and on the space $L[X_1, \dots, X_n]_r$ of homogeneous polynomials of degree r of $L[X_1, \dots, X_n]$. We required that these norms be such that the L-algebra isomorphism from $L[X_1, \dots, X_n]$ to $S(L^n)$ which sends X_i to $\mathbf{e}_i$ for $i = 1, \dots, n$ be an isometry in each degree. We also wanted, as stated in Lemma 3.2 (ii) of [4], that, for each norm preserving linear map $\phi\colon L^n \to L^n$, the induced linear maps $S^r(\phi)\colon S^r(L^n) \to S^r(L^n)$ preserve the norm. Equivalently, this condition can be written as $\|P \circ {}^t\phi\| = \|P\|$ for any $P \in L[X_1, \dots, X_n]_r$ and any such map ϕ.

First author partially supported by NSERC and CICMA
Second author partially supported by NSA grant MD A904-95-1-1087

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

In [4] the norm that we chose on $L[X_1,\dots,X_n]_r$ is the ℓ_2-norm when L is archimedean and the ℓ_∞-norm otherwise. Unfortunately, this choice satisfies the required conditions only for an ultrametric field L. So when L is archimedean part of Lemma 3.2 (ii) of [4] is wrong. This in turn invalidates Corollaries 4.3 (ii) and 4.4 (ii) as well as Proposition 4.6 and the remark at the end of §5 in [4], but only in the case where $k=\mathbb{Q}$. Note that these results have no bearing on the main theorems; the other results as well as their proofs do not need any modification.

When L is archimedean we restore the validity of Lemma 3.2 (ii) of [4] by replacing these norms on $S^r(L^n)$ and $L[X_1,\dots,X_n]_r$ by

$$\|\alpha\|^* = \left(\sum_{\mathbf{t}} \binom{r}{\mathbf{t}}^{-1} |a_{\mathbf{t}}|^2\right)^{1/2} \quad \text{and} \quad \|P\|^* = \left(\sum_{\mathbf{t}} \binom{r}{\mathbf{t}}^{-1} |p_{\mathbf{t}}|^2\right)^{1/2}$$

for $\alpha = \sum a_{\mathbf{t}} \mathbf{e}_1^{t_1}\cdots\mathbf{e}_n^{t_n}$ in $S^r(L^n)$ and $P=\sum p_{\mathbf{t}} X_1^{t_1}\cdots X_n^{t_n}$ in $L[X_1,\dots,X_n]_r$. In the above formulas, the symbol $\mathbf{t}$ stands for the n-tuple $(t_1,\dots,t_n)$, where $t_i\ge 0$ for each i and $t_1+\cdots+t_n=r$, and $\binom{r}{\mathbf{t}}$ denotes the multinomial coefficient $r!/(t_1!\cdots t_n!)$. The proof of Lemma 3.2 of [4] shows that these, in fact, are norms which satisfy the conditions stated above. The same observation also follows from Proposition 2 of [2]. Note that $\|P\|^*$ is simply the ℓ_2-norm of the symmetric multilinear polynomial attached to P. We use here the symbol $\|\ \|^*$ in order to avoid confusion with the norm $\|\ \|$ used in [4]. In the case where L is ultrametric we set $\|\ \|^*=\|\ \|$. Note also that, in either case, the norms $\|\ \|^*$ and $\|\ \|$ coincide on $L^n=S^1(L^n)$ and on $L[X_1,\dots,X_n]_1$.

Lemma 1. *Assume that L is archimedean and put $\gamma=\exp\left(\sum_{i=1}^{n-1} i^{-1}\right)$. Then for any homogeneous linear forms $P_1,\dots,P_r\in L[X_1,\dots,X_n]_1$ the product $P=P_1\cdots P_r\in L[X_1,\dots,X_n]_r$ satisfies*

$$\gamma^{-r/2}\|P_1\|\cdots\|P_r\| \le \|P\|^* \le n^{r/2}\|P_1\|\cdots\|P_r\|.$$

