Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **37** (2011), 305–322

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

POLYNOMIAL AUTOMORPHISMS OVER FINITE FIELDS: MIMICKING TAME MAPS BY THE DERKSEN GROUP

Stefan Maubach*, Roel Willems†

Communicated by V. Drensky

Abstract. If F is a polynomial automorphism over a finite field $\mathbb{F}_q$ in dimension n, then it induces a permutation $\pi_{q^r}(F)$ of $(\mathbb{F}_{q^r})^n$ for every $r \in \mathbb{N}^*$. We say that F can be 'mimicked' by elements of a certain group of automorphisms $\mathcal{G}$ if there are $g_r \in \mathcal{G}$ such that $\pi_{q^r}(g_r) = \pi_{q^r}(F)$.

Derksen's theorem in characteristic zero states that the tame automorphisms in dimension $n \geq 3$ are generated by the affine maps and the one map $(x_1 + x_2^2, x_2, \ldots, x_n)$. We show that Derksen's theorem is not true in characteristic p in general. However, we prove a modified, weaker version of Derksen's theorem over finite fields: we introduce the Derksen group $\mathrm{DA}_n(\mathbb{F}_q)$, $n \geq 3$, which is generated by the affine maps and one well-chosen nonlinear map, and show that $\mathrm{DA}_n(\mathbb{F}_q)$ mimicks any element of $\mathrm{TA}_n(\mathbb{F}_q)$. Also, we do give an infinite set E of non-affine maps which, together with the affine maps, generate the tame automorphisms in dimension 3 and up. We conjecture that such a set E cannot be finite.

We consider the subgroups $\mathrm{GLIN}_n(k)$ and $\mathrm{GTAM}_n(k)$. We prove that for k a finite field, these groups are equal if and only if $k \neq \mathbb{F}_2$. The latter result provides a tool to show that a map is not linearizable.

2010 *Mathematics Subject Classification:* 14L99, 14R10, 20B27.

Key words: Polynomial automorphisms, permutation groups, tame automorphism group.

*Research done while funded by Veni-grant of Council for the Physical Sciences, Netherlands Organisation for Scientific Research (NWO).

†Funded by Phd-grant of Council for the Physical Sciences, Netherlands Organisation for Scientific Research (NWO).

1. Preliminaries.

1.1. Introduction. Polynomial automorphisms are generally studied over $\mathbb{C}$, $\mathbb{Q}$, or any field of characteristic zero. Even if they are studied over commutative rings, then it is often assumed that $\mathbb{Q}$ (or $\mathbb{Z}$) is a subset of the ring. The characteristic p case is quite unexplored, though it is gaining some interest, in particular over finite fields (see [4, 9, 2]).

Denote by $\mathrm{MA}_n(k)$ the set of polynomial maps (i.e. endomorphisms), by $\mathrm{GA}_n(k)$ the polynomial automorphism group in dimension n over k, and $\mathrm{TA}_n(k)$ as the tame subgroup of $\mathrm{GA}_n(k)$ (a precise definition is given in the next section). Any element $F \in \mathrm{GA}_n(\mathbb{F}_q)$ (where $q = p^r$, p a prime, and $\mathbb{F}_q$ denotes the finite field with q elements) induces a permutation of $\mathbb{F}_{q^m}^n$ for each $m \in \mathbb{N}^*$. This permutation we denote by $\pi_{q^m}(F)$.

One motivation to study this group is a result from [9], namely that $\pi_q(\mathrm{TA}_n(\mathbb{F}_q))$, $n \geq 2$, equals the set of all permutations of $(\mathbb{F}_q)^n$, except if $q = 2^m$, $m \geq 2$, then any such permutation will be an even permutation of $\mathbb{F}_q^n$. This incited the search for automorphisms which were "odd", as such an example would immediately be non-tame, giving a very simple proof of the existence of wild automorphisms. Note that the proof of $\mathrm{TA}_3(k) \neq \mathrm{GA}_3(k)$ by Umirbaev-Shestakov in [12, 13] is only valid in $\operatorname{char} k = 0$. Unfortunately, all examples studied so far turned out to be even.

In this paper the goal is to understand the group $\mathrm{TA}_n(\mathbb{F}_q)$ and its images $\pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$ better. In particular, we made a preliminarly investigation on what the generators of both these groups are. We also are interested in finding subgroups H of $\mathrm{TA}_n(\mathbb{F}_q)$ satisfy $\pi_{q^m}(H) = \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$ for each $m \in \mathbb{N}$ (we say that H mimicks $\mathrm{TA}_n(\mathbb{F}_q)$). One such group H is the Derksen group $\mathrm{DA}_n(\mathbb{F}_q)$ introduced in Section 3, and the (unfortunately quite technical) proof of this fact covers a large part of this paper. We also point out that, even though in $\operatorname{char} k = 0$ we have $\mathrm{DA}_n(k) = \mathrm{TA}_n(k)$ (Derksen's theorem), that for $\operatorname{char} k = p$ such an equality is not expected to hold (see Section 2).

In the paper [11] the subgroups $\mathrm{GLIN}_n(k)$ and $\mathrm{GTAM}_n(k)$ of $\mathrm{GA}_n(k)$ are introduced. GLIN is the group generated by the set of automorphisms which are linear up to conjugation by an element of GA, and GTAM is defined in a similar way. In Section 4 we show that these groups are equal, except if the field $k = \mathbb{F}_2$, in which case they differ.

