Jacobi 多様体上の標準高さに関するアルゴリズム

内田　幸寛

首都大学東京 大学院理工学研究科 数理情報科学専攻

数学ソフトウェアとフリードキュメント XIX
2014 年 9 月 24 日

目次

目次

本講演の内容

講演者のウェブページ

`http://www.comp.tmu.ac.jp/y-uchida/programs/`

にある，種数 2 の曲線の Jacobi 多様体上の高さに関するプログラムの解説.

プログラムの内容：

- 単純な高さと標準高さとの差の評価
  - 区間演算により厳密な大域的最適化を行う.
  - C++ライブラリ Boost, CLN, GiNaC を利用している.
- 標準高さの計算
  - C++ライブラリ CLN, GiNaC を利用している.

本講演の内容

講演者のウェブページ

`http://www.comp.tmu.ac.jp/y-uchida/programs/`

にある，種数 2 の曲線の Jacobi 多様体上の高さに関するプログラムの解説.

プログラムの内容：

- 単純な高さと標準高さとの差の評価
  - 区間演算により厳密な大域的最適化を行う.
  - C++ライブラリ Boost, CLN, GiNaC を利用している.
- 標準高さの計算
  - C++ライブラリ CLN, GiNaC を利用している.

高さとは？

高さ (height)……数論的対象の「複雑さ」を測る量

有理数 $\frac{a}{b}$ $(\gcd(a,b)=1)$ の高さは

$$H\left(\frac{a}{b}\right)=\max\{|a|,|b|\}$$

で定義される.

例

$H\left(\frac{2}{3}\right)=3$, $H\left(\frac{1}{10000}\right)=10000$.

$\frac{1}{10000}$ は $\frac{2}{3}$ よりも「複雑」である.

高さとは？

高さ (height)……数論的対象の「複雑さ」を測る量

有理数 $\frac{a}{b}$ $(\gcd(a,b)=1)$ の高さは

$$H\left(\frac{a}{b}\right)=\max\{|a|,|b|\}$$

で定義される.

例

$H\left(\frac{2}{3}\right)=3$, $H\left(\frac{1}{10000}\right)=10000$.

$\frac{1}{10000}$ は $\frac{2}{3}$ よりも「複雑」である.

高さとは？

高さ (height)……数論的対象の「複雑さ」を測る量

有理数 $\frac{a}{b}$ $(\gcd(a,b)=1)$ の高さは

$$H\left(\frac{a}{b}\right)=\max\{|a|,|b|\}$$

で定義される.

例

$H\left(\frac{2}{3}\right)=3$, $H\left(\frac{1}{10000}\right)=10000$.

$\frac{1}{10000}$ は $\frac{2}{3}$ よりも「複雑」である.

高さとは？

高さ (height)……数論的対象の「複雑さ」を測る量

有理数 $\frac{a}{b}$ $(\gcd(a,b)=1)$ の高さは

$$H\left(\frac{a}{b}\right)=\max\{|a|,|b|\}$$

で定義される.

例

$H\left(\frac{2}{3}\right)=3$, $H\left(\frac{1}{10000}\right)=10000$.

$\frac{1}{10000}$ は $\frac{2}{3}$ よりも「複雑」である.

有限性

定理

任意の実数 $B > 0$ に対し，集合

$$\{x \in \mathbb{Q} \mid H(x) \leq B\}$$

は有限集合である.

実際，分子・分母が有限個に限られるから，有理数 x も有限個である.
この定理はより一般の状況に拡張され（Northcott の定理），
次のような有限性定理の証明に用いられる.

- Mordell-Weil の定理
- Faltings の定理（Mordell 予想）

有限性

定理

任意の実数 $B > 0$ に対し，集合

$$\{x \in \mathbb{Q} \mid H(x) \leq B\}$$

は有限集合である.

実際，分子・分母が有限個に限られるから，有理数 x も有限個である.

この定理はより一般の状況に拡張され（Northcott の定理），
次のような有限性定理の証明に用いられる.

- Mordell-Weil の定理
- Faltings の定理（Mordell 予想）

有限性

定理

任意の実数 $B > 0$ に対し，集合

$$\{x \in \mathbb{Q} \mid H(x) \leq B\}$$

は有限集合である.

実際，分子・分母が有限個に限られるから，有理数 x も有限個である.
この定理はより一般の状況に拡張され（Northcott の定理），
次のような有限性定理の証明に用いられる.

- Mordell-Weil の定理
- Faltings の定理（Mordell 予想）

種数 2 の曲線と Jacobi 多様体

次の式で定義される，種数 2 の代数曲線を考える．

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0 \quad (f_i \in \mathbb{Z}).$$

ただし，$f_6 \neq 0$ または $f_5 \neq 0$ であり，右辺は重根を持たないとする．

∞^+, ∞^- ：C の無限遠点（$\mathbb{Q}$ 上定義されているとは限らない）

J ：C の Jacobi 多様体
J の有理点全体 $J(\mathbb{Q})$ に対し，次の群同型が存在する．

$$J(\mathbb{Q}) \cong \{D = (P_1) + (P_2) - (\infty^+) - (\infty^-) \mid P_1, P_2 \in C(\bar{\mathbb{Q}}),$$
$$D \text{ は } \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \text{ の作用で不変 } \}/(\text{線型同値}).$$

