Canad. J. Math. Vol. **64** (2), 2012 pp. 301–317
http://dx.doi.org/10.4153/CJM-2011-046-6

Hermite's Constant for Function Fields

Chris Hurlburt and Jeffrey Lin Thunder

Abstract. We formulate an analog of Hermite's constant for function fields over a finite field and state a conjectural value for this analog. We prove our conjecture in many cases, and prove slightly weaker results in all other cases.

1 Introduction

The notion of Hermite's constant first arose in the study of quadratic forms. Later, when Minkowski introduced his geometry of numbers, he was able to greatly improve on Hermite's original bounds for this constant. Moreover, via the geometry of numbers, it turns out that Hermite's constant has many connections with diverse areas of mathematics and even other physical sciences. (See [2] for an excellent guide to these mathematical connections.) Now the geometry of numbers lends itself well to adelic formulations, meaning one can formulate the geometry of numbers over an arbitrary number field, function field, and even algebraic closures of such. It turns out that these generalizations and extensions of the geometry of numbers have important applications, too. For example, the adelic formulations of Minkowski's first and second theorems on successive minima for number fields (see [1]) and an algebraic closure (see [5]) are key ingredients of some important machinery in Diophantine approximation (see [3]). For an entirely different example, in [4] the authors used the methods of the geometry of numbers over certain function fields to construct non-linear codes with desirable attributes. The exact value of the original Hermite's constant is famously known only up to dimension eight.

In this paper we focus on an analog of Hermite's constant for function fields over a finite field. Specifically, we state a conjecture analogous to an exact determination of this constant in general, and prove our conjecture for a great many specific cases. We are also able to prove a general result (Theorem 4.4) that is just slightly weaker than our conjecture. In order to formulate this analog, we first need to introduce some notation and ideas from the adelic geometry of numbers; in particular, we need the notion of a *height* on projective space. We formally state our conjecture at the end of this introduction after the requisite definitions, notation, etc. In the following section we provide an explicit construction for the case of genus 1 (Theorem 2.6) which proves the conjecture in that case. (The case of genus 0 turns out to be relatively simple. See Corollary 2.2.) Section 3 recalls some measure theory developed by the second author in a previous paper [6], which is then used in the final section to again prove more quantitative results for genus 0 (Theorem 4.2), genus 1 (Theorem 4.3),

Received by the editors June 11, 2010.
Published electronically August 3, 2011.
AMS subject classification: **11G50**, 11G35.

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

and finally the general result (Theorem 4.4) mentioned above, which is somewhat weaker than the conjecture.

Let K be a finite algebraic extension of the field of rational functions $\mathbb{F}_q(X)$, where X is transcendental over the field with q elements $\mathbb{F}_q$. We assume that $\mathbb{F}_q$ is the field of constants for K. Let g and J denote the genus and the number of divisor classes of degree 0, respectively (J is also the cardinality of the Jacobian). Let ζ_K denote the zeta function of K which is analogous to the classical Riemann zeta function. We will write $M(K)$ for the set of places of K and $K_{\mathbb{A}}$ for the adele ring. For a place $v \in M(K)$ we let K_v denote the topological completion of K at v and let ord_v be the order function on K_v, normalized to have image $\mathbb{Z} \cup \{\infty\}$. We let $\mathfrak{O}_v$ denote the subring of K_v consisting of all elements $x \in K_v$ with $\operatorname{ord}_v(x) \geq 0$ (with the usual convention that $\infty > 0$). We extend ord_v to K_v^n by defining

$$\operatorname{ord}_v(x_1, \dots, x_n) = \min_{1 \leq i \leq n} \operatorname{ord}_v(x_i).$$

For any $\mathbf{x} = (\mathbf{x}_v) \in K_{\mathbb{A}}^n$ with $\operatorname{ord}_v(\mathbf{x}_v) \in \mathbb{Z}$ for all places v and with $\operatorname{ord}_v(\mathbf{x}_v) = 0$ for all but finitely many places, we get a divisor

$$\operatorname{div}(\mathbf{x}) := \sum_{v \in M(K)} \operatorname{ord}_v(\mathbf{x}_v) \cdot v.$$

Thus, for any non-zero $\mathbf{x} \in K^n$ and $A \in \operatorname{GL}_n(K_{\mathbb{A}})$ we have a divisor $\operatorname{div}(A\mathbf{x})$ and the additive height

$$h_A(\mathbf{x}) = -\deg \operatorname{div}(A\mathbf{x}).$$

Since the degree of a principal divisor is 0, one sees that these heights are actually functions on projective $(n-1)$-space $\mathbb{P}^{n-1}(K)$. These heights are extended to arbitrary subspaces of K^n via Grassmann coordinates. Specifically, suppose $1 \leq d \leq n$ and $S \subseteq K^n$ is a d-dimensional subspace with basis $\mathbf{x}_1, \dots, \mathbf{x}_d$. Then $\mathbf{X} = \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d \in K^{\binom{n}{d}}$ and we define

$$h_A(S) = h_{\bigwedge^d A}(\mathbf{X}) = -\deg \operatorname{div}(A\mathbf{x}_1 \wedge \cdots \wedge A\mathbf{x}_d).$$

Note that $h_A(K^n) = -\deg \operatorname{div} \det(A)$. The case where $A = I_n$, the identity element of $\operatorname{GL}_n(K_{\mathbb{A}})$, gives the usual “untwisted” height.

For $A \in \operatorname{GL}_n(K_{\mathbb{A}})$ the successive minima $\lambda_1(A) \leq \cdots \leq \lambda_n(A)$ are

$$\lambda_i(A) := \min\{m : K^n \text{ contains } i \text{ linearly independent } \mathbf{x} \text{ with } h_A(\mathbf{x}) \leq m\}$$

for $1 \leq i \leq n$. An analog of Hermite’s constant here would be the maximum of $\lambda_1(A)$ over some set of $A \in \operatorname{GL}_n(K_{\mathbb{A}})$. Unlike the case of the rational numbers or any other number field, we cannot simply normalize via a scalar multiple to look at A with fixed determinant since a scalar multiple will change the height of K^n here by some multiple of n. For this reason, we will dispense with a specific “Hermite’s constant” and instead work with the relationship between the first minima $\lambda_1(A)$ and the height $h_A(K^n)$ directly.

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

We will use capital script german letters to denote divisors: $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., and simply use 0 to denote the zero divisor. We say a divisor $\mathfrak{A}$ is non-negative, and write $\mathfrak{A} \geq 0$, if $\operatorname{ord}_v(\mathfrak{A})$ is non-negative for all places $v \in M(K)$. Such a divisor is called *effective*. More generally, we write $\mathfrak{A} \geq \mathfrak{B}$ if $\mathfrak{A} - \mathfrak{B} \geq 0$.

For a divisor $\mathfrak{A}$ and an $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, consider the following sets.

$$\Lambda(\mathfrak{A}, A) := \{\mathbf{x} = (\mathbf{x}_v) \in K_{\mathbb{A}}^n : \operatorname{ord}_v(A_v\mathbf{x}_v) \geq -\operatorname{ord}_v(\mathfrak{A}) \text{ for all } v \in M(K)\},$$
$$L(\mathfrak{A}, A) = K^n \cap \Lambda(\mathfrak{A}, A),$$
$$L'(\mathfrak{A}, A) = \{\mathbf{x} \in L(\mathfrak{A}, A) : \operatorname{ord}_v(A_v\mathbf{x}) = -\operatorname{ord}_v(\mathfrak{A}) \text{ for all } v \in M(K)\}.$$

We collect a few obvious yet useful observations here.

