Height Functions

Michael Tepper

February 10, 2006

Definition 1. An \textit{archimedean} absolute value on a field \( k \) is a real valued
function
\[
\| \cdot \| : k \to [0, \infty)
\]
with the following three properties:
\begin{enumerate}
\item \( \|x\| = 0 \) if and only if \( x = 0 \).
\item \( \|xy\| = \|x\| \cdot \|y\| \).
\item \( \|x + y\| \leq \|x\| + \|y\| \).
\end{enumerate}
A \textit{nonarchimedean} absolute value satisfies the extra condition that
\begin{enumerate}
\item[(3')] \( \|x + y\| \leq \max\{\|x\|, \|y\|\} \).
\end{enumerate}

If \( k \) is a field, we denote \( M_k \) the set of absolute values on \( k \). As an abuse of
notation we say that if \( |\cdot|_v \) is an absolute value on \( k \) then \( v \in M_k \) rather then
\( |\cdot|_v \in M_k \).

The rational numbers \( \mathbb{Q} \) have the archimedean absolute value
\[
|x|_\infty = \max\{x, -x\}.
\]
For each prime number \( p \in \mathbb{Z} \) there is a nonarchimedean absolute value (usually
called the \( p \)-adic absolute value)
\[
|x|_p = p^{-\text{ord}_p(x)}.
\]
Where \( \text{ord}_p(x) \) is the unique integer such that \( x \) can be written in the form
\[
x = p^{\text{ord}_p(x)} \cdot a/b \quad \text{with} \quad a, b \in \mathbb{Z} \quad \text{and} \quad p \nmid ab
\]

Note 1. It can be proved that up to a "power" that these are the only nontrivial
absolute values on \( \mathbb{Q} \). See [Lang - Number Theory] or [B-S Number Theory]

Theorem 2. (Power Rule 1)
\[
\prod_{v \in M_\mathbb{Q}} |x|_v = 1
\]
Proof. By the above note, there is only one archimedean absolute value, the absolute value we normally think of \( |x|_{\infty} = \max\{x, -x\} \). So

\[
\prod_{v \in \mathcal{M}_k} |x|_v = |x|_{\infty} \prod_{p \text{ prime}} |x|_p, \\
= |x|_{\infty} \prod_{p \text{ prime}} p^{-\operatorname{ord}_p(x)} \\
= |x|_{\infty} \cdot |x|^{-1}_{\infty} \\
= 1
\]

\[\square\]

**Definition 3.** A **number field** is finite extension of the rational numbers.

**Definition 4.** The **ring of integers** of a number field \( k \), denoted \( \mathcal{O}_k \), are the integral elements of \( k \). (The solutions to monic polynomials with coefficients in \( k \).)

A number field \( k \) has the archimedean absolute values for each embedding of \( k \) in \( \mathbb{C} \), \( \sigma : k \to \mathbb{C} \).

\[|x|_\sigma = |\sigma(x)|\]

Where \( |\sigma(x)| \) is the complex absolute value of \( \sigma(x) \). Since \( k \) has \( n \) distinct embeddings into \( \mathbb{C} \), \( k \) has \( n \) distinct archimedean absolute values where \( n = [k : \mathbb{Q}] \).

\( \mathcal{O}_k \) in \( k \) is the analog of \( \mathbb{Z} \) in \( \mathbb{Q} \) so we want something similar to the construction of nonarchimedean absolute values above with an absolute value for each prime. However, this situation is more complicated because \( \mathcal{O}_k \) is not necessarily a UFD. We use the fact that \( \mathcal{O}_k \) is a Dedekind domain and every fractional ideal has a unique primary factorization. [See A-M and Samuel]

With all of this we can construct a nonarchimedean absolute value for each prime ideal \( p \subseteq \mathcal{O}_k \). Let \( x \in \mathcal{O}_k \) then the fractional idea \( x\mathcal{O}_k \) has a unique primary factorization,

\[x\mathcal{O}_k = \prod p^{\operatorname{ord}_p(x)}\]

Using this we define the nonarchimedean absolute value

\[|x|_p = p^{-\operatorname{ord}_p(x)/\epsilon_p(p)}\]

where \( \epsilon_p(p) = \operatorname{ord}_p(p) \).