1.2. Definitions. Let p be a prime, $q = p^r$, $\mathbb{F}_q$ the finite field with q elements. Let $n \geq 1$. We are interested in the group $\mathrm{GA}_n(\mathbb{F}_q)$ of polynomial autmorphisms over $\mathbb{F}_q$. Subgroups of $\mathrm{GA}_n(\mathbb{F}_q)$ are the group of linear automorphisms $\mathrm{GL}_n(\mathbb{F}_q)$ and the group of affine automorphisms $\mathrm{Aff}_n(\mathbb{F}_q)$. Let us first fix a notation for some special elements of $\mathrm{Aff}_n(\mathbb{F}_q)$;

- $T_{i,c} = (X_1, \dots, X_{i-1}, X_i + c, X_{i+1}, \dots, X_n)$,
- $S_{i,c} = (X_1, \dots, X_{i-1}, cX_i, X_{i+1}, \dots, X_n)$ and
- $R_{i,j} = (X_1, \dots, X_{i-1}, X_j, X_{i+1}, \dots, X_{j-1}, X_i, X_{j+1}, X_n)$,

where $i, j \in \{1, \dots, n\}$ and $c \in \mathbb{F}_q^*$. Incidentally, the $T_{i,c}$, $S_{i,c}$, $R_{i,j}$ generate $\mathrm{Aff}_n(\mathbb{F}_q)$. Note that $R_{i,j} = R_{j,i} = R_{i,j}^{-1}$, $R_{i,j}T_{i,c}R_{i,j} = T_{j,c}$ and $R_{i,j}S_{i,c}R_{i,j} = S_{j,c}$. Now if for $\alpha \in \mathbb{N}^{n-1}$ we write $X^\alpha = X_2^{\alpha_2} X_3^{\alpha_3} \cdots X_n^{\alpha_n}$ (note the omission of X_1), then we can define an elementary automorphism $E_{1,\alpha} = (X_1 + X^\alpha, X_2, \dots, X_n) \in \mathrm{GA}_n(\mathbb{F}_q)$, and more general $E_{i,\alpha} = R_{1,i}E_{1,\alpha}R_{1,i}$.
Another subgroup of interest of $\mathrm{GA}_n(\mathbb{F}_q)$ is the group of tame automorphisms $\mathrm{TA}_n(\mathbb{F}_q) = \langle \mathrm{Aff}_n(\mathbb{F}_q), E_{1,\alpha}; \alpha \in \mathbb{N}^{n-1} \rangle$ generated by the affine and elementary automorphisms. An important result on this group is by Jung and van der Kulk [7, 8]:

Theorem 1.1. *For any field k, $\mathrm{TA}_2(k) = \mathrm{GA}_2(k)$.*

H. Derksen proved that

Theorem 1.2. *Let k be a field of characteristic zero and $n \geq 3$, then $\mathrm{TA}_n(k) = \langle \mathrm{Aff}_n(k), \varepsilon \rangle$, where $\varepsilon = (X_1 + X_2^2, X_2, \dots, X_n)$.*

For a proof, see [5] pages 95–96. More recently Bodnarchuk in [3] showed that $\mathrm{TA}_n(k) = \langle \mathrm{Aff}_n(k), F \rangle$, for k a field of characteristic zero, where F is any non-linear triangular automorphism. As such, the choice of ε is quite arbitrary. However, over finite fields Derksen's result (and Bodnarchuk's result) will for sure not hold, as shown in Section 2. In Section 3 we will prove a similar (but weaker) result for k a finite field. Let us first define our version of the Derksen automorphism group, for an appropriate automorphism ε:

Definition 1.3.

$$\mathrm{DA}_n(\mathbb{F}_q) = \langle \mathrm{Aff}_n(\mathbb{F}_q), \varepsilon \rangle \subset \mathrm{TA}_n(\mathbb{F}_q),$$

where $\varepsilon = E_{1,\alpha} = (X_1 + X^\alpha, X_2, X_3, \dots, X_n)$ where $\alpha := (p-1, \dots, p-1)$.

We furthermore need the following map:

Definition 1.4. *Let $\mathrm{Perm}(\mathbb{F}_q^n)$ be the group of permutations of $\mathbb{F}_q^n$, which is isomorphic to $\mathrm{Sym}(q^n)$. We can define*

$$\pi_q : \mathrm{GA}_n(\mathbb{F}_q) \to \mathrm{Perm}(\mathbb{F}_q^n),$$

as the canonical map, associating to an automorphism its induced permutation on the space $\mathbb{F}_q^n$.

Note that, since $\mathrm{Perm}(\mathbb{F}_q^n) \cong \mathrm{Sym}(q^n)$, it follows that π_q is a group homomorphism. In particular for $F, G \in \mathrm{GA}_n(\mathbb{F}_q)$ we have that $\pi_q(FG) = \pi_q(F)\pi_q(G)$. Furthermore since $\mathrm{GA}_n(\mathbb{F}_q) < \mathrm{GA}_n(\mathbb{F}_{q^m})$, we can talk about $\pi_{q^m} : \mathrm{GA}_n(\mathbb{F}_q) \to \mathrm{Perm}(\mathbb{F}_{q^m}^n)$.

2. Generators of the Tame Automorphism Group.

2.1. Characteristic zero versus characteristic p. We do find it necessary to point out some of the obstructions one encounters in characteristic p. If k is a field of characteristic zero, then $\mathrm{TA}_n(k) = \mathrm{DA}_n(k)$ if $n \geq 3$: essential in the proof is that for each $m \in \mathbb{N}$, linear combinations of $(x_2a_2 + \ldots, +x_na_n)^m$ yield all monomials of degree m in the variables $x_2, \ldots, x_n$. This is not true in characteristic p (pick $m = p$ for one!).