Note 1 (i) If $a \in K_{\mathbb{A}}^{\times}$, then for all divisors $\mathfrak{A}$ and all $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ we have

$$\Lambda(\mathfrak{A} + \operatorname{div}(a), A) = \Lambda(\mathfrak{A}, aA) = a^{-1}\Lambda(\mathfrak{A}, A).$$

(ii) For non-zero $\mathbf{x} \in K^n$, $\mathbf{x} \in L(\mathfrak{A}, A)$ if and only if $\mathfrak{A} \geq -\operatorname{div}\big(A(\mathbf{x})\big)$ and $\mathbf{x} \in L'(\mathfrak{A}, A)$ if and only if $\mathbf{x} \in L(\mathfrak{A} + \mathfrak{C}, A)$ for all $\mathfrak{C} \geq 0$.
(iii) We have $h_A(\mathbf{x}) = m$ if and only if $\mathbf{x} \in L'(\mathfrak{A}, A)$ for some divisor $\mathfrak{A}$ with $\deg(\mathfrak{A}) = m$. In particular, $h_A(\mathbf{x}) \leq \deg(\mathfrak{A})$ if $\mathbf{x} \in L(\mathfrak{A}, A)$.
(iv) Suppose $\mathbf{x} \in L'(\mathfrak{A}, A)$. Then $a\mathbf{x} \in L'(\mathfrak{A}, A)$ for $a \in K$ if and only if $a \in \mathbb{F}_q^{\times}$.

It is known that $L(\mathfrak{A}, A)$ is a vector space over $\mathbb{F}_q$ of finite dimension (see [8], for example); we denote its dimension by $l(\mathfrak{A}, A)$. In general, we have ([7, Theorem 3])

$$(1.1) \qquad l(\mathfrak{A}, A) = n(\deg(\mathfrak{A}) + 1 - g) + \deg\operatorname{div}\det(A) + \dim_{\mathbb{F}_q}\left(\frac{K_{\mathbb{A}}^n}{\Lambda(\mathfrak{A}, A) + K^n}\right),$$

and in the case $n = 1$ we have the Riemann–Roch Theorem

$$(1.2) \qquad l(\mathfrak{A}, A) = \deg(\mathfrak{A}) + 1 - g + \deg\operatorname{div}\det(A) + l(\mathfrak{W} - \mathfrak{A}, A^{-1}),$$

where $\mathfrak{W}$ is an element of the canonical class.

Using this, we get an important result in the geometry of numbers.

Theorem 1.1 (Minkowski's First Theorem for Function Fields) *Suppose $n \geq 2$ and let $A \in \mathrm{GL}_n(K_{\mathbb{A}})$. If $h_A(K^n) < n(1 - g)$, then $\lambda_1(A) \leq 0$. In particular, for all $A \in \mathrm{GL}_n(K_{\mathbb{A}})$*

$$\lambda_1(A) \leq g + \left[\frac{h_A(K^n)}{n}\right],$$

where $[\,\cdot\,]$ denotes the greatest integer function.

Indeed, if $-\deg\operatorname{div}\det(A) = h_A(K^n) < n(1 - g)$, then $l(0, A) > 0$. Take any non-zero $\mathbf{x} \in L(0, A)$. Then $h_A(\mathbf{x}) \leq \deg(0) = 0$ by Note 1(iii). More generally, if $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, set

$$m := g + [h_A(K^n)/n] > g + \frac{h_A(K^n)}{n} - 1$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

and let $a \in K_{\mathbb{A}}^{\times}$ with $\deg \operatorname{div}(a) = 1$. Then by the definitions,

$$h_{a^m A}(K^n) = h_A(K^n) - nm < h_A(K^n) - n\Big(g + \frac{h_A(K^n)}{n} - 1\Big) = n(1-g),$$

and by what we have already shown, $\lambda_1(A) = \lambda_1(a^m A) + m \leq m$.

One can view this as an analog to the classical Minkowski's first theorem in the case of ellipsoids, where the sharpest upper bound involves Hermite's constant. The question here is whether or not the statement above is sharp; we believe that it is.

Conjecture *For all integers $n \geq 2$ and all integers m, there is an $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ with $-\deg \operatorname{div} \det(A) = m$ and $\lambda_1(A) = g + [m/n]$.*

2 The Case of Genus 1: An Explicit Construction

We first remark that in order to prove the conjecture, it suffices via Note 1(i)–(iv) above to consider only those m for which $0 \leq m < n$. In fact, we even have the following.

Proposition 2.1 *Suppose $n \geq 2$. If there is a prime divisor of degree 1, then the conjecture holds for all m if and only if it holds for $m = 0$.*

Proof Suppose there is an $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ with $\deg \operatorname{div} \det(A) = 0$ and $\lambda_1(A) = g$. Fix m and write $m = ns + t$, where $s = [m/n]$ and $0 \leq t < n$. Let $a \in K_{\mathbb{A}}^{\times}$ be such that $-\operatorname{div}(a)$ is a prime divisor of degree 1. Let $B' = a^s A$ and let B be obtained from B' by multiplying the first t rows by a. Then $\deg \operatorname{div} \det(B) = m \deg \operatorname{div}(a) = -m$ and $\lambda_1(B') = \lambda_1(A) - \deg \operatorname{div}(a^s) = s = [m/n]$. We claim that $\lambda_1(B) \geq \lambda_1(B')$. Indeed, let $\mathbf{x} \in K^n \setminus \{\mathbf{0}\}$ and set $\mathbf{y} = B(\mathbf{x})$. Then $B'(\mathbf{x}) = \mathbf{y}'$, where $\mathbf{y}' = (y_1', \dots, y_n')$ is given by

$$y_i' = \begin{cases} a^{-1} y_i & \text{if } i \leq t, \\ y_i & \text{otherwise.} \end{cases}$$

Since $\operatorname{div}(a^{-1}) \geq 0$, we clearly have $\operatorname{ord}_v(\mathbf{y}') \geq \operatorname{ord}_v(\mathbf{y})$ for all places v, so that $h_B(\mathbf{x}) \geq h_{B'}(\mathbf{x})$ for all non-zero $\mathbf{x} \in K^n$. ■

Corollary 2.2 *The conjecture is true in the case of genus 0.*

Proof The identity matrix $I_n \in \mathrm{GL}_n(K_{\mathbb{A}})$ clearly satisfies $\deg \operatorname{div} \det(I_n) = 0$ and $\lambda_1(I_n) = 0$ for all $n \geq 2$. Moreover, there are $q + 1$ prime divisors of degree 1 when $g = 0$. ■

We will now show that the conjecture is true when the genus is 1 by an explicit construction. We first remark that in the case of genus 1 there are exactly J places, *i.e.*, prime divisors, of degree 1. Denote these places of degree 1 by $v_1, \dots, v_J$. For a non-zero $x \in K$, write $\operatorname{div}(x) = (x)_0 - (x)_\infty$, where $(x)_0$ and $(x)_\infty$ are effective divisors. The following is well known; we include a proof for completeness.

