有限体上の Anick automorphism の置換としての符号

伯田 恵輔[1,a)]

概要：本稿では，有限体上定義された Anick automorphism，及び Nagata-Anick automorphism の置換としての符号を調べる．Anick automorphism，及び Nagata-Anick automorphism が標数 2 の素体上定義されている場合，Anick automorphism，及び Nagata-Anick automorphism によって誘導される置換は奇置換であり，そうでなければ偶置換であることを証明する．

キーワード：Anick 自己同型写像，有限体，多変数多項式暗号，置換，多項式同型写像，アフィン代数幾何

Sign of permutations induced by Anick automorphisms over finite fields

Keisuke Hakuta[1,a)]

Abstract: In this paper, we investigate the sign of permutations induced by Anick automorphisms and Nagata-Anick automorphisms over finite fields. We shall prove that if Anick automorphisms and Nagata-Anick automorphisms are defined over a prime field of even characteristic, the permutations induced by Anick automorphisms and Nagata-Anick automorphisms are odd, and otherwise, the permutations are even.

Keywords: Anick automorphism, finite field, multivariate polynomial cryptography, permutation, polynomial automorphism, affine algebraic geometry

1. はじめに

k を体，$X_1, \ldots, X_n$ を不定元とし，$k[X_1, \ldots, X_n]$ を体 k 上の n 変数多項式環，$k\langle X_1, \ldots, X_n\rangle$ を体 k 上の n 変数多項式の自由結合的代数（変数が非可換である多項式代数）とする．$f_i \in k[X_1, \ldots, X_n]$ $(1 \leq i \leq m)$ とし，任意の $(a_1, \ldots, a_n) \in k^n$ に対し，n 個の多項式 f_i の組 $F = (f_1, \ldots, f_m)$ は，

$$F(a_1, \ldots, a_n) := (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)) \tag{1.1}$$

と定義することによって，k^n から k^m への写像とみなすことができる．F は多項式写像と呼ばれる．$m = n$ かつ全単射な多項式写像であって，その逆写像もまた多項式写像であるものを多項式同型写像という．多項式同型写像全体の集合は写像の合成に関して群をなす．特別な多項式同型写像として，アフィン自己同型写像と基本自己同型写像が知られており，これらの多項式同型写像全体で生成される多項式同型写像全体の群の部分群は順部分群と呼ばれ，その元は順自己同型写像と呼ばれる．順自己同型写像は有限個のアフィン自己同型写像と基本自己同型写像の合成の形であり，与えられた順自己同型写像を，上記の合成の形に分解することを tame decomposition と呼ぶ．多変数多項式暗号（[3]）の一方式である Tame Transformation Method（[14]，[15]）は，tame decomposition の求解問題に安全性の根拠を置いており，Tame Transformation Method の安全性については，[1]，[4]，[5]，[8]，[16] などの結果が知られているが，一般の tame decomposition の求解問題が計算量的に困難であるかどうかは知られていない．

体 k が要素数 q の有限体 $\mathbb{F}_q$ であるとき，多項式同型写像は有限体 $\mathbb{F}_q$ 上の有限次元線形空間上の置換とみなすことができる．有限体 $\mathbb{F}_q$ 上の順部分群を，$\mathbb{F}_q$ 上の有限次元線

[1] 島根大学大学院総合理工学研究科，〒 690-8504 島根県松江市西川津町 1060.
Interdisciplinary Graduate School of Science and Engineering, Shimane University, 1060 Nishikawatsu-cho, Matsue-shi, Shimane 690-8504, Japan.
[a)] hakuta(at)cis.shimane-u.ac.jp

形空間上の対称群の部分群（置換群）とみなすと，どのような群になるか，という問題は数学的に自然である．この問題に対し，Maubach は，$n \geq 2$ かつ $q = 2$ ならば順部分群は交代群であり，$n \geq 2$ かつ $q \neq 2$ ならば順部分群は対称群である，という結果を証明している（[12], Theorem 2.3）．つまり，$n \geq 2$ かつ $q = 2$ ならば順自己同型写像は，置換として偶置換になることも奇置換になることもあるが，$n \geq 2$ かつ $q \neq 2$ ならば常に偶置換になる，と言い換えることができる．

この結果を受け，多項式同型写像の研究に多くの示唆（cf. [6]，[19], [20]）を与えている Nagata automorphism [17], Anick automorphism, Nagata-Anick automorphism [2] などの具体的な有限体 $\mathbb{F}_q$ 上の多項式同型写像に対し，その置換としての符号を調べることは数学的に自然である．また，上述したように，有限体の多項式同型写像は多変数多項式暗号の構成要素としても利用されており，多項式同型写像の置換としての符号に関する情報は，多変数多項式暗号の観点，特に tame decomposition の困難性を評価する際にも有用な情報を与えてくれる可能性がある（cf. [11]）．そこで本稿では，有限体上定義された Anick automorphism，及び Nagata-Anick automorphism の置換としての符号を調べる．

2. 記法・数学的準備

ここでは，本稿で使用する記法，及び数学的背景について説明する．多項式同型写像に関する詳細については，例えば [2]，[7] などを参照されたい．

$\mathbb{N} := \{1, 2, \ldots\}$ を自然数全体の集合とする．$k^* := k \backslash \{0\}$ とする．$\mathrm{MA}_n(k)$ で k^n から k^n への多項式写像全体の集合を表し，$\mathrm{Maps}(k^n, k^n)$ で k^n から k^n への写像全体の集合を表す．すると，(1.1) より，自然な写像

$$\pi : \quad \mathrm{MA}_n(k) \quad \to \quad \mathrm{Maps}(k^n, k^n) \tag{2.1}$$

が存在する．$\mathrm{MA}_n(k)$，$\mathrm{Maps}(k^n, k^n))$ は写像としての合成により半群であり，これらの半群はそれぞれ恒等写像を単位元とする monoid であり，写像 π は monoid の間の準同型写像である．$\mathrm{MA}_n(k)$ の元であって，逆元を持つ元全体の集合を $\mathrm{GA}_n(k)$ と書く．$\mathrm{GA}_n(k)$ の元を多項式同型写像という．各 $i = 1, \ldots, n$ に対して $\deg f_i = 1$ であるとき，多項式同型写像 $F = (f_1, \ldots, f_n)$ はアフィン自己同型写像と呼ばれる．以下の形の多項式写像 E_{a_i}

$$\begin{aligned} E_{a_i} &= (X_1, \ldots, X_{i-1}, X_i + a_i, X_{i+1}, \ldots, X_n), \\ a_i &\in k[X_1, \ldots, \hat{X_i}, \ldots, X_n] \\ &= k[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n], \end{aligned} \tag{2.2}$$

