VOJTA'S CONJECTURE: MOTIVATION AND APPLICATIONS

COURSE: ANTHONY VÁRILLY-ALVARADO
NOTES: ROSS PATERSON

Disclaimer. These notes were taken live during lectures. In particular, any mistakes are the fault of the transcriber and not of the lecturer.

Lecture 1: Heights and Roth's Theorem

Let $K/\mathbb{Q}$ be a number field, $\mathcal{O}_K$ be the ring of integers, and let Ω_K be the set of places. We will write $\Omega)\infty \subseteq \Omega_K$ for the set of infinite places.

For each $v \in \Omega_K$ there is an associated completion K_v with an absolute value $|\cdot|_v$.

- If $K_v = \mathbb{R}$, then $v = \sigma : K \to \mathbb{R}$ and $|x|_v := |\sigma(x)|$ where $|\cdot|$ here on the right is the usual absolute value on $\mathbb{R}$.
- If $K_v = \mathbb{C}$ then $v = (\sigma, \overline{\sigma}) : K \to \mathbb{C}$ corresponds to a pair of complex conjugate embeddings and we write $|x|_v := |\sigma(x)|^2$, where $|\cdot|$ on the right is the usual absolute value on $\mathbb{C}$.
- If K_v is non-archimedean then $v = \mathfrak{p} \subseteq \mathcal{O}_K$ corresponds to a prime ideal and we take
$$|x|_v := [\mathcal{O}_K : \mathfrak{p}]^{-\mathrm{ord}_\mathfrak{p}(x)} = p^{-f \cdot \mathrm{ord}_\mathfrak{p}(x)},$$
where $f_\mathfrak{p}$ is the inertia degree, and $\mathfrak{p} \mid p$.

From this we have a product formula globally: for $x \in K^\times$
$$\prod_{v \in \Omega_K} |x|_v = 1.$$

Definition 1. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$ with $x_i \in K$. Define the *relative exponential height* of P to be
$$H_K(P) = \prod_{v \in \Omega_K} \max\{|x_0|_v, \ldots, |x_n|_v\}.$$

Note that the product formula implies that this is well defined (i.e. independent of the choice of representative x_i's).

Example 2. Take $K = \mathbb{Q}$ and $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{Q})$ where we have chosen x_i to be integers such that $\gcd(x_0, \ldots, x_n) = 1$. Then
$$H_\mathbb{Q}(P) = \max\{|x_0|, \ldots, |x_n|\},$$
where $|\cdot|$ on the right is the usual absolute value on $\mathbb{Q} \subseteq \mathbb{R}$.

For example, for $n = 1$ we have $H_\mathbb{Q}([1, 2]) = 2$ and $H_\mathbb{Q}([1, \frac{201}{100}]) = H_\mathbb{Q}([100, 201]) = 201$.

This does seem nice, this height seems to be capturing a notion of arithmetic complexity. However, there is a major issue! If L/K is a finite extension then for a point $P \in \mathbb{P}^n(K)$ we get

$$H_L(P) = H_K(P)^{[L:K]},$$

because for each $v \in \Omega_K$

$$\sum_{\substack{w \in \Omega_L \\ w \mid v}} [L_w : K_v] = [L : K].$$

So height seems to depend on a choice of field to look over. However there is a sensible solution, since these are so closely related.

Definition 3. Define the absolute exponential height of $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ to be

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]},$$

for any K such that $P \in \mathbb{P}^n(K)$. The logarithmic height is defined to be

$$h_K(P) := \log H_K(P) \text{ (relative)};$$
$$h(P) := \log H(P) \text{ (absolute)}.$$

We now consider some special cases.

Example 4. $K = \mathbb{Q}$, then $h(P) = h_{\mathbb{Q}}(P) = \log \max \{|X_0|, \dots, |x_n|\}$. If one things about $\log_2$ then this is essentially telling us the number of bits used to store all of the coordinates of P on a computer.