Lemma 2.3 *Suppose $g = 1$ and $x \in K \setminus \mathbb{F}_q$. Then $\deg \operatorname{div}(x)_0 = \deg \operatorname{div}(x)_\infty \geq 2$.*

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Proof Indeed, let $\mathfrak{A}$ be an effective divisor of degree 1. By the Riemann–Roch Theorem (1.2), the union of the set of $y \in K$ with $\operatorname{div}(y) \geq -\mathfrak{A}$ together with the element 0 is a one-dimensional vector space over $\mathbb{F}_q$. Since non zero $y \in \mathbb{F}_q$ have $\operatorname{div}(y) = 0 \geq -\mathfrak{A}$, we see that this collection consists exactly of $\mathbb{F}_q$. ■

Our first goal is construction of a particular element of $\mathrm{GL}_2(K_{\mathbb{A}})$. Let $b \in K_{\mathbb{A}}^{\times}$ with $b_v = 1$ for all $v \neq v_1$ and $b_{v_1} = \pi_1^{-1}$, where $\pi_1 \in K_{v_1}$ with $\operatorname{ord}_{v_1}(\pi_1) = 1$. Set

$$A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

We concern ourselves with elements of the form $(x, 1) \in K^2$. Now $A(x, 1) = (x + \ b, 1)$, so that $\operatorname{ord}_v(A_v(x, 1)) \leq 0$ for all places v. Moreover, $\operatorname{ord}_v(A_v(x, 1)) = \operatorname{ord}_v(x)$ for all places $v \neq v_1$ in the support of $(x)_\infty$, and $\operatorname{ord}_{v_1}(A(x, 1)) \leq -1$ if $\operatorname{ord}_{v_1}(x) \neq -1$. Thus, $h_A(x, 1) \geq 2$ except for $x \in \mathbb{F}_q$ and possibly for x satisfying $(x)_\infty = v_1 + v_i$ for some $i = 2, \ldots, J$. Via the Riemann–Roch Theorem, for each $i = 2, \ldots, J$ the set of $x \in K$ with $(x)_\infty = v_1 + v_i$ consists of all elements in some 2-dimensional vector space over $\mathbb{F}_q$ which are not in the 1-dimensional subspace $\mathbb{F}_q$. There are $q(q - 1)$ elements in such a set, and clearly at most q of them can satisfy $\operatorname{ord}_{v_1}(x + b_{v_1}) \geq 0$. In summary: $h_A(x, 1) > 0$ for all $x \in K$, there are at most Jq elements $x \in K$ with $h_A(x, 1) = 1$, and this last set includes the q elements of $\mathbb{F}_q$. In particular, there are no more than $(J - 1)q$ elements $x \in K \setminus \mathbb{F}_q$ with $h_A(x, 1) = 1$. Moreover, these possible $(J - 1)q$ elements x have $(x)_\infty = v_1 + v_i$ for some $i = 2, \ldots, J$.

Again by the Riemann–Roch Theorem, there are $J(q + 1)$ effective divisors of degree 2, exactly J of which contain v_1 in their support. This leaves Jq effective divisors of degree 2 that do not contain v_1 in their support, at least q of which are *not* equal to $(x)_0$ for any $x \in K$ with $h_A(x, 1) = 1$. Choose such a divisor $\mathfrak{A}$ and let $a \in K_{\mathbb{A}}^{\times}$ with $\operatorname{div}(a) = -\mathfrak{A}$ and $a_{v_1} = 1$. Set

$$A' = \begin{pmatrix} a & ab \\ 0 & 1 \end{pmatrix}.$$

We claim that $\lambda_1(A') = 2$. As in the proof of Proposition 2.1, $h_{A'}(\mathbf{x}) \geq h_A(\mathbf{x})$ for all non-zero $\mathbf{x} \in K^2$ since $\operatorname{div}(a) \leq 0$. It remains to show that $h_{A'}(\mathbf{x}) \geq 2$ for all $\mathbf{x}$ with $h_A(\mathbf{x}) \leq 1$. Clearly $h_{A'}(1, 0) = -\deg \operatorname{div}(a) = \deg(\mathfrak{A}) = 2$. Also, since $\mathfrak{A} \not\geq v_1$, we have $\operatorname{div}(a(y + b), 1) \leq \operatorname{div}(a)$ for all $y \in \mathbb{F}_q$. Finally, consider a possible $y \in K \setminus \mathbb{F}_q$ with $h_A(y, 1) = 1$ and write $(y)_\infty = v_1 + v_i$, where (as we showed above) $v_i \neq v_1$ is some place of degree 1. If the support of $\mathfrak{A}$ is not contained in the support of $(y)_0$, say v is in the support of $\mathfrak{A}$ and not in the support of $(y)_0$, then $\operatorname{div}\big(a(y + b), 1\big) \leq -v - v_i$. This gives $h_A(y, 1) \geq \deg(v) + \deg(v_i) = 2$. If the support of $\mathfrak{A}$ is entirely contained in the support of $(y)_0$, then since $\mathfrak{A} \neq (y)_0$ by construction, we must have $\mathfrak{A} = 2v$ and $(y)_0 = v + v'$ for some places $v, v' \neq v_1$ of degree 1. In this case we again have $\operatorname{div}\big(a(y + b), 1\big) \leq -v - v'$ and $h_A(y, 1) \geq 2$. This shows that $\lambda_1(A') = 2$.

We stop to summarize what we are able to say so far.

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Proposition 2.4 *Using the notation above, let* $c = b^{-1}$ *and*

$$A_2 = cA = \begin{pmatrix} ca & cab \\ 0 & c \end{pmatrix}.$$

Then $\deg \operatorname{div} \det(A_2) = 0$ *and* $\lambda_1(A_2) = \lambda_1(A') - \deg \operatorname{div}(c) = 1$.

We next turn to the case $n = 3$ and construct a particular element of $\mathrm{GL}_3(K_{\mathbb{A}})$. Use the notation above and set

$$B = \begin{pmatrix} c & b \\ 0 & 1 \end{pmatrix}.$$

We claim that there is at most one $y \in K$ with $h_B(y, 1) < 1$. Let $y \in K$. If $v \neq v_1$, then

$$\operatorname{ord}_v(yc_v + b_v, 1) = \operatorname{ord}_v(y + 1, 1) \leq \operatorname{ord}_v(1) = 0,$$

with equality if and only if $\operatorname{ord}(y) \geq 0$. Also,

$$\operatorname{ord}_{v_1}(yc_{v_1} + b_{v_1}, 1) = \operatorname{ord}_{v_1}(y\pi_1 + \pi_1^{-1}, 1) \leq \operatorname{ord}_{v_1}(1) = 0,$$

with equality only if $\operatorname{ord}_{v_1}(y) = -2$. Therefore, $\operatorname{div}(yc + b, 1) \leq 0$, with equality only if the pole divisor $(y)_\infty = 2v_1$. In other words, $h_B(y, 1) \geq 1$ if $(y)_\infty \neq 2v_1$. Suppose there is a $y \in K$ with pole divisor $(y)_\infty = 2v_1$. Then any $y' \in K$ with $(y')_\infty = 2v_1$ is of the form $y' = xy$ for some $x \in \mathbb{F}_q^\times$. But clearly at most one of these y' can possibly satisfy $\operatorname{ord}_{v_1}(y'\pi_1 + \pi_1^{-1}) = 0$, proving our claim.