は多項式同型写像であり，その逆元 $E_{a_i}^{-1}$ は $E_{a_i}^{-1} = E_{-a_i}$ である．(2.2) の形の多項式同型写像 E_{a_i} は基本自己同型写像と呼ばれる．

アフィン自己同型写像全体の集合を $\mathrm{Aff}(k, n)$，基本自己同型写像全体の集合を $E(k, n)$ とおき，$\mathrm{Aff}(k, n)$ と $E(k, n)$ はそれぞれ $\mathrm{GA}_n(k)$ の部分集合である．$T(k, n) := \langle \mathrm{Aff}(k, n), E(k, n) \rangle$ とおく．ここで，$\langle H_1, H_2 \rangle$ は部分群 $H_1, H_2 \subset G$ によって生成される G の部分群を表す．$T(k, n)$ も $\mathrm{GA}_n(k)$ の部分群であり，順部分群と呼ばれる．$\phi \in T(k, n)$ のとき，ϕ は順自己同型写像（tame automorphism）であるといい，そうでないとき（$\phi \in \mathrm{GA}_n(k) \backslash T(k, n)$ のとき）ϕ は野生（wild automorphism）であるという．任意の順自己同型写像 $\phi \in T(k, n)$ に対し，ある自然数 $l \in \mathbb{N}$，$\epsilon_1, \epsilon_2 \in \{0, 1\}$, $\sigma_i \in \mathrm{Aff}(k, n)$ $(1 \leq i \leq l+1)$，$\sigma_i \notin E(k, n)$ $(1 \leq i \leq l+1)$，$\tau_i \in E(k, n)$ $(1 \leq i \leq l)$，$\tau_i \notin \mathrm{Aff}(k, n)$ $(1 \leq i \leq l)$ が存在し，

$$\phi = \sigma_1^{\epsilon_1} \circ \tau_1 \circ \sigma_2 \circ \cdots \circ \sigma_l \circ \tau_l \circ \sigma_{l+1}^{\epsilon_2} \tag{2.3}$$

が成り立つ．式 (2.3) を $\phi \in T(k, n)$ の tame decomposition と呼ぶ．体上の 2 変数の順自己同型写像については [9], Kulk53 による有名な結果が知られている．

体 k に対し，k の標数を $p = \mathrm{char}(k)$ と書く．体 k が要素数 q の有限体 $\mathbb{F}_q$（$p = \mathrm{char}(\mathbb{F}_q)$, $q = p^m$, $m \geq 1$）のとき，(2.1) の写像 π を π_q と書くことにする：

$$\pi_q : \quad \mathrm{MA}_n(\mathbb{F}_q) \quad \to \quad \mathrm{Maps}(\mathbb{F}_q^n, \mathbb{F}_q^n). \tag{2.4}$$

写像 π_q は群の準同型写像

$$\pi_q : \quad \mathrm{GA}_n(\mathbb{F}_q) \quad \to \quad \mathrm{Sym}(\mathbb{F}_q^n) \tag{2.5}$$

を引き起こす，ここで $\mathrm{Sym}(S)$ は有限集合 S 上の対称群を表す．

写像 sgn

$$\mathrm{sgn} : \mathrm{Sym}(S) \to \{\pm 1\} \tag{2.6}$$

を符号関数とする．符号関数 sgn は群準同型であり，$\mathrm{Ker}(\mathrm{sgn}) = \mathrm{Alt}(S)$ である，ここで，$\mathrm{Alt}(S)$ は S 上の交代群を表す．部分群 $G \subseteq \mathrm{GA}_n(\mathbb{F}_q)$ に対し，$\pi_q(G)$ は対称群 $\mathrm{Sym}(\mathbb{F}_q^n)$ の部分群である．

対称群 $\mathrm{Sym}(\mathbb{F}_q^n)$ の部分群 $\pi_q(\mathrm{TA}_n(\mathbb{F}_q))$ の代数的構造を調べることは数学的に自然であり，Maubach による以下の結果（[12], Theorem 2.3）が知られている：

定理 1. ([12], Theorem 2.3) $n \geq 2$ とする．q が奇数，または $q = 2$ ならば $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(\mathbb{F}_q^n)$ である．$q = 2^m$，$m \geq 2$ ならば $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(\mathbb{F}_q^n)$ である．

写像 π，π_q に関する諸性質については [13] を参照されたい．

以下，本稿では，体 k 上の 3 変数多項式環を $k[x, y, z]$，体 k 上の 4 変数多項式環を $k[w, x, y, z]$ と書く．$k\langle X_1, \ldots, X_n \rangle$ 上の自己同型群を $\mathrm{Aut}_k\, k\langle X_1, \ldots, X_n \rangle$ と書く．このとき，

自然な群準同型写像

$$\theta : \mathrm{Aut}_k\, k\langle X_1, \ldots, X_n\rangle \to \mathrm{GA}_n(k) \tag{2.7}$$

が存在する（[2], pp.397–398）．多項式自己同型写像

$$\begin{aligned}\delta &:= (x + y\,(xy - yz)\,, y, z + (xy - yz)\,y) \\ &\in \mathrm{Aut}_k\, k\langle x, y, z\rangle\end{aligned} \tag{2.8}$$

は Anick automorphism と呼ばれ，多項式自己同型写像

$$\begin{aligned}\rho &:= (w, x + (wx - yz)\,z, y + w\,(wx - yz)\,, z) \\ &\in \mathrm{Aut}_k\, k\langle w, x, y, z\rangle\end{aligned} \tag{2.9}$$

は Nagata-Anick automorphism と呼ばれる（[2], p.398）．

3. 主結果 1

ここでは，Anick automorphism の置換としての符号に関する主結果（主定理 1）を示す．次の補題（補題 1）は，Anick automorphism $\theta(\delta)$ の tame decomposition である．

補題 1. (Anick automorphism $\theta(\delta)$ の tame decomposition) 基本自己同型写像 ϕ, τ を

$$\phi := (x, y, z - x)\,, \tau := \left(x - y^2 z, y, z\right) \in E(k, 3)$$

とする．このとき，

$$\theta(\delta) = \phi^{-1} \circ \tau \circ \phi \tag{3.1}$$

が成り立つ．

Proof.

$$\begin{aligned}\tau \circ \phi &= \left(x - y^2 z, y, z\right) \circ (x, y, z - x) \\ &= \left(x - y^2\,(z - x)\,, y, z - x\right) \\ &= (x + y\,(xy - yz)\,, y, z - x)\end{aligned}$$