**Note 2.** The absolute values described above are the only absolute values on the number field \( k \) up to a "power."

**Definition 5.** The **normalized absolute value** associated to \( v \in \mathcal{M}_k \) is

\[\|x\|_v = |x|_v^{n_v} \]

where \( n_v = [k_v : \mathbb{Q}_v] \) and \( k_v \) is the completion of \( k \) with respect to the absolute value \( v \).
Theorem 6. (Power Rule 2)
\[ \prod_{v \in M_k} \|x\|_v = 1 \]

Proof. I’m not going to prove it, but it follows from the power rule on \( \mathbb{Q} \) using a lemma in Lang’s Algebra book and applied in his Number Theory book. \( \square \)

Definition 7. Let \( k \) be a number field, and \( P = [x_0, \ldots, x_n] \in \mathbb{P}^n(k) \). The \textbf{(multiplicative) height} of \( P \) (relative to \( k \)) is
\[ H_k(P) = \prod_{v \in M_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}. \]

The \textbf{logarithmic or additive height} is
\[ h_k(P) = \log H_k(P) = \sum_{v \in M_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}. \]

Lemma 8. Let \( k \) be a number field and let \( P \in \mathbb{P}^n(k) \).

(a) The height \( H_k(P) \) is independent of the choice of homogeneous coordinates for \( P \).
(b) \( H_k(P) \geq 1 \) (and \( h_k(P) \geq 0 \)) for all \( P \in \mathbb{P}^n(k) \).
(c) Let \( k' \) be a finite extension of \( k \). Then
\[ H_{k'}(P) = H_k(P)^{[k':k]}. \]

Proof. (a) Let \( P = [x_0, \ldots, x_n] \). Then any other choice of coordinates of \( P \) has the form \([cx_0, \ldots, cx_n]\) with \( c \in k^\times \). Then
\[ H_k([cx_0, \ldots, cx_n]) = \prod_{v \in M_k} \max\{\|cx_0\|_v, \ldots, \|cx_n\|_v\} \]
\[ = (\prod_{v \in M_k} \|c\|_v) \cdot (\prod_{v \in M_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}) \]
\[ = \prod_{v \in M_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\} \]

(b) Since \( P \in \mathbb{P}^n(k) \) we can take homogeneous coordinates such that one coordinate is equal to 1. Then \( H_k(P) \geq 1 \).
(c)
\[ H_k(P) = \prod_{w \in M'_k} \max\{\|x_0\|_w, \ldots, \|x_n\|_w\} \]
\[ = \prod_{v \in M_k} \prod_{w \in M'_{w,v}} \max\{\|x_0\|_w, \ldots, \|x_n\|_w\} \]
\[ = \prod_{v \in M_k} \prod_{w \in M'_{w,v}} \max\{x_0^n_w, \ldots, x_n^n_w\} \]

3
Now
\[ n_w = [k'_w : \mathbb{Q}_w] = [k'_w : k_v][k_v : \mathbb{Q}_v] = [k'_w : k_v]n_v \]
and there is a number theory lemma that says
\[ \sum_{w \in M_k} [k'_w : k_v] = [k' : k]. \]

Using this we have
\[ H_{k'}(P) = \prod_{v \in M_k} \prod_{w \in M_{k'}, w | v} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}^{[k'_w : k_v]} \]
\[ = \prod_{w \in M'_k} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}^{[k' : k]} \]
\[ = H_k(P)^{[k' : k]}. \]

**Note 3.** By the lemma(a) the previous definition is well defined.

I would like to add here, because it's as good of a time as any that the set
\[ \{P \in \mathbb{P}^n(\mathbb{Q}) | H_Q(P) \leq B\} \]
is finite for any positive bound \(B\). To prove this, choose homogeneous coordinates for \(P = (x_0, \ldots, x_n)\) such that \(x_0, \ldots, x_n \in \mathbb{Z}\) and \(\gcd(x_0, \ldots, x_n) = 1\) (i.e. clear denominators). Then for each prime number \(p \in \mathbb{Z}\) there will be one coordinate with "p-adic" absolute value 1 and the rest \(\leq 1\). So for each prime the maximum will be 1. So the last contributor is the one archimedean absolute value. \(H_Q(P) = \max\{\|x_0\|, \ldots, \|x_n\|\}\) and there are only finite many integers with absolute value (the normal one) \(\leq B\).