If there is a $y' \in K$ such that $h_B(y', 1) \leq 0$, set

$$A_3 = \begin{pmatrix} ca & cab & cab(1 - y') \\ 0 & c & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Otherwise set

$$A_3 = \begin{pmatrix} ca & cab & cab \\ 0 & c & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Then in either case $\deg \operatorname{div} \det(A_3) = \deg \operatorname{div} \det(A_2) = 0$. We claim that $\lambda_1(A_3) = 1$.

First, we have $h_{A_3}(x, y, 0) = h_{A_2}(x, y) \geq 1$ for all $(x, y, 0) \in K^3 \setminus \{\mathbf{0}\}$. Suppose there is a $y' \in K$ above with $h_B(y', 1) \leq 0$. Let $(x, y, 1) \in K^3$ with $y \neq y'$. We have

$$\operatorname{div}(cax + caby + cab(1 - y'), yc + b, 1) \leq \operatorname{div}(yc + b, 1),$$

so that

$$\begin{aligned} h_{A_3}(x, y, 1) &= -\deg \operatorname{div}(cax + caby + cab(1 - y'), yc + b, 1) \\ &\geq -\deg \operatorname{div}(yc + b, 1) = h_B(y, 1) \geq 1. \end{aligned}$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Also, for any $(x, y', 1) \in K^3$ we have $\operatorname{div}(cax + cab, yc + b, 1) \le \operatorname{div}(cax + cab, 1)$ and

$$\begin{aligned} h_{A_3}(x, y', 1) &= -\deg \operatorname{div}(cax + cab, y'c + b, 1) \\ &\ge -\deg \operatorname{div}(cax + cab, 1) = h_{A_2}(x, 1) \ge 1. \end{aligned}$$

Finally, if there is no $y' \in K$ with $h_B(y', 1) \le 0$, then for all $(x, y, 1) \in K^3$ we have $\operatorname{div}(cax + caby + cab, yc + b, 1) \le \operatorname{div}(yc + b, 1)$, so that

$$\begin{aligned} h_{A_3}(x, y, 1) &= -\deg \operatorname{div}(cax + caby + cab, yc + b, 1) \\ &\ge -\deg \operatorname{div}(yc + b, 1) = h_B(y, 1) \ge 1. \end{aligned}$$

Since the height is projective, this shows the following.

Proposition 2.5 *Using the notation above,* $\deg \operatorname{div} \det(A_3) = 0$ *and* $\lambda_1(A_3) = 1$.

The three propositions above will suffice to prove our conjecture in the case of genus 1.

Theorem 2.6 *Suppose* $g = 1$. *Then for all integers* $n \ge 2$ *and all integers* m *there is an* $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ *with* $-\deg \operatorname{div} \det(A) = m$ *and* $\lambda_1(A) = 1 + [m/n]$.

Proof By Proposition 2.1 it suffices to prove the case where $m = 0$. Propositions 2.4 and 2.5 thus take care of dimensions 2 and 3, so suppose $n > 3$. Write $n = 2s + 3t$ for non-negative integers s and t. Let A_2 and A_3 be as above and set

$$A_n = \begin{pmatrix} A_2 & 0 & \dots & 0 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & A_2 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & A_3 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & \dots & 0 & A_3 \end{pmatrix},$$

where A_2 is repeated s times and A_3 is repeated t times. Then

$$\deg \operatorname{div} \det(A_n) = s \deg \operatorname{div} \det(A_2) + t \deg \operatorname{div} \det(A_3) = 0.$$

Suppose $\mathbf{x} \in K^n$ and write $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_s, \mathbf{y}_1, \dots, \mathbf{y}_t)$, where $\mathbf{x}_i \in K^2$ and $\mathbf{y}_j \in K^3$ for all $i = 1, \dots, s$ and $j = 1, \dots, t$. If $\mathbf{x} \ne \mathbf{0}$, then some $\mathbf{x}_i$ or $\mathbf{y}_j$ is non-zero. By construction $h_{A_n}(\mathbf{x}) \ge h_{A_2}(\mathbf{x}_i) \ge 1$ in the former case, and $h_{A_n}(\mathbf{x}) \ge h_{A_3}(\mathbf{y}_j) \ge 1$ in the latter. This shows that $\lambda_1(A_n) \ge 1$, completing the proof. ■

3 Some Measure Theory

In this section we fix representatives $\mathfrak{A}_1, \dots, \mathfrak{A}_J$ of the divisor classes of degree 0 and let $a_1, \dots, a_J$ be ideles with $\operatorname{div}(a_i) = \mathfrak{A}_i$ for each i.

For each place v, let α_v be the Haar measure on K_v obtained by setting $\alpha_v(\mathfrak{O}_v) = 1$. We then get the measure α on $K_{\mathbb{A}}$ given by

$$\alpha = q^{1-g} \prod_{v \in M(K)} \alpha_v.$$

We will write α^n for the resulting product measure on $K_{\mathbb{A}}^n$.

We define $G_n = \{A \in \mathrm{GL}_n(K_{\mathbb{A}}) : \deg \operatorname{div} \det(A) = 0\}$ and for notational convenience, set $\Gamma_n = \mathrm{GL}_n(K)$. Note that Γ_n is a discrete subgroup of G_n. One can construct a Haar measure on G_n (see [6]); since G_n/Γ_n is compact, $\mu_n(G_n/\Gamma_n)$ is finite. We let μ_n denote this measure, normalized so that $\mu_n(G_n/\Gamma_n) = 1$.

Let H_n be the subset of G_n consisting of those A with $[\operatorname{div} \det(A)] = [0]$, where we use brackets to denote the corresponding element of the divisor class group. Clearly $H_n \subset G_n$ is a subgroup of index J. We have $\mu_n = \tau_n \times \beta$, where τ_n is a measure on H_n and β is the counting measure on the group of divisor classes of degree 0. Then

$$J\tau_n\big(H_n/\Gamma_n\big) = \mu_n(G_n/\Gamma_n) = 1. \tag{3.1}$$

Let g_n be the subgroup of G_n defined by

$$g_n = \left\{ \begin{pmatrix} a & \mathbf{b} \\ \mathbf{0} & A \end{pmatrix} \in G_n : a \in G_1,\ \mathbf{b} \in (K_{\mathbb{A}})^{n-1},\ A \in G_{n-1} \right\}$$

and let $\gamma_n = g_n \cap \Gamma_n$. Let $g_n' \subset g_n$ consist of those matrices above with $a = 1$, and let $\gamma_n' = \gamma_n \cap g_n'$. Similarly to above, we get a measure σ_n on g_n with

$$\sigma_n(g_n/\gamma_n) = \mu_1(G_1/\Gamma_1)\mu_{n-1}(G_{n-1}/\Gamma_{n-1})\alpha^{n-1}((K_{\mathbb{A}})^{n-1}/K^{n-1})$$

and a measure σ_n' on g_n' with

$$\sigma_n'(g_n'/\gamma_n') = \mu_{n-1}(G_{n-1}/\Gamma_{n-1})\alpha^{n-1}((K_{\mathbb{A}})^{n-1}/K^{n-1}).$$

We have

$$\sigma_n'(g_n'/\gamma_n') = \sigma_n(g_n/\gamma_n), \tag{3.2}$$

since $\mu_1(G_1/\Gamma_1) = 1$.