であり，$\phi^{-1} = (x, y, z + x)$ だから

$$\begin{aligned}\phi^{-1} \circ \tau \circ \phi &= (x + y\,(xy - yz)\,, y, \\ &\qquad z - x + x + y\,(xy - yz)) \\ &= (x + y\,(xy - yz)\,, y, z + y\,(xy - yz))\end{aligned}$$

となる．よって，$\theta(\delta) = \phi^{-1} \circ \tau \circ \phi$ が成り立つ． □

主定理 1 の証明のため，次の補題（補題 2）を用意する．この補題は，補題 1 で示した基本同型写像 τ の置換としての符号に関する結果である．

補題 2. (置換 $\pi_q(\tau)$ の符号)

$$\mathrm{sgn}\,(\pi_q(\tau)) = \begin{cases} 1 & (q : \text{奇数 または } q = 2^m, m \geq 2)\,, \\ -1 & (q = 2)\,, \end{cases} \tag{3.2}$$

が成り立つ．

Proof. 任意の $y_0, z_0 \in \mathbb{F}_q^*$ を取り，固定する．写像 $\tau_{(y_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ を

$$\begin{array}{rccc} \tau_{(y_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 \\ & \cup & & \cup \\ & (x, y, z) & \longmapsto & (x - y^2 z, y, z), \\ & & & y = y_0 \text{かつ } z = z_0 \text{のとき}, \\ & (x, y, z) & \longmapsto & (x, y, z), \\ & & & \text{その他のとき}, \end{array} \tag{3.3}$$

で定義する．写像 (3.3) の定義より，$\tau_{(y_0,z_0)}$ は明らかに $\mathbb{F}_q^3$ 上の置換である．

$$\begin{aligned}B\left(\tau_{(y_0,z_0)}\right) := \{&(x, y, z) \in \mathbb{F}_q^3 \mid \\ &\tau_{(y_0,z_0)}(x, y, z) \neq (x, y, z)\}\end{aligned}$$

とおく．$(y_0, z_0) \neq (y_0', z_0')$ なる $(y_0', z_0') \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ に対し，$B\left(\tau_{(y_0,z_0)}\right) \cap B\left(\tau_{(y_0',z_0')}\right) = \emptyset$ だから

$$\tau = \prod_{y_0, z_0 \in \mathbb{F}_q^*} \tau_{(y_0,z_0)} \tag{3.4}$$

であり，式 (3.4) は τ を共通部分のない置換の積に分解している．

次に，各置換 $\tau_{(y_0,z_0)}$（$y_0, z_0 \in \mathbb{F}_q^*$）を共通部分のない巡回置換の積に分解する．そのために，$x, x' \in \mathbb{F}_q$ に対し，同値関係 $\overset{(\tau)}{\sim}$ を以下で定義する：ある $l \in \{0, 1, \ldots, p-1\}$ が存在し，$x' = x - l y_0^2 z_0$ と書けるとき，$x \overset{(\tau)}{\sim} x'$．関係 $\overset{(\tau)}{\sim}$ が同値関係であることは明らかである．

$$C_x^{(\tau)} := \{x' \in \mathbb{F}_q \mid x \overset{(\tau)}{\sim} x'\} \tag{3.5}$$

とおく．$\mathcal{R}_\tau$ を $\mathbb{F}_q$ の同値関係 $\overset{(\tau)}{\sim}$ に関する完全代表系とする．$\sharp\mathcal{R}_\tau = q/p = p^m/p = p^{m-1}$ であることに注意しよう．任意の $x_0 \in \mathcal{R}_\tau$ に対し，写像 $\tau_{x_0,(y_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ を

$$\begin{array}{rccc} \tau_{x_0,(y_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 \\ & \cup & & \cup \\ & (x, y, z) & \longmapsto & (x - y^2 z, y, z), \\ & x \in C_{x_0}^{(\tau)} \text{かつ } y = y_0 \text{かつ } z = z_0 \text{のとき}, & & \\ & (x, y, z) & \longmapsto & (x, y, z), \\ & & & \text{その他のとき}, \end{array} \tag{3.6}$$

で定義する．写像 (3.6) の定義より，$\tau_{x_0,(y_0,z_0)}$ は $\mathbb{F}_q^3$ 上の巡回置換であり，$x_0' \in \mathcal{R}_\tau$ が $x_0' \notin C_{x_0}^{(\tau)}$ を満たすならば $C_{x_0}^{(\tau)} \cap C_{x_0'}^{(\tau)} = \emptyset$ であるから，

$$\tau_{(y_0,z_0)} = \prod_{x_0 \in \mathcal{R}_\tau} \tau_{x_0,(y_0,z_0)} \tag{3.7}$$

であり，式 (3.7) は置換 $\tau_{(y_0,z_0)}$ を共通部分のない巡回置換の積に分解している．

最後に，巡回置換 $\tau_{x_0,(y_0,z_0)}$ を互換の積に分解する．

$u \in \{1, \ldots, p-1\}$ なる u に対し，写像 $\tau^{(u)}_{x_0,(y_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ を

$$\begin{array}{rccl}
\tau^{(u)}_{x_0,(y_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 \\
& \cup & & \cup \\
& (x,y,z) & \longmapsto & (x - uy^2 z, y, z), \\
& & & \quad (x,y,z) = (x_0,y_0,z_0) \text{ のとき}, \\
& (x,y,z) & \longmapsto & (x + uy^2 z, y, z), \\
& & & \quad (x,y,z) = (x_0 - uy_0^2 z_0, y_0, z_0) \text{ のとき}, \\
& (x,y,z) & \longmapsto & (x,y,z), \\
& & & \quad \text{その他のとき},
\end{array} \tag{3.8}$$

で定義する．写像 (3.8) の定義より，$\tau^{(u)}_{x_0,(y_0,z_0)}$ は (x_0,y_0,z_0) と $\left(x_0 - uy_0^2 z_0, y_0, z_0\right)$ のみを入れ替え，その他の $\mathbb{F}_q^3$ の元を入れ替えないから確かに互換である．すると，

$$\tau_{x_0,(y_0,z_0)} = \tau^{(p-1)}_{x_0,(y_0,y_0)} \circ \cdots \circ \lambda^{(1)}_{x_0,(y_0,z_0)} \tag{3.9}$$

であり，式 (3.9) は巡回置換 $\tau_{x_0,(y_0,z_0)}$ を互換の積に分解している．式 (3.4)，式 (3.7)，式 (3.9) より，

$$\tau = \prod_{y_0,z_0 \in \mathbb{F}_q^*, x_0 \in \mathcal{R}_\tau} \tau^{(p-1)}_{x_0,(y_0,z_0)} \circ \cdots \circ \tau^{(1)}_{x_0,(y_0,z_0)} \tag{3.10}$$

