数理解析研究所講究録
第1898巻 2014年 103-114

Decomposition attack for the DLP of the Jacobian group of a curve over small characteristic field

長尾孝一 (Koh-ichi Nagao)
関東学院大学 (Kanto Gakuin Univ.)

1 はじめに

Faugéreら [3] およびその修正である, Petitら [9] によって, 標数2の拡大体上定義された楕円曲線 $E/\mathbb{F}_{2^n}$ の離散対数問題の計算量は, First fall degree 仮説の下で, その入力サイズを拡大次数 n としたとき, subexponential[1]であることが示された. 彼らの方式は, 一般の小さな素数 p に対して, 標数 p の拡大体上定義された楕円曲線 $E/\mathbb{F}_{2^n}$ の離散対数問題の計算量が, First fall degree 仮説の下で, その入力サイズを拡大次数 n としたとき, subexponential であるという形に自然に拡張することができるが [7] [8], 幾つかの点で, より精密な議論をする必要がある. 本論文では, 必要となる First fall degree 仮説, Semaev 多項式と楕円分割問題, Weil descent の定義について述べ, Semaev 多項式を Weil descent 操作して得られる多項式たちの次数と関係式について, heuristical に得られる結果について述べる. ここで得られる関係式は, Field equation という多項式の集合を法とした合同式であるが, これが等式に置き換わった式をかわりに考えると, Semaev 多項式を Weil descent 操作して得られる多項式たちの First fall degree を見積もることができる. しかしながら, そこには若干の GAP が存在する為, Field equations を法をして合同な多項式の性質について調べ, Semaev 多項式を Weil descent 操作して得られる多項式たちと, Field equation に含まれる多項式たちを併せて得られた方程式系の First fall degree の上からの上からの評価を与える. また、一般のグローバル多項式[2] $\overrightarrow{F}[\overrightarrow{X_1},..,\overrightarrow{X_d}] \in \mathbb{F}_{p^n}[\overrightarrow{X_1},..,\overrightarrow{X_d}]$ から Weil descent で得られる (ローカル多項式[3]から成る) 方程式系 $\{[\overrightarrow{F}]_k^{\downarrow} | k=1,..,n\} \cup S_{fe}$ に対して, その方程式の次数 $\deg[\overrightarrow{F}]_k^{\downarrow}$ は正確には判らない. この論文では次に, 上手いグローバル多項式 $\overrightarrow{m_0} \in \mathbb{F}_{p^n}[\overrightarrow{X_1},..,\overrightarrow{X_d}]$ で,

1) 方程式系 $\{[\overrightarrow{F}]_k^{\downarrow} | k=1,..,n\} \cup S_{fe}$ の零点と, $\{[\overrightarrow{m_0}\overrightarrow{F}]_k^{\downarrow} | k=1,..,n\} \cup S_{fe}$ の零点が一致し,

2) $\deg[\overrightarrow{m_0}\overrightarrow{F}]_k^{\downarrow}$ がきちんと判る

ものが取れることを示す. このことより, 新たに作った方程式系 $\{[\overrightarrow{m_0}\overrightarrow{F}]_k^{\downarrow} | k=1,..,n\} \cup S_{fe}$ の First fall degree の上からの正確な見積もりができ, 方程式系を解く計算コストの First fall degree 仮説下での Heuristics を使わない見積もりが可能となる. また, Semaev 多項式にこの議論を適応することにより, 楕円離散対数問題

[1] $0<c<1$ である定数 c が存在して, 計算量が $O(exp(n^c))$ と書ける時, subexponential と呼ぶ
[2] 拡大体上の元を動く変数とその変数からなる多項式をベクトル記法で書きまたその多項式をグローバル多項式と呼ぶことにする
[3] 基礎体上の元を動く変数の多項式をローカル多項式と呼ぶことにする

の計算量も（First fall degree 仮説下では）heuristics を使わないで見積もることができる.

次に、この分解攻撃を曲線のヤコビアン群に対して一般化することを考え, 曲線のヤコビアン群の元をその曲線の点の部分集合から成る decomposed factor の和に分解するアルゴリズムについて述べる。これは、楕円曲線の場合の Semaev [10] の分解公式の一般化になっており、この導出の為に 著者が [6] で使ったのと同様の Riemann-Roch の定理を使う. ここで使われた議論と同様の（しかしながら少し一般化した議論と Heuristics を使う必要があり、ここでは述べない）議論を適応すれば、小標数な拡大体上定義された小種数である曲線のヤコビアン群の離散対数問題がやはり First fall degree 仮説下では subexponential であることが判る.

2 記号

$\overrightarrow{X_1}$,.. を拡大体 $\mathbb{F}_{p^n}$ の元を動く変数とし, ベクトル表記で書きグローバル変数と呼ぶこととする. また, グローバル変数たちを変数にもつ多項式 $\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ...]$ をグローバル多項式と呼び, ベクトル表記する. X_1,... を基礎体 $\mathbb{F}_p$ の元を動く変数とし, ローカル変数と呼ぶ. また, ローカル変数たちを変数にもつ多項式 $F \in \mathbb{F}_p[X_1, ...]$ をローカル多項式と呼ぶ.

3 Semaev 多項式

$E/\mathbb{F}_{p^n}$ を楕円曲線, $P_0 \in E(\mathbb{F}_{p^n})$ をその点, d を整数とする. Semaev [10] によって, グローバル多項式 $\overrightarrow{Sem_{P_0}}(\overrightarrow{X_1}, ..., \overrightarrow{X_d}) \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ で以下の 1) 2) の性質を満たすものの存在と, 漸化式を使った計算法が発見された：
1) $P_1, .., P_d \in E(\bar{\mathbb{F}}_p)$ とせよ. , $P_0 + P_1 + ..., +P_d = 0$ であることと,
$\overrightarrow{Sem_{P_0}}(x(P_1), ..., x(P_d)) = 0$ は同値である.
2) $\deg \overrightarrow{Sem_{P_0}} < 2^d$ である.

$d \sim n^{1/3}$, $n' \sim n^{2/3}$ を満たす整数 n', d を固定する. $\mathbb{F}_{p^n}$ を $\mathbb{F}_p$ 係数のベクトル空間と見たときの基底 $\{w_1, ..., w_n\}$ を fix する. また, $V := \{\sum_{i=1}^{n'} x_i w_i | x_i \in \mathbb{F}_p\}$ を $\mathbb{F}_{p^n}$ の n' 次元部分ベクトル空間とし, $DF := \{P \in E(\mathbb{F}_{p^n}) \,|\, x(P) \in V\}$ とする.

問題 1 (楕円分解問題) $P_0 \in E(\mathbb{F}_{p^n})$ とせよ. $P_1, .., P_d \in DF$ で, $P_0 + P_1 + ... + P_d = 0$ をみたすものを見つけよ.