**Definition 9.** The absolute (multiplicative) height on \(\mathbb{P}^n\) is the function,
\[ H : \mathbb{P}^n(\mathbb{Q}) \to [1, \infty) \]
\[ H(P) = H_k(P)^{1/[k : \mathbb{Q}]} \]
where \(k\) is any number field such that \(P \in \mathbb{P}^n(k)\). The absolute (logarithmic) height on \(\mathbb{P}^n\) is the function,
\[ h : \mathbb{P}^n(\mathbb{Q}) \to [0, \infty) \]
\[ h(P) = \log H(P) = \frac{1}{[k : \mathbb{Q}]}h_k(P) \]
We also define the height of \(x \in k\) by using the corresponding point in \([x, 1] \in \mathbb{P}^n(k)\) where
\[ H(x) = H([x, 1]) \]
and we similarly define \(h(x), H_k(x), h_k(x)\).
Note 4. By the previous lemma(c) the above definition is well defined.

Proposition 10. The actions of the Galois group on $\mathbb{P}^n(\overline{\mathbb{Q}})$ leaves the height invariant. That is, let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and let $\sigma \in G_{\mathbb{Q}}$. Then $H(\sigma(P)) = H(P)$.

Proof. Let $k/\mathbb{Q}$ be a number field with $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. The automorphism $\sigma$ of $\overline{\mathbb{Q}}$ defines an isomorphism $\sigma : k \cong k_{\sigma}$. It likewise identifies the sets of absolute values on $k$ and $\sigma(k)$. More precisely

$$\sigma : M_k \cong M_{\sigma(k)}, \quad v \mapsto \sigma(v),$$

where $x \in k$ and $v \in m_k$. The absolute value $\sigma(v) \in M_{\sigma(k)}$ is defined by

$$|\sigma(x)|_{\sigma(v)} = |x|_v. \quad \sigma$$

also induces an isomorphism on completions, $k_v \cong \sigma(k)v$. It follows

$$H_{\sigma(k)}(\sigma(P)) = \prod_{w \in M_{\sigma(k)}} \max\{|\sigma(x_i)|_w\} = \prod_{w \in M_{\sigma(k)}} |\sigma(x_i)|_w^{n_w} = \prod_{v \in M_k} \max\{|\sigma(x_i)|_{\sigma(v)}\}^{\sigma(v)} = \prod_{v \in M_k} \max\{|x_i|_v\}^{n_v} = \prod_{v \in M_k} \max\{|x_i|_v\} = H_k(P)$$

We also have $[k : \mathbb{Q}] = [\sigma(k) : \mathbb{Q}]$ so by taking the correct root we have $H(\sigma(P)) = H(P)$. \hfill \blacksquare

Theorem 11. For any numbers $B, D \geq 0$, the set

$$\{ P \in \mathbb{P}^n(\overline{\mathbb{Q}}) | H(P) \leq B \text{ and } |Q(P) : \mathbb{Q}| \leq D \}$$

is finite.

Proof. Choose homogeneous coordinates for $P = (x_0, ..., x_n)$ such that some coordinate equals 1. Then for some number field $k$ such that $P \in \mathbb{P}^n(k)$ and any absolute value $v \in M_k$ and index $i$.

$$\max\{|x_0|_v, ..., |x_n|_v\} \geq \max\{|x_i|_v, 1\}$$

Multiplying over all $v$ and taking the appropriate root(raise to the $1/[k : \mathbb{Q}]$.)

$$H(P) \geq H(x_i)$$

5
for all $i$.

Claim: For each $1 \leq d \leq D$, the set

$$\{ x \in \mathbb{Q} | H(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d \}$$

is finite.

This claim will prove our theorem because if we bound $H(P)$ we bound $H(x)$. The fact that $\mathbb{Q}(P) \supset \mathbb{Q}(x)$ says that if we can show that there are only a finite number of $x$’s are possible to construct $P$ then we are finished.