を得る．よって，τ は $(p-1) \times p^{m-1} \times (q-1)^2$ 個の互換の積で表される．以上より，

$$\operatorname{sgn}\left(\pi_q(\tau)\right) = (-1)^{p^{m-1}(p-1)(q-1)^2} \tag{3.11}$$

である．q が奇数ならば $p-1 \equiv 0 \mod 2$，$q-1 \equiv 0 \mod 2$ となり，$p^{m-1}(p-1)(q-1)^2 \equiv 0 \mod 2$ である．$q = 2^m$，$m \geq 2$ ならば $p^{m-1} \equiv 0 \mod 2$ となり，$p^{m-1}(p-1)(q-1)^2 \equiv 0 \mod 2$ である．したがって，q が奇数，または $q = 2^m$，$m \geq 2$ ならば $\operatorname{sgn}\left(\pi_q(\tau)\right) = 1$ である．$q = 2$ ならば $p^{m-1}(p-1)(q-1)^2 = 2^0 \times 1 \times 1^2 = 1$ だから $\operatorname{sgn}\left(\pi_q(\tau)\right) = -1$ である．よって，式 (3.2) が成り立つ． □

補題 2，及び補題 1 より，次の主結果（主定理 1）を得る．

主定理 1. (Anick automorphism $\theta(\delta) \in \mathrm{GA}_3(\mathbb{F}_q)$ の置換としての符号) q が奇数，または $q = 2^m$，$m \geq 2$ ならば $\pi_q(\theta(\delta)) \in \mathrm{Alt}(\mathbb{F}_q^3)$ であり，$q = 2$ ならば $\pi_q(\theta(\delta)) \in \mathrm{Sym}(\mathbb{F}_q^3) \setminus \mathrm{Alt}(\mathbb{F}_q^3)$ である．つまり，

$$\operatorname{sgn}\left(\pi_q(\theta(\delta))\right) = \begin{cases} 1 & (q \text{ :奇数 または } q = 2^m, m \geq 2), \\ -1 & (q = 2), \end{cases} \tag{3.12}$$

である．

Proof. 補題 1 と写像 sgn, π_q がそれぞれ群準同型であることから

$$\begin{aligned}
\operatorname{sgn}\left(\pi_q(\theta(\delta))\right) &= \operatorname{sgn}\left(\pi_q\left(\theta\left(\phi^{-1} \circ \tau \circ \phi\right)\right)\right) \\
&= \operatorname{sgn}\left(\pi_q\left(\phi^{-1}\right)\pi_q(\tau)\,\pi_q(\phi)\right) \\
&= \operatorname{sgn}\left(\pi_q\left(\phi^{-1}\right)\right)\operatorname{sgn}\left(\pi_q(\tau)\right)\operatorname{sgn}\left(\pi_q(\phi)\right) \\
&= \operatorname{sgn}\left(\pi_q(\phi)\right)^{-1}\operatorname{sgn}\left(\pi_q(\tau)\right)\operatorname{sgn}\left(\pi_q(\phi)\right) \\
&= \operatorname{sgn}\left(\pi_q(\tau)\right)
\end{aligned}$$

となる．補題 2 より，

$$\operatorname{sgn}\left(\pi_q(\tau)\right) = \begin{cases} 1 & (q \text{ :奇数 または } q = 2^m, m \geq 2), \\ -1 & (q = 2), \end{cases}$$

であるから，式 (3.12) を得る． □

[6], p.660 では，式 (2.8) における不定元 y, z を入れ替えた多項式自己同型写像

$$\begin{aligned}
\omega &:= \left(x + y(xy - yz), y, z + (xy - yz)y\right) \\
&\in \mathrm{Aut}_k\, k\langle x,y,z\rangle
\end{aligned} \tag{3.13}$$

を Anick automorphism と呼んでいる．2 つの多項式自己同型写像 $\theta(\delta)$, $\theta(\omega)$ の間には

$$\theta(\omega) = \psi \circ \theta(\delta) \circ \psi \tag{3.14}$$

なる関係がある，ここで，$\psi = (x,z,y) \in \mathrm{Aff}(k,3)$ である．主定理 1 と式 (3.14) より，以下の系を得る．

系 1. ($\theta(\omega) \in \mathrm{GA}_3(\mathbb{F}_q)$ の置換としての符号) $\delta \in \mathrm{Aut}_{\mathbb{F}_q}\mathbb{F}_q\langle x,y,z\rangle$ を式 (2.8) で定義された *Anick automorphism*，$\omega \in \mathrm{Aut}_{\mathbb{F}_q}\mathbb{F}_q\langle x,y,z\rangle$ を式 (3.13) で定義された *Anick automorphism* とする．このとき，

$$\operatorname{sgn}\left(\pi_q(\theta(\delta))\right) = \operatorname{sgn}\left(\pi_q(\theta(\omega))\right) \tag{3.15}$$

が成り立つ．つまり，*Anick automorphism* $\theta(\delta)$ の置換としての符号は *Anick automorphism* $\theta(\omega)$ の置換としての符号と等しい．

4. 主結果 2

ここでは，Nagata-Anick automorphism の置換としての符号に関する主結果（主定理 2）を示す．まず，以下の準備を行う．

t を不定元とし，有限体 $\mathbb{F}_q$ 上の一変数多項式 $f(t)$ を

$$f(t) := \prod_{c \in \mathbb{F}_q^*} (t - c) \in \mathbb{F}_q[t]$$

で定義する．$g \in \mathbb{F}_q^*$ を乗法群 $\mathbb{F}_q^*$ の生成元（すなわち $\mathbb{F}_q^* = \langle g \rangle$）とすると，

$$\begin{aligned}
f(\alpha) &= \begin{cases} 0 & \left(\alpha \in \mathbb{F}_q^*\right), \\ (-1)^{q-1}\prod_{i=0}^{q-2} g^i & (\alpha = 0), \end{cases} \\
&= \begin{cases} 0 & \left(\alpha \in \mathbb{F}_q^*\right), \\ (-1)^{q-1} g^{(q-2)(q-1)/2} & (\alpha = 0), \end{cases}
\end{aligned}$$

である．

$$c_0 := f(0) = (-1)^{q-1} g^{(q-2)(q-1)/2}$$

とおく．$c_0 \in \mathbb{F}_q^*$ であることに注意されたい．$h(t) := c_0^{-1} \times f(t) \in \mathbb{F}_q[t]$ とおくと，

$$h(\alpha) = \begin{cases} 0 & (\alpha \in \mathbb{F}_q^*), \\ 1 & (\alpha = 0), \end{cases} \tag{4.1}$$

