Journal of Mathematics Research; Vol. 9, No. 5; October 2017
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Sign of Permutation Induced by Nagata Automorphism over Finite Fields

Keisuke Hakuta[1] & Tsuyoshi Takagi[2,3]

[1] Interdisciplinary Graduate School of Science and Engineering, Shimane University, Shimane, Japan

[2] Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, Japan

[3] Japan Science and Technology Agency, CREST, Japan

Correspondence: Keisuke Hakuta, Interdisciplinary Graduate School of Science and Engineering, Shimane University, 1060 Nishikawatsu-cho, Matsue, Shimane, Japan. E-mail: hakuta@cis.shimane-u.ac.jp

Received: July 20, 2017 Accepted: August 4, 2017 Online Published: September 8, 2017

doi:10.5539/jmr.v9n5p54 URL: https://doi.org/10.5539/jmr.v9n5p54

Abstract

This paper proves that the Nagata automorphism over a finite field can be mimicked by a tame automorphism which is a composition of four elementary automorphisms. By investigating the sign of the permutations induced by the above elementary automorphisms, one can see that if the Nagata automorphism is defined over a prime field of characteristic two, the Nagata automorphism induces an odd permutation, and otherwise, the Nagata automorphism induces an even permutation.

Keywords: polynomial automorphism, finite field, permutation, nagata automorphism, multivariate polynomial cryptography

1. Introduction

Throughout the paper K denotes a field and $\mathrm{char}(K)$ denotes the characteristic of the field K. Let $K[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates $X_1, \ldots, X_n$ over K. For polynomials $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$, the n-tuple of polynomials $F = (f_1, \ldots, f_n)$ is called a polynomial map. The set of polynomial maps over K and the set of maps from K^n to itself are denoted by $\mathrm{ME}_n(K)$ and $\mathrm{Maps}(K^n, K^n)$, respectively. We can identify each polynomial map with a map from K^n to itself via the following natural map

$$\pi : \quad \mathrm{ME}_n(K) \quad \to \quad \mathrm{Maps}(K^n, K^n).$$

We denote the set of polynomial automorphisms (resp. affine automorphisms, elementary automorphisms) of K^n by $\mathrm{GA}_n(K)$ (resp. $\mathrm{Aff}_n(K)$, $\mathrm{EA}_n(K)$). Recall that

$$\mathrm{Aff}_n(K) \cong K^n \rtimes GL_n(K).$$

We use the symbol $\mathrm{TA}_n(K)$ to represent the subgroup of $\mathrm{GA}_n(K)$ generated by two subgroups $\mathrm{Aff}_n(K)$ and $\mathrm{EA}_n(K)$. For $F \in \mathrm{GA}_n(K)$, F is called *tame automorphism* if $F \in \mathrm{TA}_n(K)$, and otherwise ($F \in \mathrm{GA}_n(K) \setminus \mathrm{TA}_n(K)$) F is called *wild automorphism*. The Tame Generators Problem asks whether $\mathrm{GA}_n(K) = \mathrm{TA}_n(K)$, and is related to the Jacobian conjecture. The equality is trivially true for $n = 1$ and the equality still holds for $n = 2$ (Jung-van der Kulk theorem (Jung, 1942), (Kulk, 1953)). For $n = 3$, Nagata proved that $\sigma \in \mathrm{GA}_2(K[X_3]) \setminus \mathrm{TA}_2(K[X_3])$ (Nagata, 1972, Part 2, Theorem 1.4), and he conjectured that $\sigma \in \mathrm{GA}_3(K) \setminus \mathrm{TA}_3(K)$ (Nagata, 1972, Part 2, Conjecture 3.1). The map σ is called the *Nagata automorphism* (See Equation (1) for the definition of σ). Shestakov and Umirbaev in (Shestakov & Umirbaev, 2004, Corollary 9) finally gives an affirmative answer in the case where $\mathrm{char}(K) = 0$. An algebro-geometric proof of this fact is given by Kishimoto (Kishimoto, 2008). Smith (Smith, 1989) shows that the Nagata automorphism is stably tame, and Spodzieja (Spodzieja, 2007) gives a direct proof of this fact. We refer to (Essen, 2000) for more details.