Semaev 多項式の存在によって, 上の問題は, dn' 個のローカル変数を持つ方程式系を解く問題に帰着される. また, 様々な heuristic を仮定すると, これらの方程式系の First fall degree が $O(n^{2/3})$ であることが判り, First fall degree 仮説の下では, その計算量は $O(exp(n^{2/3+o(1)}))$ となる. また, 楕円離散対数問題の解法には $\#DF = O(exp(n^{2/3}))$ 個の楕円分解問題と, サイズ $\#DF \times \#DF$ の線形代数が必要であるが, これらの計算量も $O(exp(n^{2/3+o(1)}))$ （$o(1)$ の項に増えたコストを繰り込むことができる）であり, 楕円離散対数問題が $O(exp(n^{2/3+o(1)}))$ で解けることとなる.

4 Weil descentの定義と性質

$\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ をグローバル多項式, $\{X_{ij} \mid 1 \leq i \leq d, 1 \leq j \leq n'\}$ をローカル変数の集合とする. また,

$$S_{fe} := \{X_{ij}^p - X_{ij} \mid 1 \leq i \leq d, 1 \leq j \leq n'\}$$

とおき, これをField equations と呼ぶ. また,

$$wd(\overrightarrow{F}) := \overrightarrow{F}|_{\overrightarrow{X_i}=\sum_{j=1}^{n'} X_{ij}w_j} \bmod S_{fe} \in \mathbb{F}_{p^n}[\{X_{ij}\}]$$

(つまり, 全ての $i \in [1, 2, ..., , d]$ に対して, $\overrightarrow{X_i}$ に $\sum_{j=1}^{n'} X_{ij}w_j$ を代入し, $\bmod S_{fe}$ をとる) とおき, $[\overrightarrow{F}]_k^{\downarrow} \in \mathbb{F}_p[\{X_{ij}\}]$ を, $wd(\overrightarrow{F}) = \sum_{k=1}^{n} [\overrightarrow{F}]_k^{\downarrow} w_k$ を満たすローカル多項式とする.

ここで, Field equationsの定義より, $\deg_{X_{ij}} wd(\overrightarrow{Sem_{P_0}}) \leq p-1$, $\deg_{X_{ij}} [\overrightarrow{Sem_{P_0}}]_k^{\downarrow} \leq p-1$ が成り立つことを注意する.

この定義は判りつらいので例をあげる.

例1. α を $\alpha^7 + \alpha + 1 = 0$ を満たす $\in F_{2^7}$ の元とせよ. ベクトル空間の拡大 $\mathbb{F}_{2^7}/\mathbb{F}_2$ の基底を $[1, \alpha, ..., \alpha^6]$ と取る. (つまり. $w_i = \alpha^{i-1}$). $n' = 2$ とし、2次元の部分ベクトル空間 B を $B = \{x_1 + x_2\alpha \mid x_i \in \mathbb{F}_2\}$ と置く. $\overrightarrow{X}$ を B の元を動くグローバル多項式とする (つまり $\overrightarrow{X}$ はある $X_1, X_2 \in \mathbb{F}_2$ を使って $\overrightarrow{X} = X_1 + X_2\alpha$ と書かれてる.)

このとき次が判る.

$wd(\overrightarrow{X}^2) := (X_1 + X_2\alpha)^2 \bmod S_{fe} = X_1 + X_2\alpha^2$, $[\overrightarrow{X}^2]_1^{\downarrow} = X_1$, $[\overrightarrow{X}^2]_3^{\downarrow} = X_2$.

$wd(\overrightarrow{X}^4) := (X_1 + X_2\alpha)^4 \bmod S_{fe} = X_1 + X_2\alpha^4$, $[\overrightarrow{X}^2]_1^{\downarrow} = X_1$, $[\overrightarrow{X}^2]_5^{\downarrow} = X_2$.

$wd(\overrightarrow{X}^3) \equiv (X_1 + X_2\alpha^2)(X_1 + X_2\alpha) = X_1 + X_1X_2\alpha^2 + X_1X_2\alpha^2 + X_2\alpha^3$.

$wd(\overrightarrow{X}^8) = (X_1 + X_2\alpha)^8 \bmod S_{fe} = X_1 + X_2\alpha^8 = X_1 + X_2\alpha + X_2\alpha^2$.

$wd(\overrightarrow{X}^{16}) = (X_1 + X_2\alpha + X_2\alpha^2)^2 \bmod S_{fe} = X_1 + X_2\alpha^2 + X_2\alpha^4$.

$wd(\overrightarrow{X}^9) \equiv (X_1 + X_2\alpha + X_2\alpha^2)(X_1 + X_2\alpha) \equiv X_1 + (X_1X_2 + X_1X_2)\alpha + (X_1X_2 + X_2)\alpha^2 + X_2\alpha^3 = X_1 + (X_1X_2 + X_2)\alpha^2 + X_2\alpha^3$,

$[\overrightarrow{X}^9]_1^{\downarrow} = X_1$, $[\overrightarrow{X}^9]_2^{\downarrow} = X_1X_2 + X_1X_2$, $[\overrightarrow{X}^9]_3^{\downarrow} = X_1X_2 + X_2$, $[\overrightarrow{X}^9]_4^{\downarrow} = X_2$, $[\overrightarrow{X}^9]_5^{\downarrow} = [\overrightarrow{X}^9]_6^{\downarrow} = 0$.

Weil descentで得られた多項式の次数は元の多項式の次数よりかなり小さいことが確認できる.

例2. $d = 3$ とし、3変数からなるグローバル多項式 $\overrightarrow{F} := \alpha\overrightarrow{X_1}^9 + \overrightarrow{X_2}^4 + \overrightarrow{X_3}^3 + \alpha + 1 \in \mathbb{F}_{2^7}[\overrightarrow{X_1}, \overrightarrow{X_2}, \overrightarrow{X_3}]$ を考え、方程式 $\overrightarrow{F}(\overrightarrow{X_1}, \overrightarrow{X_2}, \overrightarrow{X_3}) = 0$ の $\overrightarrow{X_1}, \overrightarrow{X_2}, \overrightarrow{X_3} \in B$. での解を求める.

$wd(\overrightarrow{F})$ は $wd(\overrightarrow{F}) = (X_{31} + X_{21} + 1) + (X_{11} + X_{31}X_{32} + 1)\alpha + X_{31}X_{32}\alpha^2 + X_{32}\alpha^3 + (X_{12} + X_{22})\alpha^4$ のように書かれる. ここで X_{ij} たちはローカル変数である. 従って方程式系 $X_{31} + X_{21} + 1 = 0, X_{11} + X_{31}X_{32} + 1 = 0, X_{31}X_{32} = 0, X_{32} = 0, X_{12} + X_{22} = 0.$ を解き $X_{11} = 0, X_{32} = 0$, $X_{12} = X_{22} = a \in \mathbb{F}_2$, $X_{21} = X_{31} = b \in \mathbb{F}_2$, を得、これをもとのグローバル変数に復元することによって解 $(\overrightarrow{X_1}, \overrightarrow{X_2}, \overrightarrow{X_3}) = (1, 0, 1), (1, 1, 0), (1 + \alpha, \alpha, 1), (1 + \alpha, 1 + \alpha, 0)$ を得る.

