Problems and results about the Weil height

1053, November 23, 2019

We recall that the Weil heights

$$H : \overline{\mathbb{Q}}^{\times} \to [1, \infty), \quad \text{and} \quad h : \overline{\mathbb{Q}}^{\times} \to [0, \infty),$$

are defined at an algebraic number $\alpha \neq 0$ as follows: let $k \subseteq \overline{\mathbb{Q}}$ be an algebraic number field containing $\alpha \neq 0$. Then the multiplicative Weil height of α is

$$H(\alpha) = \prod_{v} \max\{1, |\alpha|_v\},$$

and the logarithmic Weil height of α is

$$h(\alpha) = \sum_{v} \log^{+} |\alpha|_v.$$

The product and sum are over the set of all places v of k, but the value of the sum is independent of the choice of k. There are no issues of convergence because for each point $\alpha \neq 0$ in k we have $|\alpha|_v = 1$ at all but finitely many places v.

Results and open problems:

Theorem 1. (Northcott, 1949) *For* $1 \leq d$ *and* $1 \leq T$, *the set of algebraic numbers*

$$\{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \text{ and } h(\alpha) \leq T\}$$

is finite.

Here is a more precise version of Northcott's theorem.

Theorem 2. (D. Masser, V., 2003) *For* $1 \leq d$ *and* $1 \leq T$, *we have*

$$\left|\{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \text{ and } h(\alpha) \leq T\}\right|$$
$$= \frac{d\gamma(d)e^{d(d+1)T}}{2\zeta(d+1)} + O\Big(e^{d^2T}(\log 2T)\Big)$$

where

$$\gamma(d) = 2^{d+1}(d+1)^f \prod_{j=1}^{f} \frac{(2j)^{d-2j}}{(2j+1)^{d-2j+1}},$$

and $f = [(d-1)/2]$.

Theorem 3. (V., M. Widmer, 2011) *Let k be a number field of degree d and discriminant Δ_k. If k has a real embedding, then there exists α in k such that $k = \mathbb{Q}(\alpha)$, and*

$$H(\alpha) \leq |\Delta_k|^{1/2d}.$$

If k has no real embedding we have only the following conditional result.

Theorem 4. (V., M. Widmer, 2011) *For each $d \geq 2$ there exists an effectively computable constant $C = C(d)$ having the following property. Let k be a number field of degree d and discriminant Δ_k. Let $l \subseteq \overline{\mathbb{Q}}$ be the Galois closure of k and assume that the Dedekind zeta-function $\zeta_l(s)$ satisfies GRH. Then there exists α in k such that $k = \mathbb{Q}(\alpha)$, and*

$$H(\alpha) \leq C|\Delta_k|^{1/2d}.$$

Units: let k be an algebraic number field, O_k the ring of algebraic integers in k,

$$O_k^{\times} = \text{ multiplicative group of units in } O_k,$$

and

$$\begin{aligned}\text{Tor}\left(O_k^{\times}\right) &= \text{ torsion subgroup of } O_k^{\times} \\ &= \text{ roots of unity in } O_k^{\times} \\ &= \text{ a finite, cyclic group.}\end{aligned}$$

Dirichlet's unit theorem: there exists a finite collection of multiplicatively independent units $\eta_1, \eta_2, \ldots, \eta_r$, and a generator ζ of Tor$\left(O_k^{\times}\right)$, so that every unit α has a unique representation as

$$\alpha = \zeta^m \eta_1^{n_1} \eta_2^{n_2} \cdots \eta_r^{n_r},$$

where m, and $n_1, n_2, \ldots, n_r$, are integers. Here

$$r = \text{rank}\left(O_k^{\times}\right).$$

Minkowski units: we now assume that $k/\mathbb{Q}$ is a *Galois* extension of degree d. Then the Galois group

$$G = \mathrm{Aut}(k/\mathbb{Q})$$

has order d, and G acts on $O_k^\times$. If $\alpha \neq 1$ belongs to $O_k^\times$, then

$$\{\sigma(\alpha) : \sigma \in G\} \subseteq O_k^\times.$$

Minkowski proved: if $k/\mathbb{Q}$ is a Galois extension and $O_k^\times$ has positive rank r, then there exists a unit α in $O_k^\times$ such that the subgroup

$$\langle \sigma(\alpha) : \sigma \in G \rangle \subseteq O_k^\times$$

generated by the conjugates of α has the maximum possible rank r. We call a unit α with this property a *Minkowski unit*.