In fact, in characteristic p it is not clear if there are finitely many automorphisms that one can add to the affine group to generate the whole tame automorphism group. Our experiments and research has convinced us that we can conjecture:

Conjecture 2.1. *There exists no finite set E (let alone one consisting of one element) such that* $\mathrm{TA}_n(\mathbb{F}_q) = \langle \mathrm{Aff}_n(\mathbb{F}_q), E\rangle$.

In characteristic zero Derksen's theorem shows that one can generate the tame automorphism group in dimension 3 and up by the affine maps and only one nonlinear map; Bodnarchuk's theorem states that for any nonlinear triangular map this is true. However:

Lemma 2.2. *Derksen's theorem is not true in characteristic* 2.

Proof. The simplest counterexample is $\pi_2(\langle \mathrm{Aff}_3(\mathbb{F}_2), (X + Y^2, Y, Z)\rangle) = \pi_2(\mathrm{Aff}_3(\mathbb{F}_2))$ which consists of only even permutations, while $\pi_2(\mathrm{TA}_3(\mathbb{F}_2))$ consists of all permutations of $(\mathbb{F}_2)^3$: hence $\langle \mathrm{Aff}_3(\mathbb{F}_2), (X + Y^2, Y, Z)\rangle$ cannot be equal to $\mathrm{TA}_3(\mathbb{F}_2)$. □

The above lemma does not claim that Derksen's theorem is not true for *any* prime characteristic, but if Conjecture 2.1 holds, this will not be the case.

2.2. Generating set of $\mathrm{TA}_n(\mathbb{F}_q)$. We were able to find the following infinite generating set E:

Theorem 2.3. $\mathrm{TA}_n(F_q) = \langle \mathrm{Aff}_n(F_q), E\rangle$, *where*
$$E = \{(x_1 + x_2^{k_2p-1} \cdots x_n^{k_np-1}, x_2, \ldots, x_n) \mid 1 \leq k_2 \leq \ldots \leq k_n\}.$$

The proof of this theorem is the topic of the current section.

Lemma 2.4. *Let p be a prime, $q = p^r$ and $\mathbb{F}_q$ be the finite field with q elements. Let $\mathbb{F}_q[Y]$ be the ring in one variable Y, over $\mathbb{F}_q$. Let $k \in \mathbb{N}$, and finally, let $kp \leq l < kp + p$ where $l \in \mathbb{N}$.*

Then there exists a vector $\alpha = (\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{F}_p^p$ such that

$$(\alpha_0, \dots, \alpha_{p-1}) \begin{pmatrix} (Y+0)^{kp+p-1} \\ (Y+1)^{kp+p-1} \\ \vdots \\ (Y+p-1)^{kp+p-1} \end{pmatrix} = Y^l + P(Y),$$

where $\deg(P(Y)) < kp$.

Proof. We will calculate modulo the $\mathbb{F}_q$-module M of polynomials of degree $< kp$. First note that $(Y+i)^{kp+p-1} = \sum_{j=0}^{p-1} \binom{kp+p-1}{j} i^j Y^{kp+p-1-j} \mod M$. So

$$\begin{pmatrix} (Y+0)^{kp+p-1} \\ \vdots \\ (Y+p-1)^{kp+p-1} \end{pmatrix} = \left(\binom{kp+p-1}{j} i^j \right)_{0 \leq i,j \leq p-1} \begin{pmatrix} Y^{kp+p-1} \\ \vdots \\ Y^{kp} \end{pmatrix} \mod M.$$

Now

$$\left(\binom{kp+p-1}{j} i^j \right)_{0 \leq i,j \leq p-1} = \begin{pmatrix} \binom{kp+p-1}{0} & & \emptyset \\ & \ddots & \\ \emptyset & & \binom{kp+p-1}{p-1} \end{pmatrix} \left(i^j \right)_{0 \leq i,j \leq p-1}.$$

Because $\binom{kp+p-1}{j} \neq 0 \mod p$ for $0 \leq j \leq p-1$, and $\left(i^j\right)_{0 \leq i,j \leq p-1}$ is a Vandermonde matrix, and invertible, it follows that this is an invertible matrix. We can take α to be the l-th column of the inverse of this matrix. □

Proof of Theorem 2.3. It suffices to show that $E_{1,v} \in \langle \mathrm{Aff}_n(F_q), E \rangle$ for all $v \in \mathbb{N}^{n-1}$. We will proceed by induction to v, with respect to the standard lexicographic ordering on $\mathbb{N}^{n-1}$. So fix $v \in \mathbb{N}^{n-1}$ and let $k_2, \dots, k_n$ be such that $(k_i - 1)p \leq v_i \leq k_i p - 1$. By a conjugation with a suitable permutation we may assume that $v_2 \leq v_3 \leq \dots \leq v_n$ and $k_2 \leq \dots \leq k_n$. Now from Lemma 2.4, it follows that there exists a vector $\alpha = (\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{F}_p^p$ such that

$$(\alpha_0, \dots, \alpha_{p-1}) \begin{pmatrix} (Y+0)^{k_np-1} \\ (Y+1)^{k_np-1} \\ \vdots \\ (Y+p-1)^{k_np-1} \end{pmatrix} = Y^{((k_n-1)p+q)} + P(Y)$$

where $v_n = (k_n - 1)p + q$ and $\deg(P(Y)) \leq (k_n - 1)p - 1$.
This means that if we let $F_i = S_{1,\alpha_i} T_{n,-i} E_{1,(k_2p-1,\dots,k_np-1)} T_{n,i} S_{1,\alpha_i^{-1}}$, then $F_0 \circ \cdots \circ F_{p-1} = \left(X_1 + X_2^{k_2p-1} \cdots X_{n-1}^{k_{n-1}p-1}\left(X_n^{v_n} + P(X_n)\right), X_2, \dots, X_n\right) \in \langle \mathrm{Aff}_n(F_q), E\rangle$. Now because $\deg(P(y)) \leq (k_n - 1)p - 1$ we have by induction that

$$(X_1 + X_2^{k_2p-1} \cdots X_{n-1}^{k_{n-1}p-1} X_n^{v_n}, X_2, \dots, X_n) \in \langle \mathrm{Aff}_n(F_q), E\rangle$$

