MA 254 notes: Diophantine Geometry
(Distilled from [Hindry-Silverman])

Dan Abramovich

Brown University

January 29, 2016
**Theorem (Canonical heights - Néron-Tate)**

Given $k$ a number field, $V/k$ smooth projective variety, $D \in \text{Div}(V)$, $\phi : V \to V$ a morphism, suppose $\phi^* D \sim \alpha D$ for $\alpha > 1$. There is a unique $\hat{h}_{V,\phi,D} : V(\bar{k}) \to \mathbb{R}$ such that

1. $\hat{h}_{V,\phi,D} = h_{V,D} + O(1)$.
2. $\hat{h}_{V,\phi,D} \circ \phi = \alpha \hat{h}_{V,\phi,D}$.

Further, $\hat{h}_{V,\phi,D}(P) = \lim_{n \to \infty} h_{V,D}(\phi^n(P))/\alpha^n$.

**Proof of Uniqueness**

- Say $\hat{h}, \hat{h}'$ both satisfy (i),(ii).
- Then by (i) $g := \hat{h} - \hat{h}'$ is bounded: $|g(P)| < C'$,
- and by (ii) $g \circ \phi = \alpha g$, giving $g(\phi^n(P)) = \alpha^n g(P)$.
- So $|g(P)| = |g(\phi^n(P))|/\alpha^n < C'/\alpha^n \to 0$,
- hence $g = 0$. ♠
Proof of convergence

- We show the latter limit exists by showing the sequence is Cauchy.
- By functoriality \(|h_{V,D}(\phi(Q)) - \alpha h_{V,D}(\phi(Q))| \leq C\).
- For \(n > m\) we have

\[
|h_{V,D}(\phi^n(P))/\alpha^n - h_{V,D}(\phi^m(P))/\alpha^m|
\]

\[
= \left| \sum_{i=m+1}^{n} \frac{(h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P)))/\alpha^i}{\alpha^i} \right|
\]

\[
\leq \sum_{i=m+1}^{n} \left| (h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P)))/\alpha^i \right|
\]

\[
\leq \sum_{m+1}^{n} \frac{C}{\alpha^i} = C(\alpha^{-m} - \alpha^{-n})/(\alpha - 1) \to 0
\]

♠
We thus define $\hat{h}_{V,\phi,D}(P) = \lim_{n \to \infty} h_{V,D}(\phi^n(P))/\alpha^n$.

Proof of (i)

Taking $m = 0$ and $n \to \infty$ in (*) gives

$$\left| \hat{h}_{V,\phi,D}(P) - h_{V,D}(P) \right| \leq C/(\alpha - 1)$$

Thus the theorem is proved.

Proof of (ii)

$$\hat{h}_{V,\phi,D}(\phi(P)) = \lim_{n \to \infty} h_{V,D}(\phi^n(\phi(P)))/\alpha^n$$

$$= \alpha \lim_{n \to \infty} h_{V,D}(\phi^{n+1}(P))/\alpha^{n+1} = \hat{h}_{V,\phi,D}(P).$$

Thus the theorem is proved.
Preperiodic points and Northcott’s theorem

Definition

$P \in V$ is preperiodic for $\phi$ if $\{\phi^n(P)\}$ is finite.

Proposition

Suppose $D$ ample and $\phi^*D \sim \alpha D$ with $\alpha > 1$.

(a) $\hat{h}_{V,\phi,D}(P) \geq 0$, with equality $\iff$ $P$ is preperiodic.

(b) The set of preperiodic $k$-rational points is finite.
Proof.