For any finite set T, we denote by $\mathrm{Sym}(T)$ (resp. $\mathrm{Alt}(T)$) the symmetric group on T (resp. the alternating group on T). Let us denote by $\mathrm{sgn} : \mathrm{Sym}(T) \to \{\pm 1\}$ the sign function. When K is a finite field $\mathbb{F}_q$ with q elements ($p = \mathrm{char}(\mathbb{F}_q)$, $q = p^m$, and $m \geq 1$), we use the symbol π_q instead of π:

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

If we restrict the map π_q to $\mathrm{GA}_n(\mathbb{F}_q)$, $\pi_q(G)$ is a subgroup of $\mathrm{Sym}(\mathbb{F}_q^n)$ for any subgroup $G \subseteq \mathrm{GA}_n(\mathbb{F}_q)$. Maubach has investigated the subgroup $\pi_q(G)$ in the case $G = \mathrm{TA}_n(\mathbb{F}_q)$ (Maubach, 2001, Theorem 2.3).

Theorem 1. *If $n \geq 2$, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(\mathbb{F}_q^n)$ if q is odd or $q = 2$. If $q = 2^m$ where $m \geq 2$ then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(\mathbb{F}_q^n)$.*

If there exists $F \in \mathrm{GA}_n(\mathbb{F}_{2^m})$ such that $\mathrm{sgn}\,(\pi_{2^m}(F)) = -1$, then we must have $F \in \mathrm{GA}_n(\mathbb{F}_{2^m}) \setminus \mathrm{TA}_n(\mathbb{F}_{2^m})$. This indicates that the polynomial automorphism F is wild. Thus, the following question is very important (Maubach, 2008, page 3, Problem).

Question 1. For $q = 2^m$ and $m \geq 2$, do there exist polynomial automorphisms such that the permutations induced by the polynomial automorphisms belong to $\mathrm{Sym}(\mathbb{F}_q^n) \setminus \mathrm{Alt}(\mathbb{F}_q^n)$?

It is a natural question to ask the sign of the famous polynomial automorphisms such as the Nagata automorphism (Nagata, 1972, Section 2.1, Equation (1.1)), the Anick automorphism (Cohn, 2006, Section 6.10, page 398), and the Nagata-Anick automorphism (Cohn, 2006, Section 6.10, page 398). This question is partially solved in the case of the Anick automorphism and the Nagata-Anick automorphism by Hakuta (Hakuta, 2017b, Main Theorem 1 and Main Theorem 2). Hakuta also derives the sign of the permutations induced by the affine automorphisms and the elementary automorphisms (Hakuta, 2017a, Main Theorem 1 and Main Theorem 2). Moreover, for a given tame automorphism over $\mathbb{F}_q$, we can compute the sign of the permutation induced by the tame automorphism over $\mathbb{F}_q$ under the knowledge of a decomposition of the tame automorphism into a finite number of affine automorphisms and elementary automorphisms (Hakuta, 2017a, Corollary 5). However, we emphasize that, at least in our knowledge, the answer of the above problem for the case of the Nagata automorphism over $\mathbb{F}_q$ is unknown yet.

Another motivation for considering the above question comes from multivariate polynomial cryptography (Ding, Gower, & Schmidt, 2006). Multivariate polynomial cryptography is a potential candidate for post-quantum cryptography. One such example is the Tame Transformation Method (See, for example, (Chen & Moh, 2001), (Ding & Hodges, 2004), (Ding & Schmidt, 2004), (Goubin & Courtois, 2000), (Hakuta, Sato, & Takagi, 2016), (Hrdina, Kureš, & Vašík, 2010), (Moh, 1999), (Moh, 2003), (Moh, Chen, & Yang, 2004)). One of the building blocks for multivariate polynomial cryptography is a bijective polynomial map over $\mathbb{F}_q$. Thus, it is important to investigate mathematical properties of bijective polynomial maps over $\mathbb{F}_q$ such as the sign of the permutations induced by bijective polynomial maps over $\mathbb{F}_q$, the classification of bijective polynomial maps over $\mathbb{F}_q$ by individual computation (Maubach & Willems, 2014), and so on.

