MA 254 notes: Diophantine Geometry

(Distilled from [Hindry-Silverman])

Dan Abramovich

Brown University

January 29, 2016

Height on $\mathbb{P}^n(k)$

Let $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(\mathbb{Q})$ with $x_i \in \mathbb{Z}, \gcd(x_0, \ldots, x_n) = 1$,

Definition (Height on $\mathbb{P}^n(\mathbb{Q})$)

$H(P) = \max\{|x_0|, \ldots, |x_n|\}$.

This has the finiteness property:

For any B the set $\{P \in \mathbb{P}^n(\mathbb{Q}) | H(P) \leq B\}$ is finite.

Definition (Height on $\mathbb{P}^n(k)$)

Let k be a number field, $x_i \in k$, and $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(k)$.
Define the relative multiplicative height
$H_k(P) = \prod_{v \in M_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}$
and the relative logarithmic height
$h_k(P) = \log H_k(P) = \sum_{v \in M_k} -n_v \min\{v(x_0), \ldots v(x_n)\}$.

Absolute height

Definition

- The absolute multiplicative height of $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ is $H(P) = H_k(P)^{1/[k:\mathbb{Q}]}$.
- The absolute logarithmic height is $h(P) := \log H(P) = h_k(P)/[k:\mathbb{Q}]$.
- The absolute height of $\alpha \in k$ is $H(\alpha) := H(1, \alpha)$.

Proposition (Basic height properties)

- $H_k(P)$ *is independent of choice of coordinates in* k.
- $H(P), H_k(P) \geq 1; h(P), h_k(P) \geq 0$ *for all* $k \in \mathbb{P}^n(\bar{\mathbb{Q}})$.
- $H(P), h(P)$ *are independent of choice of* k *or coordinates.*

Proof of basic height properties

Proof.

- $\prod_{v\in M_k} \max\{\|cx_0\|_v, \dots, \|cx_n\|_v\} = \left(\prod_{v\in M_k} \|c\|_v\right) \prod_{v\in M_k} \max\{\|x_0\|_v, \dots, \|x_n\|_v\} = \prod_{v\in M_k} \max\{\|x_0\|_v, \dots, \|x_n\|_v\}$.
- If $x_i \neq 0$ then $H_k(x) = \prod_{v\in M_k} \max\{\|x_0/x_i\|_v, \dots, \|x_n/x_i\|_v\} \geq \prod_{v\in M_k} 1 = 1.$
- If k'/k then $H_{k'}(P) = \prod_{v\in M_k} \prod_{w|v} \max\{\|x_0\|_w, \dots, \|x_n\|_w\}$ $= \prod_{v\in M_k} \prod_{w|v} \max\{|x_0|_v^{n_w}, \dots, |x_n|_v^{n_w}\}$ $= \prod_{v\in M_k} \prod_{w|v} \max\{|x_0|_v^{n_v}, \dots, |x_n|_v^{n_v}\}^{[k'_w:k_v]}$ $= \prod_{v\in M_k} \prod_{w|v} \max\{\|x_0\|_v, \dots, \|x_n\|_v\}^{[k'_w:k_v]}$ $= \prod_{v\in M_k} \max\{\|x_0\|_v, \dots, \|x_n\|_v\}^{[k':k]} = H_k(P)^{[k':k]}$ as needed.

♠

Invariance

- The Galois group $G_{\mathbb{Q}}$ acts on $\mathbb{P}^n(\bar{\mathbb{Q}})$.
- It also permutes absolute values: if $\sigma : k \to k'$ is an isomorphism then we define $|\sigma(x)|_{\sigma(v)} = |x|_v$, namely $|y|_{\sigma(v)} = |\sigma^{-1}x|_v$.
- Similarly it sends completions to completions, with $n_v = n_{\sigma(v)}$, and globally $[k : \mathbb{Q}] = [\sigma(k) : \mathbb{Q}]$.

Proposition

H is invariant under $G_{\mathbb{Q}}$: we have $H_{\sigma(k)}(\sigma(x)) = H_k(x)$ and $H(\sigma(x)) = H(x)$.

Proof.

Trace the definitions, taking the above into consideration. ♠

The strong finiteness property

Theorem

Given B, D, the set $\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) | H(P) \leq B, [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$ is finite.

Lemma

Given B, d, the set $\{x \in \bar{\mathbb{Q}}) | H(x) \leq B, [\mathbb{Q}(x) : \mathbb{Q}] = d\}$ is finite.