Example 5. $n = 1$, then if $x \in K$ we define $h(x) := h([x, 1])$ where $[x, 1] \in \mathbb{P}^1(K)$. We have

$$h(x) = \log\left(\prod_{v \in \Omega_K} \max\{|x|_v, 1\}\right) = \sum_{v \in \Omega_K} \log^+ |x|_v,$$

where $\log^+(a) := \max\{\log(a), 0\}$.

Theorem 6 (Northcott Finiteness)**.** *Fix $B \in \mathbb{R}_{>0}$ and $d \in \mathbb{Z}_{\geq 1}$. Then the set*

$$\left\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \ : \ H(P) \leq B, \ [\mathbb{Q}(P), \mathbb{Q}] \leq d\right\}$$

is finite.

Remark 7. Here by $\mathbb{Q}(P)$ we mean the residue field of P, i.e.

$$\mathbb{Q}(P) = \mathbb{Q}\left(\frac{x_0}{x_j}, \dots, \frac{x_n}{x_j}\right)$$

for any j such that $x_j \neq 0$.

Diophantine Approximation

Theorem 8 (Dirichlet, 1842)**.** *For $\alpha \in \mathbb{R} \backslash \mathbb{Q}$, there are infinitely many rational approximations $\frac{p}{q} \in \mathbb{Q}$ (with $\gcd(p, q) = 1$) such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

We should contrast this with a result of Louiville from 2 years later!

Theorem 9 (Louiville, 1844). *For $\alpha \in \overline{\mathbb{Q}}$ with $d := [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$ and fixed $\varepsilon > 0$, there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ (with $\gcd(p, q) = 1$) such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\varepsilon}}.$$

Highlight improvements on Louivilles result are:

(1) (Thue, 1909): $q^{\frac{1}{2}d+1+\varepsilon}$;
(2) (Siegel, 1921): $q^{2\sqrt{d}+\varepsilon}$;
(3) (Gelfand–Dyson, 1947): $q^{\sqrt{2d}+\varepsilon}$;
(4) (Roth, 1955): $q^{2+\varepsilon}$.

Example 10. Here is an application of Roth's result. Consider $x^3 - 7y^3 = 19$, then there are finitely many solutions with $(x, y) \in \mathbb{Z}$. Indeed, if $|x|$ or $|y|$ is large in absolute value (note that if one is large then so is the other, because 19 is not varying), then $\frac{x}{y} \sim \sqrt[3]{7}$. i.e.

$$\begin{aligned}\left|\frac{x}{y} - \sqrt[3]{7}\right| &= \left|\frac{19/y^3}{\left(\frac{x}{y}\right)^2 + \frac{x}{y}\sqrt[3]{7} + \sqrt[3]{49}}\right| \\ &= \left|\frac{19}{y(x^2 + \sqrt[3]{7}x + \sqrt[4]{49})}\right| \\ &\ll \frac{1}{y^3}.\end{aligned}$$

Roth with $\varepsilon = 1$ tells us that there are only finitely many $x/y \in \mathbb{Q}$ that can achieve this. Note that we are using that x, y being a solution must be coprime!

A generalisation of Roth's theorem is known.

Theorem 11. *Let K be a number field, $S \subseteq \Omega_K$ be a finite set of places such that $S \supseteq \Omega_\infty$. Fix $\alpha \in \overline{\mathbb{Q}}$, $\varepsilon > 0$, $C > 0$. Then there are finitely many $x \in K$ such that*

$$\prod_{v \in S} \min\{1, |x - \alpha|_v\} \leq \frac{C}{H_K(x)^{2+\varepsilon}} \tag{1}$$

Take logs of (1), to get

$$\sum_{v \in S} \log \min\{1, |x - \alpha|_v\} \leq \log(C) - (2 + \varepsilon)h_K(x)$$

Multiplying by -1 we get

$$-\sum_{v \in S} \log \min\{1, |x - \alpha|_v\} \geq -\log(C) + (2 + \varepsilon)h_K(x)$$

and hence

$$\sum_{v \in S} \max\left\{0, \log\left|\frac{1}{x - \alpha}\right|_v\right\} \geq (2 + \varepsilon)h_K(x) - \log(C),$$

so dividing by $[K : \mathbb{Q}]$ we get

$$\frac{1}{[K : \mathbb{Q}]} \sum_{v \in S} \log^+ \left|\frac{1}{x - \alpha}\right|_v \geq (2 + \varepsilon)h(x) - \frac{\log(C)}{[K : \mathbb{Q}]}.$$

Now reverse the logic, and rewrite the last term with just some constant, to obtain the following.

