種数２の超楕円曲線の２冪ねじれ点の計算アルゴリズムの改良

小崎 俊二 (情報セキュリティ大学院大学 M2)
松尾和人 (情報セキュリティ大学院大学)

2007年3月3日

大標数の定義体上の種数２の超楕円曲線の位数計算

暗号利用可能な超楕円曲線の構成を目的

- P. Gaudry and R. Harley, 2000
  Schoof**アルゴリズムを基本とし、**63bit**の素体上の位数計算**
  → 2^8 **ねじれ点を利用**

- P. Gaudry and É. Schost, 2004
  多くの改良を行ない80bit**の素体上の位数計算を**１**週間/曲線で実現**
  → ２**冪ねじれ点計算に現れる**16**次多項式の根を求める アルゴリズムを改良**
  → 2^{10} **ねじれ点を利用**

超楕円曲線の位数計算

- p: **奇素数、**$\mathbb{F}_p$**上定義された種数**2**の超楕円曲線**

  $$C : Y^2 = F(X),\ F \in \mathbb{F}_p[X] :\ \text{monic},\ \deg F = 5,\ \textbf{重根をもたない}$$

  $\mathbb{J}_C(\mathbb{F}_p)$**が素位数** $\Rightarrow$ $\underline{F\ \textbf{は}\mathbb{F}_p\textbf{上既約}}$

- p**乗**Frobenius**写像** $\phi_p : \mathbb{J}_C \to \mathbb{J}_C$ **、**ϕ_p**の特性多項式** χ

  $$\sharp\mathbb{J}_C(\mathbb{F}_p) = \chi(1)$$

- χ**の整数係数を決定するために、**$k \in \mathbb{N}$**に対し、**

  $$[\chi(\phi_p) \bmod 2^k]\mathcal{D}_k = 0,\ \text{for}\ {}^\forall\mathcal{D}_k \in \mathbb{J}_C[2^k]$$

  を満足する$\chi \bmod 2^k$**の係数を利用 →** 2^k**ねじれ点を具体的に計算する必要**

GaudryとHarleyの２冪ねじれ点の計算アルゴリズム

２ねじれ点を初期値として２等分点計算を繰り返す

$$\mathcal{D}_1 \in \mathbb{J}_C[2] \to \cdots\ \mathcal{D}_i \in \mathbb{J}_C[2^i] \to \underline{\mathcal{D}_{i+1}\ \text{s.t.}\ [2]\mathcal{D}_{i+1} = \mathcal{D}_i}\ \cdots \to \mathcal{D}_k \in \mathbb{J}_C[2^k]$$

$\mathcal{D}_i$の２等分点計算

$$\mathcal{D}_i = (X^2 + u_1X + u_0, v_1X + v_0),\ u_1, u_0, v_1, v_0 \in \mathbb{F}_q$$

$$[2](X^2 + U_1X + U_0, V_1X + V_0) = \mathcal{D}_i$$

→ 変数$U_1,\ U_0,\ V_1,\ V_0$**の条件**

→ 辞書式順序$U_1 \prec U_0 \prec V_1 \prec V_0$ Gröbner**基底 →**

$$M_1(U_1) = 0,\ U_0 = M_0(U_1),\ V_1 = L_1(U_1),\ V_0 = L_0(U_1),$$
$$M_1, M_0, L_1, L_0 \in \mathbb{F}_q[U_1],\ \deg M_0, \deg L_1, \deg L_0 < \deg M_1 = 16$$

$$M_1(\alpha) = 0$$
$$\Leftrightarrow \left(X^2 + \alpha X + M_0(\alpha), L_1(\alpha) + L_0(\alpha)\right) \in \{\mathcal{D} \mid [2]\mathcal{D} = \mathcal{D}_i\}$$

iの増加 → $\mathbb{F}_q$の拡大次数増加 → 16**次多項式**M_1**の根の計算時間増加**

GaudryとSchostのM_1の根の計算アルゴリズム

$M_0,\ L_1,\ L_0$及び$\mathbb{J}_C[2]$の作用を利用しM_1の根を計算

$$\mathbf{D}_0 := (X^2 + U_1X + M_0(U_1), L_1(U_1)X + L_0(U_1)),\ g \in \mathbb{J}_C[2]$$

$$\rightarrow \mathbf{D}_0 + g = (X^2 + \underline{U_1^{(g)}(U_1)}X + U_0^{(g)}(U_1), V_1^{(g)}(U_1)X + V_0^{(g)}(U_1))$$