Proof of Theorem given Lemma.

- Given $P = (x_0, \ldots, x_n)$ with $x_j \neq 0$ we may assume by rescaling that $x_j = 1$.
- Then $\max\{\|x_0\|_v, \ldots, \|x_n\|_v\} \geq \max\{\|x_i\|_v, 1\}$ for each i, so $H(P) \geq H(x_i)$. Also $\mathbb{Q}(P) \supset \mathbb{Q}(x_i)$.
- There are finitely many possible choices for $j, d \leq D$ and, by the lemma, for x_i, hence for P.

♠

The strong finiteness property - continued

Sublemma

Suppose the minimal polynomial of $x \in \bar{\mathbb{Q}}$ *is* $X^d - s_1(x)X^{d-1} \pm \cdots + (-1)^d s_d(x)$. *Then* $H(1, s_1(x), \ldots, s_d(x)) \leq 2^d H(x)^{d^2}$.

Proof of Lemma given Sublemma.

We have seen that $\{s \in \mathbb{P}^d(\mathbb{Q}) : H(s) < C\}$ is finite. Applying this to $C = 2^d B^{d^2}$ we find that the number of minimal polynomials of $\{x \in \bar{\mathbb{Q}}) | H(x) \leq B, [\mathbb{Q}(x) : \mathbb{Q}] = d\}$ is finite. Since there are d roots per polynomial, this set itself is finite. ♠

We write $\varepsilon_v(r) := \begin{cases} r & v \text{ archimedean} \\ 1 & \text{otherwise} \end{cases}$

so that $|\sum_{i=1}^r x_i|_v \quad \leq \quad \varepsilon_v(r) \max_i |x_i|_v$.

Note $r = \prod_v \varepsilon_v(r)^{n_v/[k:\mathbb{Q}]}$.

The strong finiteness property - continued

Proof of Sublemma.

- If x_i are the d conjugates of x, and v a valuation of the splitting field k', then
  $|s_r(x)|_v = |\sum x_{i_1}\cdots x_{i_r}|_v$
  $\leq \varepsilon_v(2^d)\max|x_{i_1}\cdots x_{i_r}|_v \quad\leq\quad \varepsilon_v(2^d)\max_i|x_i|_v^r.$
- Taking maximum we obtain
  $\max\{1,|s_1(x)|_v,\ldots,|s_d(x)|_v\} \leq \varepsilon_v(2^d)\prod_i\max\{|x_i|_v,1\}^d.$
  taking products and $[k':\mathbb{Q}]$-th root, we have
  $H(1,s_1(x),\ldots,s_d(x)) \leq 2^d\prod_i H(x_i)^d$
  $= 2^d\prod_i H(x)^d = 2^d H(x)^{d^2}$ as needed.

♠

Points of Height 1

Corollary (Kronecker's theorem)

Say $P = (x_0, \ldots, x_n) \in \mathbb{P}^n(\bar{\mathbb{Q}})$ *and* $x_i \neq 0$. *Then*
$H(P) = 1 \iff x_j/x_i \in \boldsymbol{\mu}(\bar{\mathbb{Q}}) \cup \{0\}$ *for all* j.

Proof.

- Without loss of generality $i = 0$ and $x_0 = 1$.
- If $x_j \in \boldsymbol{\mu}$ then $|x_j|_v = 1$ for all v so $H(P) = 1$.
- Assume $H(P) = 1$ and consider the sequence of points $P^r := (x_0^r, \ldots x_n^r)$. Then you check $H(P^r) = H(P)^r = 1$, in particular bounded by 1, and by the theorem $\{P^r\}$ is a finite set.
- So there are $r \neq s$ such that $P^r = P^s$, so $x_j^r = x_j^s$, so $x_j \in \boldsymbol{\mu} \cup \{0\}$ as needed.

♠

Segre and Veronese embeddings

Let $S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^{nm+n+m}$ be the Segre embedding and $V_{n,d} : \mathbb{P}^n \hookrightarrow \mathbb{P}^{\binom{n+d}{n}-1}$ the d-th Veronese.

Proposition

$h(S_{n,m}(x,y)) = h(x) + h(y)$ *and* $h(V_{n,d}(x)) = dh(x)$.

Proof.