Let

$$h_n = \left\{ \begin{pmatrix} a & \mathbf{b} \\ \mathbf{0} & A \end{pmatrix} \in G_n : a \in H_1,\ \mathbf{b} \in (K_{\mathbb{A}})^{n-1},\ A \in H_{n-1} \right\}$$

and let $h_n' \subset h_n$ be those matrices above with $a = 1$. We see that $h_n \subset g_n$ is a subgroup of index J^2. Exactly as above, we have $\sigma_n = \upsilon_n \times \beta \times \beta$, where υ_n is a measure on h_n. We have

$$\upsilon_n(h_n/\gamma_n) = 1/J^2. \tag{3.3}$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Set $(K_{\mathbb{A}}^n)^\times$ to be the set of $\mathbf{x} \in K_{\mathbb{A}}^n$ with $\mathbf{x}_v \neq \mathbf{0}$ for all v and $\operatorname{ord}_v(\mathbf{x}_v) = 0$ for almost all $v \in M(K)$; we have $(K_{\mathbb{A}}^n)^\times \cong G_n/g_n' \cong H_n/h_n'$. Let $d\nu_n$ be the relatively invariant gauge form on the homogeneous space G_n/g_n which satisfies $d\mu_n = d\nu_n d\sigma_n$. In other words, for f an integrable function on G_n,

$$\int_{G_n} f(A)\, d\mu_n(A) = \int_{G_n/g_n} d\nu_n(Ag_n) \int_{g_n} f(Aa)\, d\sigma_n(a).$$

Similarly, let ρ_n be the gauge form on H_n/h_n which satisfies $d\tau_n = d\rho_n\, d\upsilon_n$.

For any $\mathbf{x} \in (K_{\mathbb{A}}^n)^\times$ and $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ we have a unique divisor $\operatorname{div}(A(\mathbf{x}))$. Scalar multiplication of $\mathbf{x}$ by an element of G_1 clearly changes this divisor by a divisor of degree 0. Thus, for all $Bg_n \in G_n/g_n$ we get a unique element $[\operatorname{div}(A(Bg_n))]$ of the divisor class group, whence a well-defined function $\deg[\operatorname{div}(A(Bg_n))]$ on G_n/g_n. Similarly, for any $Bh_n \in H_n/h_n$ we get a unique $[\operatorname{div}(A(Bh_n))]$, so that $\deg[\operatorname{div}(A(Bh_n))]$ on H_n/h_n is well defined. Let $\kappa_n(A)$ be the measure (via $d\nu_n$) of the set of $Bg_n \in G_n/g_n$ with $\deg[\operatorname{div}(A(Bg_n))] = 0$ and let $\kappa_n'(A)$ be the measure (via $d\rho_n$) of the set of $Bh_n \in H_n/h_n$ with $\deg[\operatorname{div}(A(Bh_n))] = 0$.

Let $d\nu_n'$ be the gauge form on G_n/g_n' that satisfies $d\mu_n = d\nu_n' d\sigma_n'$. Since $g_n/g_n' = G_1$, we have $d\sigma_n = d\mu_1 d\sigma_n'$. Thus, $d\nu_n' = d\nu_n d\mu_1$. Let $\pi_v \in \mathfrak{O}_v$ generate the unique maximal ideal for each $v \in M(K)$ and set

$$S = \prod_{v\in M(K)} \mathfrak{O}_v \setminus \pi_v \mathfrak{O}_v, \qquad T = \bigcup_{i=1}^{J} a_i S.$$

Then T is a fundamental set of order $q-1$ modulo Γ_1 of G_1. Using $(K_{\mathbb{A}}^n)^\times \cong G_n/g_n'$, we have

$$(q-1)\kappa_n(A)\mu_1(G_1/\Gamma_1) = \int_{\mathbf{x}\in A^{-1}(T\mathfrak{O}^n)} d\nu_n'(\mathbf{x}). \tag{3.4}$$

In the same manner, since $H_n/h_n' \cong G_n/g_n'$, we get

$$(q-1)\kappa_n'(A)\tau_1(H_1/\Gamma_1) = \int_{\mathbf{x}\in A^{-1}(T\mathfrak{O}^n)} d\nu_n'(\mathbf{x}).$$

Thus,

$$J\kappa_n(A) = \kappa_n'(A). \tag{3.5}$$

As shown in [6], we have

$$\mu_n(G_n/\Gamma_n)\, d\alpha^n = \sigma_n'(g_n'/\gamma_n')\, d\nu_n'. \tag{3.6}$$

Also,

$$\int_{\mathbf{x}\in(K_{\mathbb{A}}^n)^\times\cap A^{-1}(T\mathfrak{O}^n)} d\alpha^n(\mathbf{x}) = q^{\deg\operatorname{div}\det(A)} \int_{\mathbf{x}\in(K_{\mathbb{A}}^n)^\times\cap T(\mathfrak{O}^n)} d\alpha^n(\mathbf{x}), \tag{3.7}$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

and since $\deg \operatorname{div}(a_i) = 0$ for all $i = 1, \dots, J$,

$$(3.8)\qquad \int_{\mathbf{x}\in (K^n_{\mathbb{A}})^\times \cap T(\mathfrak{O}^n)} d\alpha^n(\mathbf{x}) = \sum_{i=1}^{J} \int_{\mathbf{x}\in (K^n_{\mathbb{A}})^\times \cap a_i S(\mathfrak{O}^n)} d\alpha^n(\mathbf{x})$$
$$= J \int_{\mathbf{x}\in (K^n_{\mathbb{A}})^\times \cap S(\mathfrak{O}^n)} d\alpha^n(\mathbf{x})$$
$$= Jq^{n(1-g)} \prod_{v\in M(K)} (1 - q^{-n \deg \operatorname{div}(\pi_v)})$$
$$= \frac{Jq^{n(1-g)}}{\zeta_K(n)}.$$

Hence, by (3.1)–(3.8)

$$(3.9)\qquad \kappa_n(A)\sigma_n(g_n/\gamma_n) = \kappa_n(A)\frac{\sigma_n(g_n/\gamma_n)}{\mu_n(G_n/\Gamma_n)} = \kappa_n'(A)\frac{\upsilon_n(h_n/\gamma_n)}{\tau_n(H_n/\Gamma_n)}$$
$$= \frac{q^{n(1-g)}q^{\deg \operatorname{div} \det(A)} J}{(q-1)\zeta_K(n)}.$$

Now let f be the characteristic function of any interval $(-\infty, z]$. One readily verifies that

$$(3.10)\qquad \int_{G_n/g_n} f\big(-\deg[\operatorname{div}(A(Bg_n))]\big)\, d\nu_n(Bg_n) = \kappa_n(A) \sum_{l\in\mathbb{Z}} q^{ln} f(l),$$

$$(3.11)\qquad \int_{H_n/h_n} f\big(-\deg[\operatorname{div}(A(Bh_n))]\big)\, d\rho_n(Bh_n) = \kappa_n'(A) \sum_{l\in\mathbb{Z}} q^{ln} f(l).$$

As remarked in [6], we have

$$\sigma_n(g_n/\gamma_n) \int_{G_n/g_n} f(-\deg[\operatorname{div}(A(Bg_n))])\, d\nu_n(Bg_n)$$
$$= \int_{G_n/\Gamma_n} \Big[\sum_{B\gamma_n \in \Gamma_n/\gamma_n} f\big(-\deg[\operatorname{div} A(B\gamma_n))]\big) \Big]\, d\mu_n(B\Gamma_n).$$