Similarly, for any $\mathbf{x}_1,\dots,\mathbf{x}_r\in L^n$, the product $\alpha=\mathbf{x}_1\cdots\mathbf{x}_r\in S^r(L^n)$ satisfies

$$\gamma^{-r/2}\|\mathbf{x}_1\|\cdots\|\mathbf{x}_r\| \le \|\alpha\|^* \le n^{r/2}\|\mathbf{x}_1\|\cdots\|\mathbf{x}_r\|.$$

Proof. Because of the choice of norms, it suffices to prove the first assertion of the lemma. We may also assume $L=\mathbb{C}$. Following C. Jadot in his thesis [1], we define the *measure* of a homogeneous polynomial $Q\in\mathbb{C}[X_1,\dots,X_n]$ by

$$M(Q)=\gamma^{(\deg Q)/2}\exp\Big(\int_S \log|Q(\mathbf{z})|d\sigma\Big),$$

where S denotes the unit sphere of $\mathbb{C}^n$ and $d\sigma$ is the Lebesgue measure on S normalized so that $\int_S d\sigma=1$. By virtue of Proposition 5 of [2] or Proposition 4 of [3], we have $M(Q)=\|Q\|$ for any linear form $Q\in\mathbb{C}[X_1,\dots,X_n]_1$. This gives

$$\|P_1\|\cdots\|P_r\| = M(P_1)\cdots M(P_r) = M(P_1\cdots P_r) = M(P).$$

The conclusion follows from Proposition 2.4 of [1]. Note that, since $\|P\|^* \leq \|P\|$, the upper bound for $\|P\|^*$ also follows from Lemma 3.4 (iii) of [4]. The lower bound $\|P\|^* \geq \gamma^{-r/2} M(P)$ is proved in [1] by observing that for each $\mathbf{z} \in S$, one has $|P(\mathbf{z})| \leq \|P\|^*$.

Let $K \subset \overline{\mathbb{Q}}$ be a number field and let r be a positive integer. As in [4], we denote by $M(K)$ the set of all places of K, and by $K_{\mathbb{A}}$ the adele ring of K. For each $v \in M(K)$, we write K_v for the completion of K at v and we normalize the absolute value $|\ |_v$ on K_v so that it extends the usual absolute value on $\mathbb{Q}_p$ if $v|p$, or the usual absolute value on $\mathbb{R}$ if $v|\infty$. Accordingly, we get for each $v \in M(K)$ a norm $\|\ \|_v$ on K_v^n and a norm $\|\ \|_v^*$ on $S^r(K_v^n)$.

Let $A = (A_v)_{v \in M(K)}$ be an element of $\mathrm{GL}_n(K_{\mathbb{A}})$. We associate to it a twisted height on $S^r(K^n)$ by defining $H_A^*(\alpha)$ for $\alpha \in S^r(K^n)$ by

$$H_A^*(\alpha) = \prod_{v \in M(K)} \big(\|S^r(A_v)(\alpha)\|_v^*\big)^{n_v/[K:\mathbb{Q}]},$$

where n_v denotes the local degree of K at $v \in M(K)$. If $E \subset \overline{\mathbb{Q}}$ is an extension of K of finite degree, and if we view A as an element of $\mathrm{GL}_n(E_{\mathbb{A}})$ in the standard way, then the corresponding height function H_A^* on $S^r(E^n)$ extends the above one on $S^r(K^n)$. Whence, we get a height H_A^* on $S^r(\overline{\mathbb{Q}}^n)$. For $r = 1$ the norms $\|\ \|_v^*$ and $\|\ \|_v$ coincide for all $v \in M(K)$. Therefore, the height H_A^* on $\overline{\mathbb{Q}}^n$ coincides with the height denoted H_A in [4].