例3. $0 \leq a, b, c \leq p-1$ を満たす整数 a, b, c に対して, $wd(\overrightarrow{X_1}^{ap^2+bp+c})$ を計算してみる $\overrightarrow{X_1}^{ap^2+bp+c} \bmod S_{fe} = wd(\overrightarrow{X_1}^{ap^2+bp+c}) = (\sum_{j=1}^{n'} X_{1j}w_j^{p^2})^a (\sum_{j=1}^{n'} X_{1j}w_j^p)^b (\sum_{j=1}^{n'} X_{1j}w_j)^c$

より, $\deg([\overrightarrow{X_1}^{ap^2+bp+c}]_k^{\downarrow}) = a+b+c$ となる.

例3を一般化することによって次を得る：[4]

補助定理 1 $\overrightarrow{F}$ を $\deg \overrightarrow{F} \ll p^{n'}$ を満たすグローバル多項式とせよ. このとき, $\deg([\overrightarrow{F}]_k^{\downarrow}) \leq (p-1)d\lfloor \log_p \deg \overrightarrow{F} \rfloor$. が成り立つ.

また, 多くのグローバル多項式 $\overrightarrow{F}$ に対して, 自然に次の性質が成り立つのが一般的であると考えられるので, これを仮定する. (実際にはSemaev多項式に対して成り立てば良い)

仮定 1 *1)* 定数 $D_{heu} \sim (p-1)d\lfloor \log_p \deg(\overrightarrow{F}) \rfloor$ で, $\deg([\overrightarrow{F}]_k^{\downarrow}) = D_{heu}$, $\deg(\overrightarrow{X_1} \cdot [\overrightarrow{F}]_k^{\downarrow}) \leq D_{heu}$ $(k \in [1,2,...,n])$ を満たすものが存在する.

5 First fall degree仮説

$f_1,...,f_l \in \mathbb{F}_p[\{X_{ij}\}]$ をローカル多項式とする.

定義 1 (First fall degree) D_{ff} を以下を満たす最小の自然数とし, 方程式系 $f_1,...,f_l$ の *First fall degree* と呼ぶ.
ローカル多項式 $g_1,...,g_l \in \mathbb{F}_p[\{X_{ij}\}]$ で以下の4つの性質を満たすものが存在する.
1) $\max_{1\leq i\leq l} \deg(g_i f_i) = D_{ff}$,
2) $\max_{1\leq i\leq l} \deg(f_i) \leq D_{ff}$,
3) $\deg(\sum_{i=1}^{l} g_i f_i) < D_{ff}$,
4) $\sum_{i=1}^{l} g_i f_i \neq 0$.

仮定 2 (First fall degree仮説) $< f_1,...,f_l >$ のグレブナ基底計算 *(F4アルゴリズム)* に出てくる多項式の最大次数は $\leq D_{ff} + O(1)$ である.

実際にはこの仮定は強すぎて反例をつくることができる. 方程式系の解の個数（の上限）をfixするといった工夫が必要であるが, ここでは触れない. 基本的に、First fall degree仮説は方程式系をグレブナ基底を使って解く場合のベンチマークであると考えるのが妥当な解釈であると思われる.

補助定理 2 $< f_1,...,f_l >$ のグレブナ基底計算にかかるコストは, *First fall degree* 仮説の下で,

$$O(N^{(D_{ff}+O(1))\times C})$$

である. ここで, $N = n'd$ は（ローカル）変数の個数であり, C は線形代数定数である.

[4] これはFaugére らのテクニックを $p > 2$ に拡張したものである

6 Weil decentから得られる曲線のFirst fall degree

$\overrightarrow{F_0} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, ..., \overrightarrow{X_d}]$ とせよ. $a_{i,j,k} \in \mathbb{F}_p$ を基底の関係式 $w_i w_j = \sum_{k=1}^{n} a_{i,j,k} w_k$ を満たす基礎体の元とする. このとき, 以下の補助定理が成り立つ.

補助定理 3 $k = 1, ..., n$ に対して, 式

$$[\overrightarrow{m_1} \cdot \overrightarrow{F_0}]_k^{\downarrow} \equiv \sum_{i=1}^{n} [w_i \cdot \overrightarrow{m_1}]_k^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow} \bmod S_{fe}$$

が成り立つ.

証明関係式 $\sum_{k=1}^{n} [w_i \overrightarrow{m_1}]_k^{\downarrow} w_k = wd(w_i \overrightarrow{m_1})$
$= \sum_{k=1}^{n} w_i [\overrightarrow{m_1}]_k^{\downarrow} w_k = \sum_{j=1}^{n} [\overrightarrow{m_1}]_j^{\downarrow} w_i w_j$
$= \sum_{k=1}^{n} (\sum_{j=1}^{n} a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}) w_k$ より,
$[w_i \overrightarrow{m_1}]_k^{\downarrow} = \sum_{j=1}^{n} a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}$ が判る.

これを使って $wd(\overrightarrow{m_1} \cdot \overrightarrow{F_0})$ を式変形することにより,
$wd(\overrightarrow{m_1} \cdot \overrightarrow{F_0}) \equiv wd(\overrightarrow{m_1}) \times wd(\overrightarrow{F_0}) \bmod S_{fe}$
$= wd(\overrightarrow{m_1}) \times wd(\overrightarrow{F_0})$
$= \sum_{i=1}^{n} \sum_{j=1}^{n} [\overrightarrow{m_1}]_j^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow} w_i w_j$
$= \sum_k (\sum_i (\sum_j a_{i,j,k} [\overrightarrow{m_1}]_j^{\downarrow}) [\overrightarrow{F_0}]_i^{\downarrow}) w_k$
$= \sum_k (\sum_i [w_i \overrightarrow{m_1}]_k^{\downarrow} [\overrightarrow{F_0}]_i^{\downarrow}) w_k$ が判り, 証明が完成する. (証明終)

また, heuristicalな仮定1より,

仮定 3 $\deg[w_i \overrightarrow{X_1}]_1^{\downarrow} = ... = \deg[w_i \overrightarrow{X_1}]_n^{\downarrow} = 1$ 及び, $(p-1)d\lfloor \log_p \deg(\overrightarrow{F}) \rfloor \sim D_{heu} := \deg[\overrightarrow{F}]_1^{\downarrow} = ... = \deg[\overrightarrow{F}]_n^{\downarrow} \geq \deg[\overrightarrow{X_1} \cdot \overrightarrow{F}]_k^{\downarrow}$ が成り立つ.