This paper proves that the Nagata automorphism over a finite field can be mimicked by a tame automorphism which is a composition of four elementary automorphisms. By investigating the sign of the permutations induced by the above elementary automorphisms, one can see that if the Nagata automorphism is defined over a prime field of characteristic two, the Nagata automorphism induces an odd permutation, and otherwise, the Nagata automorphism induces an even permutation.

2. Sign of Permutation Induced by Nagata Automorphism

The Nagata automorphism is defined by

$$\sigma := (x - 2(xz + y^2)y - (xz + y^2)^2 z, y + (xz + y^2)z, z) \in \mathrm{GA}_3(K). \tag{1}$$

The inverse of the Nagata automorphism σ is given by

$$\sigma^{-1} = (x + 2(xz + y^2)y - (xz + y^2)^2 z, y - (xz + y^2)z, z). \tag{2}$$

We call $\pi_q(\sigma)$ the permutation induced by the Nagata automorphism. This section investigates the sign of the permutation $\pi_q(\sigma)$. Let t be a new variable. We first show that there exists a polynomial $h(t) \in \mathbb{F}_q[t]$ such that $h(\alpha) = 0$ for $\alpha \in \mathbb{F}_q^*$ and $h(0) = 1$ for $\alpha = 0$. In order to prove this claim, we define the polynomial $f(t) \in \mathbb{F}_q[t]$ as follows:

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

We put $c_0 := f(0)$. By (Hakuta, 2017b, page 26), we have $c_0 \in \mathbb{F}_q^*$ and $h(t) := c_0^{-1} \times f(t) \in \mathbb{F}_q[t]$ satisfies the condition

$$h(\alpha) = \begin{cases} 0 & (\alpha \in \mathbb{F}_q^*), \\ 1 & (\alpha = 0). \end{cases} \tag{3}$$

We say that $F \in \mathrm{GA}_n(\mathbb{F}_q)$ can be *mimicked* by an element of a certain group $\mathcal{G}$ if there exists $G \in \mathcal{G}$ such that $\pi_q(F) = \pi_q(G)$ (See (Maubach & Willems, 2011, page 305) for more details). We prove the following lemma (Lemma 1) which states that the Nagata automorphism over $\mathbb{F}_q$ can be mimicked by a composition of four elementary automorphisms.

Lemma 1. *Let ϕ, λ, and $\hat{\lambda}$ be elementary automorphisms defined by*

$$\phi := (x + z^{q-2}y^2, y, z), \lambda := (x, y + z^2x, z), \hat{\lambda} := (x - 2h(z)y^3, y, z) \in \mathrm{EA}_3(\mathbb{F}_q).$$

Then we have

$$\pi_q(\sigma) = \pi_q(\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi). \tag{4}$$

In other words, the Nagata automorphism σ can be mimicked by $\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi \in \mathrm{TA}_3(\mathbb{F}_q)$ which is a composition of four elementary automorphisms.

Proof. It is easy to see that

$$\begin{aligned}
\pi_q(\lambda \circ \phi) &= \pi_q((x, y + z^2x, z) \circ (x + z^{q-2}y^2, y, z)) \\
&= \pi_q((x + z^{q-2}y^2, y + z^2(x + z^{q-2}y^2), z)) \\
&= \pi_q((x + z^{q-2}y^2, y + (xz^2 + z^qy^2), z)) \\
&= \pi_q((x + z^{q-2}y^2, y + (xz^2 + zy^2), z)) \\
&= \pi_q((x + z^{q-2}y^2, y + z(xz + y^2), z)).
\end{aligned}$$