Theorem 5 (S. Akhtari-V.). *Let* $\eta_1, \eta_2, \ldots, \eta_r$*, be multiplicatively independent elements in* $O_k^\times$*, where* $r = \mathrm{rank}\Big(O_k^\times\Big)$*. Let*

$$\mathfrak{A} = \langle \eta_1, \eta_2, \ldots, \eta_r \rangle \subseteq O_k^\times$$

be the subgroup they generate. Then there exists a Minkowski unit β *in* $\mathfrak{A}$ *such that*

$$h(\beta) \le 2\Big(h(\eta_1) + h(\eta_2) + \cdots + h(\eta_r)\Big).$$

Moreover, if

$$\mathfrak{B} = \langle \sigma(\beta) : \sigma \in G \rangle,$$

is the subgroup of $O_k^\times$ *generated by the conjugates of* β*, then*

$$\mathrm{Reg}(k)[O_k^\times : \mathfrak{B}] \le \Big([k : \mathbb{Q}] h(\beta)\Big)^r,$$

where $\mathrm{Reg}(k)$ *is the regulator of* k*.*

The Northcott property: We say that a (possibly infinite) algebraic extension $K/\mathbb{Q}$ has the *Northcott property,* if for each positive T the set

$$\{\alpha \in K : h(\alpha) \leq T\}$$

is finite. A basic problem is to identify infinite extensions $K/\mathbb{Q}$ that have the Northcott property.

Let k be a number field and let $k^{(e)}$ be the infinite algebraic extension of $\mathbb{Q}$ obtained by adjoining to k all algebraic numbers α such that $[k(\alpha) : k] \leq e$.

Theorem 6. (E. Bombieri, U. Zannier, 2001) *For each number field k, the field $k^{(2)}$ has the Northcott property: the set*

$$\{\alpha \in k^{(2)} : h(\alpha) \leq T\}$$

is finite.

For $3 \leq e$ it is not known if $k^{(e)}$ has the Northcott property.

The Bogomolov property: We say that a (possibly infinite) algebraic extension $K/\mathbb{Q}$ has the *Bogomolov property* if there exists $\delta > 0$ such that

$$\{\alpha \in K^\times : h(\alpha) \leq \delta\}$$

consists only of roots of unity in K.

Theorem 7. (A. Schinzel, 1973) *Let K be the infinite Galois extension of $\mathbb{Q}$ generated by totally real algebraic numbers. Then K has the Bogomolov property.*

Theorem 8. (F. Amoroso, R. Dvornicich, 2000) *Let K be the infinite Galois extension of $\mathbb{Q}$ generated by all roots of unity. Then K has the Bogomolov property.*

Theorem 9. (E. Bombieri, U. Zannier, 2001) *Let $K/\mathbb{Q}$ be a (possibly infinite) Galois extension, and assume that K has an embedding in a finite extension of $\mathbb{Q}_p$ for some prime p. Then K has the Bogomolov property.*

Lehmer's problem: In 1931, D. H. Lehmer asked if there exists a positive constant c such that

$$0 < h(\alpha) \text{ implies that } c \le [\mathbb{Q}(\alpha):\mathbb{Q}]h(\alpha),$$

for all algebraic numbers α.

The smallest known positive value is

$$0.16235761434 \cdots = [\mathbb{Q}(\alpha):\mathbb{Q}]h(\alpha)$$

which occurs if α a root of

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 = 0.$$

The strongest unconditional result is

Theorem 10. (E. Dobrowolski, 1979) *There exists a positive constant c_0 such that if $0 < h(\alpha)$ then*

$$c_0 \left(\frac{\log\log 5[\mathbb{Q}(\alpha):\mathbb{Q}]}{\log 2[\mathbb{Q}(\alpha):\mathbb{Q}]} \right)^3 \le [\mathbb{Q}(\alpha):\mathbb{Q}]h(\alpha).$$

A Banach space: Let $\text{Tor}\left(\overline{\mathbb{Q}}^{\times}\right)$ denote the torsion subgroup of $\overline{\mathbb{Q}}^{\times}$ and write

$$\mathcal{G} = \overline{\mathbb{Q}}^{\times} / \text{Tor}\left(\overline{\mathbb{Q}}^{\times}\right)$$

for the quotient group. If ζ is a point in $\text{Tor}\left(\overline{\mathbb{Q}}^{\times}\right)$, then $h(\alpha) = h(\zeta\alpha)$ for all points α in $\overline{\mathbb{Q}}^{\times}$. Thus we may regard the height as a map

$$h : \mathcal{G} \to [0, \infty).$$

The height satisfies:

(i) $h(\alpha) = 0$ if and only if α is the identity element in $\mathcal{G}$,

(ii) $h(\alpha^{-1}) = h(\alpha)$ for all α in $\mathcal{G}$,

(iii) $h(\alpha\beta) \le h(\alpha) + h(\beta)$ for all α and β in $\mathcal{G}$.