ここで, 先の補助定理の式の $\equiv \bmod S_{fe}$ を $=$ に置き換えてみると, 方程式系 $\{[\overrightarrow{F}]_i^{\downarrow} | 1 \leq i \leq n\}$ の First fall degree が $D_{heu} + 1 (= 1 + \deg[\overrightarrow{F}]_1^{\downarrow})$ で抑えられるという意味の式がfall出てくる. 実際にはこのような置き換えはそのままでは意味を為さないので, その修正を行う.

7 Field Equations を法として合同な多項式の性質

まず、次の小さな例を考える.

例 4. X, Y, Z を $\mathbb{F}_2$ を動くローカル変数とする. Field quationは $S_{fe} = \{X^2 + X, Y^2 + Y, Z^2 + Z\}$ のように書かれていることに注意せよ.
$F = (X^2 + X)(Y^2 + Y) + (X^2 + X)(Y^2 + Z) \in \mathbb{F}_2[X, Y, Z]$ とおく. 作り方より, $F \equiv 0 \bmod S_{fe}$ であるが、式を展開して確認すると $F = X^2Y + Y^2Z + YZ + X^2Z + XY^2 + XZ$ であり次数は $\deg F = 3$ である.

実際 F は以下のように式変形でき, $F = (X^2+X)(Y^2+Y) + (X^2+X)(Y^2+Z)$
$= (X^2+X)(Y^2+Y) + (X^2+X)(Y^2+Y) + (X^2+X)(Y^2+Y) + (X^2+X)(Y^2+Z)$
$= (X+Z)(Y^2+Y) + (X^2+X)(Y+Z)$. F はより次数の小さなField equationで割り切れる多項式の和で書けてることが判る.
これを一般化することによって次の補助定理が得られる

補助定理 4 $G_1,...,G_N \in \mathbb{F}_p[X_1,..,X_N]$ をローカル多項式とし, $F := \sum_{i=1}^{N} G_i \cdot (X_i^p - X_i)$, $D := \deg F$ と置く. このとき, ローカル多項式 $G'_1,...,G'_N \in \mathbb{F}_p[X_1,..,X_N]$ で $F := \sum_{i=1}^{N} G'_i \cdot (X_i^p - X_i)$ 及び $\deg G'_i \leq D - p$ $(i = 1,...,N)$ を満たすものが存在する.

補助定理11 より導かれる式 $F := -[\overrightarrow{X_1} \cdot \overrightarrow{F}]_k^{\downarrow} + \sum_{i=1}^{n} [w_i \overrightarrow{X_1}]_i^{\downarrow} [\overrightarrow{F}]_i^{\downarrow}$ $(\equiv 0 \bmod S_{fe})$ に上の補助定理を適応する. $\deg F$ は仮定 3 より, $D_{heu}+1 \sim (p-1)d\lfloor \log_p \deg(\overrightarrow{F}) \rfloor + 1$ であるので, $F = \sum_{ij} G_{ij}(X_{ij}^p - X_{ij})$ を満たすローカル多項式 $G_{ij} \in \mathbb{F}_p[\{X_{ij}\}$ で $\deg G_{ij} \leq (p-1)d\lfloor \log_p \deg(\overrightarrow{F}) \rfloor + 1 - p$ を満たすものが存在することが判る. したがって, 次を得る :

定理 1 仮説 *3* の下で, $\{[\overrightarrow{F}]_i^{\downarrow} | 1 \leq i \leq n\} \cup S_{fe}$ の *First fall degree* は $\leq (p-1)d\lfloor \log_p \deg(\overrightarrow{F}) \rfloor + 1$ である.

また, §3 で述べた議論より, 以下を得る :

系 1 *Semave* 多項式 (の多く) は仮説 *3* を満たしているとせよ. また, *First fall degree* 仮説が成り立っているとせよ. この時, 楕円曲線 $E/\mathbb{F}_{p^n}$ (p は小さな素数) の離散対数問題は $O(exp(n^{2/3+o(1)}))$ で解けると見積もられる.

8 重みの理論と First fall degree の正確な見積もり

$\overrightarrow{F}$ を条件 $\deg \overrightarrow{F} \ll p^{n'-1}$ を満たすグローバル多項式とする. ここでは, その Weil descent から得られる曲線の $\deg(wd(\overrightarrow{F}))$ や $\deg([\overrightarrow{F}]_i^{\downarrow})$ $(i = 1,...,n)$ といった次数について考察する. 一般にこれらの次数を正確に知ることはできないが, あるグローバル多項式 $\overrightarrow{m_0}$ で, $\deg_{\overrightarrow{X_i}}(\overrightarrow{m_0}\overrightarrow{F}) = p^{\alpha} - 1$ 型となるものをとり, 積の Weil descent を考えることにより, $\deg(wd(\overrightarrow{m_0}\overrightarrow{F}))$ や $\deg([\overrightarrow{m_0}\overrightarrow{F}]_i^{\downarrow})$ $(i = 1,...,n)$ を正確に見積もることができる.

定義 2 $e = \sum_{k=0}^{\lfloor \log_p e \rfloor} e_k p^k$ $(0 \leq e_k \leq p-1)$ を $\leq p^{n'-1}$ を満たす自然数とする. またその重みを $wt(e) := \sum_{k=0}^{\lfloor \log_p e \rfloor} e_k$ と置く.
グローバル変数 $\overrightarrow{X}$ と自然数 e $(\leq p^{n'-1})$ に対して, $wt(\overrightarrow{X}^e) := wt(e)$ と置き, グローバル単項式 $\overrightarrow{m} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i}$ で $0 \leq e_i \leq p^{n'-1}$ を満たすものに対して, $wt(\overrightarrow{m}) := \sum_{i=1}^{d} wt(e_i)$ と置く.

以下では, ベクトル空間 $\mathbb{F}_{p^n}/\mathbb{F}_p$ の基底 $\{w_i\}$ のとり方について, 一般性を失わない仮定をする;

仮定 4 (基底の取り方) サイズが $n' \times n'$ の行列 $M := (w_j^{p^{i-1}})_{1 \leq i,j \leq n'}$ は可逆である.

補助定理 5 グローバル単項式
$\overrightarrow{m} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i}$ で $0 \leq e_i \leq p^{n'-1}$
を満たすものについて,
$\deg(wd(\overrightarrow{m})) = \sum_{i=1}^{d} wt(e_i)$ が成り立つ.