$U_1^{(g)} \in \mathbb{F}_q[U_1]/(M_1)$は、$g$の作用による$M_1$の根の置換

$$\begin{array}{ccccc} \mathbb{J}_C[2] \supsetneq & G_3 \supsetneq & G_2 \supsetneq & G_1 \supsetneq & G_0 \\ \wr| & \wr| & \wr| & \wr| & \wr\| \\ (\mathbb{Z}/2\mathbb{Z})^4 & (\mathbb{Z}/2\mathbb{Z})^3 & (\mathbb{Z}/2\mathbb{Z})^2 & (\mathbb{Z}/2\mathbb{Z}) & \{0\} \end{array}$$

に対し、

$$s_{G_j}(U_1) := \sum_{g \in G_j} U_1^{(g)}(U_1) \in \mathbb{F}_q[U_1]/(M_1)$$

→ G_jの元の作用で置換されるM_1の根の部分和

→ $s_{G_j}(U_1)$の$\mathbb{F}_q$上の最小多項式の次数は、$[\mathbb{J}_C[2] : G_j]$

GaudryとSchostのM_1の根の計算アルゴリズム

$s_{G_3}(U_1)$の$\underline{\mathbb{F}_q}$上の最小多項式 → 2次多項式$\underline{T_3}$の根α_3
→$s_{G_2}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3)}$上の最小多項式 → 2次多項式$\underline{T_2}$の根$\alpha_2$
→$s_{G_1}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3,\alpha_2)}$上の最小多項式 → 2次多項式$\underline{T_1}$の根$\alpha_1$
→$s_{G_0}(U_1)$の$\underline{\mathbb{F}_q(\alpha_3,\alpha_2,\alpha_1)}$上の最小多項式 → 2次多項式$\underline{T_0}$の根$\alpha_0$
→ α_0はM_1の根

4つの2次多項式$T_3,\ T_2,\ T_1,\ T_0$を順次解きM_1の根を得る

→ $T_2,\ T_1,\ T_0$の係数体は、$\underline{\mathbb{F}_q}$の拡大体となる可能性
→ M_1の根の計算時間に影響

$T_3,\ T_2,\ T_1,\ T_0$を構成する$G_3,\ G_2,\ G_1$の選び方は？

本研究の概要

2006年12月 JANT第16回研究集会

計算実験より、

- M_1 **の既約因子パターン → すべて1次、またはすべて2次のみ**
- M_1 **の根の共役写像を与える2ねじれ点 → 冪指数に依存せず同一**

適切な G_3, G_2, G_1 **を構成し** T_3, T_2, T_1, T_0 **の根の計算を効率化**

→ Gaudry **と** Schost **の** M_1 **の根を求めるアルゴリズムを改良**

- F **が** $\mathbb{F}_p$ **上既約であるとき、2冪ねじれ点の2等分点の性質より上記事実を証明**
- T_3, T_2, T_1, T_0 **の既約判定を省略 →** M_1 **の根を求めるアルゴリズムを高速化**
- **改良アルゴリズムの実装実験**

M_1 の根の定義される体

命題 1 $M_1 \in \mathbb{F}_q[U_1]$ **の根は、** $\mathbb{F}_q$ **の高々** 2 **次の拡大体上に存在**

$i \in \mathbb{N}$, $\mathcal{D}_i \in \mathbb{J}_C[2^i] \backslash \mathbb{J}_C[2^{i-1}]$、$\mathcal{D}_i^{p^j} := \phi_{p^j}(\mathcal{D}_i)$, $0 \leq j \leq 3$

F: $\mathbb{F}_p$ **上既約** $\Rightarrow \mathbb{J}_C[2^i] = \langle \mathcal{D}_i, \mathcal{D}_i^p, \mathcal{D}_i^{p^2}, \mathcal{D}_i^{p^3} \rangle$

$\mathbb{F}_q$: $\mathcal{D}_i$ **の定義される最小の体** $\Rightarrow \mathbb{J}_C[2] \subset \mathbb{J}_C[2^i] \subset \mathbb{J}_C(\mathbb{F}_q)$