Let $x \in \mathbb{Q}$ have degree $d$ and let $k = \mathbb{Q}(x)$. Let $x_1, ..., x_d$ be the conjugates of $x$ over $\mathbb{Q}$ and

$$F_x(T) = \prod_{j=1}^{d} (T - x_j) = \sum_{r=0}^{d} (-1)^r s_r(x) T^{d-r}$$

be the minimal polynomial of $x$ over $\mathbb{Q}$ where $s_r(x)$ is the r-th symmetric polynomial. For any absolute value $v \in M_k$,

$$|s_r(x)|_v = \sum_{1 \leq i_1 \leq ... \leq i_r \leq d} |x_{i_1}...x_{i_r}|_v \leq c(v, r, d) \max_{1 \leq i_1 \leq ... \leq i_r \leq d} |x_{i_1}...x_{i_r}|_v \leq c(v, r, d) \max |x_i|^r_v.$$

Where $c(v, r, d) = \binom{d}{r} \leq 2^d$ if $v$ is archimedean and $c(v, r, d) = 1$ otherwise.

This follows from the triangle inequality.

From this we have

$$\max\{|s_0(x)|_v, ..., |s_d(x)|_v\} \leq c(v, d) \prod_{i=1}^{d} \max\{|x_i|^v, 1\}^d.$$

where $c(v, d) = 2^d$ if $v$ is archimedean and $c(v, d) = 1$ otherwise. Now we multiply over all $v \in M_k$ and raise to the $1/[k : \mathbb{Q}]$ power to get

$$H(s_0(x), ..., s_d(x)) \leq 2^d \prod_{i=1}^{d} H(x_i)^d.$$

But the $x_i$’s are conjugates, so each $H(x_i)$ is equal. Hence

$$H(s_0(x), ..., s_d(x)) = 2^d H(x_i)^d.$$

Now suppose that $x$ is in the set

$$\{ x \in \mathbb{Q} | H(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d \}.$$
We have just proven that $x$ is a root of a polynomial $F_x(T) \in \mathbb{Q}[T]$ whose coefficients $s_0, \ldots, s_d$ satisfy

$$H(s_0, \ldots, s_d) \leq 2^d B^{d^2}.$$ 

But from earlier, $\mathbb{P}^d(\mathbb{Q})$ has only points of finite height. This means there are only finitely many possibilities for $s_0, \ldots, s_d$ and therefore only finitely many possibilities for the polynomial $F_x(T)$, hence only finitely many choices for $x$.

This proves are claim, hence proves our theorem. \hfill \square

**Proposition 12.** Let

$$S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N
\quad (x,y) \mapsto (x_0 y_0, x_0 y_1, \ldots, x_i y_j, \ldots, x_n y_m).$$

where $N = (n+1)(m+1) - 1$. Let $H_n$, $H_m$ and $H_N$ be hyperplanes in $\mathbb{P}^n$, $\mathbb{P}^m$ and $\mathbb{P}^N$ respectively.

(a) $S_{n,m}^*(H_N) \sim H_n \times \mathbb{P}^m + \mathbb{P}^n \times H_m \in \text{Div}(\mathbb{P}^n \times \mathbb{P}^m)$.

(b) $h(S_{n,m}(x,y)) = h(x) + h(y)$ for all $x \in \mathbb{P}^n(\mathbb{Q})$ and $y \in \mathbb{P}^m(\mathbb{Q})$.

(c) Let the map

$$\Phi_d : \mathbb{P}^n \to \mathbb{P}^N
\quad x \mapsto (M_0(x), \ldots, M_N(x))$$

be the $d$-uple embedding. (i.e. $N = \binom{n+d}{n+1} - 1$ and the collection $M_0(x), \ldots, M_N(x)$ is the complete collection of monomials of degree $d$ in the variables $x_0, \ldots, x_n$.) Then $h(\Phi_d(x)) = dh(x)$ for all $x \in \mathbb{P}^n(\mathbb{Q})$.