証明式 $\deg(wd(\overrightarrow{X_l}^{e_l})) = wt(e_l)$ が成り立つことを言えば充分である. $e_{l,k}$ を $e_l = \sum_{k=0}^{\lfloor \log_p e_l \rfloor} e_{l,k}p^k$ $(0 \leq e_{l,k} \leq p-1)$ を満たす整数とし, $\begin{pmatrix} Y_1 \\ \vdots \\ Y_{n'} \end{pmatrix} := M \begin{pmatrix} X_{l,1} \\ \vdots \\ X_{l,n'} \end{pmatrix}$ と置く. $\overrightarrow{X_l} = \sum_{j=1}^{n'} X_{l,j}w_j$ より, $\overrightarrow{X_l}^{p^{i-1}} \equiv \sum_{j=1}^{n'} X_{l,j}w_j^{p^{i-1}} \bmod S_{fe} = Y_i$ 及び $wd(\overrightarrow{X_l}^{e_l}) \equiv \prod_{i=0}^{\lfloor \log_p e_l \rfloor} Y_{i+1}^{e_{l,i}} \bmod S_{fe}$ が判る. (ここで $e_l \leq p^{n'-1}$ という条件が $\log_p e_l \leq n'-1$ の形で使われることに注意せよ.) 従って, $\deg_{Y_1,\ldots,Y_{n'}} wd(\overrightarrow{X_l}^{e_l}) = wt(e_l)$ が判り, 行列 M の可逆性より, $\deg wd(\overrightarrow{X_l}^{e_l}) = \deg_{X_{l,1},\ldots,X_{l,n'}} wd(\overrightarrow{X_l}^{e_l}) = wt(e_l)$ という式も判る. (もし $wt(e_l) > \deg wd(\overrightarrow{X_l}^{e_l}) = \deg_{X_{l,1},\ldots,X_{l,n'}} wd(\overrightarrow{X_l}^{e_l})$ を仮定すると, $X_{l,i} := \sum_{j=1}^{n'} M_{i,j}^{-1}Y_j$ を $wd(\overrightarrow{X_l}^{e_l})$ に代入することにより, $\deg_{Y_1,\ldots,Y_{n'}} wd(\overrightarrow{X_l}^{e_l}) < wt(e_l)$ を得るが, これは矛盾である.) (**証明終**).

補助定理 6 グローバル単項式
$\overrightarrow{m} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i}$
で性質 $0 \leq e_i \leq p^{n'-1}$ を満たすものについて, ある定数 $c \in \mathbb{F}_{p^n}^{\times}$ で
$\deg[c\overrightarrow{m}]_j^{\downarrow} = wt(\overrightarrow{m})$ が任意の $j = 1, \ldots, n$ について成り立つものが存在する.

証明 $c_0 \cdot m$ $(c_0 \in \mathbb{F}_{p^n}^{\times}, m \in Mon(\{X_{i,j}\}))$ を $wd(\overrightarrow{m})$ でその次数が丁度 $\deg wd(\overrightarrow{m})$ と一致する項 (のうちの 1 つ) とせよ. $c := c_0^{-1} \cdot \sum_{i=1}^{n} w_i$ は, 上の補助定理の性質を満たす. (**証明終**).

補助定理 7 α を自然数とせよ. $wt(p^\alpha - 1) = (p-1)\alpha$ かつ $x \leq 2p^\alpha - p^{\alpha-1} - 2$ で $x = p^\alpha - 1$ でない自然数 x に対して, $wt(x) < (p-1)\alpha$ が成り立つ.

$\overrightarrow{F} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, \ldots, \overrightarrow{X_d}]$ を $\deg \overrightarrow{F} \ll p^{n'-1}$ を満たすグローバル多項式とせよ. $\overrightarrow{F}$ の単項式で, その (総) 次数が最大となるもの ($\deg \overrightarrow{M}_{max} \geq \deg \overrightarrow{M}$ for any $M \in Mon(\overrightarrow{F})$) (複数存在する) のうち一つを $\overrightarrow{M}_{max} = \prod_{i=1}^{d} \overrightarrow{X_i}^{E_i} \in Mon(\overrightarrow{F})$ として固定せよ. $\alpha = \alpha(\overrightarrow{F})$ を自然数で $p^\alpha - 1 + \deg \overrightarrow{F} < 2p^\alpha - p^{\alpha-1} - 2 \leq p^{n'-1}$ を満たすものとせよ.
条件 $\deg \overrightarrow{F} \ll p^{n'-1}$ より, α は $O(\log_p \deg \overrightarrow{F})$ 程度の大きさでとることができることを注意する.
$H := p^\alpha - p^{\alpha-1} - \deg \overrightarrow{F} - 1 (> 0)$, $D := \sum_{i=1}^{d} E_i = \deg \overrightarrow{F}$ と置く.
$\tau \in \mathbb{F}_{p^n} \setminus \{\sum_{i=1}^{n'} x_i w_i \,|\, x_i \in \mathbb{F}_p\}$, を固定し, グローバル多項式 $\overrightarrow{m}_0$ を以下で定義する ; $\overrightarrow{m_0} := \prod_{i=1}^{d} (\overrightarrow{X_i} - \tau)^{p^\alpha - 1 - E_i} \in \mathbb{F}_{p^n}[\overrightarrow{X_1}, \ldots, \overrightarrow{X_d}]$. $\tau \notin \{\sum_{i=1}^{n'} x_i w_i \,|\, x_i \in \mathbb{F}_p\}$ であるので, 次の補助定理が成り立つ;

補助定理 8 方程式系
$\{[\overrightarrow{F}]_i^{\downarrow} = 0 \,|\, 1 \leq i \leq n\} \cup \{f = 0 \,|\, f \in S_{fe}\}$ の解は, 方程式系
$\{[\overrightarrow{m_0}\overrightarrow{F}]_i^{\downarrow} = 0 \,|\, 1 \leq i \leq n\} \cup \{f = 0 \,|\, f \in S_{fe}\}$ の解と一致する.

$\overrightarrow{M} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e_i} \in Mon(\overrightarrow{F})$ 及び $\overrightarrow{m} = \prod_{i=1}^{d} \overrightarrow{X_i}^{e'_i} \in Mon(\overrightarrow{m_0})$ とせよ. $wt(\overrightarrow{m}\overrightarrow{M}) = wt(\prod_{i=1}^{d} \overrightarrow{X_i}^{e_i+e'_i}) = \sum_{i=1}^{d} wt(e_i+e'_i)$ に注意すると, $0 \leq e_i + e'_i \leq p^\alpha - 1 + (e_i - E_i) <$

$p^\alpha-1+\deg\overrightarrow{F}\leq 2p^\alpha-p^{\alpha-1}-1$ が判る. また, 補助定理7より, $wt(e_i+e_i')\leq(p-1)\alpha$ 及び $wt(\overrightarrow{m}\overrightarrow{M})\leq(p-1)d\alpha$ が判る. 以下 $wt(\overrightarrow{m}\overrightarrow{M})=(p-1)d\alpha$ が成り立つ必要十分条件を調べる. この条件は $e_i+e_i'=p^\alpha-1$ が全ての $i\in[1,...,d]$ に対して成り立つことである. $\sum_{i=1}^d e_i\leq\deg\overrightarrow{F}=\sum_{i=1}^d E_i=D$ 及び $\sum_{i=1}^d e_i'\leq\sum_{i=1}^d p^\alpha-1-E_i=d(p^\alpha-1)-D$ より, この条件は $e_i'=p^\alpha-1-E_i$ かつ $e_i=E_i$ $(i\in[1,...,d])$ が成り立つ事と同値である. (つまり $\overrightarrow{M}=\overrightarrow{M}_{max}$, $\overrightarrow{m}=\prod_{i=1}^d\overrightarrow{X_i}^{p^\alpha-1-E_i}$ という場合に限り等式が成り立つ.) 従って補助定理6より, 次の結果を得る;