By repeating this procedure for $X_{n-1}, \dots, X_2$, we get that

$$E_{1,v} \in \langle \mathrm{Aff}_n(F_q), E\rangle$$

which proves our statement. □

3. Derksen Automorphisms as permutations.

3.1. Statement of the theorem. In this section we will prove the following weaker version of Derksen's Theorem 1.2:

Theorem 3.1. *Let $q = p^r$ and let $\mathbb{F}_q$ be the finite field with q elements, and $n \geq 3$. Then*

$$\pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) = \pi_{q^m}(\mathrm{DA}_n(\mathbb{F}_q)).$$

In regard to Conjecture 2.1, let us elaborate shortly on why it is plausible that $\mathrm{DA}_n(\mathbb{F}_q)$ is itself actually smaller than $\mathrm{TA}_n(\mathbb{F}_q)$. Let us pick $n = 3$, $q = 2$ for example. Assuming that $\mathrm{DA}_3(\mathbb{F}_2) = \mathrm{TA}_3(\mathbb{F}_2)$ implies that we can construct any map $(x + y^a z^b, y, z)$ where $a, b \in \mathbb{N}$ by taking a finite composition of affine maps and $(x+yz, y, z)$. In characteristic zero this is easy, one conjugates $(x+yz, y, z)$ by some affine maps, and then composes the results. However, if one attempts this in characteristic 2 (see the beginning of Section 2), then it is impossible to obtain $a = 1, b = 2$ or $a = 2, b = 1$ in this case (it is possible to get $(x + y^2z + yz^2, y, z)$, but isolating the terms does not work). Of course, this does not mean that it *has* to be impossible, but if it is possible, then the way to do it is very strange and (in view of results of [14] where defining relations for $\mathrm{TA}_3(k)$ $\mathrm{char}(k) = 0$ are given) very particular to characteristic p.

The rest of this section is dedicated to proving Theorem 3.1. First, we need some intermediate results. In particular, the main tool in the proof of Theorem 3.1 is the below proposition:

Proposition 3.2. *Let $\mathcal{X} = \mathbb{F}_{q^m}^n$ and $\tilde{\mathcal{X}} = \mathcal{X} \setminus \{u \in \mathbb{F}_{q^m}^n \mid u_n = 0\}$, then define the permutation $\psi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}$ by $\psi(u_1, \ldots, u_n) = (u_1 u_n^{-1}, u_2 u_n, u_3, \ldots, u_n)$. Then there exist a tame automorphism $T_m \in \mathrm{DA}_n(\mathbb{F}_q)$ such that $\pi_{q^m}(T_m)|_{\tilde{\mathcal{X}}} = \psi$.*

We were not able to avoid quite some technicalities in the proof of this theorem. Before we give the proof, we need to derive some intermediate results in the following subsections.

3.2. Tools for the odd characteristic case.

Lemma 3.3. *Let $\alpha = (\alpha_2, \ldots, \alpha_n) \in \{0, \ldots, p-1\}^{n-1}$, then $E_{1,\alpha} \in \mathrm{DA}_n(\mathbb{F}_q)$.*

Proof. It follows from Lemma 2.4, that for $l \in \{0, \ldots, p-1\}$, there exists a vector $\beta_l = (\beta_l^0, \beta_l^1, \ldots, \beta_l^{p-1}) \in \mathbb{F}_p^p$, such that

$$(\beta_l^0, \ldots, \beta_l^{p-1}) \begin{pmatrix} (Y+0)^{p-1} \\ (Y+1)^{p-1} \\ \vdots \\ (Y+p-1)^{p-1} \end{pmatrix} = Y^l.$$

In particular there exist such a vector for $l = \alpha_2$. For $0 \le t \le p-1$ define $c_t = \beta_{k_2}^t$ and let $F_{2,t} = S_{1,c_t} \circ T_{2,-t} \circ \varepsilon \circ T_{2,t} \circ S_{1,c_t^{-1}} = (X_1 + c_t(X_2 + t)^{p-1} X_3^{p-1} \cdots X_n^{p-1}, X_2, \ldots, X_n)$, where ε is as in Definition 1.3.
So

$$\begin{aligned} G_{\alpha_2} &= F_{2,0} \circ F_{2,1} \circ \cdots \circ F_{2,p-1} \\ &= (X_1 + (\textstyle\sum_{i=0}^{p-1} c_t^i (X_2 + i)^{p-1}) X_3^{p-1} \cdots X_n^{p-1}, X_2, \ldots, X_n) \\ &= (X_1 + X_2^{\alpha_2} X_3^{p-1} \cdots X_n^{p-1}, X_2, \ldots, X_n). \end{aligned}$$

Now repeating this for $l = \alpha_3$ with $T_{3,t}$ and G_{α_2} instead of ε and so on, gives us the required result. □

Proposition 3.4. *Let $\alpha \in \mathbb{N}^{n-1}$ with $\alpha_j = 0$ for some $j \in \{2, \ldots, n\}$, then $E_{i,\alpha} \in \mathrm{DA}_n(\mathbb{F}_q)$ if $i \ne j$.*

Proof. First consider $\alpha = (0, \alpha_3, \ldots, \alpha_n) \in \mathbb{N}^{n-1}$ and $E_{1,\alpha}$. If $\alpha_i \le p-1$ for all $3 \le i \le n$, then the result follows from Lemma 3.3. In particular it follows that $E_{1,(1,p-1,\ldots,p-1)} \in \mathrm{DA}_n(\mathbb{F}_q)$.