$\mathbb{J}_C[2] \subset \mathbb{J}_C(\mathbb{F}_q)$ **のとき、** $[2]\mathcal{D} = \mathcal{D}_i \Rightarrow \mathcal{D}^{q^2} = \mathcal{D}$

$$\{\mathcal{D} \mid [2]\mathcal{D} = \mathcal{D}_i\} = \left\{ \left(X^2 + \alpha X + M_0(\alpha), L_1(\alpha) + L_0(\alpha) \right) \mid M_1(\alpha) = 0 \right\}$$

M_1 の既約因子の次数

命題 2 $M_1 \in \mathbb{F}_q[U_1]$ **の** $\mathbb{F}_q$ **上の既約因子は、すべて同じ次数**

$i \in \mathbb{N}$, $\mathcal{D}_i \in \mathbb{J}_C[2^i] \backslash \mathbb{J}_C[2^{i-1}]$, $\mathcal{D}_{i+1}$ s.t. $[2]\mathcal{D}_{i+1} = \mathcal{D}_i$, $g \in \mathbb{J}_C[2]$、

$\mathbb{J}_C[2] \subset \mathbb{J}_C(\mathbb{F}_q) \Rightarrow \mathcal{D}_{i+1}$ **と** $\mathcal{D}_{i+1} + g$ **の定義される最小の体は同一**

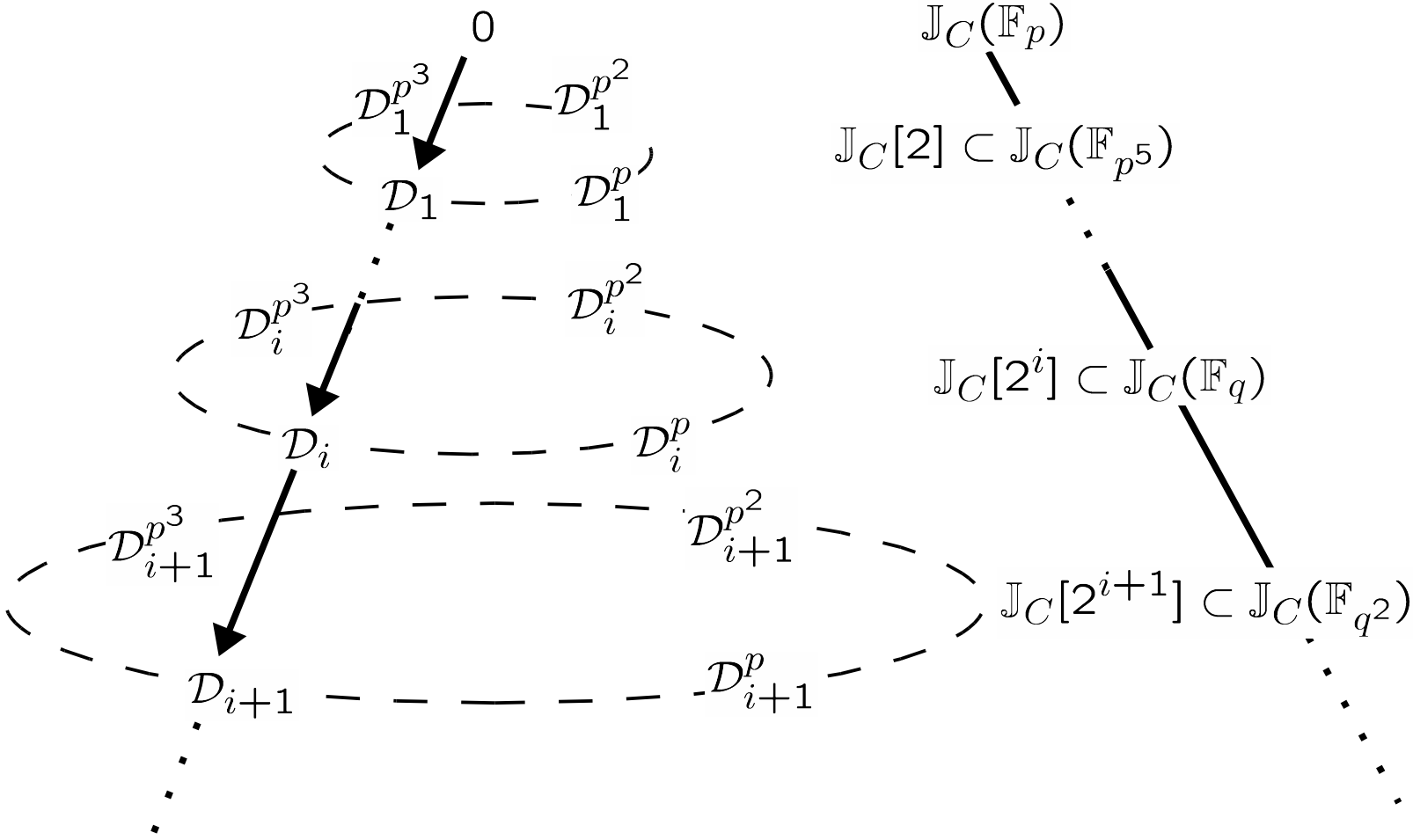
$$\{\mathcal{D}_{i+1} + g \mid g \in \mathbb{J}_C[2]\} = \{\mathcal{D} \mid [2]\mathcal{D} = \mathcal{D}_i\}$$
$$= \left\{ \left(X^2 + \alpha X + M_0(\alpha), L_1(\alpha) + L_0(\alpha) \right) \mid M_1(\alpha) = 0 \right\}$$