（D は C 上の因子であり，右辺は形式的な和である．）

種数 2 の曲線と Jacobi 多様体

次の式で定義される，種数 2 の代数曲線を考える．

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0 \quad (f_i \in \mathbb{Z}).$$

ただし，$f_6 \neq 0$ または $f_5 \neq 0$ であり，右辺は重根を持たないとする．
∞^+, ∞^- ：C の無限遠点（$\mathbb{Q}$ 上定義されているとは限らない）

J ：C の Jacobi 多様体
J の有理点全体 $J(\mathbb{Q})$ に対し，次の群同型が存在する．

$$J(\mathbb{Q}) \cong \{D = (P_1) + (P_2) - (\infty^+) - (\infty^-) \mid P_1, P_2 \in C(\bar{\mathbb{Q}}),\ D \text{ は } \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \text{ の作用で不変 }\}/(\text{線型同値}).$$

（D は C 上の因子であり，右辺は形式的な和である．）

種数 2 の曲線と Jacobi 多様体

次の式で定義される，種数 2 の代数曲線を考える．

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0 \quad (f_i \in \mathbb{Z}).$$

ただし，$f_6 \neq 0$ または $f_5 \neq 0$ であり，右辺は重根を持たないとする．
∞^+, ∞^-：C の無限遠点（$\mathbb{Q}$ 上定義されているとは限らない）

J：C の Jacobi 多様体
J の有理点全体 $J(\mathbb{Q})$ に対し，次の群同型が存在する．

$$J(\mathbb{Q}) \cong \{D = (P_1) + (P_2) - (\infty^+) - (\infty^-) \mid P_1, P_2 \in C(\bar{\mathbb{Q}}),$$
$$D \text{ は } \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \text{ の作用で不変 } \}/(\text{線型同値}).$$

（D は C 上の因子であり，右辺は形式的な和である．）

Mordell-Weil の定理

定理 (Mordell-Weil)

$J(\mathbb{Q})$ は有限生成 Abel 群である．すなわち，

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\text{有限 Abel 群}).$$

r を $J(\mathbb{Q})$ の階数という．

$J(\mathbb{Q})$ の生成元を求める問題を考える．
通常，これは次の 2 つの手順に分かれる．

1. $J(\mathbb{Q})/2J(\mathbb{Q})$ などを計算し，$J(\mathbb{Q})$ の階数 r を求める．
   （常に計算が停止するアルゴリズムは知られていない．）
2. 無限降下法 (infinite descent) によって $J(\mathbb{Q})$ の生成元を求める．
   $\rightsquigarrow$ 高さの計算が必要．

Mordell-Weil の定理

定理 (Mordell-Weil)

$J(\mathbb{Q})$ は有限生成 Abel 群である．すなわち，

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\text{有限 Abel 群}).$$

r を $J(\mathbb{Q})$ の階数という．

$J(\mathbb{Q})$ の生成元を求める問題を考える．
通常，これは次の 2 つの手順に分かれる．

1. $J(\mathbb{Q})/2J(\mathbb{Q})$ などを計算し，$J(\mathbb{Q})$ の階数 r を求める．
   （常に計算が停止するアルゴリズムは知られていない．）
2. 無限降下法 (infinite descent) によって $J(\mathbb{Q})$ の生成元を求める．
   $\rightsquigarrow$ 高さの計算が必要．

Mordell-Weil の定理

定理 (Mordell-Weil)

$J(\mathbb{Q})$ は有限生成 Abel 群である．すなわち，

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\text{有限 Abel 群}).$$

r を $J(\mathbb{Q})$ の階数という．

$J(\mathbb{Q})$ の生成元を求める問題を考える．
通常，これは次の 2 つの手順に分かれる．

1. $J(\mathbb{Q})/2J(\mathbb{Q})$ などを計算し，$J(\mathbb{Q})$ の階数 r を求める．
   （常に計算が停止するアルゴリズムは知られていない．）
2. 無限降下法 (infinite descent) によって $J(\mathbb{Q})$ の生成元を求める．
   $\rightsquigarrow$ 高さの計算が必要．

Mordell-Weil の定理

定理 (Mordell-Weil)

$J(\mathbb{Q})$ は有限生成 Abel 群である．すなわち，

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus (\text{有限 Abel 群}).$$

r を $J(\mathbb{Q})$ の階数という．

$J(\mathbb{Q})$ の生成元を求める問題を考える．
通常，これは次の 2 つの手順に分かれる．

1. $J(\mathbb{Q})/2J(\mathbb{Q})$ などを計算し，$J(\mathbb{Q})$ の階数 r を求める．
   （常に計算が停止するアルゴリズムは知られていない．）
2. 無限降下法 (infinite descent) によって $J(\mathbb{Q})$ の生成元を求める．
   $\rightsquigarrow$ 高さの計算が必要．

Kummer 曲面

Jacobi 多様体 J は 15 次元射影空間 $\mathbb{P}^{15}$ に埋め込むことができる.
$\rightsquigarrow$ $\mathbb{P}^{15}$ は大きすぎて扱いにくい.
J を -1 倍の作用で割った商多様体は $\mathbb{P}^3$ に埋め込めむことができる：

$$K := J/\langle [-1] \rangle \hookrightarrow \mathbb{P}^3.$$

（J 上の m 倍写像を $[m]$ で表す.）
K を J の Kummer 曲面という.
以下，上の埋め込みを固定し，K を $\mathbb{P}^3$ の部分多様体と見なす.
$\kappa\colon J \to K$ を自然な写像とする.