**Theorem 13.** Let $\phi : \mathbb{P}^n \to \mathbb{P}^m$ be a rational map of degree $d$ defined over $\mathbb{Q}$, so $\phi$ is given by a $(m+1)$-tuple $\phi = (f_0, \ldots, f_m)$ of homogeneous polynomials of degree $d$. Let $Z \subset \mathbb{P}^n$ be the subset of common zeros of the $f_i$’s. Notice that $\mathbb{P}^n \setminus Z$.

(a) We have

$$h(\phi(P)) \leq dh(P) + O(1) \text{ for all } P \in \mathbb{P}^n(\mathbb{Q}) \setminus Z.$$
(b) Let $X$ be a closed subvariety of $\mathbb{P}^n$ with the property that $X \cap Z = \emptyset$. (Thus $\phi$ defines a morphism $X \to \mathbb{P}^m$.) Then

$$h(\phi(P)) = dh(P) + O(1) \text{ for all } P \in X(\mathbb{Q})$$

**Corollary 14.** Let $A : \mathbb{P}^n \to \mathbb{P}^m$ be a linear map defined over $\mathbb{Q}$. In other words, $A$ is given by $m + 1$ linear forms $(L_0, ..., L_m)$. Let $Z \subset \mathbb{P}^n$ be the linear subspace where $L_0, ..., L_m$ simultaneously vanish, and let $X \subset \mathbb{P}^n$ be a closed subvariety with $X \cap Z = \emptyset$. Then

$$h(A(P)) = h(P) + O(1) \text{ for all } P \in X(\mathbb{Q}).$$

**Definition 15.** Let $\phi : V \to \mathbb{P}^n$ be a morphism. The (absolute logarithmic) height on $V$ relative to $\phi$ is the function

$$h_\phi : V(\mathbb{Q}) \to [0, \infty), \ h_\phi(P) = h(\phi(P)),$$

where $h : \mathbb{P}^n(\mathbb{Q}) \to [0, \infty)$ is the height function on projective space defined earlier.

**Theorem 16.** Let $V$ be a projective variety defined over $\mathbb{Q}$, let $\phi : V \to \mathbb{Q}^n$ and $\psi : V \to \mathbb{Q}^m$ be morphisms, and let $H$ and $H'$ be hyperplanes in $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively. Suppose that $\phi^*H$ and $\psi^*H'$ are linearly equivalent. Then

$$h_\phi(P) = h_\psi(P) + O(1) \text{ for all } P \in V(\mathbb{Q}).$$

Here the $O(1)$ constant will depend on $V, \phi$ and $\psi$, but independent of $P$.

**Theorem-Definition 17.** (Weil’s Height Machine) Let $k$ be a number field. For every smooth projective variety $V/k$ there exists a map

$$h_V : \text{Div}(V) \to \{ \text{functions } V(k) \to \mathbb{R} \}$$

with the following properties

(a) (Normalization) Let $H \subset \mathbb{P}^n$ be a hyperplane, and let $h(P)$ be the absolute logarithmic height on $\mathbb{P}^n$. Then

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1) \text{ for all } P \in \mathbb{P}^n(k).$$

(b) (Functorality) Let $\phi : V \to W$ be a morphism and let $D \in \text{Div}(W)$. Then

$$h_{V,\phi^*D}(P) = h_{W,D}(\phi(P)) + O(1) \text{ for all } P \in V(k).$$

(c) (Additivity) Let $D, E \in \text{Div}(V)$. Then

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1) \text{ for all } P \in V(k).$$
(d) (Uniqueness) The height functions $h_{V,D}$ are determined, up to $O(1)$, by normalization, functoriality just for embeddings $\phi : V \hookrightarrow \mathbb{P}^n$, and additivity.