Theorem 12. *Let K be a number field and fix a finite set S with $\Omega_\infty \subseteq S \subseteq \Omega_K$. Fix $\alpha \in K$, $\varepsilon > 0$, $C \in \mathbb{R}$. Then for all but finitely many $x \in K$ we have*

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S}\log^+\left|\frac{1}{x-\alpha}\right|_v \le (2+\varepsilon)h(x) + C$$

Lecture 2: One Variable Nevonlinna Theory

Goal: Study the distributon of values of a meromorphic function

$$f : \mathbb{C} \to \overline{\mathbb{C}} := \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C}).$$

If f is a polynomial then in fact $f(z) = a$ has $\deg(f)$-many solutions z counted with multiplicity. What if f is some transcendental function? For example, $f(z) = e^z$. Here, $e^z = a$ has infinitely many solutions if $a \neq 0, \infty$, and no solutions if $a = 0, \infty$.

Definition 13. Let $f : \mathbb{C} \to \overline{\mathbb{C}}$ be meromorphic, and fix $r > 0$ and $a \in \mathbb{C}$. Then the *counting function* of f is:

$$n_f(r,a) = \#\left\{ z \ : \ \substack{|z|<r \\ f(z)=a \\ \text{counted with multiplicity}} \right\}$$

counted with multiplicity. We also define

$$n_f(0,a) = \text{multiplicity of } f(z)-a \text{ at zero (w/ mult)}$$
$$n_f(r,\infty) = \text{number of poles of } f(z) \text{ in } |z|<r \text{ (w/ mult)}$$

Recall the argument principle:

$$n_f(r,a) - n_f(r,\infty) = \frac{1}{2\pi i}\int_{|z|=r}\frac{f'(z)}{f(z)-a} \tag{2}$$

Exercise 14. Use Cauchy–Riemann in the form $\frac{\partial f}{\partial r} = \frac{1}{ir}\frac{\partial f}{\partial \theta}$ to show that the right hand side of (2) equals

$$\frac{r}{2\pi}\frac{d}{dr}\int_{-\pi}^{\pi}\log\left|f(re^{i\theta}-a)\right|d\theta.$$

Our running assumption today is htat $f(0) \neq a, \infty$. Take the argument principal, assuming the exercise, to write

$$n_f(t,a) - n_f(t,\infty) = \frac{t}{2\pi}\int_{-\pi}^{\pi}\log\left|f(te^{i\theta}-a)\right|d\theta.$$

Divide by t and integrate with respect to t to get

$$\int_0^r n_f(t,a)\frac{dt}{t} - \int_0^r n_f(t,\infty)\frac{dt}{t} = \frac{1}{2\pi}\int_{-\pi}^{\pi}\log\left|f(re^{i\theta}-a)\right|d\theta - \log|f(0)-a|.$$

We define

$$N_f(r,a) := \int_0^r n_f(t,a)\frac{dt}{t}$$

and similarly $N_f(r,\infty)$, and refer to these as integrated counting functions. This is Jensen's formula (or a version of it), and we can break up the right hand side a little more by using $\log|x| = \log^+|x| - \log^+\left|\frac{1}{x}\right|$, so that the formula becomes

$$N_f(r,a) - N_f(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi}\log^+\left|f(re^{i\theta})-a\right|d\theta - \frac{1}{2\pi}\int_{-\pi}^{\pi}\log^+\left|\frac{1}{f(re^{i\theta})-a}\right|d\theta + O(1)$$

as $r \to \infty$.

Definition 15. Define the proximity function of f to be

- $m_f(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \left|f(re^{i\theta})\right| d\theta$
- $m_f(r,a) = m_{\frac{1}{f-a}}(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \frac{1}{|f(re^{i\theta})-a|} d\theta$

Informally, note that:

- the main contributions to $m_f(r,a)$ come from z on the circle of radius r such that $f(z)$ is close to a.
- $m_f(r,a)$ is "average proximity of $f(z)$ to a on $|z|=r$".