Since $\Gamma_n/\gamma_n \cong \mathbb{P}^{n-1}(K)$, we also have

$$\sum_{B\gamma_n\in\Gamma_n/\gamma_n} f(-\deg[\operatorname{div} A(B\gamma_n)]) = \#\{\xi \in \mathbb{P}^{n-1}(K) : h_{AB}(\xi) \le z\},$$

so that

$$(3.12)\qquad \sigma_n(g_n/\gamma_n) \int_{G_n/g_n} f\big(-\deg\big[\operatorname{div}(A(Bg_n))\big]\big)\, d\nu_n(Bg_n)$$
$$= \int_{H_n/\Gamma_n} \#\{\xi \in \mathbb{P}^{n-1}(K) : h_{AB}(\xi) \le z\}\, d\mu_n(B\Gamma_n).$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Similarly

$$(3.13)\quad v_n(h_n/\gamma_n)\int_{H_n/h_n} f\big(-\deg[\mathrm{div}(A(Bh_n))]\big)\,d\rho_n(Bh_n) = \int_{H_n/\Gamma_n} \#\{\xi\in\mathbb{P}^{n-1}(K) : h_{AB}(\xi)\le z\}\,d\tau_n(B\Gamma_n).$$

Equations (3.9)–(3.13) give us the following.

Theorem 3.1 *For any $A\in\mathrm{GL}_n(K_{\mathbb{A}})$ and any $z\in\mathbb{Z}$ we have*

$$\frac{q^{n(1-g)}q^{\deg\operatorname{div}\det(A)}Jq^{nz}}{(1-q^{-n})(q-1)\zeta_K(n)} = \int_{G_n/\Gamma_n}\#\{\xi\in\mathbb{P}^{n-1}(K) : h_{AB}(\xi)\le z\}\,d\mu_n(B\Gamma_n),$$

$$\frac{q^{n(1-g)}q^{\deg\operatorname{div}\det(A)}q^{nz}}{(1-q^{-n})(q-1)\zeta_K(n)} = \int_{H_n/\Gamma_n}\#\{\xi\in\mathbb{P}^{n-1}(K) : h_{AB}(\xi)\le z\}\,d\tau_n(B\Gamma_n).$$

4 Applications of Theorem 3.1

We use Theorem 3.1 to get close to a complete answer to our conjecture. We also use it to give a rather definitive quantitative answer in many cases, including the case of genus 1. We first consider the quantity $(q-1)\zeta_K(n)$ occurring in Theorem 3.1, though.

Lemma 4.1 *Suppose $n>1$. If $g=0$, then*

$$(q-1)\zeta_K(n) = \left(\frac{q}{1-q^{1-n}} - \frac{1}{1-q^{-n}}\right) > \frac{1}{1-q^{-n}}.$$

If $g=1$, then

$$(q-1)\zeta_K(n) = J\Big(\frac{1}{q^{n-1}-1} - \frac{1}{q^n-1}\Big) + (q-1).$$

In all cases $\zeta_K(n)>1$.

Proof We have $\zeta_K(n)=\sum_{l=0}^{\infty} a_l q^{-ln}$, where a_l is the number of divisors $\mathfrak{A}\ge 0$ with $\deg(\mathfrak{A})=l$. For a fixed divisor $\mathfrak{A}$, the number of linearly equivalent divisors $\mathfrak{C}\ge 0$ is equal to $\frac{1}{q-1}(q^{l(\mathfrak{A},1)}-1)$. An application of the Riemann–Roch Theorem (1.2) gives

$$a_l \ge J\frac{q^{l+1-g}-1}{q-1},$$

with equality if $l\ge 2g-1$. We clearly have $a_0=1$. This gives $\zeta_K(n)>1$.

In the case $g=0$ we have $J=1$, so that

$$(q-1)\zeta_K(n) = \sum_{l=0}^{\infty}(q^{l+1}-1)q^{-ln} = \frac{q}{1-q^{1-n}} - \frac{1}{1-q^{-n}}.$$

In the case $g = 1$, we get

$$\begin{aligned}(q-1)\zeta_K(n) &= J\sum_{l=1}^{\infty}(q^l-1)q^{-ln} + (q-1)\\ &= J\Big(\frac{1}{q^{n-1}-1} - \frac{1}{q^n-1}\Big) + (q-1).\end{aligned}$$ ■

Theorem 4.2 *Suppose $g = 0$. Then the set $X \subset G_n/\Gamma_n$ of $B\Gamma_n \in G_n/\Gamma_n$ with $\lambda_1(B) = 0$ satisfies*

$$\mu_n(X) \geq 1 - \frac{1}{(1-q^{-n})(q-1)\zeta_K(n)} > 0.$$

Moreover, if $n = 2$, we have

$$\mu_2(X) = \frac{q-1}{q}.$$

Proof Let $Y \subset G_n/\Gamma_n$ be the subset of $B\Gamma_n$ with $\lambda_1(B) < 0$. By Theorem 3.1 and Lemma 4.1 we have

$$\begin{aligned}\mu_n(Y) &\leq \int_{G_n/\Gamma_n} \#\{\xi \in \mathbb{P}^{n-1}(K) : h_B(\xi) \leq -1\}\, d\mu_n(B\Gamma_n)\\ &= \frac{1}{(1-q^{-n})(q-1)\zeta_K(n)}\\ &< 1.\end{aligned}$$

By Minkowski's Theorem (1.1) and since $\mu_n(G_n/\Gamma_n) = 1$, we get $\mu_n(X) = 1 - \mu_n(Y)$.

We can say more when $n = 2$. In general we have ([7, Theorem 1])

$$\lambda_1(A) + \cdots + \lambda_n(A) + \deg\operatorname{div}\det(A) \geq 0$$

for all $A \in \mathrm{GL}_n(K_{\mathbb{A}})$. In particular, if $n = 2$ and $B \in G_2$, we have $\lambda_1(B) + \lambda_2(B) \geq 0$. This implies that all elements of $B\Gamma_2 \in Y$ have exactly one point $\xi \in \mathbb{P}^1(K)$ with $h_B(\xi) < 0$, because $\lambda_2(B) > 0$. Therefore, when $n = 2$, we have

$$\begin{aligned}\mu_2(Y) &= \int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^{n-1}(K) : h_B(\xi) \leq -1\}\, d\mu_2(B\Gamma_2)\\ &= \frac{1}{(1-q^{-2})(q-1)\zeta_K(2)}.\end{aligned}$$

Via Lemma 4.1, we have

$$\begin{aligned}(1-q^{-2})(q-1)\zeta_K(2) &= (1-q^{-2})\Big(\frac{q}{1-q^{-1}} - \frac{1}{1-q^{-2}}\Big)\\ &= \frac{q(1-q^{-2})}{1-q^{-1}} - 1 = \frac{q^2(1-q^{-2})}{q-1} - 1\\ &= q.\end{aligned}$$

Therefore, $\mu_2(Y) = 1/q$, so that $\mu_2(X) = (q-1)/q$. ■

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

Theorem 4.3 *Suppose $g = 1$. Then the set $X \subset G_2/\Gamma_2$ of of $B\Gamma_2$ with $\lambda_1(AB) = 1$ satisfies*

$$\mu_2(X) = 1 - \frac{(q^2+1)}{2q + 2J^{-1}(q^2-1)(q-1))} > 0.$$

Proof Write $G_2/\Gamma_2 = X \cup Y \cup Z$, where

$$Y := \{B\Gamma_2 \in G_2/\Gamma_2 : \lambda_1(B) = 0\}, \quad Z := \{B\Gamma_2 \in G_2/\Gamma_2 : \lambda_1(B) \le -1\}.$$