命題1, **命題**2 **より**

$$M_1 = \overbrace{(X - a_1)(X - a_2) \cdots (X - a_{15})(X - a_{16})}^{16}$$

または $\overbrace{(X^2 + a_1 X + a_0) \cdots (X^2 + h_1 X + h_0)}^{8}$

２冪ねじれ点の２等分点の定義される体



$M_1 \in \mathbb{F}_q[U_1]$ **が２次の既約因子を持つ場合、**

T_3, T_2, T_1: **可約、** T_0: **既約 → 効率的に** M_1 **の根を計算**

T_0を既約とするG_3，G_2，G_1の構成

T_0が$\mathbb{F}_q$上既約 $\Rightarrow$ T_1の根 $\alpha_1 \in \mathbb{F}_q$ $\Rightarrow$ $s_{G_1}(U_1)$がM_1の共役根の和

$\mathbb{J}_C[2] = \langle g_1, g_2, g_3, g_4 \rangle$

$$G_1 = \langle g_1 \rangle \subsetneq G_2 = \langle g_1, g_2 \rangle \subsetneq G_3 = \langle g_1, g_2, g_3 \rangle$$

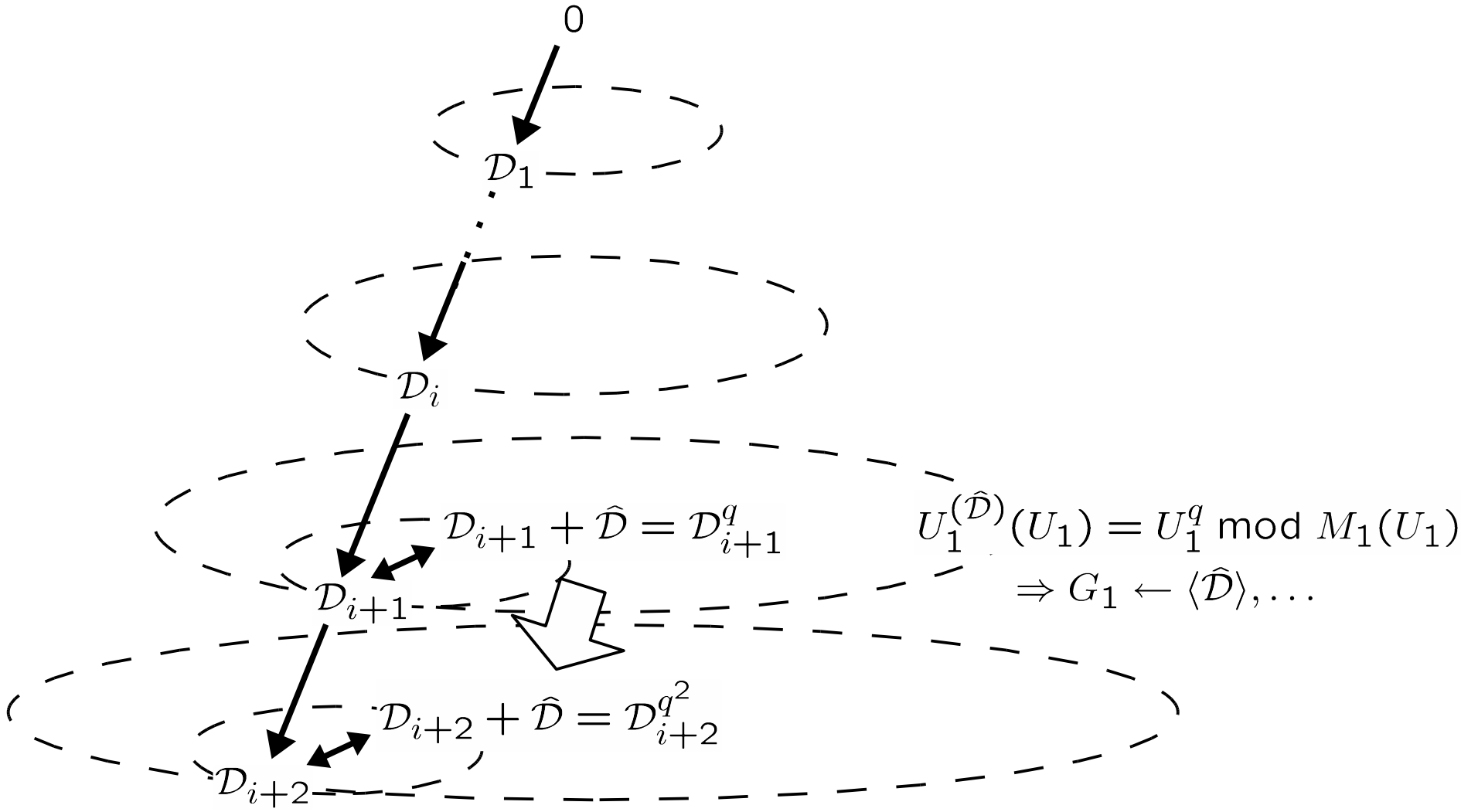
$$\underline{U_1^{(\widehat{\mathcal{D}})}(U_1) = U_1^q \bmod M_1(U_1)}$$