Exercise 16. Use $\log^+|x \pm y| \leq \log^+|x| + \log^+|y| + 2$ for $x,y \in \mathbb{R}$ to show that

$$m_f(r,\infty) = m_{f-a}(r,\infty) + O(1).$$

Hence we can rewrite Hensen's formula:

$$N_f(r,a) - N_f(r,\infty) = m_{f-a}(r,\infty) - m_f(r,a) + O(1)$$

and obtain

$$N_f(r,\infty) + m_f(r,\infty) = N_f(r,a) + m_f(r,a) + O(1).$$

We define the characteristic function of f (Vojta calls this the height function of f) to be

$$T_f(r) := N_f(r,\infty) + m_f(r,\infty).$$

This is cool because the left hand side does not depend on a, but the right hand side appears to! Note, however, that our error has some f and a dependence. Hence we have proved the first main theorem of Nevanlinna theory.

Theorem 17 (First main theorem of Nevanlinna theory)**.** *If $f : \mathbb{C} \to \overline{\mathbb{C}}$ is meromorphic then*

$$T_f(r) = N_f(r,a) + m_f(r,a) + O(1)$$

for $a \in \mathbb{C}$, where the error may depend on f and a but is independent of r as $r \to \infty$.

Example 18. $f(z) = z^d$, then show that $T_f(r) = d\log(r)$. If $f(z)$ is rational then show that $T_f(r) = O(\log(r))$. If $f(z) = e^z$ then $T_f(r) = \frac{r}{\pi}$.

Theorem 19 (Second main theorem of Nevanlinna theory)**.** *Let $f : \mathbb{C} \to \overline{\mathbb{C}}$ be meromorphic. Fix $a_1, \ldots, a_n \in \mathbb{C}$ distinct elements. Then*

$$\sum_{i=1}^{n} m_f(r,a_i) \leq_{\text{exc}} 2T_f(r) + O\left(\log^+ T_f(r)\right) - o(\log(r))$$

as $r \to \infty$. Here the $\leq_{\text{exc}}$ means that the inequality holds for $r > 0$ outwith a set of finite Lebesgue measure. In particular,

$$\sum_{i=1}^{n} m_f(r,a_i) \leq_{\text{exc}} (2+\varepsilon)T_f(r) + C$$

for any $\varepsilon > 0$ and $C \in \mathbb{R}$.

Remark 20. When $n=1$ we will see a direct analogy to Roth's theorem, and so this gives us a higher dimensional analogy by which Vojta's conjecture will be inspired!

Complex World	Number Theory World
$f : \mathbb{C} \to \overline{\mathbb{C}}$ meromorphic	infinite subset of K
$f\|_{D(r)}$ or just r	$x \in K$
θ	$v \in S$
$\left\|f(re^{i\theta})\right\|$	$\|x\|_v$
$\mathrm{ord}_z(f)$	$\mathrm{ord}_v(x)$
$\log \frac{r}{\|z\|}$	$\log[\mathcal{O}_K : \mathfrak{p}]$
$m_f(r,a) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \left\|\frac{1}{f(re^{i\theta})-a}\right\| d\theta$	$m_S(x,a) := \sum_{v\in S} \log^+ \left\|\frac{1}{x-a}\right\|_v$
$m_f(r,\infty) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \log^+ \left\|f(re^{i\theta})\right\| d\theta$	$m_S(x) := \sum_{v\in S} \log^+ \|x\|_v$

Table 1. Vojta's dictionary

Vojta's vision

Let K be a number field and S be a finite set of places containing the archimedean places. We introduce Vojta's dictionary.

Look at what happens if we take the second equation from the Second main theorem (with $n = 1$)!

$$\sum_{v\in S} \log^+ \left|\frac{1}{x-a}\right|_v \leq_{\text{exc}} (2+\varepsilon)h_K(x) + C$$

where we have added $T_f(r) \leftrightarrow h_K(x)$ to our dictionary and the $\leq_{\text{exc}}$ means now away from finitely many x.