Kummer 曲面

Jacobi 多様体 J は 15 次元射影空間 $\mathbb{P}^{15}$ に埋め込むことができる.
$\rightsquigarrow$ $\mathbb{P}^{15}$ は大きすぎて扱いにくい.
J を -1 倍の作用で割った商多様体は $\mathbb{P}^3$ に埋め込めむことができる：

$$K := J/\langle [-1] \rangle \hookrightarrow \mathbb{P}^3.$$

（J 上の m 倍写像を $[m]$ で表す.）
K を J の Kummer 曲面という.
以下，上の埋め込みを固定し，K を $\mathbb{P}^3$ の部分多様体と見なす.
$\kappa\colon J \to K$ を自然な写像とする.

Kummer 曲面

Jacobi 多様体 J は 15 次元射影空間 $\mathbb{P}^{15}$ に埋め込むことができる.
$\rightsquigarrow \mathbb{P}^{15}$ は大きすぎて扱いにくい.
J を -1 倍の作用で割った商多様体は $\mathbb{P}^3$ に埋め込めむことができる：

$$K := J/\langle [-1] \rangle \hookrightarrow \mathbb{P}^3.$$

(J 上の m 倍写像を $[m]$ で表す.)
K を J の Kummer 曲面という.
以下，上の埋め込みを固定し，K を $\mathbb{P}^3$ の部分多様体と見なす.
$\kappa\colon J \to K$ を自然な写像とする.

Kummer 曲面

Jacobi 多様体 J は 15 次元射影空間 $\mathbb{P}^{15}$ に埋め込むことができる.
$\rightsquigarrow \mathbb{P}^{15}$ は大きすぎて扱いにくい.
J を -1 倍の作用で割った商多様体は $\mathbb{P}^3$ に埋め込めむことができる：

$$K := J/\langle [-1] \rangle \hookrightarrow \mathbb{P}^3.$$

(J 上の m 倍写像を $[m]$ で表す.)
K を J の Kummer 曲面という.
以下，上の埋め込みを固定し，K を $\mathbb{P}^3$ の部分多様体と見なす.
$\kappa\colon J \to K$ を自然な写像とする.

単純な高さと標準高さ

定義

J 上の単純な高さ (naive height) $h\colon J(\mathbb{Q}) \to \mathbb{R}$ を次で定義する.

$$h(P) := \log \max\{|\xi_1|, |\xi_2|, |\xi_3|, |\xi_4|\}.$$

ただし, $\kappa(P) = (\xi_1 : \xi_2 : \xi_3 : \xi_4) \in K(\mathbb{Q}) \subset \mathbb{P}^3(\mathbb{Q})$, $\xi_1, \xi_2, \xi_3, \xi_4 \in \mathbb{Z}$, $\gcd(\xi_1, \xi_2, \xi_3, \xi_4) = 1$ とする.

定義

J 上の標準高さ (canonical height) $\hat{h}\colon J(\mathbb{Q}) \to \mathbb{R}$ を次で定義する.

$$\hat{h}(P) := \lim_{m \to \infty} \frac{h([2^m]P)}{4^m}.$$

単純な高さと標準高さ

定義

J 上の単純な高さ (naive height) $h\colon J(\mathbb{Q}) \to \mathbb{R}$ を次で定義する.

$$h(P) := \log \max\{|\xi_1|, |\xi_2|, |\xi_3|, |\xi_4|\}.$$

ただし, $\kappa(P) = (\xi_1 : \xi_2 : \xi_3 : \xi_4) \in K(\mathbb{Q}) \subset \mathbb{P}^3(\mathbb{Q})$, $\xi_1, \xi_2, \xi_3, \xi_4 \in \mathbb{Z}$, $\gcd(\xi_1, \xi_2, \xi_3, \xi_4) = 1$ とする.

定義

J 上の標準高さ (canonical height) $\hat{h}\colon J(\mathbb{Q}) \to \mathbb{R}$ を次で定義する.

$$\hat{h}(P) := \lim_{m \to \infty} \frac{h([2^m]P)}{4^m}.$$

高さの性質

以下の性質が知られている.

定理

定数 $c_1, c_2 \in \mathbb{R}$ が存在して，任意の $P \in J(\mathbb{Q})$ に対し，

$$c_1 \leq h(P) - \hat{h}(P) \leq c_2.$$

定理

任意の $P, Q \in J(\mathbb{Q})$ に対し，次が成り立つ.

1. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.
2. $\hat{h}([m]P) = m^2 \hat{h}(P)$ $(\forall m \in \mathbb{Z})$.

高さの性質

以下の性質が知られている.

定理

定数 $c_1, c_2 \in \mathbb{R}$ が存在して，任意の $P \in J(\mathbb{Q})$ に対し，

$$c_1 \leq h(P) - \hat{h}(P) \leq c_2.$$

定理

任意の $P, Q \in J(\mathbb{Q})$ に対し，次が成り立つ.

1. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.
2. $\hat{h}([m]P) = m^2\hat{h}(P)$ $(\forall m \in \mathbb{Z})$.

本講演で扱う問題

問題

1. $P \in J(\mathbb{Q})$ が与えられたとき，$\hat{h}(P)$ を計算せよ．
2. 曲線 C が与えられたとき，不等式

$$c_1 \leq h(P) - \hat{h}(P) \leq c_2 \quad (P \in J(\mathbb{Q}))$$

を成り立たせる定数 c_1, c_2 のうちできるだけ良いものを計算せよ．

以下のアルゴリズムが知られている：

1. Flynn-Smart (1997), 吉冨 (1998), Stoll (2002), U. (2011), Holmes (2012), Müller (2013), Müller-de Jong (preprint).
2. Flynn-Smart (1997), Stoll (1999, 2002), U. (2011).

本講演で扱う問題

問題

1. $P \in J(\mathbb{Q})$ が与えられたとき，$\hat{h}(P)$ を計算せよ．
2. 曲線 C が与えられたとき，不等式

$$c_1 \leq h(P) - \hat{h}(P) \leq c_2 \quad (P \in J(\mathbb{Q}))$$

を成り立たせる定数 c_1, c_2 のうちできるだけ良いものを計算せよ．

以下のアルゴリズムが知られている：

1. Flynn-Smart (1997), 吉冨 (1998), Stoll (2002), U. (2011), Holmes (2012), Müller (2013), Müller-de Jong (preprint).
2. Flynn-Smart (1997), Stoll (1999, 2002), U. (2011).

補足：Magma での実装状況・最近の進展

計算機代数システム Magma には今回の問題を扱う関数が実装されている.

- `Height`: 標準高さを計算する.
  - Flynn-Smart (1997), Stoll (2002) のアルゴリズムに基づく.
  - 定義体が代数体の場合や種数 3 以上の超楕円曲線の場合も計算可能.
    （Holmes (2012), Müller (2013) の Arakelov 理論によるアルゴリズム.）
- `HeightConstant`: 単純な高さと標準高さの差の上界を計算する.
  - Stoll (1999, 2002) のアルゴリズムに基づく.

Stoll (preprint) は彼のアルゴリズムを種数 3 の超楕円曲線にも拡張した.

目次

設定

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0 \quad (f_i \in \mathbb{Z}).$$

ただし，$f_6 \neq 0$ または $f_5 \neq 0$ であり，右辺は重根を持たないとする．
J：C の Jacobi 多様体
$K = J/\langle[-1]\rangle \subset \mathbb{P}^3$：$J$ の Kummer 多様体
$\kappa\colon J \to K$：自然な写像

$M_{\mathbb{Q}} = \{$ 素数全体 $\} \cup \{\infty\}$
$v \in M_{\mathbb{Q}}$ に対し，絶対値 $|\cdot|_v : \mathbb{Q} \to \mathbb{R}$ を次で定義する．

$$v = \infty\colon \qquad |x|_\infty = |x| \quad (\text{通常の絶対値}),$$

$$v = p\ (\text{素数})\colon \qquad |x|_p = p^{-e}, \quad x = p^e\frac{m}{n}, p \nmid m, n,$$

$$|0|_p = 0.$$

設定

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0 \quad (f_i \in \mathbb{Z}).$$

ただし，$f_6 \neq 0$ または $f_5 \neq 0$ であり，右辺は重根を持たないとする．
J：C の Jacobi 多様体
$K = J/\langle[-1]\rangle \subset \mathbb{P}^3$：$J$ の Kummer 多様体
$\kappa\colon J \to K$：自然な写像

$M_{\mathbb{Q}} = \{$ 素数全体 $\} \cup \{\infty\}$
$v \in M_{\mathbb{Q}}$ に対し，絶対値 $|\cdot|_v : \mathbb{Q} \to \mathbb{R}$ を次で定義する．

$v = \infty$: $\quad |x|_\infty = |x|$ (通常の絶対値),

$v = p$ (素数): $\quad |x|_p = p^{-e}, \quad x = p^e\frac{m}{n}, p \nmid m, n,$

$|0|_p = 0.$

2 倍写像

次の可換図式を満たす $\delta\colon K \to K$ が存在する.

$$\begin{array}{ccc} J & \xrightarrow{[2]} & J \\ \downarrow{\scriptstyle \kappa} & \circlearrowright & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\delta} & K \end{array}$$

さらに,

$$\delta(P) = (\delta_1(P) : \cdots : \delta_4(P))$$

となる 4 次斉次多項式 $\delta_i \in \mathbb{Z}[\xi_1, \ldots, \xi_4]$ が計算されている (Flynn (1993)).