である．

次の補題（補題 3）は，ある tame decomposition と Nagata-Anick automorphism $\theta(\rho)$ が置換として等しいことを示している．

補題 3. (Nagata-Anick automorphism $\theta(\rho)$ と置換として等しい tame automorphism) 基本自己同型写像 ψ, ξ, λ を

$$\psi := \left(w, x, y - wxz^{q-2}, z\right) \in E(\mathbb{F}_q, 4),$$
$$\xi := \left(w, x - yz^2, y, z\right) \in E(\mathbb{F}_q, 4),$$
$$\lambda := \left(w, x, y + w^2 x h(z), z\right) \in E(\mathbb{F}_q, 4)$$

とする．このとき，

$$\pi_q(\theta(\rho)) = \pi_q\left(\lambda \circ \psi^{-1} \circ \xi \circ \psi\right) \tag{4.2}$$

が成り立つ．

Proof.

$$\begin{aligned} &\pi_q(\xi \circ \psi) \\ &= \pi_q\left(\left(w, x - yz^2, y, z\right) \circ \left(w, x, y - wxz^{q-2}, z\right)\right) \\ &= \pi_q\left(\left(w, x - \left(y - wxz^{q-2}\right) z^2, y - wxz^{q-2}, z\right)\right) \\ &= \pi_q\left(\left(w, x + (wx - yz) z, y - wxz^{q-2}, z\right)\right) \end{aligned}$$

である．上の等式変形において，最後の式を導出する際に q 乗 Frobenius 写像の性質を用いた．$\psi^{-1} = \left(w, x, y + wxz^{q-2}, z\right) \in E(\mathbb{F}_q, 4)$ だから

$$\begin{aligned} &\pi_q\left(\psi^{-1} \circ \xi \circ \psi\right) \\ &= \pi_q\Big(\left(w, x, y + wxz^{q-2}, z\right) \\ &\qquad \circ \left(w, x + (wx - yz) z, y - wxz^{q-2}, z\right)\Big) \\ &= \pi_q\Big(\left(w, x + (wx - yz) z, y - wxz^{q-2}\right. \\ &\qquad \left. + w\left(x + (wx - yz) z\right) z^{q-2}, z\right)\Big) \\ &= \pi_q\left(\left(w, x + (wx - yz) z, y + w(wx - yz) z^{q-1}, z\right)\right) \end{aligned}$$

である．したがって，

$$\begin{aligned} &\pi_q\left(\lambda \circ \psi^{-1} \circ \xi \circ \psi\right) \\ &= \pi_q\Big(\left(w, x, y + w^2 x h(z), z\right) \\ &\quad \circ \left(w, x + (wx - yz) z, y + w(wx - yz) z^{q-1}, z\right)\Big) \\ &= \pi_q\Big(\left(w, x + (wx - yz) z, y + w(wx - yz) z^{q-1}\right. \\ &\qquad \left. + w^2\left(x + (wx - yz) z\right) h(z), z\right)\Big) \\ &= \pi_q(\theta(\rho)) \end{aligned}$$

となる．上の等式変形において，最後の式を導出する際に，式 (4.1) を用いた．よって，式 (4.2) が成り立つ． □

注意 1. Anick automorphism の場合，多項式同型写像として式 (3.1) が成り立つのに対し，Nagata-Anick automorphism の場合には，多項式同型写像としては

$$\theta(\rho) \neq \lambda \circ \psi^{-1} \circ \xi \circ \psi$$

である．式 (4.2) は，$\mathbb{F}_q^4$ 上の置換として等しい，という点に注意されたい．

補題 3，及び補題 1 と同様の議論を用いて次の主結果（主定理 2）を証明する．

主定理 2. (Nagata-Anick automorphism $\theta(\rho) \in \mathrm{GA}_4(\mathbb{F}_q)$ の置換としての符号) q が奇数，または $q = 2^m$，$m \geq 2$ ならば $\pi_q(\theta(\rho)) \in \mathrm{Alt}(\mathbb{F}_q^4)$ であり，$q = 2$ ならば $\pi_q(\theta(\rho)) \in \mathrm{Sym}(\mathbb{F}_q^4) \setminus \mathrm{Alt}(\mathbb{F}_q^4)$ である．つまり，

$$\mathrm{sgn}(\pi_q(\theta(\rho))) = \begin{cases} 1 & (q : \text{奇数 または } q = 2^m, m \geq 2), \\ -1 & (q = 2), \end{cases} \tag{4.3}$$

である．

Proof. 補題 3 と写像 sgn, π_q がそれぞれ群準同型であることから

$$\begin{aligned} &\mathrm{sgn}(\pi_q(\theta(\rho))) \\ &= \mathrm{sgn}\left(\pi_q\left(\theta\left(\lambda \circ \psi^{-1} \circ \xi \circ \psi\right)\right)\right) \\ &= \mathrm{sgn}\left(\pi_q(\lambda)\, \pi_q\left(\psi^{-1}\right) \pi_q(\xi)\, \pi_q(\psi)\right) \\ &= \mathrm{sgn}(\pi_q(\lambda)) \,\mathrm{sgn}\left(\pi_q\left(\psi^{-1}\right)\right) \\ &\qquad \mathrm{sgn}(\pi_q(\xi)) \,\mathrm{sgn}(\pi_q(\psi)) \\ &= \mathrm{sgn}(\pi_q(\lambda)) \,\mathrm{sgn}(\pi_q(\psi))^{-1} \\ &\qquad \mathrm{sgn}(\pi_q(\xi)) \,\mathrm{sgn}(\pi_q(\psi)) \\ &= \mathrm{sgn}(\pi_q(\lambda)) \,\mathrm{sgn}(\pi_q(\xi)) \end{aligned} \tag{4.4}$$

となる．したがって，$\mathrm{sgn}(\pi_q(\lambda))$，及び $\mathrm{sgn}(\pi_q(\xi))$ の値を調べればよい．

まず，$\mathrm{sgn}(\pi_q(\lambda))$ の値を調べる．任意の $w_0, x_0 \in \mathbb{F}_q^*$ を取り，固定する．写像 $\lambda_{(w_0,x_0)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc} \lambda_{(w_0,x_0)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\ & \cup & & \cup \\ & (w, x, y, z) & \longmapsto & (w, x, y + w^2 x h(z), z), \\ & & & (w, x, z)(w_0, x_0, 0) \text{ のとき}, \\ & (w, x, y, z) & \longmapsto & (w, x, y, z), \\ & & & \text{その他のとき}, \end{array} \tag{4.5}$$