補助定理 9 $\deg\overrightarrow{F}\ll p^{n'-1}$ とせよ. α を $p^\alpha-1+\deg\overrightarrow{F}<2p^\alpha-p^{\alpha-1}-2\leq p^{n'-1}$ を満たす自然数とせよ. このとき次が成り立つ
1) $\deg wd(\overrightarrow{m_0}\cdot\overrightarrow{F})=(p-1)d\alpha$.
2) $c_0\in\mathbb{F}_{p^n}^\times$ で, 全ての $j=1,...,n$ に対して式
$\deg[c_0\overrightarrow{m_0}\cdot\overrightarrow{F}]_j^\downarrow=(p-1)d\alpha$ が成り立つものが存在する.

また, $\overrightarrow{m_1}:=\prod_{i=1}^d\overrightarrow{X_i}^{f_i}$ $(0\leq f_i\leq H)$ と置け. $\overrightarrow{M}=\prod_{i=1}^d\overrightarrow{X_i}^{e_i}\in Mon(\overrightarrow{F})$ 及び $\overrightarrow{m}=\prod_{i=1}^d\overrightarrow{X_i}^{e_i'}\in Mon(\overrightarrow{m_0})$ とする. このとき, $wt(\overrightarrow{m_1}\overrightarrow{m}\cdot\overrightarrow{M})=wt(\prod_{i=1}^d\overrightarrow{X_i}^{p^\alpha-1+f_i+(e_i-E_i)})$ であり, また, $0\leq f_i+e_i+e_i'<p^\alpha-1+f_i+(e_i-E_i)\leq p^\alpha-1+\deg\overrightarrow{F}+N\leq 2p^\alpha-p^{\alpha-1}-1$ であることと補助定理7から, $wt(\overrightarrow{m_1}\overrightarrow{m_0}\cdot\overrightarrow{M})\leq(p-1)d\alpha$ が判る. 従って補助定理6より, 次の結果が判る;

補助定理 10 $\deg\overrightarrow{F}\ll p^{n'-1}$ とし, α を $p^\alpha-1+\deg\overrightarrow{F}<2p^\alpha-p^{\alpha-1}-2\leq p^{n'-1}$ を満たす自然数とする. このとき次が成り立つ
1) $\deg(wd(\overrightarrow{m_1}\cdot\overrightarrow{m_0}\cdot\overrightarrow{F}))\leq(p-1)d\alpha$.
2) 任意の $c\in\mathbb{F}_{p^n}^\times$ に対して, $\deg([c\cdot\overrightarrow{m_1}\cdot\overrightarrow{m_0}\cdot\overrightarrow{F}]_j^\downarrow)\leq(p-1)d\alpha$ $(j=1,...,n)$ が成り立つ.

以下では $\overrightarrow{F_0}:=c_0\cdot\overrightarrow{m}_0\cdot\overrightarrow{F}$ と置く.
任意の $I\in[1,..,n]$ に対して, $\overrightarrow{m_1}$ が定数で無い事と $\deg wd(w_I\overrightarrow{m_1})\geq 1$ である事から, ある自然数 $k(I)\in[1,...,n]$ で $\deg[w_I\overrightarrow{m_1}]_{k(I)}^\downarrow\geq 1$ であるものが存在する. 補助定理3で得られた式より,

$$[\overrightarrow{m_1}\overrightarrow{F_0}]_{k(I)}^\downarrow\equiv\sum_{i=1}^n[w_i\overrightarrow{m_1}]_{k(I)}^\downarrow[\overrightarrow{F_0}]_i^\downarrow \bmod S_{fe}$$

が判るが, 補助定理 9 と補助定理 10 より, 不等式 $\deg[\overrightarrow{F_0}]_i^\downarrow=(p-1)d\alpha$ と, $1\leq\deg[\overrightarrow{m_1}\overrightarrow{F_0}]_{k(I)}^\downarrow\leq(p-1)d\alpha$ が成り立つことを思い出し, §7 で述べた field equations に関する結果を使うことによって, 次の First fall degree の精密な上からの見積もりが完成する;

定理 2 方程式系

$$\{[\overrightarrow{F_0}]_k^\downarrow\,|\,k=1,...,n\}\cup S_{fe}$$

の *First fall degree* は上から $\leq(p-1)d\alpha+1$ で抑えられる. [5]

[5] $\overrightarrow{m_1}$ は次数1のグローバル単項式に取ることが可能であることを注意せよ

この補題の $\overrightarrow{F}$ に Semaev 多項式を適応することにより, §7 で述べた議論より Heuristics を除いた議論を行うことがでる. 従って以下を得る :

系 2 *First fall degree* 仮説が成り立っているとせよ. この時, 楕円曲線 $E/\mathbb{F}_{p^n}$ (p は小さな素数) の離散対数問題は $O(exp(n^{2/3+o(1)}))$ で解けると見積もられる.

9 ヤコビアン群の理論に関する記号

以下では、$C : f(x,y) = 0$ を体 $\mathbb{F}_{p^n}$ 上定義された標数 g の plane 曲線, ∞ を曲線上の無限遠点にある, ある点 (fix する), $D_0 = Q_1 + Q_2 + ... + Q_g - g\infty$ をそのヤコビアン群 $\mathbf{Jac}(C/\mathbb{F}_{p^n})$ の元とする. また、D_0 も以下の議論では fix して考え、D_0 を曲線上の点から得られる ($P - \infty$ 型の) ヤコビアン群の元の一次結合に分解する条件について調べる. また, $d_y := \deg_y f(x,y)$ および $\phi_1(x) := \prod_{i=1}^{g} x - x(Q_i)$ と置く.

10 Riemann-Roch 空間

補題 1 (Riemann-Roch) D を $\deg D \geq 2g-1$ である (曲線の)*divisor* とする. このとき $dimL(D) = \deg D - g + 1$ が成り立つ.

d を $d > 2g-1$ を満たす整数とする. $D := d\infty - D_0 = (d+g)\infty - Q_1 - Q_2 - ... - Q_g$ と置く. Riemann-Roch の定理 (Proposition 1) より, 関数体の Riemann-Roch 空間内で線形独立な元 $f_i(x,y) \in \mathbb{F}_{p^n}(C)$ $(i = 0, 1, .., d-g)$ で $f_i(x,y)$ が全ての $Q_1, .., Q_g$ で zero を取り、∞ 以外の点では pole をもたないものが取れる. また、$f_i(x,y)$ の順序を入れ替えて $\mathrm{ord}_\infty f_i(x,y) < -d-g$ $(i = 1, 2, .., d-g)$ の時かつ $\mathrm{ord}_\infty f_0(x,y) = -d-g$ と取る事ができる. また、Riemann-Roch の定理より, 関数体 $F_{p^n}(C)$ の元 $h(x,y)$ で全ての $Q_1, .., Q_g$ で $h(x,y) = 0$ となり, また ∞ 以外で pole をもたず、$\mathrm{ord}_\infty h(x,y) = -d-g$ であるものは, 定数倍を除いて $h(x,y) = f_0(x,y) + a_1 f_1(x,y) + ... + a_{d-g} f_{d-g}(x,y)$ $(a_i \in \mathbb{F}_{p^n})$ の形で書かれる事が判る.