Since $\phi^{-1} = (x - z^{q-2}y^2, y, z) \in \mathrm{EA}_3(\mathbb{F}_q)$, we obtain

$$\begin{aligned}
&\pi_q(\phi^{-1} \circ \lambda \circ \phi) \\
&= \pi_q((x - z^{q-2}y^2, y, z) \circ (x + z^{q-2}y^2, y + z(xz + y^2), z)) \\
&= \pi_q(((x + z^{q-2}y^2) - z^{q-2}(y + z(xz + y^2))^2, y + z(xz + y^2), z)) \\
&= \pi_q((x - 2(xz + y^2)yz^{q-1} - (xz + y^2)^2z, y + (xz + y^2)z, z)).
\end{aligned}$$

Then we can see that

$$(\phi^{-1} \circ \lambda \circ \phi)(x, y, z) = \begin{cases} \sigma(x, y, z) & (z \in \mathbb{F}_q^*), \\ (x, y, 0) \neq \sigma(x, y, z) = (x - 2y^3, y, 0) & (z = 0). \end{cases}$$

From Equation (3), we have $(\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi)(x, y, z) = \sigma(x, y, z)$ for all $(x, y, z) \in \mathbb{F}_q^3$. Therefore, $\pi_q(\sigma) = \pi_q(\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi)$. □

From Lemma 1, it is sufficient to derive the sign of $\pi_q(\lambda)$ and $\pi_q(\hat{\lambda})$. We compute $\mathrm{sgn}(\pi_q(\lambda))$ (resp. $\mathrm{sgn}(\pi_q(\hat{\lambda}))$) in Lemma 2 (resp. Lemma 3). We will use these lemmas to prove the main result of this paper (Main Theorem 1).

Lemma 2. (Sign of $\pi_q(\lambda)$) *Let λ be as in Lemma* 1. *Then we have*

$$\mathrm{sgn}(\pi_q(\lambda)) = (-1)^{p^{m-1}(p-1)(q-1)^2}. \tag{5}$$

Namely, if q is odd or $q = 2^m$, $m \geq 2$ then we have $\pi_q(\lambda) \in \mathrm{Alt}(\mathbb{F}_q^3)$. If $q = 2$ then we have $\pi_q(\lambda) \in \mathrm{Sym}(\mathbb{F}_q^3) \setminus \mathrm{Alt}(\mathbb{F}_q^3)$.

Proof. Let us take two elements $x_0, z_0 \in \mathbb{F}_q^*$. We consider the following map $\lambda_{(x_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$,

$$\begin{array}{rccll}
\lambda_{(x_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 & \\
& (x, y, z) & \longmapsto & (x, y + z^2x, z), & \text{if } x = x_0 \text{ and } z = z_0, \\
& (x, y, z) & \longmapsto & (x, y, z), & \text{otherwise.}
\end{array}$$

One can see that the map $\lambda_{(x_0,z_0)}$ is bijective. We take

$$B(\lambda_{(x_0,z_0)}) := \left\{(x, y, z) \in \mathbb{F}_q^3 \;\middle|\; \lambda_{(x_0,z_0)}(x, y, z) \neq (x, y, z)\right\}.$$

Since $B(\lambda_{(x_0,z_0)}) \cap B\left(\lambda_{(x_0',z_0')}\right) = \emptyset$ for any $\left(x_0', z_0'\right) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \setminus \{(x_0, z_0)\}$, we have

$$\lambda = \prod_{x_0,z_0 \in \mathbb{F}_q^*} \lambda_{(x_0,z_0)},$$

which is a composition of disjoint permutations on $\mathbb{F}_q^3$. We decompose the permutation $\lambda_{(x_0,z_0)}$ as a composition of disjoint cycles on $\mathbb{F}_q^3$ for each $(x_0, z_0) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. In order to find such a decomposition, we define an equivalence relation $\overset{(\lambda)}{\sim}$ on $\mathbb{F}_q$: $y \in \mathbb{F}_q$ and $y' \in \mathbb{F}_q$ are equivalent if and only if there exists $l \in \{0, 1, \ldots, p-1\}$ such that $y' = y - lz_0^2 x_0$. We set