2 倍写像

次の可換図式を満たす $\delta\colon K \to K$ が存在する.

$$\begin{array}{ccc} J & \xrightarrow{[2]} & J \\ \downarrow{\scriptstyle \kappa} & \circlearrowright & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\delta} & K \end{array}$$

さらに,

$$\delta(P) = (\delta_1(P) : \cdots : \delta_4(P))$$

となる 4 次斉次多項式 $\delta_i \in \mathbb{Z}[\xi_1, \ldots, \xi_4]$ が計算されている (Flynn (1993)).

m 倍写像

m を正の整数とする.
次の可換図式を満たす $\mu_m \colon K \to K$ が存在する.

$$\begin{array}{ccc} J & \xrightarrow{[m]} & J \\ \downarrow{\scriptstyle \kappa} & \circlearrowright & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\mu_m} & K \end{array}$$

定理 (U. (2011))

$$\mu_m(P) = (\mu_{m,1}(P) : \cdots : \mu_{m,4}(P))$$

となる m^2 次斉次多項式 $\mu_{m,i} \in \mathbb{Z}[\xi_1, \ldots, \xi_4]$ が存在し，計算可能である.

注意

証明中，ある多項式の既約性判定に Risa/Asir を用いた.

m 倍写像

m を正の整数とする.
次の可換図式を満たす $\mu_m \colon K \to K$ が存在する.

$$\begin{array}{ccc} J & \xrightarrow{[m]} & J \\ \downarrow{\scriptstyle \kappa} & \circlearrowright & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\mu_m} & K \end{array}$$

定理 (U. (2011))

$$\mu_m(P) = (\mu_{m,1}(P) : \cdots : \mu_{m,4}(P))$$

となる m^2 次斉次多項式 $\mu_{m,i} \in \mathbb{Z}[\xi_1, \ldots, \xi_4]$ が存在し，計算可能である.

注意

証明中，ある多項式の既約性判定に Risa/Asir を用いた.

m 倍写像

m を正の整数とする.
次の可換図式を満たす $\mu_m \colon K \to K$ が存在する.

$$\begin{array}{ccc} J & \xrightarrow{[m]} & J \\ \downarrow{\scriptstyle \kappa} & \circlearrowright & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\mu_m} & K \end{array}$$

定理 (U. (2011))

$$\mu_m(P) = (\mu_{m,1}(P) : \cdots : \mu_{m,4}(P))$$

となる m^2 次斉次多項式 $\mu_{m,i} \in \mathbb{Z}[\xi_1, \ldots, \xi_4]$ が存在し，計算可能である.

注意

証明中，ある多項式の既約性判定に Risa/Asir を用いた.

Tate 級数

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} \left|\delta_i(\xi_1, \ldots, \xi_4)\right|_v}{\max_{1 \le i \le 4} \left|\xi_i\right|_v^4}$$

で定義する．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4) \in K(\mathbb{Q})$ である．

標準高さ $\hat{h} \colon J(\mathbb{Q}) \to \mathbb{R}$ は次の式で表される．

$$\hat{h}(P) = h(P) + \sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

Tate 級数

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} \left|\delta_i(\xi_1, \ldots, \xi_4)\right|_v}{\max_{1 \le i \le 4} \left|\xi_i\right|_v^4}$$

で定義する．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4) \in K(\mathbb{Q})$ である．

標準高さ $\hat{h} \colon J(\mathbb{Q}) \to \mathbb{R}$ は次の式で表される．

$$\hat{h}(P) = h(P) + \sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

標準高さの計算

$$\hat{h}(P) = h(P) + \sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

となるから，右辺の無限和を計算すればよい．
有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であることに注意する．

- $v = \infty$ のとき，浮動小数点演算によって直接計算する．
- $v = p$（素数）のとき，次のように，無限和を避けて計算する．
  - Flynn-Smart (1997) は，P のかわりに $[m]P$ を考え，$\log \Phi_v([2^n][m]P) = 0$ となるようにした．
  - Stoll (2002) は，$\Phi_v([2^n]P)$ が n について途中から循環することを使い，無限和を有限和に書き換えた．
  - U. (2011) は，m 倍写像を表す多項式 $\mu_{m,v}$ を用いて Φ_v を一般化した関数 $\Phi_{m,v}$ を構成し，無限和を別の関数で書き換えた．

標準高さの計算

$$\hat{h}(P) = h(P) + \sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

となるから，右辺の無限和を計算すればよい．
有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であることに注意する．

- $v = \infty$ のとき，浮動小数点演算によって直接計算する．
- $v = p$（素数）のとき，次のように，無限和を避けて計算する．
  - Flynn-Smart (1997) は，P のかわりに $[m]P$ を考え，$\log \Phi_v([2^n][m]P) = 0$ となるようにした．
  - Stoll (2002) は，$\Phi_v([2^n]P)$ が n について途中から循環することを使い，無限和を有限和に書き換えた．
  - U. (2011) は，m 倍写像を表す多項式 $\mu_{m,i}$ を用いて Φ_v を一般化した関数 $\Phi_{m,v}$ を構成し，無限和を別の関数で書き換えた．

標準高さの計算

$$\hat{h}(P) = h(P) + \sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

となるから，右辺の無限和を計算すればよい．
有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であることに注意する．

- $v = \infty$ のとき，浮動小数点演算によって直接計算する．
- $v = p$（素数）のとき，次のように，無限和を避けて計算する．
  - Flynn-Smart (1997) は，P のかわりに $[m]P$ を考え，$\log \Phi_v([2^n][m]P) = 0$ となるようにした．
  - Stoll (2002) は，$\Phi_v([2^n]P)$ が n について途中から循環することを使い，無限和を有限和に書き換えた．
  - U. (2011) は，m 倍写像を表す多項式 $\mu_{m,i}$ を用いて Φ_v を一般化した関数 $\Phi_{m,v}$ を構成し，無限和を別の関数で書き換えた．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002)).
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