で定義する．写像 (4.5) の定義より，$\lambda_{(w_0,x_0)}$ は明らかに $\mathbb{F}_q^4$ 上の置換である．

$$B\left(\lambda_{(w_0,x_0)}\right) := \{(w,x,y,z) \in \mathbb{F}_q^4 \mid \lambda_{(w_0,x_0)}(w,x,y,z) \neq (w,x,y,z)\}$$

とおく．$(w_0,x_0) \neq (w_0',x_0')$ なる $(w_0',x_0') \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ に対し，$B\left(\lambda_{(w_0,x_0)}\right) \cap B\left(\lambda_{(w_0',x_0')}\right) = \emptyset$ だから

$$\lambda = \prod_{w_0,x_0 \in \mathbb{F}_q^*} \lambda_{(w_0,x_0)} \tag{4.6}$$

であり，式 (4.6) は λ を共通部分のない置換の積に分解している．

次に，各置換 $\lambda_{(w_0,x_0)}$（$w_0,x_0 \in \mathbb{F}_q^*$）を共通部分のない巡回置換の積に分解する．そのために，$y,y' \in \mathbb{F}_q$ に対し，同値関係 $\overset{(\lambda)}{\sim}$ を以下で定義する：ある $l \in \{0,1,\ldots,p-1\}$ が存在し，$y' = y + lw_0^2x_0$ と書けるとき，$y \overset{(\lambda)}{\sim} y'$．関係 $\overset{(\lambda)}{\sim}$ が同値関係であることは明らかである．

$$C_y^{(\lambda)} := \{y' \in \mathbb{F}_q \mid y \overset{(\lambda)}{\sim} y'\} \tag{4.7}$$

とおく．$\mathcal{R}_\lambda$ を $\mathbb{F}_q$ の同値関係 $\overset{(\lambda)}{\sim}$ に関する完全代表系とする．$\sharp\mathcal{R}_\lambda = q/p = p^m/p = p^{m-1}$ であることに注意しよう．任意の $y_0 \in \mathcal{R}_\lambda$ に対し，写像 $\lambda_{y_0,(w_0,x_0)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc}
\lambda_{y_0,(w_0,x_0)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\
& \cup & & \cup \\
& (w,x,y,z) & \longmapsto & (w,x,y+w^2xh(z),z), \\
& (w,x,z) = (w_0,x_0,0) \text{ かつ } y \in C_{y_0}^{(\lambda)} \text{かつ } z = 0 \text{ のとき}, & & \\
& (w,x,y,z) & \longmapsto & (w,x,y,z), \\
& & & \text{その他のとき},
\end{array} \tag{4.8}$$

で定義する．写像 (4.8) の定義より，$\lambda_{y_0,(w_0,x_0)}$ は $\mathbb{F}_q^4$ 上の巡回置換であり，$y_0' \in \mathcal{R}_\lambda$ が $y_0' \notin C_{y_0}^{(\lambda)}$ を満たすならば $C_{y_0}^{(\lambda)} \cap C_{y_0'}^{(\lambda)} = \emptyset$ であるから，

$$\lambda_{(w_0,x_0)} = \prod_{y_0 \in \mathcal{R}_\lambda} \lambda_{y_0,(w_0,x_0)} \tag{4.9}$$

であり，式 (4.9) は置換 $\lambda_{(w_0,x_0)}$ を共通部分のない巡回置換の積に分解している．

最後に，巡回置換 $\lambda_{y_0,(w_0,x_0)}$ を互換の積に分解する．$u \in \{1,\ldots,p-1\}$ なる u に対し，写像 $\lambda_{y_0,(w_0,x_0)}^{(u)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc}
\lambda_{y_0,(w_0,x_0)}^{(u)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\
& \cup & & \cup \\
& (w,x,y,z) & \longmapsto & (w,x,y+uw^2x,z), \\
& (w,x,y,z) = (w_0,x_0,y_0,0) \text{ のとき}, & & \\
& (w,x,y,z) & \longmapsto & (w,x,y-uw^2x,z), \\
& (w,x,y,z) = (w_0,x_0,y_0+uw_0^2x_0,0) \text{ のとき}, & & \\
& (w,x,y,z) & \longmapsto & (w,x,y,z), \\
& & & \text{その他のとき},
\end{array} \tag{4.10}$$

で定義する．写像 (4.10) の定義より，$\lambda_{y_0,(w_0,x_0)}^{(u)}$ は $(w_0,x_0,y_0,0)$ と $\left(w_0,x_0,y_0+uw_0^2x_0,0\right)$ のみを入れ替え，その他の $\mathbb{F}_q^4$ の元を入れ替えないから確かに互換である．すると，

$$\lambda_{y_0,(w_0,x_0)} = \lambda_{y_0,(w_0,x_0)}^{(p-1)} \circ \cdots \circ \lambda_{y_0,(w_0,x_0)}^{(1)} \tag{4.11}$$

であり，式 (4.11) は巡回置換 $\lambda_{y_0,(w_0,x_0)}$ を互換の積に分解している．式 (4.6)，式 (4.9)，式 (4.11) より，

$$\lambda = \prod_{w_0,x_0 \in \mathbb{F}_q^*, y_0 \in \mathcal{R}_\lambda} \lambda_{y_0,(w_0,x_0)}^{(p-1)} \circ \cdots \circ \lambda_{y_0,(w_0,x_0)}^{(1)} \tag{4.12}$$

を得る．よって，λ は $(p-1) \times p^{m-1} \times (q-1)^2$ 個の互換の積で表される．以上より，

$$\operatorname{sgn}\left(\pi_q\left(\lambda\right)\right) = (-1)^{p^{m-1}(p-1)(q-1)^2} \tag{4.13}$$

である．

$\operatorname{sgn}\left(\pi_q\left(\lambda\right)\right)$ の場合と同様の手順で $\operatorname{sgn}\left(\pi_q\left(\xi\right)\right)$ の値を調べる．任意の $y_0,z_0 \in \mathbb{F}_q^*$ を取り，固定する．写像 $\xi_{(y_0,z_0)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc}
\xi_{(y_0,z_0)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\
& \cup & & \cup \\
& (w,x,y,z) & \longmapsto & (w,x-yz^2,y,z), \\
& & & (y,z) = (y_0,z_0) \text{ のとき}, \\
& (w,x,y,z) & \longmapsto & (w,x,y,z), \\
& & & \text{その他のとき},
\end{array} \tag{4.14}$$

