超楕円曲線の Hasse-Witt 行列計算アルゴリズムの改良

An improvement in computation of the Hasse-Witt matrix

[1)] 古元 宏樹, [1,*)] 小崎 俊二, [1)] 松尾 和人

1) 情報セキュリティ大学院大学

[1)]Hiroki KOMOTO, [1)]Shunji KOZAKI, [1)]Kazuto MATSUO

1) Institute of Information Security

*Email: dgs074103 @ iisec.ac.jp

キーワード: 超楕円曲線, 超楕円曲線暗号, 位数計算, Hasse-Witt 行列

Keywords: hyperelliptic curves, hyperelliptic curve cyrptosystems, point counting, Hasse-Witt matrices

1. はじめに

安全な超楕円曲線暗号を構成するためには曲線の Jacobian の有理点群の位数を知る必要がある．超楕円曲線の Jacobian の位数はその Frobenius 写像の特性多項式より計算可能である．曲線の Hasse-Witt 行列は定義体の標数 p を法とした Frobenius 写像の特性多項式の係数を与えることから，曲線の Jacobian の位数計算に利用可能である.[1]–[4]

超楕円曲線の Hasse-Witt 行列の成分は曲線の定義式から得られる多項式の特定次数の係数からなる．この Hasse-Witt 行列の計算方法として，Bostan-Gaudry-Schost[3]による Chudnovsky-Chudnovsky アルゴリズム[5]の改良が知られている．このアルゴリズムの基礎演算には有限精度 p-進整数が用いられる．

本論文では，多項式の reversal を利用して計算に必要な p-進整数の精度を下げることにより，Hasse-Witt 行列計算を高速化する．

次節では，Hasse-Witt 行列の定義とその計算法についてまとめる．3. で Hasse-Witt 行列計算の改良を示し，4. で実装実験により改良の効果を確認する．最後に 5. で Hasse-Witt 行列計算の改良についてまとめる．

2. Hasse-Witt 行列

p を奇素数，$\mathbb{F}_q$ を位数 p^m の有限体とする．$\mathbb{F}_q$ 上定義された種数 $g > 1$ の超楕円曲線 C を

$$C : Y^2 = F(X),\ F(X) = \sum_{i=0}^{2g+1} f_i X^i \in \mathbb{F}_q[X] \quad (1)$$

と定義する．ここで，$F(X)$ はモニックで重根を持たないものとする．また，議論の簡略化のため $f_0 \neq 0$ とする．

定義 1 *(Hasse-Witt 行列)* 式 (1) の $F(X)$ に対して多項式 $(F(X))^{\frac{p-1}{2}}$ の k 次の係数を h_k とあらわすとき，(i,j) 成分が h_{jp-i} となる $\mathbb{F}_q$ 上の $g \times g$ 行列

$$H = (h_{jp-i})_{1 \leq i,j \leq g}$$

を C の *Hasse-Witt* 行列と定義する．

$1 \leq i \leq m-1$ に対して Hasse-Witt 行列 H の各成分を p^i 乗した行列を $H^{(p^i)}$ と書き，$H_\pi = HH^{(p)} \cdots H^{(p^{m-1})}$ とおくと，次の定理が成り立つ．

定理 1 *(Manin[6])* 超楕円曲線 C の *Jacobian* の q 乗 *Frobenius* 写像の特性多項式を $\chi_q(X)$ とすると，

$$\chi_q(X) \equiv (-1)^g X^g \det(H_\pi - XI) \mod p$$

である．ここで，I は $g \times g$ 単位行列である．

この定理 1 より，q 乗 Frobenius 写像の特性多項式 $\chi_q(X)$ の mod p における係数は Hasse-Witt 行列 H から計算可能である．

Bostan-Gaudry-Schost[3]は，多項式 $(F(X))^{\frac{p-1}{2}}$ の係数に関する漸化式に対して Chudnovsky-Chudnovsky アルゴリズム[5]を適用・改良し，Hasse-Witt 行列 H を $\tilde{O}(\sqrt{p})$ の時間計算量で計算するアルゴリズムを示した．

多項式 $(F(X))^{\frac{p-1}{2}}$ の k 次係数を h_k と書き，これらを成分に持つ $2g+1$ 縦ベクトルを $U_k = {}^t\begin{pmatrix} h_{k-2g} & h_{k-2g-1} & \cdots & h_k \end{pmatrix}$ とおく．ただし，$h_{-2g} = \cdots = h_{-1} = 0$ とする．また，有理関数を成分に持つ $(2g+1) \times (2g+1)$ 行列を

$$A(X) = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \\ r_{2g+1}(X) & r_{2g}(X) & \cdots & r_1(X) \end{pmatrix}, \quad (2)$$

$$r_i(X) = \frac{f_i\left(i\left(p+1\right)/2 - X\right)}{f_0 X},\ 1 \leq i \leq 2g+1$$