These conditions imply that the map $(\alpha, \beta) \mapsto h(\alpha\beta^{-1})$ defines a metric on the group $\mathcal{G}$ and therefore induces a metric topology.

Let r/s denote a rational number, where r and s are relatively prime integers and s is positive. If α is in $\overline{\mathbb{Q}}^{\times}$ and ζ_1 and ζ_2 are in $\mathrm{Tor}\Big(\overline{\mathbb{Q}}^{\times}\Big)$, then all roots of the two polynomial equations

$$x^s - (\zeta_1\alpha)^r = 0 \quad \text{and} \quad x^s - (\zeta_2\alpha)^r = 0$$

belong to the same coset in $\mathcal{G}$. If we write $\alpha^{r/s}$ for this coset, we find that

$$(r/s, \alpha) \mapsto \alpha^{r/s}$$

defines a scalar product in the abelian group $\mathcal{G}$. This shows that $\mathcal{G}$ is a vector space (written multiplicatively) over the field $\mathbb{Q}$ of rational numbers. Moreover, we have

$$h\Big(\alpha^{r/s}\Big) = |r/s|_{\infty} h(\alpha).$$

Therefore the map $\alpha \mapsto h(\alpha)$ is a norm on the vector space $\mathcal{G}$ with respect to the usual archimedean absolute value $|\ |_{\infty}$ on its field $\mathbb{Q}$ of scalars. From these observations we conclude that the completion of $\mathcal{G}$ is a Banach space over the field $\mathbb{R}$ of real numbers.

Let $\alpha_1, \alpha_2, \ldots, \alpha_N$ be points in the $\mathbb{Q}$-vector space $\mathcal{G}$. Then write

$$\mathfrak{A} = \left\{ \prod_{n=1}^{N} \alpha_n^{\xi_n} : \boldsymbol{\xi} \in \mathbb{Z}^N \right\}$$

for the subgroup of rank $M < N$ which they generate in $\mathcal{G}$. The $\mathbb{Z}$-module $\mathcal{Z}$ of multiplicative dependencies is given by

$$\mathcal{Z} = \left\{ \boldsymbol{z} \in \mathbb{Z}^N : \prod_{n=1}^{N} \alpha_n^{z_n} = 1 \right\}.$$

Using geometry of numbers in the completion of $\mathcal{G}$ with respect to the height, we obtain a bound for the product

$$\prod_{l=1}^{L} |\boldsymbol{z}_l|_\infty,$$

where $\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_L$ are linearly independent elements of $\mathcal{Z}$, and also the product of the heights of M multiplicatively independent elements from the group $\mathfrak{A}$.

Theorem 11. [V, 2014] *Let*

$$\alpha_1, \alpha_2, \ldots, \alpha_N$$

be elements of the vector space $\mathcal{G}$ *which generate a subgroup* $\mathfrak{A}$ *of positive rank* M. *If* $1 \le M < N$ *then there exist* $L = N - M$ *linearly independent elements*

$$\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_L$$

in the $\mathbb{Z}$*-module* $\mathcal{Z}$, *and* M *multiplicatively independent elements*

$$\beta_1, \beta_2, \ldots, \beta_M$$

in the subgroup $\mathfrak{A}$, *such that*

$$\left\{ \prod_{l=1}^{L} |\boldsymbol{z}_l|_\infty \right\} \left\{ \prod_{m=1}^{M} h(\beta_m) \right\} \le \left\{ \sum_{n=1}^{N} h(\alpha_n) \right\}^M.$$

Heights on vectors and subspaces: Let k be a number field of degree d over $\mathbb{Q}$, and let $\boldsymbol{x} = (x_n)$ be a column vector in k^N. If v is an archimedean place we define

$$|\boldsymbol{x}|_v = \left(\|x_1\|_v^2 + \|x_2\|_v^2 + \cdots + \|x_N\|_v^2\right)^{d_v/2d}.$$

And if v is a non-archimedean place of k we define

$$|\boldsymbol{x}|_v = \max\Big\{|x_1|_v, |x_2|_v, \ldots, |x_N|_v\Big\}.$$

The Arakelov height of the nonzero vector $\boldsymbol{x}$ in k^N is

$$h(\boldsymbol{x}) = \sum_v \log|\boldsymbol{x}|_v.$$

The Arakelov height is well defined on projective space over k. That is, if $\alpha \neq 0$ belongs to k then $\alpha\boldsymbol{x}$ and $\boldsymbol{x}$ represent the same point in $\mathbb{P}^{N-1}(k)$. This follows from the product formula:

$$h(\alpha\boldsymbol{x}) = \sum_v \Big(\log|\alpha|_v + \log|\boldsymbol{x}|_v\Big) = h(\boldsymbol{x}).$$