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

We fix a complete system of representatives $\mathcal{R}_\lambda$ for the equivalence relation $\overset{(\lambda)}{\sim}$ on $\mathbb{F}_q$. Remark that $\sharp\mathcal{R}_\lambda = q/p = p^m/p = p^{m-1}$. For arbitrary $x_0 \in \mathcal{R}_\lambda$, we define the bijective map $\lambda_{y_0,(x_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ by

$$\begin{array}{rccll} \lambda_{y_0,(x_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 & \\ & (x,y,z) & \longmapsto & \left(x, y + z^2 x, z\right), & \text{if } y \in C_{y_0}^{(\lambda)}, x = x_0, \text{ and } z = z_0, \\ & (x,y,z) & \longmapsto & (x,y,z), & \text{otherwise.} \end{array}$$

It is obvious from the definition of the map $\lambda_{y_0,(x_0,z_0)}$ that $\lambda_{y_0,(x_0,z_0)}$ is a cycle of length p. Namely,

$$\operatorname{sgn}\left(\pi_q\left(\lambda_{y_0,(x_0,z_0)}\right)\right) = (-1)^{p-1}.$$

Let us take $y_0' \in \mathcal{R}_\lambda$. If $y_0' \notin C_{y_0}^{(\lambda)}$ then from $C_{y_0}^{(\lambda)} \cap C_{y_0'}^{(\lambda)} = \emptyset$, we have

$$\lambda_{(x_0,z_0)} = \prod_{y_0 \in \mathcal{R}_\lambda} \lambda_{y_0,(x_0,z_0)},$$

which is a composition of disjoint cycles on $\mathbb{F}_q^3$. Since π_q and sgn are homomorphisms of groups, we obtain

$$\begin{aligned} \operatorname{sgn}\left(\pi_q(\lambda)\right) &= \prod_{x_0,z_0 \in \mathbb{F}_q^*, y_0 \in \mathcal{R}_\lambda} \operatorname{sgn}\left(\pi_q\left(\lambda_{y_0,(x_0,z_0)}\right)\right) \\ &= \prod_{x_0,z_0 \in \mathbb{F}_q^*, y_0 \in \mathcal{R}_\lambda} (-1)^{p-1} = (-1)^{p^{m-1}(p-1)(q-1)^2}. \end{aligned}$$

Thus, Equation (5) holds. □

Lemma 3. (Sign of $\pi_q(\hat{\lambda})$) *Let $\hat{\lambda}$ be as in Lemma* 1. *Then we have*

$$\operatorname{sgn}(\pi_q(\hat{\lambda})) = 1. \tag{6}$$

Namely, we have $\pi_q(\hat{\lambda}) \in \operatorname{Alt}(\mathbb{F}_q^3)$.

Proof. Since $\operatorname{sgn}(\pi_q(\hat{\lambda})) = 1$ when $\operatorname{char}(\mathbb{F}_q) = 2$, it is sufficient to show the assertion for $\operatorname{char}(\mathbb{F}_q) \neq 2$. We suppose that $\operatorname{char}(\mathbb{F}_q) \neq 2$. By the definition of $\hat{\lambda}$ and by Equation (3), we can easily see that

$$\hat{\lambda}(x,y,z) = \begin{cases} (x,y,z) & (z \in \mathbb{F}_q^*), \\ (x - 2y^3, y, 0) & (z = 0). \end{cases}$$

Let us take an element $y_0 \in \mathbb{F}_q^*$ and we put $z_0 := 0$. We consider the following map $\hat{\lambda}_{(y_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$,

$$\begin{array}{rccll} \hat{\lambda}_{(y_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 & \\ & (x,y,z) & \longmapsto & (x - 2y^3, y, z), & \text{if } y \in \mathbb{F}_q^* \text{ and } z = 0, \\ & (x,y,z) & \longmapsto & (x,y,z), & \text{otherwise.} \end{array}$$