By virtue of Lemma 1 (for the archimedean places) and Lemma 3.4 of [4] (for the non archimedean ones), this height satisfies:

Lemma 2. *Let γ be as in Lemma 1. Let K be a number field and let $A \in \mathrm{GL}_n(K_{\mathbb{A}})$. Then for any $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \overline{\mathbb{Q}}^n$ the product $\alpha = \mathbf{x}_1 \cdots \mathbf{x}_r \in S^r(\overline{\mathbb{Q}}^n)$ satisfies*

$$\gamma^{-r/2} H_A(\mathbf{x}_1) \cdots H_A(\mathbf{x}_r) \leq H_A^*(\alpha) \leq n^{r/2} H_A(\mathbf{x}_1) \cdots H_A(\mathbf{x}_r).$$

2. Refinement of the constants

The next proposition which we shall prove below shows that Proposition 6.2 (ii) of [4] holds for $n = 2$ with the constant $2^{\delta(n-1)/2}$ replaced by $e^{\delta(n-1)/4}$.

Proposition. *Let $K \subset \overline{\mathbb{Q}}$ be a number field and let $A \in \mathrm{GL}_2(K_{\mathbb{A}})$. Then for any $\epsilon > 0$ there exists a basis $\{\mathbf{y}_1, \mathbf{y}_2\}$ of $(\overline{\mathbb{Q}})^2$ such that*

$$H_A(\mathbf{y}_1) H_A(\mathbf{y}_2) \leq \big(e^{1/2} + \epsilon\big) |\det A|_{\mathbb{A}},$$

where by definition $|\det A|_{\mathbb{A}} = \prod_{v \in M(K)} |\det A_v|_v^{n_v/[K:\mathbb{Q}]}$.

Following the arguments in §§5–8 of [4], we deduce, for example, that Theorems 6.3 and 7.1 of that paper hold in general with the term $2^{\delta n(n-1)}$ replaced by $e^{\delta n(n-1)/2}$ and that Theorems 2.2 and 8.1 hold with $2^{\delta m(m-1)}$ replaced by $e^{\delta m(m-1)/2}$. In particular, we get the theorem stated in the introduction and also

Theorem 2. *Let n be an integer ≥ 2, let $K \subset \overline{\mathbb{Q}}$ be a number field and let $A \in \mathrm{GL}_n(K_{\mathbb{A}})$. For $i = 1, \dots, n$, define the i-th absolute minimum $\mu_i(A)$ of A as the infimum of the set of all real numbers $\mu > 0$ for which there exist i linearly independent elements $\mathbf{x}_1, \dots, \mathbf{x}_i$ of $\overline{\mathbb{Q}}^n$ with $H_A(\mathbf{x}_j) < \mu$ for $j = 1, \dots, i$. Then*

$$|\det A|_{\mathbb{A}} \leq \prod_{i=1}^{n} \mu_i(A) \leq e^{n(n-1)/4} |\det A|_{\mathbb{A}}.$$

Proof of the Proposition. Let r be an arbitrary large positive integer. We first construct a K-linear map $\theta\colon S^r(K^2) \to K^{r+1}$ and an element B of $\mathrm{GL}_{r+1}(K_{\mathbb{A}})$ such that $H_B(\theta(\alpha)) = H^*_A(\alpha)$ for any $\alpha \in S^r(K^2)$. To define θ, we simply require

$$\theta\big(\mathbf{e}_1^i \mathbf{e}_2^{r-i}\big) = \mathbf{e}_{i+1} \quad \text{for } i = 0, \dots, r.$$

For each place v of K let $\theta_v\colon S^r(K_v^2) \to K_v^{r+1}$ be the K_v-linear map which extends θ. For an archimedean place v define also a K_v-linear map $\omega_v\colon K_v^{r+1} \to K_v^{r+1}$ by the condition

$$\omega_v(\mathbf{e}_{i+1}) = \binom{r}{i}^{-1/2} \mathbf{e}_{i+1} \quad \text{for } i = 0, \dots, r.$$

For the other places of K, define ω_v to be the identity map of K_v^{r+1}. By construction, these maps satisfy $\|(\omega_v \circ \theta_v)(\beta)\|_v = \|\beta\|_v^*$ for each $v \in M(K)$ and each $\beta \in S^r(K_v^2)$. Let $B = (B_v)_{v \in M(K)}$ be the element of $\mathrm{GL}_{r+1}(K_{\mathbb{A}})$ given by

$$B_v = \omega_v \circ \theta_v \circ (S^r A_v) \circ \theta_v^{-1}$$

for each $v \in M(K)$. For any $\alpha \in S^r(K^2)$ and any $v \in M(K)$, we get

$$\|B_v(\theta(\alpha))\|_v = \|(\omega_v \circ \theta_v \circ S^r A_v)(\alpha)\|_v = \|(S^r A_v)(\alpha)\|_v^*.$$

This implies $H_B(\theta(\alpha)) = H^*_A(\alpha)$, as required.