を満足する$\widehat{\mathcal{D}} \in \mathbb{J}_C[2]$を探索 → $g_1 := \widehat{\mathcal{D}}$

冪指数の増加に伴い、$U_1^q \bmod M_1(U_1)$の計算時間増加

冪指数に依らず、同一の$\widehat{\mathcal{D}}$ → G_3, G_2, G_1の構成は1回行なえばよい

２冪ねじれ点の２等分点の共役写像を与える２ねじれ点



２冪ねじれ点の２等分点に作用する２ねじれ点の性質

$\mathcal{D}_i$の２等分点 → $\mathbf{D}_{i+1} := (X^2 + U_1 X + M_0^{(i+1)}, L_1^{(i+1)} X + L_0^{(i+1)})$
$\mathcal{D}_{i+1}$の２等分点 → $\mathbf{D}_{i+2} := (X^2 + U_1 X + M_0^{(i+2)}, L_1^{(i+2)} X + L_0^{(i+2)})$

命題 ３ $i > 1$、$\mathcal{D}_i \in \mathbb{J}_C[2^i] \backslash \mathbb{J}_C[2^{i-1}]$、$\mathbb{F}_q$: $\mathcal{D}_i$の定義される最小の体、
$[2]\mathcal{D}_{i+1} = \mathcal{D}_i$, $\mathcal{D}_{i+1} \in \mathbb{J}_C(\mathbb{F}_{q^2}) \backslash \mathbb{J}_C(\mathbb{F}_q)$のとき、

$$^{\exists}\hat{\mathcal{D}} \in \mathbb{J}_C[2] \backslash \{0\} : \mathbf{D}_{i+1} + \hat{\mathcal{D}} = \mathbf{D}_{i+1}^q$$