One can see that the map $\hat{\lambda}_{(y_0,z_0)}$ is bijective. We take

$$B\left(\hat{\lambda}_{(y_0,z_0)}\right) := \left\{(x,y,z) \in \mathbb{F}_q^3 \;\middle|\; \hat{\lambda}_{(y_0,z_0)}(x,y,z) \neq (x,y,z)\right\}.$$

Since $B\left(\hat{\lambda}_{(y_0,z_0)}\right) \cap B\left(\hat{\lambda}_{(y_0',z_0)}\right) = \emptyset$ for any $y_0' \in \mathbb{F}_q^* \setminus \{y_0\}$, we have

$$\hat{\lambda} = \prod_{y_0 \in \mathbb{F}_q^*} \hat{\lambda}_{(y_0,z_0)},$$

which is a composition of disjoint permutations on $\mathbb{F}_q^3$. We decompose the permutation $\hat{\lambda}_{(y_0,z_0)}$ as a composition of disjoint cycles on $\mathbb{F}_q^3$ for each $y_0 \in \mathbb{F}_q^*$. In order to find such a decomposition, we define an equivalence relation $\overset{(\hat{\lambda})}{\sim}$ on $\mathbb{F}_q$: $x \in \mathbb{F}_q$ and $x' \in \mathbb{F}_q$ are equivalent if and only if there exists $l \in \{0, 1, \ldots, p-1\}$ such that $x' = x - 2ly_0^3$. We set

$$C_x^{(\hat{\lambda})} := \{x' \in \mathbb{F}_q \mid x \overset{(\hat{\lambda})}{\sim} x'\}.$$

We fix a complete system of representatives $\mathcal{R}_{\hat{\lambda}}$ for the equivalence relation $\overset{(\hat{\lambda})}{\sim}$ on $\mathbb{F}_q$. Remark that $\sharp\mathcal{R}_{\hat{\lambda}} = q/p = p^m/p = p^{m-1}$. For arbitrary $x_0 \in \mathcal{R}_{\hat{\lambda}}$, we define the bijective map $\hat{\lambda}_{x_0,(y_0,z_0)} : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ by

$$\begin{array}{rccll} \hat{\lambda}_{x_0,(y_0,z_0)} : & \mathbb{F}_q^3 & \longrightarrow & \mathbb{F}_q^3 & \\ & (x,y,z) & \longmapsto & \left(x, y + z^2 x, z\right), & \text{if } x \in C_{x_0}^{(\hat{\lambda})}, y = y_0, \text{ and } z = z_0, \\ & (x,y,z) & \longmapsto & (x,y,z), & \text{otherwise.} \end{array}$$

It is obvious from the definition of the map $\hat{\lambda}_{x_0,(y_0,z_0)}$ that $\hat{\lambda}_{x_0,(y_0,z_0)}$ is a cycle of length p. Namely,

$$\operatorname{sgn}\left(\pi_q\left(\hat{\lambda}_{x_0,(y_0,z_0)}\right)\right) = (-1)^{p-1}.$$

Let us take $x_0' \in \mathcal{R}_{\hat{\lambda}}$. If $x_0' \notin C_{x_0}^{(\hat{\lambda})}$ then from $C_{x_0}^{(\hat{\lambda})} \cap C_{x_0'}^{(\hat{\lambda})} = \emptyset$, we have

$$\hat{\lambda}_{(y_0,z_0)} = \prod_{x_0 \in \mathcal{R}_{\hat{\lambda}}} \hat{\lambda}_{x_0,(y_0,z_0)},$$

which is a composition of disjoint cycles on $\mathbb{F}_q^3$. Since π_q and sgn are homomorphisms of groups, we obtain

$$\begin{aligned} \operatorname{sgn}\left(\pi_q\left(\hat{\lambda}\right)\right) &= \prod_{x_0 \in \mathcal{R}_{\hat{\lambda}}, y_0 \in \mathbb{F}_q^*} \operatorname{sgn}\left(\pi_q\left(\hat{\lambda}_{x_0,(y_0,z_0)}\right)\right) \\ &= \prod_{x_0 \in \mathcal{R}_{\hat{\lambda}}, y_0 \in \mathbb{F}_q^*} (-1)^{p-1} = (-1)^{p^{m-1}(p-1)(q-1)} = 1. \end{aligned}$$