(e) (Linear Equivalence) Let $D, E \in \text{Div}(V)$ with $D$ linearly equivalent to $E$. Then
$$h_{V,D}(P) = h_{V,E}(P) + O(1) \text{ for all } P \in V(\overline{k}).$$

(f) (Positivity) Let $D \in \text{Div}(V)$ be an effective divisor, and let $B$ be the base locus of the linear system $|D|$. Then
$$h_{V,D}(P) \geq O(1) \text{ for all } P \in (V \setminus B)(\overline{k}).$$

(g) (Algebraic Equivalence) Let $D, E \in \text{Div}(V)$ with $D$ ample and $E$ algebraically equivalent to 0. Then
$$\lim_{h_{V,D}(P) \to \infty} \frac{h_{V,E}(P)}{h_{V,D}(P)} = 0 \text{ where } P \in V(\overline{k})$$

(h) (Finiteness) Let $D \in \text{Div}(V)$ be ample. Then for every finite extension $k'/k$ and every constant $B$, the set
$$\{P \in V(k') | h_{V,D}(P) \leq B\}$$
is finite.

**Corollary 18.** Let $V/k$ be a smooth variety defined over a number field, let $D \in \text{Div}(V)$, and let $\phi : V \to V$ be a morphism. Suppose that $\phi^*D \sim \alpha D$ for some $n \geq 1$. Then there exists a constant $C$ such that
$$|h_{V,D}(\phi(P)) - \alpha h_{V,D}(P)| \leq C \text{ for all } P \in V(\overline{k}).$$

**Note 5.** The $O(1)$ here is dependent on the variety, divisor and morphism but not the points. It is possible to compute the $h_{V,D}$'s explicitly and to give bounds of $O(1)$ in terms of the defining equations the varieties, divisors and morphisms. However, it is difficult in practice to bound the $O(1)$'s.

**Theorem-Definition 19.** (Neron, Tate) Let $V/k$ be a smooth variety defined over a number field, let $D \in \text{Div}(V)$, and let $\phi : V \to V$ be a morphism. Suppose that $\phi^*D \sim \alpha D$ for some $n \geq 1$. Then there exists a unique function, called the **canonical height** on $V$ relative to $\phi$ and $D$,
$$\hat{h}_{V,\phi,D} : V(\overline{k}) \to \mathbb{R}$$
with the following two properties:

(i) $\hat{h}_{V,\phi,D}(P) = h_{V,D}(P) + O(1) \text{ for all } P \in V(\overline{k})$.  

9
(ii) \( \hat{h}_{V,\phi,D}(\phi(P)) = a\hat{h}_{V,\phi,D}(P) \) for all \( P \in V(\overline{k}) \).

The canonical height depends only on the linear equivalence class of \( D \). Further, it can be computed as the limit

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

where \( \phi^n \) is the \( n \)-th iterate of \( \phi \).

**Proof.** By the previous corollary there exists a constant \( C \) such that

\[
|h_{V,D}(\phi(Q)) - ah_{V,D}(Q)| \leq C \text{ for all } Q \in V(\overline{k}).
\]

Now take any point \( P \in V(\overline{k}) \). We prove the sequence \( \{\alpha^{-n}h_{V,D}(\phi^n(P))\} \) converges by showing it is Cauchy. Take \( n \geq m \) and

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

by a telescoping sum. Then

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

by the triangle inequality. Then

\[
\leq \sum_{i=m+1}^{n} \alpha^{-i}C
\]

from above and \( Q = \phi^{i-1}P \). Then

\[
\leq (\frac{\alpha^{-m} - \alpha^{-n}}{\alpha^{-1}})C.
\]

This quantity goes to 0 as \( n > m \to \infty \), which proves the sequence is Cauchy, hence converges. So we can define the \( \hat{h}_{V,\phi,D}(P) \) to be the limit

\[
\hat{h}_{V,\phi,D}(P) = \lim_{n \to \infty} \frac{h_{V,D}(\phi^n(P))}{\alpha^n}.
\]

To verify property (i), take \( m = 0 \) and let \( n \to \infty \) in the inequality above. This gives

\[
|\hat{h}_{V,Q,D}(P) - h_{V,D}(P)| \leq \frac{C}{\alpha - 1},
\]

which gives us the desired inequality.
Property (ii) follows directly from the limit definition of canonical height.

\[
\tilde{h}_{V, \phi, D}(\phi(P)) = \lim_{n \to \infty} \frac{h_{V, D}(\phi^n(\phi(P)))}{\alpha^n} = \lim_{n \to \infty} \frac{\alpha h_{V, D}(\phi^{n+1}(P))}{\alpha^{n+1}} = \alpha \tilde{h}_{V, \phi, D}(P).
\]