Now remark that if $\gamma = (1, \gamma_3, \dots, \gamma_n) \in \mathbb{N}^{n-1}$ and $\beta = (0, \beta_3, \dots, \beta_n) \in \mathbb{N}^{n-1}$, then

$$[E_{1,\gamma}, E_{2,\beta}] = E_{1,(0,\gamma_3+\beta_3,\dots,\gamma_n+\beta_n)}.$$

This can be used to construct $E_{1,\alpha}$ for any α by induction. The general case now follows from Proposition 3.4 and the fact that $R_{2,i} \in \mathrm{DA}_n(\mathbb{F}_q)$. □

3.3. Tools for the characteristic 2 case. The above lemma and proposition will be enough to tackle the characteristic $\neq 2$ case. However, the characteristic 2 case proof of Proposition 3.2 unfortunately requires special (technical) attention in the following two lemmas:

Lemma 3.5. *Let* $\mathrm{char}(\mathbb{F}_q) = 2$ *and let* $A, F, G, H, B_m, k_m, h_m$ *be as in the proof of Proposition* 3.2. *Then*

$$B_m = \quad (X_1(X_n^{k_m} + h_m) + X_2X_n^{k_m-1}, X_1X_n^{k_m-1} + X_2(h_m), X_3, \dots, X_n).$$

Proof. One can verify by an elementary computation that $B_1 = (AH)^4 = (X_1+X_1X_n^2+X_2X_n, X_1X_n+X_2, X_3, \dots, X_n)$. Now notice that $k_{m+1} = 2^{2(m+1)-1} = 2^{2m-1+2} = 2^2 * 2^{2m-1} = 4k_m$, so $B_{m+1} = B_m^4$. Write $B_m = (\tilde{B}_m, X_3, \dots, X_n)$, where $\tilde{B}_m = (X_1(X_1^{k_m} + h_m) + X_2X_n^{k_m-1}, X_1X_n^{k_m-1} + X_2h_m)$ and notice that $B_{m+1} = (\tilde{B}_{m+1}, X_3, \dots, X_n) = (\tilde{B}_m^4, X_3, \dots, X_n) = B_m^4$. So we have to verify that $\tilde{B}_m^4$ equals $\tilde{B}_{m+1}$:

$$\tilde{B_m}^4 = \begin{pmatrix} X_n^{k_m} + h_m & X_n^{k_m-1} \\ X_n^{k_m-1} & h_m \end{pmatrix}^4 \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

$$= \begin{pmatrix} X_n^{k_{m+1}} + h_m^4 + X_n^{k_{m+1}-2} + X_n^{k_{m+1}-4} & X_n^{k_{m+1}-1} \\ X_n^{k_{m+1}-1} & h_m^4 + X_n^{k_{m+1}-2} + X_n^{k_{m+1}-4} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

We leave it to the reader to verify that $h_m^4 + X_n^{k_{m+1}-2} + X_n^{k_{m+1}-4} = h_{m+1}$. □

Lemma 3.6. *Let* $q = 2^m$, *for some* $m \geq 1$, *let* $u \in \mathbb{F}_q^*$ *and let* $h_m(X) = \sum_{j=1}^{2m-1} X^{2^{2m-1}-2^j}$. *Then the following statements are true:*

i) $u^{2^{2m}} = u$;

ii) $h_m(u) = u^{2^{2m-1}-1}$.

Proof. Define $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*$ as $\varphi(u) = u^2$, the Frobenius automorphism. First of all notice that $\varphi^m(u) = u^{2^m} = u$. Now i) readily follows: $u^{2^{2m}} = \varphi^{2m}(u) = \varphi^m(\varphi^m(u)) = \varphi^m(u) = u$. For ii), define $v = u^{-1}$ and note that $u^{2^{2m}-1} = 1$, then we have that

$$\begin{aligned}
h_m(u) &= \sum_{j=1}^{2m-1} u^{2^{2m-1}-2^j} \\
&= \sum_{j=1}^{2m-1} u^{2^{2m-1}} u^{-2^j} \\
&= u^{2^{2m-1}} \sum_{j=1}^{2m-1} v^{2^j} \\
&= u^{2^{2m-1}} \sum_{j=1}^{2m-1} v^{2^j} + 2u^{2^{2m-1}} v^{2^{2m}} \\
&= u^{2^{2m-1}} \sum_{j=1}^{2m} v^{2^j} + u^{2^{2m-1}} v^{2^{2m}} \\
&= u^{2^{2m-1}} \sum_{j=1}^{2m} \varphi^j(v) + u^{2^{2m-1}} v \\
&= u^{2^{2m-1}} \left(\sum_{j=1}^{m} \varphi^j(v) + \textstyle\sum_{i=1}^{m} \varphi^{m+i}(v) \right) + u^{2^{2m-1}} u^{-1} \\
&= u^{2^{2m-1}} \left(\sum_{j=1}^{m} \varphi^j(v) + \textstyle\sum_{i=1}^{m} \varphi^{i}(\varphi^m(v)) \right) + u^{2^{2m-1}-1} \\
&= u^{2^{2m-1}} \left(\sum_{j=1}^{m} \varphi^j(v) + \textstyle\sum_{i=1}^{m} \varphi^{i}(v) \right) + u^{2^{2m-1}-1} \\
&= u^{2^{2m-1}} \left(2 \sum_{j=1}^{m} \varphi^j(v) \right) + u^{2^{2m-1}-1} \\
&= u^{2^{2m-1}-1}
\end{aligned}$$