Thus we always have $\operatorname{sgn}(\pi_q(\hat{\lambda})) = 1$. Hence, Equation (6) holds. □

From Lemma 2 and Lemma 3, we have the following main result of this paper (Main Theorem 1).

Main Theorem 1. (Sign of Nagata automorphism) *If q is odd or $q = 2^m$, $m \geq 2$ then we have $\pi_q(\sigma)) \in \operatorname{Alt}(\mathbb{F}_q^3)$. If $q = 2$ then we have $\pi_q(\sigma) \in \operatorname{Sym}(\mathbb{F}_q^3) \setminus \operatorname{Alt}(\mathbb{F}_q^3)$. Namely,*

$$\operatorname{sgn}(\pi_q(\sigma)) = \begin{cases} 1 & (q \text{ is odd or } q = 2^m \text{ and } m \geq 2), \\ -1 & (q = 2). \end{cases} \tag{7}$$

Proof. From Lemma 1, we have

$$\operatorname{sgn}(\pi_q(\sigma)) = \operatorname{sgn}(\pi_q(\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi)).$$

Since π_q and sgn are group homomorphisms, we can derive

$$\begin{aligned} \operatorname{sgn}(\pi_q(\hat{\lambda} \circ \phi^{-1} \circ \lambda \circ \phi)) &= \operatorname{sgn}(\pi_q(\hat{\lambda})\pi_q(\phi^{-1})\pi_q(\lambda)\pi_q(\phi)) \\ &= \operatorname{sgn}(\pi_q(\hat{\lambda}))\operatorname{sgn}(\pi_q(\phi^{-1}))\operatorname{sgn}(\pi_q(\lambda))\operatorname{sgn}(\pi_q(\phi)) \\ &= \operatorname{sgn}(\pi_q(\hat{\lambda}))\operatorname{sgn}(\pi_q(\phi))^{-1}\operatorname{sgn}(\pi_q(\lambda))\operatorname{sgn}(\pi_q(\phi)) \\ &= \operatorname{sgn}(\pi_q(\hat{\lambda})) \times \operatorname{sgn}(\pi_q(\lambda)). \end{aligned}$$

Thus, it follows immediately from Lemma 2 and Lemma 3. □

Remark 1. One can also prove Lemma 2 and Lemma 3 by avoiding the cycle decomposition of permutations. Here, we give a more simple proof of Lemma 2 and Lemma 3. It follows immediately from (Hakuta, 2017a, Main Theorem 1) that $\operatorname{sgn}(\pi_q(\hat{\lambda})) = 1$. Again from (Hakuta, 2017a, Main Theorem 1), we have

$$\operatorname{sgn}(\pi_q(\lambda)) = \begin{cases} 1 & (q \text{ is odd or } q = 2^m \text{ and } m \geq 2), \\ -1 & (q = 2). \end{cases}$$

Thus, Lemma 2 and Lemma 3 hold.

References

Chen, J.-M., & Moh, T. T. (2001). *On the Goubin-Courtois attack on TTM*. Cryptology ePrint Archive, Report 2001/072.

Cohn, P. M. (2006). *Free Ideal Rings and Localization in General Rings*. Cambridge University Press.

van den Essen, A. (2000). *Polynomial Automorphisms and the Jacobian Conjecture*. Birkhäuser.

Ding, J., Gower, J. E., & Schmidt, D. S. (2006). *Multivariate Public Key Cryptosystems*. Springer.

Ding, J., & Hodges, T. (2004). Cryptanalysis of an implementation scheme of TTM. *J. Algebra Appl., 3*(3), 273–282.