(a) Can take \( h_{V,D} > 0 \) hence \( \hat{h}_{V,\phi,D} \geq 0 \).
- Assume \( P \) preperiodic. \( \{\phi^n(P)\} \) is finite so \( \{\hat{h}_{V,\phi,D}(\phi^n(P))\} \) finite hence bounded. But then \( \hat{h}(P) = \hat{h}(\phi^n(P))/\alpha^n \to 0 \), so \( \hat{h}(P) = 0 \).
- Assume \( \hat{h}(P) = 0 \). Extend the field so that \( P \in V(k) \), hence \( \phi^n(P) \in V(k) \). So \( h_{V,D}(\phi^n(P)) = \hat{h}_{V,\phi,D}(\phi^n(P)) + O(1) = \alpha^n \hat{h}_{V,\phi,D}(P) + O(1) = O(1) \). So by the finiteness property the set \( \{\phi^n(P)\} \) is finite.

(b) By (a) the rational preperiodic points satisfy \( \hat{h}_{V,\phi,D}(P) = 0 \) hence \( h_{V,D}(\phi^n(P)) = O(1) \). By the finiteness property the set is finite.
Theorem (Néron-Tate)

Given abelian variety $A$ over number field $k$ and divisor $D$ with $O_A(D)$ symmetric, there is $\hat{h}_{A,D} : A(\bar{k}) \to \mathbb{R}$ with

(a) $\hat{h}_{A,D} = h_{A,D} + O(1)$.

(b) $\hat{h}_{A,D}([m]P) = m^2 \hat{h}_{A,D}(P)$.

(c) $\hat{h}_{A,D}(P + Q) + \hat{h}_{A,D}(P - Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q)$

(d) $\hat{h}_{A,D}$ is a quadratic form on the group $A(\bar{k})$.

(e) $\hat{h}_{A,D}$ is independent of the choice of $D \in |D|$. It is uniquely determined by (a) and (b) applied to any $m > 1$. 
Construction and proof of (a)

We define \( \hat{h}_{A,D} := \hat{h}_{A,[2],D} \). This is possible since \([2]^* D \sim 4D\).

Explicitly \( \hat{h}_{A,D}(P) = \lim h_{A,D}([2^n]P)/4^n \). Thus (a) follows from (i).

Proof of (c)

- We have seen
  \[
  h_{A,D}(P + Q) + h_{A,D}(P - Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1).
  \]
- The same \(O(1)\) applies to \([2^n]P, [2^n]Q\).
- Dividing by \(4^n\) the \(O(1)\) evaporates, giving the result in the limit.

End of proof.

A function on an abelian group satisfying the parallelogram law (c) is a quadratic form, giving (b) and (d) (see the book for a direct proof of (b)). Uniqueness of \( \hat{h}_{A,[m],D}(P) \) implies (e).
Definition (polarized height pairing)

We define the height pairing \( \langle P, Q \rangle_D = \frac{\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q)}{2} \).

By (d) it is bilinear, by (b) we have \( \langle P, P \rangle_D = \hat{h}_{A,D}(P) \).

Proposition (real positivity of canonical heights)

Assume further \( D \) is ample.

(a) \( \hat{h}_{A,D}(P) \geq 0 \), with equality \( \Leftrightarrow \) \( P \) torsion.

(b) The real extension \( q : A(\bar{k}) \otimes \mathbb{R} \) of \( \hat{h}_{A,D} \) is a positive definite quadratic form.

(b') If \( x_i \in A(\bar{k}) \otimes \mathbb{R} \) linearly independent then the height regulator \( \det(\langle x_i, x_j \rangle_{ij}) > 0 \).
If \([2^m]P = [2^n]P\) for \(m \neq n\), then \([2^m - 2^n]P = O\), hence a preperiodic point is torsion. Part (a) of Northcott gives (a).

Consider \(x \in A(\bar{k}) \otimes \mathbb{R}\) with \(\hat{h}_{A,D}(x) = 0\), and write \(x = \sum a_i P_i\), with \(a_i \in \mathbb{R}\). Extending \(k\) we may assume \(P_i \in A(k)\).

Write \(\Lambda = \sum \mathbb{Z}P_i \subset A(\bar{k}) \otimes \mathbb{R}\) and \(V = \sum \mathbb{R}P_i\). Note that \(V = \Lambda \otimes \mathbb{R}\), so \(\Lambda \subset V\) is a lattice.