What’s left to prove is uniqueness. Let \( \tilde{h} \) and \( \tilde{h}' \) be two functions with properties (i) and (ii). Let \( g = \tilde{h} - \tilde{h}' \). Then (i) implies that \( g \) is bounded, say \( |g(P)| \leq C' \) for all \( P \in V(\overline{k}) \). While (ii) says that \( g \circ \phi = \alpha^n g \) for all \( n \leq 1 \). Hence

\[
|g(P)| = \frac{g(\phi^n(P))}{\alpha^n} \leq \frac{C'}{\alpha^n}
\]

where \( \frac{C'}{\alpha^n} \to 0 \) as \( n \to 0 \). This says that \( g(P) = 0 \) for all \( P \), so \( \tilde{h} = \tilde{h}' \). \( \square \)

**Definition 20.** Let \( S \) be a set and let \( \phi : S \to S \) be a function, for each \( n \geq 1 \) let \( \phi^n : S \to S \) denote the \( n \)-th iterate of \( \phi \). An element \( P \in S \) is called periodic for \( \phi \) if \( \phi^n(P) = P \) for some \( n \geq 1 \). It is called preperiodic for \( \phi \) if \( \phi^n(P) \) is periodic for some \( n \geq 1 \). Equivalently, \( P \) is preperiodic if its forward orbit

\[ \{ P, \phi(P), \phi^2(P), \phi^3(P), \ldots \} \]

is finite.

**Proposition 21.** Let \( \phi : V \to V \) be a morphism of a variety defined over a number field \( k \). Let \( D \in \text{Div}(V) \) be an ample divisor such that \( \phi^* D \sim \alpha D \) for some \( \alpha > 1 \), and let \( \tilde{h}_{V, \phi, D} \) be the associated canonical height.

(a) Let \( P \in V(\overline{k}) \). Then \( \tilde{h}_{V, \phi, D}(P) \geq 0 \), and

\[
\tilde{h}_{V, \phi, D}(P) = 0 \iff P \text{ is periodic for } \phi.
\]

(b) The Set

\[
\{ P \in V(k) \mid P \text{ is preperiodic for } \phi \}
\]

is finite.

**Proof.** (a) Since \( D \) is ample, we can choose a height function \( h_{V, D} \) with nonnegative values. Then by the definition, the canonical height is nonnegative.

Let \( P \in V(\overline{k}) \). Replacing \( k \) by a finite extension, we may assume that \( P \in V(k) \) and that \( D \) and \( \phi \) are defined over \( k \). Suppose that \( P \) is preperiodic for \( \phi \). Then the sequence \( \{ \phi^n P \}_{n \geq 1} \) repeats, therefore the sequence of heights \( \{ h_{V, D}(\phi^n P) \}_{n \geq 1} \) is bounded. Therefore

\[
\alpha^{-n} h_{V, D}(\phi^n P) \to 0
\]

11
as \( n \to 0 \). Therefore the canonical height \( \hat{h}_{V,\phi,D}(P) = 0 \).

Conversely, let \( \hat{h}_{V,\phi,D}(P) = 0 \). Then for any \( n \geq 1 \) we have

\[
\begin{align*}
    h_{V,D}(\phi^n P) &= \hat{h}_{V,\phi,D}(P) + O(1) \\
                     &= \alpha^n \hat{h}_{V,\phi,D}(P) + O(1) \\
                     &= O(1)
\end{align*}
\]

Note that all the points \( \phi^n P \) are in \( V(k) \). Therefore there is a constant \( B \) such that

\[
\{ P, \phi(P), \phi^2(P), \ldots \} \subset \{ Q \in V(k) | h_{V,D}(Q) \leq B \}
\]

because \( h_{V,D}(\phi^n P) \) is bounded. But \( D \) is ample, so there are only finitely many points in \( V(k) \) with bounded height. Hence the set \( \{ P, \phi(P), \phi^2(P), \ldots \} \) must be finite and therefore \( P \) is preperiodic for \( \phi \).