とおき，$A(X)$ の X に k を代入した行列を $A(k)$ と書く．このとき多項式 $(F(X))^{\frac{p-1}{2}}$ の係数に関する $2g+1$ 項の漸化式[7]より，

$$U_k = A(k)U_{k-1} = A(k)A(k-1)\cdots A(1)U_0 \quad (3)$$

が成り立つ．従って Hasse-Witt 行列 H を得るためには，$U_0 = {}^t\begin{pmatrix} 0 & \cdots & 0 & f_0^{\frac{p-1}{2}} \end{pmatrix}$ を初期値として式 (3) を利用して $U_{p-1}, U_{2p-1}, \cdots, U_{gp-1}$ を計算すればよい．

Chudnovsky-Chudnovsky アルゴリズム[5]は，式 (3) で与えられた U_k を U_0 から $\tilde{O}(\sqrt{k})$ で計算するものである．ここで，式 (3) は標数 0 の体を前提とするものであり，Hasse-Witt 行列計算は $\mathbb{F}_q$ の元を p-進体 $\mathbb{Q}_p$ に持ち上げて行なう必要がある．Bostan-Gaudry-Schost[3]は，U_{gp-1} の分母 $(gp-1)!$ に対する p-進付値より Hasse-Witt 行列 H に必要な $U_{p-1}, U_{2p-1}, \cdots, U_{gp-1}$ の計算を $\mathbb{Z}/p^g\mathbb{Z}$ 上で行なった．次節では，式 (3) の計算に必要な p-進整数の精度を下げることにより，Hasse-Witt 行列計算の高速化を行なう．

3. Hasse-Witt 行列計算の改良

本節では Bostan-Gaudry-Schost[3]の Hasse-Witt 行列計算の高速化を行なう．

3·1 p-進整数の必要精度 Bostan-Gaudry-Schost[3]の Hasse-Witt 行列計算では，U_0 から U_{p-1}, $U_{2p-1}, \cdots, U_{gp-1}$ を式 (3) を利用して順次計算する．一方，式 (3) の計算では，$A(p), A(2p), \cdots, A((g-1)p)$ においてそれぞれ p による除算が発生することから p-進整数の精度が落ちる．従って，$1 \leq i < g$ に対して $U_{(i-1)p}$ から U_{ip} を求める計算は $\mathbb{Z}/p^{g-i+1}\mathbb{Z}$ 上で行なえばよく，$U_{(g-1)p}$ から U_{gp-1} を求める計算は $\mathbb{Z}/p\mathbb{Z}$ 上で行なえば十分である．

以上より，Hasse-Witt 行列計算における各 U_{ip} $(1 \leq i < g)$ の計算ステップに必要な p-進整数の精度は，最終ステップが $\mathbb{Z}/p\mathbb{Z}$ 上で計算可能となるように下げることが可能である．次節では Hasse-Witt 行列に必要な U_k の計算を 2 分割し p-進整数の必要精度を下げることで，高速化を行なう．

3·2 多項式の reversal を利用した Hasse-Witt 行列計算の改良 多項式 $P(X)$ の reversal[8]を $\mathrm{rev}(P(X)) := X^{\deg P}P(1/X)$ と定義し，$\mathrm{rev}(P(X))$ と書く．多項式の reversal の性質より，$F(X)$ について

$$\mathrm{rev}((F(X))^{\frac{p-1}{2}}) = (\mathrm{rev}(F(X)))^{\frac{p-1}{2}}$$

が成り立つ．即ち，$(F(X))^{\frac{p-1}{2}}$ の高次の係数を $(\mathrm{rev}(F(X)))^{\frac{p-1}{2}}$ の低次の係数として得ることが可能である．以下では，この reversal の性質を利用して，Hasse-Witt 行列計算において必要な p-進整数の精度を下げる．

多項式 $\mathrm{rev}(F(X))$ に対して式 (2) で定義された $(2g+1)\times(2g+1)$ 行列を $\hat{A}(X)$ と書き，同様に式 (3) で定義された $2g+1$ 縦ベクトルを $\hat{U}_k$ と書く．すると Hasse-Witt 行列の成分は，$U_p, \cdots, U_{gp-1}$ の代わりに，$U_p, \cdots, U_{\lceil \frac{g}{2} \rceil p-1}$ と $\hat{U}_{\frac{p-1}{2}}, \cdots, \hat{U}_{\lfloor \frac{g}{2} \rfloor p-\frac{p+1}{2}}$ を計算することで得られる．従って，$F(X)$ から

$$U_p \text{を } \mathbb{Z}/p^{\lceil \frac{g}{2} \rceil}\mathbb{Z} \text{ 上で}, \cdots, U_{\lceil \frac{g}{2} \rceil p-1} \text{を } \mathbb{Z}/p\mathbb{Z} \text{ 上で}$$