Note that \(q|\Lambda \geq 0\) with equality only for \(\lambda = 0\), since \(\ker(A(\bar{k}) \to A(\bar{k}) \otimes \mathbb{R}) = A(\bar{k})_{torsion}\). This is (i) below.
Proof of real positivity of canonical heights, conclusion

Real positivity of canonical heights follows from these two results:

**Lemma**

The set \( \{ \lambda \in \Lambda \mid q(\lambda) \leq B \} \) is finite.

**Proposition (Real positivity of forms)**

Let \( q : \mathbb{Z}^r \rightarrow \mathbb{R} \) be a quadratic form such that

(i) \( q(\lambda) \geq 0 \) with equality only for \( \lambda = 0 \), and

(ii) for all \( B \) the set \( \{ \lambda \in \mathbb{Z}^r \mid q(\lambda) \leq B \} \) is finite.

Then the extension of \( q_{\mathbb{R}} \) to \( \mathbb{R}^n \) is positive definite.

Indeed, by the lemma we have (ii), and (i) was shown before, so the proposition applies giving (b). Statement (b’) is an immediate consequence of (b).
Proof of Lemma

- Say $\lambda$ is the image of $Q \in A(k)$.
- Since $|\hat{h} - h| < C$ for some $C$ we have $q(\lambda) \leq B \Rightarrow h_{A,D}(Q) \leq B + C$.
- So the set $\{\lambda \in \Lambda | q(\lambda) \leq B\}$ is the image of the finite set $\{Q \in A(K) | h_{A,D}(Q) \leq B + C\}$, as needed.

Lemma (This I won’t prove)

- Let $q_{s,t} : \mathbb{R}^r \to \mathbb{R}$, $q(x_1, \ldots, x_r) = \sum_{i=1}^{s} x_i^2 - \sum_{i=s+1}^{s+t} x_i^2$ be the standard quadratic form of signature $(s, t)$.
- Let $U(L, M) = \{(x_1, \ldots, x_r) | \sum_{i=1}^{s} x_i^2 < L, \sum_{i=s+1}^{s+t} x_i^2 < M\}$.

Then

(i) $\text{Vol}(U(L, M)) < \infty \iff s + t = r$

(ii) in which case $\text{Vol}(U(L, M)) = V_s V_t L^{s/2} M^{t/2}$, where $V_s$ is the volume of the unit ball in $\mathbb{R}^s$.  

♠♠
By (ii) there are finitely many elements of $\Lambda \setminus \{0\}$ with bounded $q(\lambda)$, and by (i) these values of $q(\lambda)$ are $> 0$, so they have a minimum $L = \inf\{q(\lambda) | \lambda \in \Lambda, \lambda \neq 0\}$.

Say the signature of $q_\mathbb{R}$ is $(s, t)$, choose an isomorphism with the standard form and consider $U(\delta, \epsilon)$.

Since $L > 0$ we have that $U(L/2, M) \cap \Lambda = \{0\}$ for all $M > 0$.

But $U(L/2, M)$ is symmetric and convex. By Minkowski $\text{Vol}(U(L/2, M)) \leq 2^r \text{Vol}(V/\Lambda)$ is bounded for all $M$.

By the Lemma part (i) $s + t = r$ and by part (ii) $t = 0$, hence $s = r$ and $q_\mathbb{R}$ is positive definite. ♠
Antisymmetric canonical height

**Theorem**

Given $A/k$ as before and divisor $D$ with $O_A(D)$ antisymmetric, there is $\hat{h}_{A,D} : A(\bar{k}) \to \mathbb{R}$ with

(a) $\hat{h}_{A,D} = h_{A,D} + O(1)$ and

(c) $\hat{h}_{A,D}(P + Q) = \hat{h}_{A,D}(P) + \hat{h}_{A,D}(Q),$

so $\hat{h}_{A,D} : A(\bar{k}) \to \mathbb{R}$ is a homomorphism. Furthermore such $\hat{h}_{A,D}$ is unique.