By Lemma 5.2 of [4] there is a basis $\{\mathbf{y}_1, \dots, \mathbf{y}_{r+1}\}$ of K^{r+1} such that

$$H_B(\mathbf{y}_1) \cdots H_B(\mathbf{y}_{r+1}) \leq (r+1)^{(r+1)/2} C(K)^{r+1} |\det B|_{\mathbb{A}}$$

where $C(K)$ is a constant depending only on K. For each $i = 1, \dots, r+1$, put $\alpha_i = \theta^{-1}(\mathbf{y}_i)$. Then $\{\alpha_1, \dots, \alpha_{r+1}\}$ is a basis of $S^r(K^2)$ with $H_B(\mathbf{y}_i) = H^*_A(\alpha_i)$ for all i. On the other hand, as in the proof of Proposition 5.3 of [4], each α_i factors in $S^r(\overline{\mathbb{Q}}^2)$ as a product $\alpha_i = \mathbf{x}_{i1} \cdots \mathbf{x}_{ir}$ of r elements of $\overline{\mathbb{Q}}^2$. Lemma 2 applied to this decomposition (with n=2 and thus $\gamma = e$) gives

$$H_A(\mathbf{x}_{i1}) \cdots H_A(\mathbf{x}_{ir}) \leq e^{r/2} H^*_A(\alpha_i) = e^{r/2} H_B(\mathbf{y}_i).$$

Moreover, using Lemma 4.5 of [4], we find

$$|\det B|_{\mathbb{A}} = \left(\prod_{i=0}^{r} \binom{r}{i}^{-1/2} \right) |\det A|_{\mathbb{A}}^{r(r+1)/2}.$$

Finally, the asymptotic estimates of M. Laurent in Proposition 3 of [2] show that, for large values of r, one has

$$\prod_{i=0}^{r} \binom{r}{i} \geq (r+1)^{-(r+1)} e^{r(r+1)/2}.$$

All together this gives, for large r,

$$\prod_{i=1}^{r+1} \prod_{j=1}^{r} H_A(\mathbf{x}_{ij}) \leq \left(e^{1/2} (r+1)^{2/r} C(K)^{2/r} |\det A|_{\mathbb{A}} \right)^{r(r+1)/2}.$$

Arguing as in the proof of Proposition 5.3 of [4], we deduce that from the points $\mathbf{x}_{ij}$ we can extract a basis $\{\mathbf{y}_1, \mathbf{y}_2\}$ of $\overline{\mathbb{Q}}^2$ with

$$H_A(\mathbf{y}_1) H_A(\mathbf{y}_2) \leq e^{1/2} (r+1)^{2/r} C(K)^{2/r} |\det A|_{\mathbb{A}}.$$

For sufficiently large values of r, this basis has the required property.

References

1. C. Jadot, *Critères pour l'indépendance algébrique et linéaire*, Thèse de Doctorat de l'Université Paris 6, 1996.
2. M. Laurent, *Hauteur de matrices d'interpolation*, in: Approximations diophantiennes et nombres transcendants, Luminy 1990, P. Philippon ed., W. de Gruyter, Berlin (1992), 215–238.
3. P. Philippon, *Sur les hauteurs alternatives. I*, Math. Ann. **289** (1991), 255–283.
4. D. Roy and J. Thunder, *An absolute Siegel's Lemma*, J. reine angew. Math. **476** (1996), 1–26.

Dépt. de Math., Univ. d'Ottawa, Ottawa, Ontario, Canada K1N 6N5
E-mail address: `droy@mathstat.uottawa.ca`

Dept. of Math., Northern Illinois Univ., DeKalb, IL 60115
E-mail address: `jthunder@math.niu.edu`