A_i を変数とし,

$$H(x,y) := f_0(x,y) + A_1 f_1(x,y) + ... + A_{d-g} f_{d-g}(x,y)$$

と置く. また、 $S(x) := \mathrm{resultant}_y(f(x,y), H(x,y))$ と置く.

補助定理 11 *1.* $\deg_x S(x) = d + g$.
2. $\phi_1(x) \mid S(x)$
3. $g(x) := S(x)/\phi_1(x)$ と置くと $\deg_x g(x) = d$ である.
4. C_i を $g(x)$ の X^i の係数 とする ($g(x) = \sum_{i=0}^{d} C_i x^i$ と書かれたとする). このとき C_i は $A_1, ..., A_{d-g}$ の全次数が $\leq d_y$ 以下である多項式である.

11 多次多変数方程式系

§10 での議論から次の補助定理が得られる;

補助定理 12 $P_i=(x_i,y_i)\in C(\bar{\mathbb{F}}_p)$ $(i=1,2,..,d)$ とせよ. また、s_i を $\prod_{i=1}^{d}(x-x_i)$ の x^i の係数とする. 関係式 $D_0+P_1+...+P_d-d\infty\sim 0$ が成り立つ時, $a_i\in\bar{\mathbb{F}}_p$ $(i=1,2,..,d-g)$ で以下を満たすものが存在する:
1. $h(x,y)=Constant\times H(x,y)|_{A_i=a_i}$,
2. $s_i\cdot C_d|_{A_i=a_i}=C_i|_{A_i=a_i}$ $(i=0,1,..,d-1)$.

以下では $X_i\,(i=1,..,d)$ を変数とし、$S_i=S_i(X_1,..,X_d)\in\mathbb{F}_{p^n}[X_1,..,X_d]$ を $\prod_{i=1}^{d}(X-X_i)$ の X^i の係数と置く.

$$g_i(A_1,..,A_{d-g};X_1,..,X_d):=S_i(X_1,..,X_d)C_d(A_1,..,A_{d-g})-C_i(A_1,..,A_{d-g}),\quad (i=0,..,d-1)$$

と置き, 次の多次多変数方程式系を考える;

$$EQS_1:\{g_i(A_1,..,A_{d-g};X_1,..,X_d)=0|i=0,..,d-1\}.$$

補助定理 13 EQS_1 が解 $(a_1,..a_{d-g};x_1,..,x_d)\in\mathbb{A}^{2d-g}(\bar{\mathbb{F}}_p)$ をもつ時, $P_i\in C(\bar{\mathbb{F}}_p)$ $(i=1,..,d)$ で $D_0+P_1+...+P_d-d\infty\sim 0$ および $x(P_i)=x_i$ $(i=1,..,d)$ を満たすものが存在する.

証明 $h(x,y)=f_0(x,y)+\sum_{i=1}^{d-g}a_if_i(x,y)$ と置き, P_i たちを $C(\bar{\mathbb{F}}_p)$ 上の点で $h(x,y)=0$ と交わる $Q_1,..,Q_g$ 以外の点とする. このとき $\{x(P_i)|i=1,..,d\}=\{x_1,..,x_d\}$ であり証明が完成する. (**証明終**)
補助定理 12,13 より, 次が判る;

補題 2 次の *(1) (2)* は同値である;
1) EQS_1 は解 $(a_1,..,a_{d-g};x_1,..,x_d)\in\mathbb{A}^{2d-g}(\bar{\mathbb{F}}_p)$ を持つ
2) 曲線上の点 $P_i\in C(\bar{\mathbb{F}}_p)$ $(i=1,..,d)$ で $x(P_i)=x_i$ $(i=1,..,d)$ および $D_0+P_1+...+P_d\sim 0$ を満たすものが存在する.

$T_1,...,T_g$ を新たな変数とし
$h_i(A_1,..,A_{d-g};X_1,..,X_d;T_1,..,T_g):=g_i(A_1,..,A_{d-g};X_1,..,X_d),\quad (i=0,..,d-g-1)$,
$h_{d-g}(A_1,..,A_{d-g};X_1,..,X_d;T_1,..,T_g):=\sum_{i=1}^{g}T_i\cdot g_{i+d-g-1}(A_1,..,A_{d-g};X_1,..,X_d)$,
とし、次の多次多変数方程式系を考える;

$$EQS_2:\{h_i(A_1,..,A_{d-g};X_1,..,X_d;T_1,..,T_g)=0|i=0,..,d-g\}.$$

12 絶対終結式

ここのセクションでは方程式系 EQS_2 の絶対終結式 (cf.[1] §3) についての性質をを調べる. ここでは、まず $\{A_i\}$ のみを変数と考え、$\{X_i\}\cup\{T_i\}$ たちを定数と思い $\{A_i\}$ を EQS_2 から消去する. 厳密な議論をするためには、斎次多項式たちから成る方程式系を使う必要があるが (無限遠点上の点に関する取り扱いも必要であるが)、これはややこしいので、通常の斎次でない多項式に対する簡略化した形の議論を行う.

$D_i:=\deg_{\{X_i\}}h_i(\leq d_y)$ $(i=0,..,d-g)$ 及び $D=\sum_{i=0}^{d-g}D_i-(d-g)\infty$ と置く. このとき $D\leq(d-g)d_y$ であることに注意する. M_{all} を $A_1,..,A_{d-g}$ の単項式で次数が

$\leq D$であるものの全体とする. このような単項式全体の数$\#M_{all}$は$\begin{pmatrix} d-g+D \\ d-g \end{pmatrix}$
$\leq \begin{pmatrix} (d-g)(d_y-1) \\ d-g \end{pmatrix}$であり、Stirling公式, つまり$N! \sim \sqrt{2\pi N} N^N exp(-N)$が成り立つという式, を使うと$\#M_{all} \leq \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \{\frac{(d_y+1)^{d_y+1}}{d_y^{d_y}}\}^{d-g}$が判る.
$S_0 := \{m \in M_{all} \,|\, \deg_{\{X_i\}} m \leq D - D_0\}$,
$S_1 := \{m \in M_{all} \,|\, \deg_{\{X_i\}} m > D - D_0, X_1^{D_1} | m\}$,
$S_2 := \{m \in M_{all} \,|\, \deg_{\{X_i\}} m > D - D_0, X_1^{D_1} \not| m, X_2^{D_2} | m\}$,
$\cdots\cdots$
$S_{d-g} := \{m \in M_{all} \,|\, \deg_{\{X_i\}} m > D - D_0, X_1^{D_1} \not| m, \cdots, X_{d-g-1}^{D_{d-g-1}} \not| m, X_{d-g}^{D_{d-g}} | m\}$,
と置く. $\#S_{d-g} = D_0 D_1 ... D_{d-g-1}$及び、$M_{all} = \cup_{i=0}^{d-g} S_i$ (M_{all}のdisjointな分割), $\#M_{all} = \sum_{i=1}^{d-g} \#S_i$といった性質が成り立つ事が知られている.