**Proof.**

Using $[m^*]D \sim mD$ we can again define $\hat{h}_{A,D} := \hat{h}_{A,[2],D}$ and the proof flows as before.

♠
Definition (Quadratic functions)

Let $A$ and $R$ be abelian groups, with $R$ uniquely 2-divisible. A **quadratic function** $h : A \rightarrow R$ is a function satisfying

$$\sum_{I \subset \{1,2,3\}} (-1)^{\#I} h(\sum_{i} a_i) = 0$$

for all triples of $a_i \in A$.

This includes constants, linear and quadratic forms (and that’s really it).
Theorem

Let $A/k$ as before and $D \in \text{Div}(A)$.

(a) $\exists!$ quadratic $\hat{h}_{A,D}: A(\bar{k}) \to \mathbb{R}$, the canonical height, such that $\hat{h}_{A,D} = h_{A,D} + O(1)$ and $\hat{h}_{A,D}(O) = 0$.

(b) If $D \sim D'$ then $\hat{h}_{A,D} = \hat{h}_{A,D'}$.

(c) $\hat{h}_{A,D+E} = \hat{h}_{A,D} + \hat{h}_{A,E}$.

(d) For $\phi: B \to A$ a morphism of abelian varieties $\hat{h}_{B,\phi^*D} = \hat{h}_{A,D} \circ \phi - \hat{h}_{A,D}(\phi(O))$.

(e) There is a unique quadratic form $\hat{q}_{A,D}$ and unique linear $\hat{\ell}_{A,D}$ such that $\hat{h}_{A,D} = \hat{q}_{A,D} + \hat{\ell}_{A,D}$.

- $\hat{q}_{A,D} = \hat{h}_{A,D^+}/2$ and $\hat{\ell}_{A,D} = \hat{h}_{A,D^-}/2$, where $D^+ = D + [-1]^*D$ and $D^- = D - [-1]^*D$.

- If $D$ symmetric $\hat{h}_{A,D} = \hat{q}_{A,D}$ and if $D$ antisymmetric $\hat{h}_{A,D} = \hat{\ell}_{A,D}$. 

Sketch proof (a)-(d) ((e) skipped)

(a) Define \( \hat{h}_{A,D} := (\hat{h}_{A,D+} + \hat{h}_{A,D-})/2 \).
- \( \hat{h}_{A,D} \) is a quadratic function with \( \hat{h}_{A,D}(O) = 0 \).
- \( 2\hat{h}_{A,D} = \hat{h}_{A,D+} + \hat{h}_{A,D-} = h_{A,D+} + h_{A,D-} + O(1) = 2h_{A,D} + O(1) \) by additivity of Weil heights, hence \( \hat{h}_{A,D} = h_{A,D} + O(1) \).
- If \( \hat{h}'_{A,D} \) another, then \( \hat{h}_{A,D} - \hat{h}'_{A,D} \) is a bounded quadratic with \( f(O) = 0 \) so \( f = 0 \), so \( \hat{h}_{A,D} \) unique.

(b) \( D \sim D' \) then \( h_{A,D'} = h_{A,D} + O(1) \) so \( \hat{h}_{A,D'} \) satisfies (a), and by uniqueness \( \hat{h}_{A,D} = \hat{h}_{A,D'} \).

(c) \( h_{A,D+E} = h_{A,D} + h_{A,E} + O(1) \) so \( \hat{h}_{A,D} + \hat{h}_{A,E} \) satisfies (a) for \( D + E \), and by uniqueness \( \hat{h}_{A,D+E} = \hat{h}_{A,D} + \hat{h}_{A,E} \).

(d) Since \( \phi \) is a translated homomorphism, the function \( \hat{h}_{A,D} \circ \phi - \hat{h}_{A,D}(\phi(O)) = h_{A,D} \circ \phi + O(1) \), it is quadratic, vanishes at \( O \), so by uniqueness agrees with \( \hat{h}_{B,\phi^*D} \).
Canonical height pairing

Definition

Define the **canonical height pairing** \( A(\overline{k}) \times \hat{A}(\overline{k}) \to \mathbb{R} \) by

\[
[P, Q] = \hat{h}_{A,D_Q}(P)
\]

for any \( D_Q \) representing \( Q \).