この$\hat{\mathcal{D}}$は、

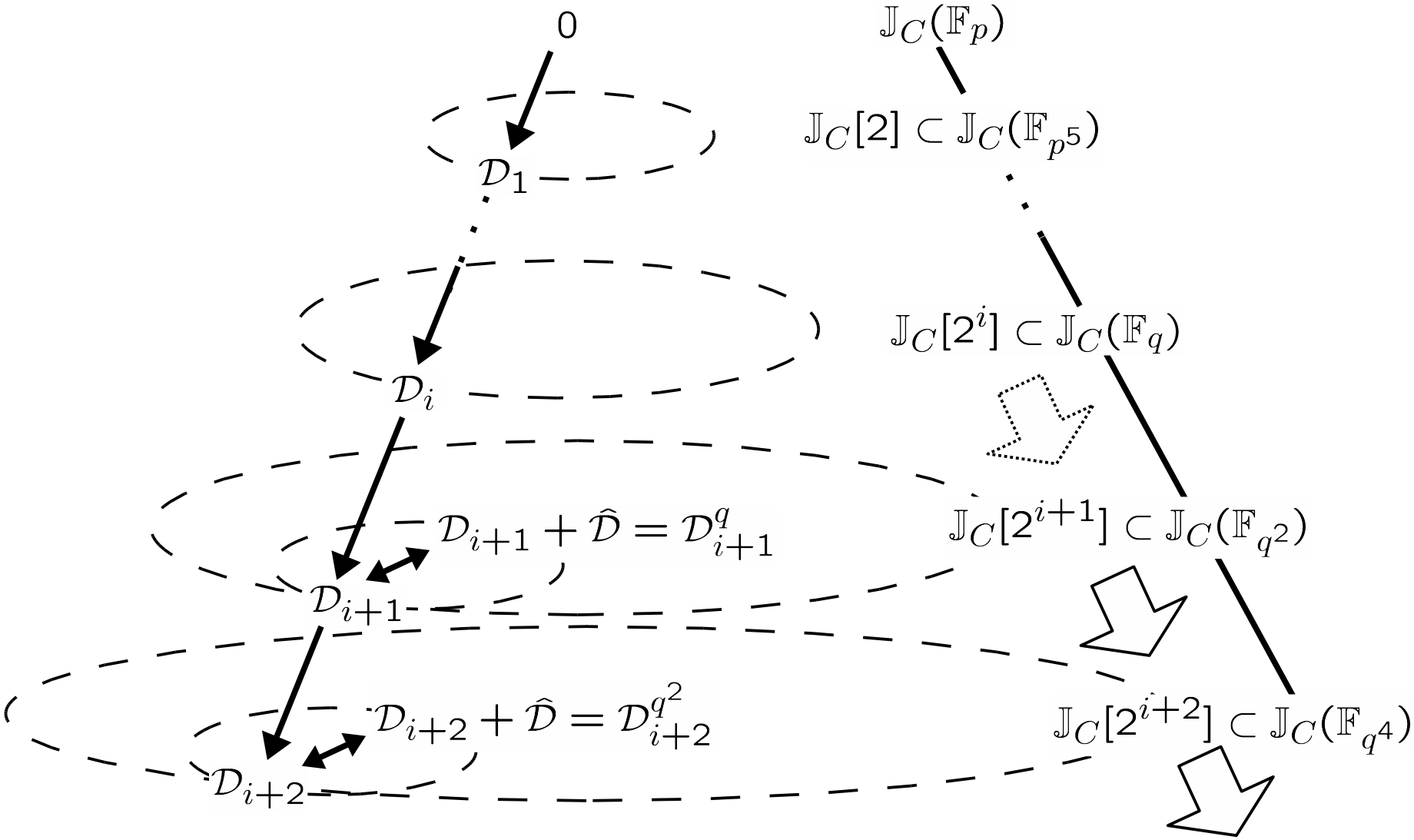
$$\mathbf{D}_{i+2} + \hat{\mathcal{D}} = \mathbf{D}_{i+2}^{q^2}$$

を満足する.

$$i > 1 \Rightarrow \mathbb{J}_C[4] \subset \mathbb{J}_C[2^i] \subset \mathbb{J}_C(\mathbb{F}_q) \Rightarrow \mathcal{D}_{i+1}^q - \mathcal{D}_{i+1} = \mathcal{D}_{i+2}^{q^2} - \mathcal{D}_{i+2}$$

→ ある冪指数i以上で、常にT_3, T_2, T_1は可約、T_0は既約
→ T_3, T_2, T_1, T_0の既約判定を省略し高速化

２等分計算過程における定義体の拡大



実装実験

- CPU: Athlon64 2.4GHz、Magma V2.12-22
- $p = 5 \times 10^{24} + 8503491$, C: Gaudry と Schost の示した曲線
- 同一の $\mathcal{D}_2 \in \mathbb{J}_C[4]$ を初期値として 2 等分点を計算

2^i ねじれ点 $\mathcal{D}_i$ の計算時間 $(3 \leq i \leq 10)$　(単位 秒)