Flynn-Smart (1997) 数値的な大域的最適化を行った．
$\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．
Stoll (1999) 三角不等式により厳密な評価式を得た．
U (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty : J(\mathbb{R}) \to \mathbb{R}$ として考える．
  - Flynn-Smart (1997) 数値的な大域的最適化を行った．
    $\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．
  - Stoll (1999) 三角不等式により厳密な評価式を得た．
  - U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

Flynn-Smart (1997) 数値的な大域的最適化を行った．
$\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．

Stoll (1999) 三角不等式により厳密な評価式を得た．

U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

  Flynn-Smart (1997) 数値的な大域的最適化を行った．

  $\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．

  Stoll (1999) 三角不等式により厳密な評価式を得た．

  U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

  Flynn-Smart (1997) 数値的な大域的最適化を行った．
  $\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．

  Stoll (1999) 三角不等式により厳密な評価式を得た．

  U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

  Flynn-Smart (1997) 数値的な大域的最適化を行った．
  $\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．

  Stoll (1999) 三角不等式により厳密な評価式を得た．

  U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

標準高さと単純な高さの差の評価

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であり，有限個を除く $v \in M_{\mathbb{Q}}$ に対して $\log \Phi_v([2^n]P) = 0$ であった．
残った有限個の $v \in M_{\mathbb{Q}}$ に対して $\Phi_v(P)$ の上界・下界を求めればよい．

- $v = p$（素数）のときは良い評価が知られている (Stoll (2002))．
- $v = \infty$ のとき，定義域を拡張して $\Phi_\infty \colon J(\mathbb{R}) \to \mathbb{R}$ として考える．

  Flynn-Smart (1997) 数値的な大域的最適化を行った．
  $\rightsquigarrow$ 厳密でなく，得られた評価が正しくなかった．

  Stoll (1999) 三角不等式により厳密な評価式を得た．

  U. (2011) 区間解析を用いて厳密な大域的最適化を行った．さらに，理論的には m 倍写像によって評価を改善できる場合があるが，計算量は著しく増大する．

区間解析

(Ref. E. Hansen, G. W. Walster, *Global Optimization Using Interval Analysis*, 2nd ed., Marcel Dekker, Inc., 2004.)
実数を計算機で扱う際，有限の精度で近似するために誤差が生じる．
区間解析では，区間で実数を包み込むことで精度を保証する．

閉区間 X, Y と $\mathbb{R}$ 上の演算 $\bullet$ に対して，次のように定める．

$$X \bullet Y = \{x \bullet y \mid x \in X, y \in Y\}.$$

このとき，区間 $X = [a, b]$, $Y = [c, d]$ に対し，次のように計算される．

$$X + Y = [a + c, b + d], \quad X - Y = [a - d, b - c],$$
$$X \times Y = [\min\{ac, ad, bc, bd\}, \max\{ac, ad, bc, bd\}].$$

区間演算を用いて，非線形大域的最適化問題を厳密に解くことができる．

区間解析

(Ref. E. Hansen, G. W. Walster, *Global Optimization Using Interval Analysis*, 2nd ed., Marcel Dekker, Inc., 2004.)
実数を計算機で扱う際，有限の精度で近似するために誤差が生じる．
区間解析では，区間で実数を包み込むことで精度を保証する．

閉区間 X, Y と $\mathbb{R}$ 上の演算 $\bullet$ に対して，次のように定める．

$$X \bullet Y = \{x \bullet y \mid x \in X, y \in Y\}.$$

このとき，区間 $X = [a, b]$, $Y = [c, d]$ に対し，次のように計算される．

$$X + Y = [a + c, b + d], \quad X - Y = [a - d, b - c],$$
$$X \times Y = [\min\{ac, ad, bc, bd\}, \max\{ac, ad, bc, bd\}].$$

区間演算を用いて，非線形大域的最適化問題を厳密に解くことができる．

区間解析

(Ref. E. Hansen, G. W. Walster, *Global Optimization Using Interval Analysis*, 2nd ed., Marcel Dekker, Inc., 2004.)
実数を計算機で扱う際，有限の精度で近似するために誤差が生じる．
区間解析では，区間で実数を包み込むことで精度を保証する．

閉区間 X, Y と $\mathbb{R}$ 上の演算 $\bullet$ に対して，次のように定める．

$$X \bullet Y = \{x \bullet y \mid x \in X, y \in Y\}.$$

このとき，区間 $X = [a, b]$, $Y = [c, d]$ に対し，次のように計算される．

$$X + Y = [a + c, b + d], \quad X - Y = [a - d, b - c],$$
$$X \times Y = [\min\{ac, ad, bc, bd\}, \max\{ac, ad, bc, bd\}].$$

区間演算を用いて，非線形大域的最適化問題を厳密に解くことができる．

区間解析

(Ref. E. Hansen, G. W. Walster, *Global Optimization Using Interval Analysis*, 2nd ed., Marcel Dekker, Inc., 2004.)
実数を計算機で扱う際，有限の精度で近似するために誤差が生じる．
区間解析では，区間で実数を包み込むことで精度を保証する．