で定義する．写像 (4.14) の定義より，$\xi_{(y_0,z_0)}$ は明らかに $\mathbb{F}_q^4$ 上の置換である．

$$B\left(\xi_{(y_0,z_0)}\right) := \{(w,x,y,z) \in \mathbb{F}_q^4 \mid \xi_{(y_0,z_0)}(w,x,y,z) \neq (w,x,y,z)\}$$

とおく．$(y_0,z_0) \neq (y_0',z_0')$ なる $(y_0',z_0') \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ に対し，$B\left(\xi_{(y_0,z_0)}\right) \cap B\left(\xi_{(y_0',z_0')}\right) = \emptyset$ だから

$$\lambda = \prod_{y_0,z_0 \in \mathbb{F}_q^*} \lambda_{(y_0,z_0)} \tag{4.15}$$

であり，式 (4.15) は ξ を共通部分のない置換の積に分解している．

次に，各置換 $\xi_{(y_0,z_0)}$（$y_0,z_0 \in \mathbb{F}_q^*$）を共通部分のない巡回置換の積に分解する．そのために，$x,x' \in \mathbb{F}_q$ に対し，同値関係 $\overset{(\xi)}{\sim}$ を以下で定義する：ある $l \in \{0,1,\ldots,p-1\}$ が存在し，$x' = x - ly_0z_0^2$ と書けるとき，$y \overset{(\xi)}{\sim} y'$．関係 $\overset{(\xi)}{\sim}$ が同値関係であることは明らかである．

$$C_x^{(\xi)} := \{x' \in \mathbb{F}_q \mid x \overset{(\xi)}{\sim} x'\} \tag{4.16}$$

とおく．$\mathcal{R}_\xi$ を $\mathbb{F}_q$ の同値関係 $\overset{(\xi)}{\sim}$ に関する完全代表系と

する．$\sharp\mathcal{R}_\xi = q/p = p^m/p = p^{m-1}$ であることに注意しよう．任意の $x_0 \in \mathcal{R}_\xi$ と任意の $w_0 \in \mathbb{F}_q$ に対し，写像 $\xi_{(w_0,x_0),(y_0,z_0)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc} \xi_{(w_0,x_0),(y_0,z_0)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\ & \cup & & \cup \\ & (w,x,y,z) & \longmapsto & (w, x-yz^2, y, z), \\ & (w,y,z) = (w_0,y_0,z_0) \text{ かつ } x \in C_{x_0}^{(\xi)} \text{のとき}, & & \\ & (w,x,y,z) & \longmapsto & (w,x,y,z), \\ & & & \text{その他のとき}, \end{array} \tag{4.17}$$

で定義する．写像 (4.17) の定義より，$\xi_{(w_0,x_0),(y_0,z_0)}$ は $\mathbb{F}_q^4$ 上の巡回置換であり，$x_0' \in \mathcal{R}_\xi$ が $x_0' \notin C_{x_0}^{(\xi)}$ を満たすならば $C_{x_0}^{(\xi)} \cap C_{x_0'}^{(\xi)} = \emptyset$ であるから，

$$\xi_{(y_0,z_0)} = \prod_{\substack{w_0 \in \mathbb{F}_q \\ x_0 \in \mathcal{R}_\xi}} \xi_{(w_0,x_0),(y_0,z_0)} \tag{4.18}$$

であり，式 (4.18) は置換 $\xi_{(y_0,z_0)}$ を共通部分のない巡回置換の積に分解している．

最後に，巡回置換 $\xi_{(w_0,x_0),(y_0,z_0)}$ を互換の積に分解する．$u \in \{1,\ldots,p-1\}$ なる u に対し，写像 $\xi_{(w_0,x_0),(y_0,z_0)}^{(u)} : \mathbb{F}_q^4 \to \mathbb{F}_q^4$ を

$$\begin{array}{rccc} \xi_{(w_0,x_0),(y_0,z_0)}^{(u)} : & \mathbb{F}_q^4 & \longrightarrow & \mathbb{F}_q^4 \\ & \cup & & \cup \\ & (w,x,y,z) & \longmapsto & (w, x-uyz^2, y, z), \\ & (w,x,y,z) = (w_0,x_0,y_0,z_0) \text{ のとき}, & & \\ & (w,x,y,z) & \longmapsto & (w, x+uyz^2, y, z), \\ & (w,x,y,z) = (w_0, x_0-uy_0z_0^2, y_0, z_0) \text{ のとき}, & & \\ & (w,x,y,z) & \longmapsto & (w,x,y,z), \\ & & & \text{その他のとき}, \end{array} \tag{4.19}$$

で定義する．写像 (4.19) の定義より，$\xi_{(w_0,x_0),(y_0,z_0)}^{(u)}$ は (w_0,x_0,y_0,z_0) と $\left(w_0, x_0-uy_0z_0^2, y_0, z_0\right)$ のみを入れ替え，その他の $\mathbb{F}_q^4$ の元を入れ替えないから確かに互換である．すると，

$$\xi_{(w_0,x_0),(y_0,z_0)} = \xi_{(w_0,x_0),(y_0,z_0)}^{(p-1)} \circ \cdots \circ \xi_{(w_0,x_0),(y_0,z_0)}^{(1)} \tag{4.20}$$

であり，式 (4.20) は巡回置換 $\xi_{(w_0,x_0),(y_0,z_0)}$ を互換の積に分解している．式 (4.15)，式 (4.18)，式 (4.20) より，

$$\lambda = \prod_{\substack{w_0 \in \mathbb{F}_q, x_0 \in \mathcal{R}_\xi \\ y_0,z_0 \in \mathbb{F}_q^*}} \xi_{(w_0,x_0),(y_0,z_0)}^{(p-1)} \circ \cdots \circ \xi_{(w_0,x_0),(y_0,z_0)}^{(1)} \tag{4.21}$$

を得る．よって，ξ は $(p-1)\times p^{m-1}\times(q-1)^2\times q$ 個の互換の積で表される．以上より，

$$\operatorname{sgn}\left(\pi_q\left(\xi\right)\right) = (-1)^{p^{m-1}(p-1)(q-1)^2 q} \tag{4.22}$$

である．

式 (4.13)，及び式 (4.22) を式 (4.4) に代入することにより，

$$\begin{aligned} & \operatorname{sgn}\left(\pi_q\left(\theta\left(\rho\right)\right)\right) \\ &= \operatorname{sgn}\left(\pi_q\left(\lambda\right)\right)\operatorname{sgn}\left(\pi_q\left(\xi\right)\right) \\ &= (-1)^{p^{m-1}(p-1)(q-1)^2} \times (-1)^{p^{m-1}(p-1)(q-1)^2 q} \\ &= (-1)^{p^{m-1}(p-1)(q-1)^2 + p^{m-1}(p-1)(q-1)^2 q} \\ &= (-1)^{p^{m-1}(p-1)(q-1)^2(q+1)} \end{aligned} \tag{4.23}$$