Ding, J., & Schmidt, D. (2004). The new implementation schemes of the TTM cryptosystem are not secure. In Feng, K., Niederreiter, H., & Xing, C. (Eds.), *Coding, Cryptography and Combinatorics*, 113–127. Birkhäuser Verlag. https://doi.org/10.1007/978-3-0348-7865-4_6

Goubin, L., & Courtois, N., (2000). Cryptanalysis of the TTM cryptosystem. In Okamoto, T. (Eds.), *Advances in Cryptology – ASIACRYPT 2000*, 44–57. Springer. https://doi.org/10.1007/3-540-44448-3_4

Hakuta, K. (2017a). *On permutations induced by tame automorphisms over finite fields*. *Acta Math. Vietnam.*, to appear. https://doi.org/10.1007/s40306-017-0217-0

Hakuta, K. (2017b). Sign of permutations induced by Anick and Nagata-Anick automorphisms over finite fields. *Journal of Mathematics Research, 9*(4), 23–29. https://doi.org/10.5539/jmr.v9n4p23

Hakuta, K., Sato, H., & Takagi, T. (2016). On tameness of Matsumoto-Imai central maps in three variables over the finite field $\mathbb{F}_2$. *Adv. Math. Commun., 10*(2), 221–228. https://doi.org/10.3934/amc.2016002

Hrdina, J., Kureš, M., & Vašík, P. (2010). A note on tame polynomial automorphisms and the security of TTM cryptosystem. *Appl. Comput. Math., 9*(2), 226–233.

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

Kishimoto, T. (2008). A new proof of the non-tameness of the Nagata automorphism from the point of view of the Sarkisov program. *Compositio Math., 144*, 963–977. https://doi.org/10.1112/S0010437X10004781

van der Kulk, W. (1953). On polynomial rings in two variables. *Nieuw Archief voor Wiskunde, 3*(1), 33–41.

Maubach, S. (2001). Polynomial automorphisms over finite fields. *Serdica Math. J., 27*(4), 343–350.

Maubach, S. (2008). *A problem on polynomial maps over finite fields*. arXiv preprint, arXiv:0802.0630.

Maubach, S., & Willems, R. (2011). Polynomial automorphisms over finite fields: Mimicking tame maps by the Derksen group. *Serdica Math. J., 37*(4), 305–322.

Maubach, S., & Willems, R. (2014). Keller maps of low degree over finite fields. In Cheltsov, I., Ciliberto, C., Flenner, H., McKernan, J., Prokhorov, Y., & Zaidenberg, M. (Eds.), *Automorphisms in Birational and Affine Geometry*, 477–493. Springer. https://doi.org/10.1007/978-3-319-05681-4_26

Moh, T. T. (1999). A Fast Public Key System with Signature and Master Key Functions. *Comm. Algebra, 27*(5), 2207–2222.

Moh, T. T. (2003). An application of algebraic geometry to encryption: tame transformation method. *Rev. Mat. Iberoamericana, 19*(2), 667–685. https://doi.org/10.4171/RMI/364

Moh, T. T., Chen, J.-M., & Yang, B.-Y. (2004). *Building instances of TTM immune to the Goubin-Courtois attack and the Ding-Schmidt attack*. Cryptology ePrint Archive, Report 2004/168.

Nagata, M. (1972). *On automorphism group of* $k[x, y]$. Kinokuniya Book Store Co. Ltd.

Smith, M. K. (1989). Stably tame automorphisms. *J. Pure Appl. Algebra, 58*(2), 209–212. https://doi.org/10.1016/0022-4049(89)90158-8

Spodzieja, S. (2007). On the Nagata automorphism. *Univ. Iagell. Acta Math., 1298*(45), 131–136.

Shestakov, I. P., & Umirbaev, U. U. (2004). The tame and the wild automorphisms of polynomial rings in three variables. *J. Amer. Math. Soc., 17*, 197–227. https://doi.org/10.1090/S0894-0347-03-00440-5