閉区間 X, Y と $\mathbb{R}$ 上の演算 $\bullet$ に対して，次のように定める．

$$X \bullet Y = \{x \bullet y \mid x \in X, y \in Y\}.$$

このとき，区間 $X = [a, b]$, $Y = [c, d]$ に対し，次のように計算される．

$$X + Y = [a + c, b + d], \quad X - Y = [a - d, b - c],$$
$$X \times Y = [\min\{ac, ad, bc, bd\}, \max\{ac, ad, bc, bd\}].$$

区間演算を用いて，非線形大域的最適化問題を厳密に解くことができる．

目次

問題の確認

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} |\delta_i(\xi_1, \ldots, \xi_4)|_v}{\max_{1 \le i \le 4} |\xi_i|_v^4}$$

で定義した．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4)$ である．

次の計算を行いたい．

- $v \in M_{\mathbb{Q}}$, $P \in J(\mathbb{Q})$ に対し，$\Phi_v(P)$ の計算
- $v = \infty$ に対し，$\Phi_\infty(P)$ の最大値・最小値の計算

必要なアルゴリズム：

- 多倍長演算
- 多変数多項式の計算
- 区間演算

問題の確認

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} |\delta_i(\xi_1, \ldots, \xi_4)|_v}{\max_{1 \le i \le 4} |\xi_i|_v^4}$$

で定義した．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4)$ である．
次の計算を行いたい．

- $v \in M_{\mathbb{Q}}$, $P \in J(\mathbb{Q})$ に対し，$\Phi_v(P)$ の計算
- $v = \infty$ に対し，$\Phi_\infty(P)$ の最大値・最小値の計算

必要なアルゴリズム：

- 多倍長演算
- 多変数多項式の計算
- 区間演算

問題の確認

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} \left|\delta_i(\xi_1, \ldots, \xi_4)\right|_v}{\max_{1 \le i \le 4} \left|\xi_i\right|_v^4}$$

で定義した．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4)$ である．
次の計算を行いたい．

- $v \in M_{\mathbb{Q}}$, $P \in J(\mathbb{Q})$ に対し，$\Phi_v(P)$ の計算
- $v = \infty$ に対し，$\Phi_\infty(P)$ の最大値・最小値の計算

必要なアルゴリズム：

- 多倍長演算
- 多変数多項式の計算
- 区間演算

問題の確認

$v \in M_{\mathbb{Q}}$ に対し，関数 $\Phi_v \colon J(\mathbb{Q}) \to \mathbb{R}$ を

$$\Phi_v(P) = \frac{\max_{1 \le i \le 4} |\delta_i(\xi_1, \ldots, \xi_4)|_v}{\max_{1 \le i \le 4} |\xi_i|_v^4}$$

で定義した．ここで，$\kappa(P) = (\xi_1 : \cdots : \xi_4)$ である．
次の計算を行いたい．

- $v \in M_{\mathbb{Q}}$, $P \in J(\mathbb{Q})$ に対し，$\Phi_v(P)$ の計算
- $v = \infty$ に対し，$\Phi_\infty(P)$ の最大値・最小値の計算

必要なアルゴリズム：

- 多倍長演算 →CLN(+GMP)
- 多変数多項式の計算 →GiNaC
- 区間演算 →Boost (boost::numeric::interval)

CLN—Class Library for Numbers

`http://www.ginac.de/CLN/`
任意精度の数を扱う C++ライブラリ.

- 豊富な「数」のクラスを持つ：
  - 整数
  - 有理数
  - 浮動小数点数
  - 複素数
  - 法付き整数 ($\mathbb{Z}/N\mathbb{Z}$)
  - 一変数多項式
- GNU MP Library (GMP) を利用できる.
- GiNaC が内部で利用している.
- GPL ライセンス.

GiNaC

`http://www.ginac.de/`
数式処理のための C++ライブラリ.
GiNaC は **G**iNaC **i**s **N**ot **a** **C**AS の再帰的頭字語である.
（CAS は計算機代数システム (Computer Algebra System) を意味する.）

- 以下のような対象を扱うことができる：
  - 多変数多項式
  - べき級数
  - 初等関数（三角関数，指数関数，対数関数，...）
  - 特殊関数（ガンマ関数，ゼータ関数，...）
  - 行列
  - ...
- CLN を内部で利用している.
- GPL ライセンス.

Boost

`http://www.boost.org/`
C++のオープンソースライブラリ.

- 幅広い分野にわたるライブラリからなる：
  - 文字列処理
  - コンテナ・イテレータ・アルゴリズム
  - 関数オブジェクト・高階プログラミング
  - ジェネリックプログラミング
  - メタプログラミング
  - 数学と数値
    - 区間解析 (boost::numeric::interval)
    - ...
  - データ構造
  - ...
- いくつかのライブラリは最新の C++標準 (C++11) に採用された.
- Boost Software License（商用・非商用ともに無償）.

boost::numeric::interval

Boost に含まれる区間解析のための C++ライブラリ.

- テンプレートにより，全順序を持つ数値型 (float, double, . . .) に対して利用可能.
- 四則演算，絶対値，べき乗，三角関数，指数・対数関数などが利用可能.