計算し，また $\mathrm{rev}(F(X))$ から

$$\hat{U}_{\frac{p-1}{2}} \text{を } \mathbb{Z}/p^{\lfloor \frac{g}{2} \rfloor}\mathbb{Z} \text{ 上で}, \cdots, \hat{U}_{\lfloor \frac{g}{2} \rfloor p-\frac{p+1}{2}} \text{を } \mathbb{Z}/p\mathbb{Z} \text{ 上で}$$

計算することで，各ステップに必要な p-進整数の精度を下げられる．例えば $g=3$ の場合には U_p を $\mathbb{Z}/p^2\mathbb{Z}$ で計算し，U_{2p-1} と $\hat{U}_{\frac{p-1}{2}}$ を $\mathbb{Z}/p\mathbb{Z}$ で計算することで Hasse-Witt 行列が得られる．

4. 実験結果

Bostan-Gaudry-Schost[3]のアルゴリズムを計算代数システム Magma 上に実装し，3·2 節の改良の効果を確認する．実験環境として AMD Opteron 246 2.0GHz を用いて実験を行なった．実験では 16 から 32 ビットの有限素体 $\mathbb{F}_p$ 上の種数 3 の超楕円曲線に対する Hasse-Witt 行列計算の実行時間を計測した．

実験結果を Fig.1 に示す．縦軸を Hasse-Witt 行列の計算時間，横軸を p のビット数として，“Original” と記した線は $\mathbb{Z}/p^3\mathbb{Z}$ のみを用いて計算した実行時間を示し，“This work” と記した線は 3·2 節の方法を利用した実行時間を示す．

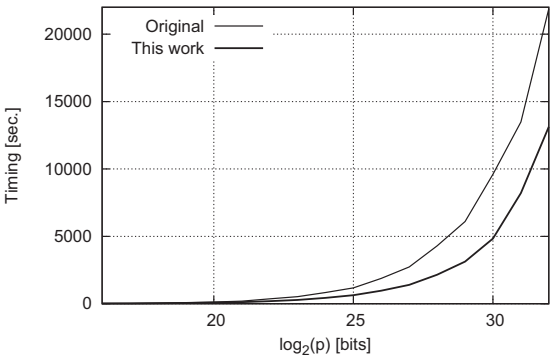

Fig. 1 実行時間計測結果

実験結果より 3·2 節の方法を利用したものは $\mathbb{Z}/p^3\mathbb{Z}$ のみを用いて計算したものと比べて 1.6 から 2 倍高速化することが判った．

5. まとめ

本論文では，超楕円曲線の位数計算に利用される Hasse-Witt 行列計算の高速化を行なった．多項式の reversal を利用して Hasse-Witt 行列計算に必要な有限精度 p-進整数の精度を下げることで計算を高速化する方法を示した．16 から 32 ビットの有限素体上の種数 3 の超楕円曲線に対して提案方法を用いて Hasse-Witt 行列計算実験を行なった結果，本方法を用いない場合と比較して 1.6 から 2 倍高速化することが確認された．

参考文献

[1] P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. *ANTS-IV*, LNCS 1838, pp. 313–332. Springer-Verlag, 2000.

[2] K. Matsuo, J. Chao, and S. Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. *ANTS-V*, LNCS 2369, pp. 461–474. Springer-Verlag, July 2002.

[3] A. Bostan, P. Gaudry, and É. Schost. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. LNCS 2948, pp. 40–58. Springer-Verlag, 2004.

[4] Mark Bauer, Edlyn Teske, and Annegret Weng. Point counting on Picard curves in large characteristic. *Math. Comp.*, Vol. 74, pp. 1983–2005, 2005.

[5] D. V. Chudnovsky and G. V. Chudnovsky. Approximations and complex multiplication according to Ramanujan. In *Ramanujan revisited*, pp. 375–472. Academic Press, 1988.

[6] J. I. Manin. The Hasse-Witt matrix of an algebraic curve. *Trans. AMS*, Vol. 45, pp. 245–264, 1965.

[7] L. Eulero. *Introductio in analysin infinitorum*. Lausannæ: Marcum-Michaelem Bousquet, 1748.

[8] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge U. P., 2nd edition, 1999.