As with the Weil height, it can be shown that $h(\boldsymbol{x})$ does not depend on the number field that contains the coordinates of the vector $\boldsymbol{x}$. Thus we find that

$$h : \mathbb{P}^{N-1}(\overline{\mathbb{Q}}) \to [0, \infty).$$

Let $\Lambda_N(\overline{\mathbb{Q}})$ be the exterior algebra over the field $\overline{\mathbb{Q}}$. Let

$$A = \begin{pmatrix} \boldsymbol{a}_1 & \boldsymbol{a}_2 & \cdots & \boldsymbol{a}_L \end{pmatrix}$$

be an $N \times L$ matrix with entries in $\overline{\mathbb{Q}}$ and $1 \leq L = \operatorname{rank} A < N$. We recall that the wedge product

$$\boldsymbol{a}_1 \wedge \boldsymbol{a}_2 \wedge \cdots \wedge \boldsymbol{a}_L$$

belongs to $\Lambda_N(\overline{\mathbb{Q}})$ and has $\binom{N}{L}$ coordinates. Each coordinate is one of the $L \times L$ subdeterminants of the matrix A. Therefore we define

$$h(A) = h(\boldsymbol{a}_1 \wedge \boldsymbol{a}_2 \wedge \cdots \wedge \boldsymbol{a}_L)$$

by applying the Arakelov height to the vector of $\binom{N}{L}$ subdeterminants.

If the columns of the $N \times L$ matrix

$$B = \Big(\boldsymbol{b}_1 \ \boldsymbol{b}_2 \ \cdots \ \boldsymbol{b}_L\Big)$$

span the same L-dimensional subspace $\mathcal{A}$ as the columns of A, then it is known that the two wedge products satisfy

$$\boldsymbol{a}_1 \wedge \boldsymbol{a}_2 \wedge \cdots \wedge \boldsymbol{a}_L = \alpha\Big(\boldsymbol{b}_1 \wedge \boldsymbol{b}_2 \wedge \cdots \wedge \boldsymbol{b}_L\Big)$$

for some algebraic number $\alpha \neq 0$. Therefore using the product formula we get

$$h(A) = h(B)$$

We define the Arakelov height of a subspace $\mathcal{A} \subseteq \overline{\mathbb{Q}}^N$ of dimension L by setting

$$h(\mathcal{A}) = h(A) = h(\boldsymbol{a}_1 \wedge \boldsymbol{a}_2 \wedge \cdots \wedge \boldsymbol{a}_L).$$

Our remarks show that $h(\mathcal{A})$ depends on the subspace $\mathcal{A}$ but does *not* depend on the choice of basis. Hence it is a well defined height on the collection of subspaces of $\overline{\mathbb{Q}}^N$ having dimension L.

For a number field k and positive integer L let $\gamma_k(L)$ be Hermite's constant for $k_{\mathbb{A}}$. The following result is the "dual" of Siegel's Lemma:

Theorem 12. [E. Bombieri, V, 1983] *Let*

$$\mathcal{X} \subseteq k^N$$

be a subspace of dimension L. Then there exists a basis

$$\Big\{\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_L\Big\}$$

for $\mathcal{X}$ such that

$$\sum_{\ell=1}^{L} h(\boldsymbol{\xi}_\ell) \le \tfrac{1}{2} L \log \gamma_k(L) + h(\mathcal{X}).$$

Moreover, the constant $\gamma_k(L)$ cannot be replaced by a smaller constant.

The usual form of Siegel's Lemma is now:

Theorem 13. [E. Bombieri, V, 1983] *Let A be an $M \times N$ matrix with* $\operatorname{rank} A = M < N$ *and entries in k. Then there exist $L = N - M$ linearly independent solutions*

$$\Big\{\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots, \boldsymbol{\xi}_L\Big\}$$

to the system of M linear equations

$$A\boldsymbol{x} = \mathbf{0},$$

such that

$$\sum_{\ell=1}^{L} h(\boldsymbol{\xi}_\ell) \le \tfrac{1}{2} L \log \gamma_k(L) + h\Big(A^T\Big).$$

It follows from the product formula that $h\Big(A^T\Big)$ is equal to the Arekalov height of the subspace

$$\mathcal{X} = \{\boldsymbol{x} \in k^N : A\boldsymbol{x} = \mathbf{0}\}.$$

Hence this form of Siegel's Lemma is equivalent to the previous "dual" version. Note that $\binom{N}{L} = \binom{N}{M}$.