- The point $z = S_{n,m}(x,y)$ has coordinates $(\ldots, x_i y_j, \ldots)$. For any v we have $\max_{ij} |x_i y_j|_v = (\max_i |x_i|_v)(\max_j |y_j|_v)$. So $h(z) = \log \prod_v \max_{ij} |x_i y_j|_v^{n_v/[k:\mathbb{Q}]} =$ $\log \left(\prod_v \max_i |x_i|_v^{n_v/[k:\mathbb{Q}]} \prod_v \max_j |y_j|_v^{n_v/[k:\mathbb{Q}]} \right) = h(x) + h(y)$.
- $w = V_{n,d}(x)$ has coordinates the monomials $M_I(x)$ of degree d. We have $|M_I(x)|_v \le \max_i |x_i|_v^d$ so $\max_I |M_I(x)|_v = \max_i |x_i|_v^d$, and proceed as before.

♠

Functoriality of heights on projective spaces

An $m+1$-tuple $(f_0,\ldots,f_m)$ of homomgeneous forms of degree d in $n+1$ variables defines a rational map $\phi : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$, which is a morphism away from the base locus $Z = V(f_0,\ldots,f_m)$.

Theorem (Functoriality of heights on projective spaces)

- $h(\phi(P)) \quad \leq \quad dh(P) + O(1) \qquad$ *for all* $P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \smallsetminus Z$.
- *If* $X \subset \mathbb{P}^n$ *closed,* $X \cap Z = \emptyset$*, then*
  $h(\phi(P)) \quad = \quad dh(P) + O(1) \qquad$ *for all* $P \in X(\bar{\mathbb{Q}})$.

It is convenient to take absolute values of P, f_j and height of ϕ. Represent $P = (x_0,\ldots,x_n)$ and in monomial notation $f_j = \sum_{|I|=d} a_{j,I} x^I$. We write
$|P|_v = \max_i\{|x_i|_v\}, \quad |f_j|_v = \max_I\{|a_{j,I}|_v\}$ and
$H(\phi) = H((a_{j,I})_{j,I}) = \prod_v \max_j\{|f_j|_v\}^{n_v/[k:\mathbb{Q}]}$.

We write $N_d = \binom{n+d}{d}$.

Proof of functoriality, first part.

- $$|f_j(P)|_v = |\sum_I a_{j,I}x^I|_v \leq \varepsilon_v(N_d)(\max_I |a_{j,I}|_v)(\max_I |x^I|_v)$$
  $$\leq \varepsilon_v(N_d)|f_j|_v(\max_i |x_i|_v^d)$$
  $$= \varepsilon_v(N_d)|f_j|_v|P|_v^d.$$
- We get
  $$\prod_v \max_j |f_j(P)|_v^{n_v/[k:\mathbb{Q}]} \leq N_d \cdot (\prod_v \max_j |f_j|_v^{n_v/[k:\mathbb{Q}]})H(P)^d$$
  $$= N_d \cdot H(\phi)H(P)^d.$$
- so $h(\phi(P)) \leq dh(P) + h(\phi) + \log N_d$.

♠

Proof of functoriality, second part, beginning

- Let $I_X = (p_1, \ldots, p_r)$. By Hilbert's Nullstellensatz, after a finite extension of k we have
  $\sqrt{(p_1, \ldots, p_r, f_0, \ldots, f_m)} = (X_0, \ldots, X_n)$.
- In other words, there is $t \geq d$, forms g_{kj} of degree $t - d$ and forms q_{lj} such that for all j
  $g_{0j} f_0 + \cdots + g_{mj} f_m \quad + \quad q_{1j} p_1 + \cdots + q_{rj} p_r = X_j^t$.
- Plugging in $P = (x_0, \ldots, x_n) \in X$ we get
  $g_{0j}(P) f_0(P) + \cdots + g_{mj}(P) f_m(P) = x_j^t$.

Proof of functoriality, second part, concluded.

- $$\begin{aligned} |P|_v^t = \max_j |x_j^t|_v &= \max_j |g_{0j}(P)f_0(P) + \cdots + g_{mj}(P)f_m(P)|_v \\ &\leq \varepsilon_v(m+1)\ (\max_{i,j} |g_{ij}(x)|_v)\ (\max_i |f_i(x)|_v) \\ &\leq (\varepsilon_v(m+1)\ N_{t-d}|(g_{ij})|_v)\ |P|_v^{t-d}\ |\phi(P)|_v. \end{aligned}$$
- So as before $H(P)^t \leq c \cdot H(P)^{t-d} H(\phi(P))$.
- Hence $dh(P) \leq h(\phi(P)) + O(1)$ as required.

♠