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$
G_j の再構成なし	39	92	354	684	4062	17716	65665	367387
前回 JANT 発表	45	55	288	326	921	4950	21648	89978
今回改良	44	52	260	275	719	3162	13061	42215

２冪ねじれ点計算におけるT_jの根の計算時間

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$
T_3	0	1	1	3	14	57	279	1669
	0	1	7	13	72	746	2329	10676
	0	1	7	24	73	490	3539	13295
T_2	1	9	13	71	484	2906	10678	82808
	1	1	7	21	59	610	5354	21498
	1	1	10	16	58	735	4154	10294
T_1	1	7	15	148	1377	2306	13592	54902
	1	1	9	18	59	617	2362	10619
	1	1	7	13	86	743	2347	10426
T_0	1	7	13	58	483	5317	10849	83371
	1	1	1	3	14	59	288	1671
	1	0	1	3	14	58	284	1644
$U_1^q \bmod M_1$	-	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-
	5	-	-	-	-	-	-	-

上段:G_jの再構成なし、中段:前回JANT、下段:今回改良、単位 秒

２冪ねじれ点計算におけるT_jの既約判定計算時間

	$\mathcal{D}_3$	$\mathcal{D}_4$	$\mathcal{D}_5$	$\mathcal{D}_6$	$\mathcal{D}_7$	$\mathcal{D}_8$	$\mathcal{D}_9$	$\mathcal{D}_{10}$
T_3	0	1	11	20	90	717	3432	15694
	0	0	5	10	46	359	1717	7866
	0	0	0	0	0	0	0	0
T_2	0	5	10	45	354	1694	7815	40140
	0	0	5	10	45	351	1699	7642
	0	0	0	0	0	0	0	0
T_1	0	5	10	45	352	1698	7866	40614
	0	0	5	10	46	356	1727	7765
	0	0	0	0	0	0	0	0
T_0	0	5	10	45	353	1700	7938	40383
	0	1	11	20	92	714	3439	15604
	0	0	0	0	0	0	0	0

上段:G_jの再構成なし、中段:前回JANT、下段:今回改良、単位 秒

Algorithm 1 2冪ねじれ点計算の改良アルゴリズム

Input: $C : Y^2 = F(X)$, Fは$\mathbb{F}_p$上既約なモニック5次多項式, 自然数$m \geq 3$

Output: $\mathcal{D}_m \in \mathbb{J}_C[2^m] \backslash \mathbb{J}_C[2^{m-1}]$

1: $\mathcal{D}_1 \in \mathbb{J}_C[2]$及び$\mathcal{D}_2 \in \mathbb{J}_C[4]$を計算
2: $G_0 \leftarrow \{0\}$, $G_1 \leftarrow \langle \mathcal{D}_1 \rangle$, $G_2 \leftarrow \langle \mathcal{D}_1, \mathcal{D}_1^p \rangle$, $G_3 \leftarrow \langle \mathcal{D}_1, \mathcal{D}_1^p, \mathcal{D}_1^{p^2} \rangle$
3: flag $\leftarrow$ false
4: **for** $i = 2$ to $m - 1$ **do**
5: 　$\mathcal{D}_i$の2等分点の条件より、M_1, M_0, L_1, L_0を計算
6: 　**if** flag=false **then**
7: 　　M_0, L_1, L_0及びG_iを用いて、M_1の根αを計算
8: 　　**if** $\alpha \notin \mathbb{F}_q$ **then**
9: 　　　flag $\leftarrow$ ture
10: 　　　$U_1^{(\widehat{\mathcal{D}})}(U_1) = U_1^q \bmod M_1$を満足する2ねじれ点$\widehat{\mathcal{D}}$を探索
11: 　　　$G_1 \leftarrow \langle \widehat{\mathcal{D}} \rangle$, $G_2 \leftarrow \langle \widehat{\mathcal{D}}, \widehat{\mathcal{D}}^p \rangle$, $G_3 \leftarrow \langle \widehat{\mathcal{D}}, \widehat{\mathcal{D}}^p, \widehat{\mathcal{D}}^{p^2} \rangle$
12: 　**else**
13: 　　M_0, L_1, L_0及びG_iを用いて、M_1の根αを計算(T_jの既約判定省略)
14: 　$\mathcal{D}_{i+1} \leftarrow (X^2 + \alpha X + M_0(\alpha), L_1(\alpha)X + L_0(\alpha))$
return $\mathcal{D}_m$