□

3.4. Proof of the proposition.

Proof of Proposition 3.2. First we need some elements from $\mathrm{Aff}_n(\mathbb{F}_q)$, define $G = E_{1,(1,0,\ldots,0)}$ and $H = R_{1,2}$. There are two cases

- $\mathrm{char}(\mathbb{F}_q) = 2$, or
- $\mathrm{char}(\mathbb{F}_q) \neq 2$.

First the easier case where $\mathrm{char}(\mathbb{F}_q) \neq 2$. It follows that for every $m \geq 1$ we can define $A_m = E_{1,(1,0,\ldots,0,q^m-2)} = (X_1 + X_2 X_n^{q^m-2}, X_2, \ldots, X_n)$, $B = E_{1,(1,0,\ldots,0)} \circ S_{1,-1} \circ E_{1,(1,0\ldots,0,1)} \circ S_{1,-1} = (X_1 + X_2 - X_2 X_n, X_2, \ldots X_n)$, and $C_m = E_{1,(1,0,\ldots,0)} \circ S_{1,-1} \circ E_{1,(1,0,\ldots,0,q^m-2)} \circ S_{1,-1} = (X_1 + X_2 - X_2 X_n^{q^m-2}, X_2, \ldots, X_n)$. Note that we need $-1(\neq 0,1) \in \mathbb{F}_q$, which is the reason why this will not work for $\mathrm{char}(\mathbb{F}_q) = 2$.

From Proposition 3.4 it follows that $A_m, B, C_m \in \mathrm{DA}_n(\mathbb{F}_q)$. So it follows that $T_m = A_m H B H G^{-1} H C_m H \in \mathrm{DA}_n(\mathbb{F}_q)$. One verifies that $T_m = (2X_1 X_n^{q^m-2} - X_1 X_n^{2q^m-3} + X_2 X_n^{q^m-1} - X_2, X_1 - X_1 X_n^{q^m-1} + X_2 X_n, X_3, \ldots, X_n)$. Now for $t \in \mathbb{F}_{q^m}^*$ Fermat's little theorem states that $t^{q^m-1} = 1$, so it follows that for $u \in \tilde{X}$ we have that $T_m(u) = (u_1 u_n^{-1}, u_2 u_n, u_3, \ldots, u_n)$, which shows that $\pi_{q^m}(T_m)_{|\tilde{\mathcal{X}}} = \psi$.

If $\mathrm{char}(\mathbb{F}_q) = 2$, then let $A = E_{1,(1,0,\ldots,0,1)} = (X_1 + X_2 X_n, X_2, \ldots, X_n) \in \mathrm{DA}_n(\mathbb{F}_q)$. Define $F = HG$ and $B_m = (AH)^{k_m}$, where $k_m = 2^{2m-1}$. We claim that $T_m = (FB_mF)^2$ satisfies all our requirements.

Write $h_m = \sum_{j=1}^{2m-1} X_n^{k_m - 2^j}$. From Lemma 3.5 we have that

$$B_m = (X_1(X_n^{k_m} + h_m) + X_2 X_n^{k_m-1}, X_1 X_n^{k_m-1} + X_2(h_m), X_3, \ldots, X_n).$$

Now write $\tilde{F} = (X_2, X_1 + X_2)$, so $F = (\tilde{F}, X_3, \ldots, X_n)$ and $FB_mF = (\tilde{F}\tilde{B}_m\tilde{F}, X_3, \ldots, X_n)$.

$$\begin{aligned}\tilde{F}\tilde{B}_m\tilde{F} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_n^{k_m} + h_m & X_n^{k_m-1} \\ X_n^{k_m-1} & h_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \\ &= \begin{pmatrix} h_m & X_n^{k_m-1} + h_m \\ X_n^{k_m-1} + h_m & X_n^{k_m} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix},\end{aligned}$$

hence $T_m = (FB_mF)^2 = ((\tilde{F}\tilde{B}_m\tilde{F})^2, X_3, \ldots, X_n)$. So

$$(\tilde{F}\tilde{B}_m\tilde{F})^2 = \begin{pmatrix} h_m & X_n^{k_m-1} + h_m \\ X_n^{k_m-1} + h_m & X_n^{k_m} \end{pmatrix}^2 \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$$

$$= \begin{pmatrix} X_n^{2(k_m-1)} & X_n^{2k_m-1} + (X_n^{k_m} + X_n^{k_m-1} + h_m)h_m \\ X_n^{2k_m-1} + (X_n^{k_m} + X_n^{k_m-1} + h_m)h_m & X_n^{2k_m} + X_n^{2(k_m-1)} + h_m^2 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix},$$

where we define the latter matrix as M, so we get as a result

$$M \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}.$$

All we still have to show now is that $\pi_{2^m}(T_m)|_{\tilde{\mathcal{X}}} = \psi$. For this we have to show that for $u \in \mathbb{F}_{2^m}^*$, we have that

1) $u^{2(k_m-1)} = u^{-1}$;

2) $u^{2k_m-1} + (u^{k_m} + u^{k_m-1} + h_m(u))h_m(u) = 0$;

3) $u^{2k_m} + u^{2(k_m-1)} + h_m^2(u) = u$.