$M_{all} = \{\overrightarrow{M}_1, ..., \overrightarrow{M}_{\#M_{all}}\}$及び$\cup_{i=0}^{d-g} \{h_i m \,|\, m \in S_i\} = \{G_1, ..., G_{\#M_{all}}\}$と置く. また、$G_{ij} \in \mathbb{F}_p[\{X_i\} \cup \{T_i\}]$を$G_i = \sum_{j=1}^{\#M_{all}} G_{ij} \overrightarrow{M}_j$である多項式とし、絶対終結式を下記で定義する:

$$Res(X_1, .., X_d; T_1, .., T_g) = \text{deteminant of}([G_{ij}]_{1 \leq i,j \leq \#M_{all}}) \in \mathbb{F}_p[\{X_i\} \cup \{T_i\}].$$

Resは絶対終結式として知られ次の性質をもつ; [6]

補助定理 14 $(x_1, ..., x_d) \in \mathbb{A}^d(\overline{\mathbb{F}}_p)$とせよ. 次の *1) 2)* は（実質的に）同値である;
1) $Res(x_1, .., x_d; T_1, .., T_g) = 0$ *(T_iたちは変数のままである).*
2) $(a_1, ..., a_{d-g}) \in \mathbb{A}^{d-g}(\overline{\mathbb{F}}_p)$で$(a_1, .., a_{d-g}; x_1, .., x_g)$が方程式系$EQS_1$の解であるものが存在する.

補助定理 15 *1)* $\deg_{\{T_i\}} Res(X_1, .., X_d; T_1, .., T_g) \leq d_y^{d-g}$.
2) $\deg_{\{X_i\}} Res(X_1, .., X_d; T_1, .., T_g) \leq d \cdot \#M_{all} \leq d \cdot \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \{\frac{(d_y+1)^{d_y+1}}{d_y^{d_y}}\}^{d-g}$.

証明絶対終結式を表す行列でT_iの出てくる行数は$\#S_{d-g} = D_0 D_1 ... D_{d-g-1} \leq d_y^{d-g}$であり、その行において出てくる行列成分の$\{T_i\}$に関する次数は1である. これより 1) が判る. また、行列成分の$\{X_i\}$に関する次数は$\leq d$であり、行列のサイズが$\#M_{all}$であることにより.2) を得る. (**証明終**)

$\{m_1, ..., m_N\}$を$\{T_1, .., T_g\}$の単項式で絶対終結式$Res(X_1, .., X_d; T_1, .., T_g)$のある項を割り切るもの全体の集合とし、$Res(X_1, .., X_d; T_1, .., T_g) = \sum_{i=1}^{N} H_i(X_1, .., X_d) \cdot m_i$と置く. 補助定理14より, $\deg_{\{T_i\}} Res \leq d_y^{d-g}$, 及び$N = \begin{pmatrix} \deg_{\{T_i\}} Res + g \\ g \end{pmatrix} \leq \frac{(d_y^{d-g}+g)^g}{g!}$を得る. また、補助定理14より, $\deg_{\{X_i\}} H_i(X_1, .., X_d) \leq \sqrt{\frac{d_y+1}{2\pi(d-g)d_y}} \{\frac{(d_y+1)^{d_y+1}}{d_y^{d_y}}\}^{d-g}$ $(i = 1, .., N)$が判る.

補助定理14及び補題2で述べた結果を纏めると, 次を得る;

補題 3 $(x_1, ..., x_d) \in \mathbb{A}^d(\overline{\mathbb{F}}_p)$とせよ. 次の *1) 2)* は実質的に同値である;
1) $H_i(x_1, .., x_d) = 0$ *$(i = 1, .., N)$.*
2) $P_i \in C(\overline{\mathbb{F}}_p)$ *$(i = 1, .., d)$*で$x(P_i) = x_i$ *$(i = 1, .., d)$*及び$D_0 + P_1 + ... + P_d \sim 0$を満たすものが存在する.

[6] 実際には、斎次多項式の絶対終結式と、無限遠点上の曲線の点に関する議論が必要であるが、この議論の差異は本議論には余り影響しないとして議論を続ける

この結果によって、ヤコビアン群の元 D_0 の. d 個の曲線上の点への分解[7]が、方程式系 $H_i(x_1,..,x_d)=0$ $(i=1,..,N)$ を解く問題に帰着する.

謝辞 神奈川大学の松尾和人教授には, 本研究を進める上でのアイデア等の討論をして頂いた事に, 九州大学の高木剛教授には最近の研究動向についての情報をお教え頂いた事に, 深く感謝する.

参考文献

[1] D. Cox, J.Little, D. O'Shea, Using Algebraic Geometry, Springer, 1997.

[2] C. Diem, On the discrete logarithm problem in class groups II, preprint, 2011.

[3] J-C. Faugére, L. Perret, C. Petit, and G. Renault, Improving the complexity of index calculus algorithms in elliptic curves over binary fields, EUROCRYPTO 2012, LNCS **7237**, pp.27-44.

[4] F.S. Macaulay, The algebraic Theory of modular systems, 1916, Cambridge.

[5] K. Nagao, Index calculus for Jacobian of hyperelliptic curve of small genus using two large primes, Japan Journal of Industrial and Applied Mathematics, **24**, no.3, 2007.

[6] K. Nagao, Decomposition Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field, 9th International Symposium,ANTS-IX., Nancy, France, July 2010, Proceedings LNCS 6197,Springer, pp.285–300, 2010.

[7] K. Nagao, Decomposition formula of the Jacobian group of plane curve, draft, 2013, https://eprint.iacr.org/2013/548.pdf.

[8] K. Nagao, Equations System coming from Weil descent and subexponential attack for algebraic curve cryptosystem, draft, 2013, https://eprint.iacr.org/2013/549.pdf.

[9] C. Petit and J-J. Quisquater. On Polynomial Systems Arising from a Weil Descent, Asiacrypt 2012, Springer LNCS **7658**, Springer, pp.451-466.

[10] I. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint, 2004.

[7]実際には、x_i に条件をつけた点たちへの分解が必要であるので、ここで得られる H_i たちに、関係式を足して得られる方程式系を解く問題に帰着される