を得る．q が奇数ならば $p-1 \equiv 0 \mod 2$, $q-1 \equiv 0 \mod 2$, $q+1 \equiv 0 \mod 2$ となり，$p^{m-1}\left(p-1\right)\left(q-1\right)^2\left(q+1\right) \equiv 0 \mod 2$ である．$q = 2^m$，$m \geq 2$ ならば $p^{m-1} \equiv 0 \mod 2$ となり，$p^{m-1}\left(p-1\right)\left(q-1\right)^2\left(q+1\right) \equiv 0 \mod 2$ である．したがって，q が奇数，または $q = 2^m$，$m \geq 2$ ならば $\operatorname{sgn}\left(\pi_q\left(\theta\left(\rho\right)\right)\right) = 1$ である．$q = 2$ ならば $p^{m-1}\left(p-1\right)\left(q-1\right)^2\left(q+1\right) = 2^0 \times 1 \times 1^2 \times 3 = 3$ だから $\operatorname{sgn}\left(\pi_q\left(\theta\left(\rho\right)\right)\right) = -1$ である．よって，式 (4.3) が成り立つ． □

主定理 1 と主定理 2 より，Anick automorphism と Nagata-Anick automorphism の置換としての符号の関係について以下の系（系 2）を得る．

系 2. (Anick automorphism と Nagata-Anick automorphism の置換としての符号の関係) $\delta \in \operatorname{Aut}_{\mathbb{F}_q}\mathbb{F}_q\langle x,y,z\rangle$ を式 (2.8) で定義された *Anick automorphism*，$\rho \in \operatorname{Aut}_{\mathbb{F}_q}\mathbb{F}_q\langle w,x,y,z\rangle$ を式 (2.9) で定義された *Nagata-Anick automorphism* とする．このとき，

$$\operatorname{sgn}\left(\pi_q\left(\theta\left(\delta\right)\right)\right) = \operatorname{sgn}\left(\pi_q\left(\theta\left(\rho\right)\right)\right) \tag{4.24}$$

が成り立つ．つまり，*Anick automorphism* $\theta\left(\delta\right)$ の置換としての符号は，*Nagata-Anick automorphism* $\theta\left(\rho\right)$ の置換としての符号と等しく，等式 (4.24) は有限体の要素数 q に依らない．

5. まとめ

本稿では，有限体上定義された Anick automorphism，及び Nagata-Anick automorphism について考察を行い，Anick automorphism の tame decomposition，及び Anick automorphism の置換としての符号を明らかにした．また，Nagata-Anick automorphism と置換として等しい tame decomposition，及び Nagata-Anick automorphism の置換としての符号を明らかにした．さらに，Anick automorphism の置換としての符号は，有限体の要素数に依らず，Nagata-Anick automorphism の置換としての符号と等しいことを示した．

謝辞 本研究は JSPS 科研費 若手研究 (B) 16K16066 の助成を受けたものです．

参考文献

[1] J.-M. Chen and T. T. Moh, On the Goubin-Courtois attack on TTM, Cryptology ePrint Archive, Report 2001/072, 2001. Available from: `http://eprint.iacr.org/2001/072`.

[2] P. M. Cohn, Free Ideal Rings and Localization in General Rings, New Mathematical Monographs 3, Cambridge University Press, Cambridge, 2006.

[3] J. Ding, J. E. Gower and D. S. Schmidt, Multivariate Public Key Cryptosystems, Advances in Information Security, Vol.25, Springer, 2006.

[4] J. Ding and T. Hodges, Cryptanalysis of an implementation scheme of TTM, J. Algebra Appl., **3** (2004), No.3, 273–282.

[5] J. Ding, and D. Schmidt, The new TTM implementation is not secure, Workshop Coding Crypt. Combin., CCC 2003, Vol.23 of Progress in Computer Science and Applied Logic (2004), Birkhauser Verlag, 113–128.

[6] V. Drenski and J.-T. Yu, The strong Anick conjecture is true, J. European Math. Soc., **9** (2007), No.4, 659–679.

[7] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, Progress in Mathematics, Vol.190, Birkhäuser Verlag, Basel-Boston-Berlin, 2000.

[8] L. Goubin, N. Courtois, Cryptanalysis of the TTM cryptosystem, Advances in Cryptology – ASIACRYPT 2000, volume 1976 of Lecture Notes in Computer Science, (2000), Springer-Verlag, 44–57.

[9] H. W. E. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math., **184** (1942), 161–174.

[10] W. van der Kulk, On polynomial rings in two variables, Nieuw Archief voor Wiskunde, **3** (1953), No.1, 33–41.

[11] K. Hakuta, H. Sato, and T. Takagi, On tameness of Matsumoto-Imai central maps in three variables over the finite field $\mathbb{F}_2$, Adv. Math. Commun., **10** (2016), No.2, 221–228.

[12] S. Maubach, Polynomial automorphisms over finite fields, Serdica Math. J., **27** (2001), No.4, 343–350.

[13] S. Maubach and A. Rauf, The profinite polynomial automorphism group, J. Pure Appl. Algebra, **219** (2015), No.10, 4708–4727.

[14] T. T. Moh, A Fast Public Key System with Signature and Master Key Functions, Comm. Algebra, **27** (1999), No.5, 2207–2222.

[15] T. T. Moh, An application of algebraic geometry to encryption: tame transformation method, Rev. Mat. Iberoamericana, **19** (2003), No.2, 667–685.

[16] T. T. Moh, J.-M. Chen and B.-Y. Yang, Building instances of TTM immune to the Goubin-Courtois attack and the Ding-Schmidt attack, Cryptology ePrint Archive, Report 2004/168, 2004. Available from: `http://eprint.iacr.org/2004/168`.

[17] M. Nagata, On automorphism group of $k[x, y]$, Department of Mathematics, Kyoto University, Lectures in Mathematics, No.5, Kinokuniya Book Store Co. Ltd., Tokyo, 1972.

[18] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, 35th Ann. Symp. Found. Comp. Sci., IEEE (1994), 124–134.

[19] M. K. Smith, Stably tame automorphisms, J. Pure Appl. Algebra, **58** (1989), No.2, 209–212.

[20] S. Spodzieja, On the Nagata automorphism, Univ. Iagell. Acta Math., **1298** (2007), No.45, 131–136.