1) follows from Lemma 3.6 i). From Lemma 3.6 ii) it follows that $h_m(u) = u^{2^{2m-1}-1}$, so 2) becomes

$$\begin{aligned}
& u^{2k_m-1} + (u^{k_m} + u^{k_m-1} + h_m(u))h_m(u) \\
= \; & u^{2^{2m}-1} + (u^{2^{2m-1}} + u^{2^{2m-1}-1} + u^{2^{2m-1}-1})u^{2^{2m-1}-1} \\
= \; & 1 + u^{2^{2m-1}}u^{2^{2m-1}-1} \\
= \; & 1 + u^{2^{2m}-1} \\
= \; & 1 + 1 = 0.
\end{aligned}$$

Finally 3)

$$\begin{aligned}
& u^{2k_m} + u^{2(k_m-1)} + h_m^2(u) \\
= \; & u^{2^{2m}} + u^{2^{2m}-2} + u^{2(2^{2m-1}-1)} \\
= \; & u + u^{-1} + u^{-1} \\
= \; & u.
\end{aligned}$$

This proves that for the above matrix M, we have

$$\pi_{2^m}(M)|_{\tilde{X}} = \begin{pmatrix} X_n^{-1} & 0 \\ 0 & X_n \end{pmatrix}|_{\tilde{X}}$$

hence $\pi_{q^m}(T_m)|_{\tilde{\mathcal{X}}} = \psi$. □

3.5. More tools and proof of Theorem 3.1. Now that we proved Proposition 3.2, we have a map T_m "almost mimicking" $(u_1u_n^{-1}, u_2u_n, u_3, \ldots, u_n)$, namely perfectly mimicking it on $u_n \neq 0$ (which is $\tilde{\mathcal{X}}$) but stating nothing on what it does on $u_n = 0$.

Proposition 3.7. *Let q, n, $m, \mathcal{X}, \tilde{\mathcal{X}}, \psi$ and T_m as in Proposition 3.2. Let $\alpha = (\alpha_2, \ldots, \alpha_n) \in \mathbb{N}^{n-1}$. Now $\pi_{q^m}(T_m^{-1} \circ E_{1,\alpha} \circ T_m) = \pi_{q^m}(E_{1,\beta})$, where $\beta = (\alpha_2, \ldots, \alpha_{n-1}, \alpha_n + \alpha_2 + 1)$.*

Proof. For $u \in \mathcal{X}\backslash\tilde{\mathcal{X}}$, $\pi_{q^m}(E_{1,\alpha}) = \pi_{q^m}((x_1, \ldots, x_n)) = \pi_{q^m}(E_{1,\beta})$, so the statement is clearly true in $\mathcal{X}\backslash\tilde{\mathcal{X}}$. Now if we restrict ourselves to $\tilde{\mathcal{X}}$ we have that

$$\begin{aligned}
& \pi_{q^m}(T_m^{-1} \circ E_{1,\alpha} \circ T_m) \\
= \; & \pi_{q^m}(T_m^{-1})\pi_{q^m}(E_{1,\alpha})\pi_{q^m}(T) \\
= \; & \psi^{-1}\pi_{q^m}(E_{1,\alpha})\psi \\
= \; & \pi_{q^m}((X_1X_n, X_2X_n^{-1}, X_3, \ldots, X_n))\pi_{q^m}(E_{1,\alpha})\pi_{q^m}((X_1X_n^{-1}, X_2X_n, X_3, \ldots, X_n)) \\
= \; & \pi_{q^m}((X_1X_n, X_2X_n^{-1}, X_3, \ldots, X_n)) \cdot \\
& \quad \pi_{q^m}((X_1X_n^{-1} + X_2^{\alpha_2} \cdots X_{n-1}^{\alpha_{n-1}} X_n^{\alpha_2+\alpha_n}, X_2X_n, X_3, \ldots, X_n)) \\
= \; & \pi_{q^m}(X_1 + X_2^{\alpha_2} \cdots X_{n-1}^{\alpha_{n-1}} X_n^{\alpha_2+\alpha_n+1}, X_2, X_3, \ldots, X_n) \\
= \; & \pi_{q^m}(E_{1,\beta}).
\end{aligned}$$

□

Lemma 3.8. *Let $a, b, m \in \mathbb{Z}$. If $\gcd(a, b, m) = d$, then there exists $t \in \mathbb{Z}$ such that $\gcd(a + tb, m) = d$.*

Proof. First assume $d = 1$. Define

$$t = \prod_{\substack{p \ prime \\ p \mid m \\ p \nmid a}} p,$$

then we show that $\gcd(a+tb, m) = 1$: Let p be a prime such that $p|\gcd(a+tb, m)$. This means that $p|m$ and $p|a + tb$. Now suppose $p|a$, then $p|tb$ and by definition $p \nmid t$ so $p|b$, but then $p|\gcd(a, b, m) = 1$, contradiction. Now suppose $p \nmid a$, then by definition $p|t$, so p does divide a. Contradiction.
So there does not exist a prime p, that divides $\gcd(a + tb, m)$, which hence must be one.