As above in the proof of Theorem 4.2, $\lambda_1(B) + \lambda_2(B) \ge 0$ for all $B \in G_2$. In particular,

$$\int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) \le -1\}\, d\mu_2(B\Gamma_2) = \mu_2(Z) \tag{4.1}$$

and

$$\begin{aligned} \int_{G_2/\Gamma_2} &\#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\}\, d\mu_2(B\Gamma_2) \\ &= \int_Y \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\}\, d\mu_2(B\Gamma_2). \end{aligned} \tag{4.2}$$

By Theorem 3.1 and equations (4.1) and (4.2),

$$\begin{aligned} \mu_2(Z) &= \int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) \le -1\}\, d\mu_2(B\Gamma_2) \\ &= \frac{Jq^{-2}}{(1-q^{-2})(q-1)\zeta_K(2)} \\ &= \frac{J}{(q^2-1)(q-1)\zeta_K(2)}. \end{aligned} \tag{4.3}$$

We now turn to Y. We will see that elements of Y have either $1, 2$, or $q+1$ points of height 0 and that, on average, the elements of Y have exactly 2 points of height 0. First, let $\mathfrak{A}_1, \dots, \mathfrak{A}_J$ be representatives of the divisor classes of degree 0 and choose ideles $a_1, \dots, a_J \in G_1$ with $\operatorname{div}(a_i) = \mathfrak{A}_i$ for all $i = 1, \dots, J$. Set

$$U_n := \{U \in H_n : \operatorname{ord}_v(U_v(\mathbf{x}_n)) = \operatorname{ord}_v(\mathbf{x}_v) \text{ for all } v \in M(K) \text{ and } \mathbf{x}_v \in K_v^n\}.$$

Clearly $\operatorname{div}(UA(\mathbf{x})) = \operatorname{div}(A(\mathbf{x}))$ for all $U \in U_n$, $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, and non-zero $\mathbf{x} \in K^n$.

For any i and j we have by Note 1(i) and (1.1) (and since $a_i \in K_{\mathbb{A}}^{\times}$)

$$\begin{aligned} \dim_{\mathbb{F}_q}\Big(\frac{K_{\mathbb{A}}}{a_iK + \Lambda(0, a_j^{-1})}\Big) &= \dim_{\mathbb{F}_q}\Big(\frac{K_{\mathbb{A}}}{K + a_i^{-1}\Lambda(0, a_j^{-1})}\Big) \\ &= \dim_{\mathbb{F}_q}\Big(\frac{K_{\mathbb{A}}}{K + \Lambda(\operatorname{div}(a_ia_j^{-1}), 1)}\Big) \\ &= l\big(\mathfrak{W} - \operatorname{div}(a_ia_j^{-1}), 1\big), \end{aligned}$$

where $\mathfrak{W}$ is any divisor in the canonical class. But since $g = 1$, we can take $\mathfrak{W} = 0$. Since $\operatorname{div}(a_i a_j^{-1}) = \mathfrak{A}_i - \mathfrak{A}_j$, we get

$$\dim_{\mathbb{F}_q}\Big(\frac{K_{\mathbb{A}}}{a_i K + \Lambda(0, a_j^{-1})}\Big) = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

For each i let $b_i + (a_i K + \Lambda(0, a_i^{-1}))$ be a basis element of $\frac{K_{\mathbb{A}}}{a_i K + \Lambda(0, a_i^{-1})}$.

Let $B \in Y$. Then for some $C_1 \in \Gamma_2$ and some $D_1 \in U_2$ we have $D_1 B C_1$ is upper triangular of the form

$$D_1 B C_1 = \begin{pmatrix} a_i & b \\ 0 & a_j \end{pmatrix}$$

for some i and j. If $i \neq j$, then we can write $-b = c + d$, where $c \in a_i K$ and $d \in \Lambda(0, a_j^{-1})$. Set $c = a_i c'$ and $d = a_j d'$, where $c' \in K$ and $d' \in \Lambda(0, 1)$. Then

$$C_2 = \begin{pmatrix} 1 & c' \\ 0 & 1 \end{pmatrix} \in \Gamma_2, \quad D_2 = \begin{pmatrix} 1 & d' \\ 0 & 1 \end{pmatrix} \in U_2$$

and

$$D_2 D_1 B C_1 C_2 = B_{i,j} := \begin{pmatrix} a_i & 0 \\ 0 & a_j \end{pmatrix}.$$

Similarly, if $i = j$, then for some $C_2 \in \Gamma_2$ and $D_2 \in U_2$ we have

$$D_2 D_1 B C_1 C_2 = B_{i,a} := \begin{pmatrix} a_i & a b_i \\ 0 & a_i \end{pmatrix}$$

for some $a \in \mathbb{F}_q$. In this manner we see that for each $B\Gamma_2 \in Y$ there are $C \in \Gamma_2$ and $D \in U_2$ with

$$DBC = \begin{cases} B_{i,j} & \text{for some } i \neq j, \text{ or} \\ B_{i,a} & \text{for some } i \text{ and } a \in \mathbb{F}_q. \end{cases}$$

Let Y_1 denote those in the first case, let Y_2 denote those in the second case with $a = 0$, and let Y_3 denote the remainder. Then Y is a disjoint union of Y_1, Y_2, and Y_3. Moreover, we clearly have

$$\mu_2(Y_3) = (q-1)\mu_2(Y_2). \tag{4.4}$$

Suppose $i \neq j$. Then clearly $\operatorname{div}(B_{i,j}(1,0)) = \operatorname{div}(a_i)$ and $\operatorname{div}(B_{i,j}(0,1)) = \operatorname{div}(a_j)$. This gives two linearly independent elements of K^2 with height 0. But if x is a non-zero element of K, then $\operatorname{div}(x, a_j a_i^{-1}) < \operatorname{div}(x)$ since $\operatorname{div}(a_j a_i^{-1}) = \mathfrak{A}_j - \mathfrak{A}_i$ is not a principal divisor. Hence

$$\begin{aligned} \operatorname{div}(B_{i,j}(x,1)) = \operatorname{div}(a_i x, a_j) &= \operatorname{div}(a_i) + \operatorname{div}(x, a_j a_i^{-1}) \\ &< \operatorname{div}(a_i) + \operatorname{div}(x) \end{aligned}$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

and $h_{B_{i,j}}(x,1) > 0$. Thus

$$\#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\} = 2, \quad \text{for all } B\Gamma_2 \in Y_1. \tag{4.5}$$

We have $\operatorname{div}(B_{i,0}(1,0)) = \operatorname{div}(B_{i,0}(0,1)) = \operatorname{div}(a_i)$ for all i. Also, for all $x \in K$,

$$\begin{aligned}\operatorname{div}\big(B_{i,0}(x,1)\big) &= \operatorname{div}(a_i x, a_i) = \operatorname{div}(a_i) + \operatorname{div}(x,1)\\ &\le \operatorname{div}(a_i),\end{aligned}$$

with equality if and only if $x \in \mathbb{F}_q$. Therefore

$$\#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\} = q+1, \quad \text{for all } B\Gamma_2 \in Y_2. \tag{4.6}$$