注意

区間演算を行うライブラリは，他にも C ライブラリの MPFI (**M**ultiple **P**recision **F**loating-point **I**nterval library) などがある.

boost::numeric::interval

Boost に含まれる区間解析のための C++ライブラリ.

- テンプレートにより，全順序を持つ数値型 (float, double, . . .) に対して利用可能.
- 四則演算，絶対値，べき乗，三角関数，指数・対数関数などが利用可能.

注意

区間演算を行うライブラリは，他にも C ライブラリの MPFI (**M**ultiple **P**recision **F**loating-point **I**nterval library) などがある.

実行例：標準高さの計算

Stoll (2002) による次の例を考える.

$$C\colon y^2 = 4x^6 + 4x^5 + 3x^4 - 3x^3 - x - 6,$$
$$P = \infty^+ - \infty^-, \quad Q = (-1,-1) - \infty^- \in J(\mathbb{Q}).$$

このとき，$\kappa(P+Q) = (24 : 19 : 25 : 32) \in K(\mathbb{Q})$.
$\hat{h}(P+Q)$ を計算する.

$$\hat{h}(P+Q) = 4.101180013\ldots$$

実行例：標準高さの計算

Stoll (2002) による次の例を考える.

$$C\colon y^2 = 4x^6 + 4x^5 + 3x^4 - 3x^3 - x - 6,$$
$$P = \infty^+ - \infty^-, \quad Q = (-1,-1) - \infty^- \in J(\mathbb{Q}).$$

このとき，$\kappa(P+Q) = (24 : 19 : 25 : 32) \in K(\mathbb{Q})$.
$\hat{h}(P+Q)$ を計算する.

$$\hat{h}(P+Q) = 4.101180013\ldots$$

実行例：標準高さの計算

Stoll (2002) による次の例を考える.

$$C\colon y^2 = 4x^6 + 4x^5 + 3x^4 - 3x^3 - x - 6,$$
$$P = \infty^+ - \infty^-, \quad Q = (-1,-1) - \infty^- \in J(\mathbb{Q}).$$

このとき，$\kappa(P+Q) = (24 : 19 : 25 : 32) \in K(\mathbb{Q})$.
$\hat{h}(P+Q)$ を計算する.

$$\hat{h}(P+Q) = 4.101180013\ldots$$

実行例：高さ関数の差の評価

Flynn-Smart (1997) による次の例を考える.

$$C\colon y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であった.

$$\Psi_\infty(P) := -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_\infty([2^n]P)$$

と定め，$\Psi_\infty(P)$ の上界を求める.

Flynn-Smart (1997) 数値計算により，$\Psi_\infty(P) \leq 1.474$ としたが，誤っていることが指摘された.

Stoll (1999) $\Psi_\infty(P) \leq 2.6$ を示した．さらに，ある $P \in J(\mathbb{R})$ に対して $\Psi_\infty(P) = 2.241\ldots$ となることを示した.

U. (2011) $\Psi_\infty(P) \leq 2.24110646$ を示した.

実行例：高さ関数の差の評価

Flynn-Smart (1997) による次の例を考える．

$$C\colon y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であった．

$$\Psi_\infty(P) := -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_\infty([2^n]P)$$

と定め，$\Psi_\infty(P)$ の上界を求める．

Flynn-Smart (1997) 数値計算により，$\Psi_\infty(P) \leq 1.474$ としたが，誤っていることが指摘された．

Stoll (1999) $\Psi_\infty(P) \leq 2.6$ を示した．さらに，ある $P \in J(\mathbb{R})$ に対して $\Psi_\infty(P) = 2.241\ldots$ となることを示した．

U. (2011) $\Psi_\infty(P) \leq 2.24110646$ を示した．

実行例：高さ関数の差の評価

Flynn-Smart (1997) による次の例を考える．

$$C\colon y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

$$h(P) - \hat{h}(P) = -\sum_{v \in M_{\mathbb{Q}}} \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P)$$

であった．

$$\Psi_\infty(P) := -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_\infty([2^n]P)$$

と定め，$\Psi_\infty(P)$ の上界を求める．

Flynn-Smart (1997) 数値計算により，$\Psi_\infty(P) \leq 1.474$ としたが，誤っていることが指摘された．

Stoll (1999) $\Psi_\infty(P) \leq 2.6$ を示した．さらに，ある $P \in J(\mathbb{R})$ に対して $\Psi_\infty(P) = 2.241\ldots$ となることを示した．

U. (2011) $\Psi_\infty(P) \leq 2.24110646$ を示した．

まとめ

- 数論的対象の「複雑さ」を測る高さが数論において重要である.
- 種数 2 の曲線の Jacobi 多様体上でアルゴリズムの改良を行った.
- これらのアルゴリズムは級数の計算や大域的最適化問題に帰着できる.
- Boost, CLN, GiNaC などのライブラリを用いてこれらを実装した.

ご清聴ありがとうございました.

まとめ

- 数論的対象の「複雑さ」を測る高さが数論において重要である.
- 種数 2 の曲線の Jacobi 多様体上でアルゴリズムの改良を行った.
- これらのアルゴリズムは級数の計算や大域的最適化問題に帰着できる.
- Boost, CLN, GiNaC などのライブラリを用いてこれらを実装した.

ご清聴ありがとうございました.