Theorem (Canonical height pairing)

- **This is bilinear, kernels are** \( A_{\text{torsion}} \) and \( \hat{A}_{\text{torsion}} \)
- \([P, Q] = \hat{h}_{A \times \hat{A}, \mathbb{P}}(P, Q)\).

Consequence:

Theorem (Strong algebraic equivalence)

\( V/k \) variety over number field, \( D \) ample, \( E \sim_{\text{alg}} 0 \). There is \( c \) such that \( h_{V,E} \leq c \sqrt{h_{V,D}(P) + 1} \)
Proof of Strong algebraic equivalence, first steps

- Let $A = \text{Alb}(V)$ with $\pi : V \to A$. There is $E_1 \in \text{Div}(A)$, $E_1 \sim_{\text{alg}} 0$, such that $E = \pi^*E_1$.

- If $D_1 \in \text{Div}(A)$ symmetric ample, then there is $a \in A$ such that $E_1 = t_a^*D_1 - D_1$.

- For $P \in V(\kbar)$ write $Q = \pi(P)$.

\[ h_{V,E}(P) = h_{V,\pi^*E_1}(P) = h_{A,E_1}(Q) + O(1) \]
\[ = \hat{h}_{A,E_1}(Q) + O(1) = \hat{h}_{A,t_a^*D_1}(Q) - \hat{h}_{A,D_1}(Q) + O(1) \]
\[ = \hat{h}_{A,D_1}(t_a(Q)) - \hat{h}_{A,D_1}(t_a(O)) - \hat{h}_{A,D_1}(Q) + O(1) \]
\[ = \hat{h}_{A,D_1}(Q + a) - \hat{h}_{A,D_1}(a) - \hat{h}_{A,D_1}(Q) + O(1) \]
\[ = 2\langle A, a \rangle + O(1) \leq 2\sqrt{\hat{h}_{A,D_1}(Q)\hat{h}_{A,D_1}(a)} + O(1) \]

by Cauchy-Schwartz.
On the other hand

\[ \hat{h}_{A,D_1}(Q) = \hat{h}_{A,D_1}(\pi(P)) = \hat{h}_{V,\pi^*D_1}(P). \]

But \( cD - D_1 \) is an effective class since \( D \) ample, so

\[ \hat{h}_{V,\pi^*D_1}(P) < c\hat{h}_{V,\pi^*D}(P). \]

Plugging in we get the result.
Recall that for any ample symmetric divisor class $D$ we have a surjective homomorphism with torsion kernel
\[ \lambda_D : A \to \hat{A} \quad P' \mapsto Q := [t_P^*, D - D]. \]

Mumford shows \((id, \lambda_D)^* P = m^* D - \pi_1^* D - \pi_2^* D\), so
\[
\hat{h}_{A \times \hat{A}, \mathcal{P}}((P, Q)) = \hat{h}_{A \times A, m^* D - \pi_1^* D - \pi_2^* D}((P, P'))
= \hat{h}_{A, D}(P + P') - \hat{h}_{A, D}(P) - \hat{h}_{A, D}(P') = 2\langle P, P' \rangle_D
\]

Hence $\hat{h}_{A \times \hat{A}, \mathcal{P}}((P, Q))$ is bilinear with kernels on both sides being the torsion subgroups.

Also we had
\[
\hat{h}_{A, D}(P + P') - \hat{h}_{A, D}(P) - \hat{h}_{A, D}(P') = \hat{h}_{A, t_P^*, D}(P) - \hat{h}_{A, D}(P)
= \hat{h}_{A, t_P^*, D - D}(P)
= \hat{h}_{A, Q}(P) = [P, Q]_A
\]