Next, for all i and all non-zero $a \in \mathbb{F}_q$ we have $\operatorname{div}(B_{i,a}(1,0)) = \operatorname{div}(a_i)$. For any $x \in K$ we have

$$\operatorname{div}(B_{i,a}(x,1)) = \operatorname{div}(a_i x + ab_i, a_i) < \operatorname{div}(a_i),$$

since by construction $a_i x + ab_i \notin \Lambda(0, a_i^{-1})$, *i.e.*, $\operatorname{div}(a_i x + ab_i) \ngeq \operatorname{div}(a_i)$. Thus

$$\#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\} = 1, \quad \text{for all } B\Gamma_2 \in Y_3. \tag{4.7}$$

By (4.4)–(4.7) we get

$$\begin{aligned}\int_Y \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\}\, d\mu_2(B\Gamma_2)&\\ &= 2\mu_2(Y_1) + (q+1)\mu_2(Y_2) + \mu_2(Y_3)\\ &= 2\mu_2(Y_1) + 2\mu_2(Y_2) + (q-1)\mu_2(Y_2) + \mu_2(Y_3)\\ &= 2\big(\mu_2(Y_1) + \mu_2(Y_2) + \mu_2(Y_3)\big)\\ &= 2\mu_2(Y).\end{aligned} \tag{4.8}$$

Now by (4.1)–(4.3), (4.8), and Theorem 3.1

$$\begin{aligned}2\mu_2(Y) &= \int_Y \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\}\, d\mu_2(B\Gamma_2)\\ &= \int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) = 0\}\, d\mu_2(B\Gamma_2)\\ &= \int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) \le 0\}\, d\mu_2(B\Gamma_2)\\ &\qquad - \int_{G_2/\Gamma_2} \#\{\xi \in \mathbb{P}^1(K) : h_B(\xi) \le -1\}\, d\mu_2(B\Gamma_2)\\ &= (q^2-1)\mu_2(Z).\end{aligned}$$

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press

This together with (4.3) once more yields

$$\begin{aligned}\mu_2(X) &= 1-\mu_2(Y)-\mu_2(Z) = 1-\frac{q^2-1}{2}\mu_2(Z)-\mu_2(Z)\\ &= 1-\frac{J(q^2+1)}{2(q^2-1)(q-1)\zeta_K(2)}.\end{aligned}$$

But by Lemma 4.2

$$\begin{aligned}(q^2-1)(q-1)\zeta_K(2) &= (q^2-1)J(\frac{1}{q-1}-\frac{1}{q^2-1})+(q^2-1)(q-1)\\ &= Jq+(q^2-1)(q-1),\end{aligned}$$

so that

$$\mu_2(X) = 1-\frac{q^2+1}{2q+2J^{-1}(q^2-1)(q-1))}.$$

Finally, one consequence of the "Riemann Hypothesis" is the Hasse–Weil bound for the number N of places of degree 1: $N \le q+1+2gq^{1/2}$. In our case where $g=1$, we have $N=J$, so that $J \le q+1+2q^{1/2} < 2(q+1)$. Using this, we see

$$\frac{q^2+1}{2q+2J^{-1}(q^2-1)(q-1)} < \frac{q^2+1}{2q+(q-1)^2} = 1,$$

so that

$$\mu_2(X) = 1-\frac{q^2+1}{2q+2J^{-1}(q^2-1)(q-1))} > 0.$$

■

Theorem 4.4 *Suppose $g>1$. Let n_K be the smallest integer satisfying*

$$(q^{n_K}-1)(q-1) \ge J.$$

Then for all $n > n_K$ and all $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ with $n_K \le -\deg\operatorname{div}\det(A) < n$, the set of $B\Gamma_n \in G_n/\Gamma_n$ with $\lambda_1(AB) = g$ has positive measure. Moreover, the set of $B\Gamma_n \in G_n/\Gamma_n$ with $\lambda_1(B) \ge g-1$ has positive measure.

Proof Let $n > n_K$ and suppose $n_K \le m < n$. Let $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ with

$$-\deg\operatorname{div}\det(A) = m.$$

Denote the set of $B\Gamma_n \in G_n/\Gamma_n$ with $\lambda_1(AB) < g$ by X. Then by Theorem 3.1 and Lemma 4.1

$$\begin{aligned}\mu_n(X) &\le \int_{G_n/\Gamma_n} \#\{\xi \in \mathbb{P}^{n-1}(K) : h_{AB}(\xi) \le g-1\}\, d\mu_n(B\Gamma_n)\\ &= \frac{Jq^{-m}}{(1-q^{-n})(q-1)\zeta_K(n)} < \frac{Jq^{-m}}{(1-q^{-n})(q-1)}\\ &< \frac{Jq^{-n_K}}{(1-q^{-n_K})(q-1)} = \frac{J}{(q^{n_K}-1)(q-1)}\\ &\le 1.\end{aligned}$$

Since $\mu_n(X) < 1$, its complement (namely, the set of $B\Gamma_n$ with $\lambda_1(AB) = g$) has positive measure.

Similarly, let Y denote the set of $B\Gamma_n$ with $\lambda_1(B) \leq g - 2$. Then

$$\begin{aligned}\mu_n(Y) &\leq \int_{G_n/\Gamma_n} \#\{\xi \in \mathbb{P}^{n-1}(K) : h_B(\xi) \leq g-2\}\, d\mu_n(B\Gamma_n)\\ &= \frac{Jq^{-n}}{(1-q^{-n})(q-1)\zeta_K(n)} < \frac{J}{(q^n-1)(q-1)}\\ &< \frac{J}{(q^{n_K}-1)(q-1)}\\ &\leq 1.\end{aligned}$$

Therefore the complement of Y has positive measure. ■

References

[1] E. Bombieri and J. Vaaler, *On Siegel's lemma.* Invent. Math. **73**(1983), no. 1, 11–32. http://dx.doi.org/10.1007/BF01393823

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Grundlehren der Mathematischen Wissenschaften 290. Springer-Verlag, New York, 1991.

[3] J.-H. Evertse and H. P. Schlikewei, *The absolute subspace theorem and linear equations with unknowns from a multiplicative group.* In: Number Theory in Progress. De Gruyter, Berlin, 1999, pp. 121–142.

[4] C. Hurlburt and J. L. Thunder, *Non-linear codes from points of bounded height.* Finite Fields Appl. **13**(2007), no. 2, 281–292. http://dx.doi.org/10.1016/j.ffa.2005.11.001

[5] D. Roy and J. L. Thunder, *An absolute Siegel's lemma.* J. Reine Angew. Math. **476**(1996), 1–26.

[6] J. L. Thunder, *An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma*. J. Reine Angew. Math. **475**(1996), 167–185. http://dx.doi.org/10.1515/crll.1996.475.167

[7] ———, *Siegel's lemma for function fields.* Michigan Math. J. **42**(1995), no. 1, 147–162. http://dx.doi.org/10.1307/mmj/1029005160

[8] A. Weil *Basic Number Theory*. Third edition. Die Grundlehren der Mathematischen Wissenschaften 144. Springer-Verlag, New York, 1974.

Center for Communications Research, 4320 Westerra Court, San Diego, CA, 92121 USA
e-mail: hurlburt@ccrwest.org

Dept. of Mathematics, Northern Illinois University, DeKalb, IL 60115 USA
e-mail: jthunder@math.niu.edu

https://doi.org/10.4153/CJM-2011-046-6 Published online by Cambridge University Press