Now the general case, $\gcd(a, b, m) = d$. Define $a' = a/d$, $b' = b/d$ and $m' = m/d$, then $\gcd(a', b', m') = 1$. By the previous argument, there exists an t such that $\gcd(a' + tb', m') = 1$. Thus $\gcd(a + tb, m) = d$. □

Lemma 3.9. *Let $a, m \in \mathbb{Z}$, with $\gcd(a, m) = d$, then $\bar{a}$ is a generator of the additive subgroup $d\mathbb{Z}/m\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. According to the Extended Euclidean Algorithm, there exist $u, v \in \mathbb{Z}$ such that $ua + vm = d$, so $\bar{u}\bar{a} = \bar{d}$. Thus $\bar{u}\bar{a}$ is a generator of $d\mathbb{Z}/m\mathbb{Z}$, hence so is $\bar{a}$. □

Now we will first prove a special case of Theorem 3.1, namely the three dimensional one, before we give the proof of the general case. The proof of this proposition is perhaps the most technical part of this article.

Proposition 3.10. *Let $q = p^r$ and let $\mathbb{F}_q$ be the finite field with q elements, $m \in \mathbb{N}^*$. Then*

$$\pi_{q^m}(\mathrm{TA}_3(\mathbb{F}_q)) = \pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q)).$$

Proof. It suffices to prove that $\pi_{q^m}((X + Y^a Z^b, Y, Z)) \in \pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$ for $(a, b) \in (\mathbb{Z}/(q^m - 1)\mathbb{Z})^2$. Let $\mathcal{X} = \mathbb{F}_{q^m}^3$ and $\tilde{\mathcal{X}} = X \setminus \{u \in \mathbb{F}_q^3 \mid u_3 = 0\}$, then define the permutation $\psi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}$ by $\psi(u_1, u_2, u_3) = (u_1 u_3^{-1}, u_2 u_3, u_3)$. Now from Proposition 3.2 it follows that there exists an automorphism $T_m \in DA_3(\mathbb{F}_q)$, such that $\pi_{q^m}(T_m)|_{\tilde{\mathcal{X}}} = \psi$.

Suppose $\pi_{q^m}(E_{1,(\alpha,\beta)}) \in \pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$, then

$$\pi_{q^m}(T_m^{-1} E_{1,(\alpha,\beta)} T_m) = \pi_{q^m}(E_{1,(\alpha,\beta+\alpha+1)}), \tag{1}$$

$$\pi_{q^m}(R_{2,3} E_{1,(\alpha,\beta)} R_{2,3}) = \pi_{q^m}(E_{1,(\beta,\alpha)}). \tag{2}$$

Equation (1) follows from Proposition 3.7.
Since $E_{1,(p-1,p-1)} \in \pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$ by definition, we need to prove that, starting with $E_{1,(p-1,p-1)}$ and applying (1) and (2), we can get $\pi_{q^m}(E_{1,(\alpha,\beta)}) \in \pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$, for any pair (α, β). The equations (1) and (2) translate into operations

$$\begin{aligned} \varrho(\alpha, \beta) &= (\alpha, \beta + \alpha + 1) \\ \tau(\alpha, \beta) &= (\beta, \alpha) \end{aligned}$$

on the space $(\mathbb{Z}/(q^m - 1)\mathbb{Z})^2$, where we can compute mod $(q^m - 1)\mathbb{Z}$ as $\alpha^{q^m} = \alpha$ for any $\alpha \in \mathbb{F}_{q^m}$. So rephrasing the quoestion: Starting with $(\overline{p-1}, \overline{p-1}) \in (\mathbb{Z}/(q^m - 1)\mathbb{Z})^2)$ and iterating these two operation ϱ and τ, do we reach all of $(\mathbb{Z}/(q^m - 1)\mathbb{Z})^2$?

Unfortunately the answer is no. But we can reach almost every point and thereafter we show that we can mimic the maps we can not reach this way as well: Suppose $\gcd(a + 1, b + 1, q^m - 1) = 1$, then from Lemma 3.8 it follows that there exists a t such that $\gcd(a + 1 + t(b + 1), q^m - 1) = 1$. From Lemma 3.9 and the fact that $\gcd(p, q^m - 1) = 1$ it follows that p is a generator of the additive group $\mathbb{Z}/(q^m - 1)\mathbb{Z}$ so there exists a k_1 such that $p - 1 + k_1 p = a + t(b + 1) \bmod q^m - 1$. So from $\varrho^{k_1}((p-1, p-1)) = (p-1, a+t(b+1))$ and since $\gcd(a+1+t(b+1), q^m-1) = 1$, it follows that there exists a k_2 such that $p - 1 + k_2(a + 1 + t(b + 1)) = b$, thus $\varrho^{k_2} \tau \varrho^{k_1}((p-1, p-1)) = (a+t(b+1), b)$ So $\tau \varrho^{q^m - 1 - t} \tau \varrho^{k_2} \tau \varrho^{k_1}((p-1, p-1)) = (a, b)$.

Now if $\gcd(a + 1, b + 1, q^m - 1) = d$, we need a little more work. From Lemma 3.8 it follows that there exists a t such that $\gcd(a+1+t(b+1), q^m - 1) = d$.

Now suppose we start with $(d-1,d-1)$, then we can write $a+t(b+1)=k_1d+(d-1)$ so $\varrho^{k_1}((d-1,d-1))=(d-1,a+t(b+1))$. Since $\gcd(a+1+t(b+1),q^m-1)=d$ it follows from Lemma 3.9 that $a+1+t(b+1)$ is a generator for the additive group $d\mathbb{Z}/(q^m-1)\mathbb{Z}$. