Heights of rational fractions and interpolation

Jean Kieffer
Supervision: D. Robert, A. Page

Journées Nationales de Calcul Formel
Luminy, 2–6 March 2020

LFANT team, IMB (Univ. Bordeaux)

Heights over the rationals

- For $\alpha \in \mathbb{Q}$, write $\alpha = \dfrac{p}{q}$ with p, q coprime.

$$h(\alpha) = \log \max\{|p|, |q|\}.$$

- For $F \in \mathbb{Q}(X)$, write $F = \dfrac{P}{Q}$ with $P, Q \in \mathbb{Z}[X]$ coprime.

$$h(F) = \max\{\log |c| : c \text{ nonzero coefficient of } P \text{ or } Q\}.$$

- $\deg F = \max\{\deg P, \deg Q\}$.

Example

$$h\left(\frac{103X^3 + 653X^2 + 383X + 175}{268X^3 + 197X^2 + 237X + 21}\right) = \log(653) = 6.48\cdots$$

Posing the problem

If $h(F)$ and $h(x)$ are known, it is easy to bound $h(F(x))$.

Question

Let $F \in \mathbb{Q}(X)$ of degree d. Let $x_1, \ldots x_N \in [\![0, D]\!]$ distinct that are not poles of F. Assume that

$$h(F(x_i)) \leq H \quad \text{for every } i.$$

What can we say about $h(F)$?

- When N is minimal ($d + 1$ or $2d + 1$): analyze the interpolation algorithm (well known).
- Better bounds when N is larger?

Remarks

- Easier for polynomials.
- Generalized to $[\![A, B]\!]$, number fields.

Plan

1. The case of polynomials

2. Ideas of proof

3. The case of rational fractions

The case of polynomials

Lagrange interpolation

Proposition

Let $P \in \mathbb{Q}[X]$ of degree $d \geq 1$, and $x_1, \ldots, x_{d+1} \in [\![0, D]\!]$ distinct. Assume that $h(P(x_i)) \leq H$ for every i. Then

$$h(P) \leq (d+1)H + D\log(D) + d\log(2D) + \log(d+1).$$

Height bound is multiplied by the degree.

Remarks on Lagrange interpolation

Height bound is multiplied by the degree.

- We cannot hope to do better in general:

x_i	1	2	3	4	5
$P(x_i)$	$\frac{261}{758}$	$\frac{496}{543}$	$\frac{16}{143}$	$\frac{683}{258}$	$\frac{278}{495}$

  gives

$$P(X) = -\frac{480830812799}{911120942160}X^4 + \frac{552317768903}{91112094216}X^3 + \cdots$$

- However, we actually see the huge coefficients when we add an evaluation point:

$$P(0) = -\frac{360058657852}{18981686295}.$$

Using more evaluation points

Proposition

Let $P \in \mathbb{Q}[X]$ of degree $d \geq 1$, and $x_1, \ldots, x_{2d} \in [\![0, D]\!]$ distinct. Assume that $h(P(x_i)) \leq H$ for every i. Then

$$h(P) \leq 2H + D\log(D) + d\log(2D) + \log(d+1)$$

Using twice the number of points gives a linear bound on $h(P)$.

Ideas of proof

Alternative definition of heights

- Let $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ not all zero. The projective height of $(\alpha_1 : \cdots : \alpha_n)$ is

$$h(\alpha_1 : \cdots : \alpha_n) = \sum_{v \in \mathcal{P} \cup \{\infty\}} \log \max\{|\alpha_i|_v : 1 \leq i \leq n\}.$$

- For $F \in \mathbb{Q}(X)$, the height $h(F)$ is the projective height of the tuple formed by all the coefficients of F.

Examples

- For $\alpha = p/q \in \mathbb{Q}$,

$$h(\alpha) = h(\alpha : 1) = h(p : q) = \log \max\{|p|, |q|\}.$$

- For $P = \sum_{i=0}^{d} c_i X^i \in \mathbb{Q}[X]$,

$$h(P) = \sum_v \log \max\{1, |P|_v\}, \quad |P|_v = \max\{|c_i|_v : 0 \leq i \leq d\}.$$

Lagrange interpolation

Proposition

Let $P \in \mathbb{Q}[X]$ of degree $d \geq 1$, and $x_1, \ldots, x_{d+1} \in [\![0, D]\!]$ distinct. Assume that $h(P(x_i)) \leq H$ for every i. Then

$$h(P) \leq (d+1)H + D\log(D) + d\log(2D) + \log(d+1).$$

Proof.

Lagrange: $P = \sum_{i=1}^{d+1} \frac{\prod_{k \neq i}(X - x_k)}{\prod_{k \neq i}(x_i - x_k)} P(x_i).$

- v archimedean: $|P|_v \leq (d+1)2^d D^d \prod_{i=1}^{d+1} \max\{1, |P(x_i)|_v\}$
- v nonarchimedean: $|P|_v \leq \left|\frac{1}{D!}\right|_v \prod_{i=1}^{d+1} \max\{1, |P(x_i)|_v\}.$

Sum all contributions to conclude. □

Using more evaluation points

Proposition

Let $P \in \mathbb{Q}[X]$ of degree $d \geq 1$, and $x_1, \dots, x_{2d} \in [\![0, D]\!]$ distinct. Assume that $h(P(x_i)) \leq H$ for every i. Then

$$h(P) \leq 2H + D\log(D) + d\log(2D) + \log(d+1)$$

Sketch of proof.

If v is nonarchimedean, then $|P(x_i)|_v \geq |D! \cdot P|_v$ for at least d values of i (Lagrange).

Therefore

$$\log\max\{1, |P|_v\} \leq \log\left|\frac{1}{D!}\right|_v + \frac{1}{d}\sum_{i=1}^{2d}\log\max\{1, |P(x_i)|_v\}. \quad \square$$

The case of rational fractions

Fractional interpolation

Proposition

Let $F \in \mathbb{Q}(X)$ of degree $d \geq 1$, and let $x_1, \ldots, x_{2d+1} \in [\![0, D]\!]$ distinct that are not poles of F. Assume that $h(P(x_i)) \leq H$ for every i. Then

$$h(F) \leq (d+1)(2d+1)H + (d+1)D\log(D) + (4d^2+3d)\log(2D) + (2d+2)\log(2d+1)$$

Remark

We cannot hope for better in general: when interpolating the same values as before by a fraction of degree 2, we obtain

$$F = \frac{22062125284572X^2 + \cdots}{57777551642321X^2 + \cdots}$$

Fractional interpolation: sketch of proof

Proof.

- Let A be the polynomial interpolating the points $(x_i, F(x_i))$:

$$h(A) \leq (2d+1)H + \cdots$$

- Let $Z = \prod_{i=1}^{2d+1}(X - x_i)$:

$$h(Z) \leq (2d+1)\log(2D).$$

- Write a Bézout relation for the d-th subresultant of A and Z:

$$QA + RZ = P.$$

  Height estimates on subresultants give

$$\max\{h(P), h(Q)\} \leq (d+1)(2d+1)H + \cdots$$

- $F = P/Q$. □

Better bounds using more evaluation points

Question

Can we obtain better height bounds on F when $h(F(x)) \leq H$ for more than $2d+1$ evaluation points?

Problems

- No simple formula as was the case for Lagrange interpolation.
- Simplifications can occur: imagine the case where $F = P/Q$, with $P, Q \in \mathbb{Z}[X]$ coprime, has large height. Then $P(x_i)$ and $Q(x_i)$ are large (most of the time), but it could be that

$$F(x_i) = \frac{P(x_i)}{Q(x_i)}$$

is a very small rational number.

Proposition

Let $F \in \mathbb{Q}(X)$ of degree $d \geq 1$. Let $S \subset [\![0, D]\!]$ containing at least $2D/3$ elements and no poles of F.

Let $H \geq \max\{3, \log(2D)\}$, and assume that:

1. $h(F(x)) \leq H$ for every $x \in S$.
2. $D > \max\{d^4 H \log(dH), 6d\}$.

Then

$$h(F) \leq 3H + C \log(dH) + 3d \log(2D)$$

where C is an absolute constant.

Sketch of proof

Write $F = P/Q$ with $P, Q \in \mathbb{Z}[X]$ coprime, and

$$F(x_i) = \frac{n_i}{d_i}, \quad P(x_i) = n_i s_i, \quad Q(x_i) = d_i s_i.$$

Idea: show that cancellations cannot happen too often, i.e. s_i is (at least) sometimes small.

- The s_i must divide $r = \mathrm{Res}(P, Q)$. By fractional interpolation,

$$\max\{h(P), h(Q)\} \leq Cd^2 H + \cdots, \quad \text{so}$$
$$h(r) \leq Cd^3 H + \cdots$$

- For each prime $p|r$, estimate carefully the number of times that P (or Q) can vanish mod p. We obtain

$$\log\left(\prod s_i\right) \leq C(d^4 H \log(D) + D\log(dH)).$$

- Since we have $d^4 H$ evaluation points, we can conclude. □

Conclusion

- **Corollary:** if $F \in \mathbb{Q}(X)$ of degree $d \geq 1$ has the property that

$$h(F(x)) = O(d\, h(x))$$

  for every x, then $h(F) = O(d \log(d))$.
- **Application:** height bounds for modular equations in a very general setting.
- The result about fractions seems suboptimal: would a smaller number of evaluation points, say $O(d)$, be sufficient?

Questions and remarks

Thank you!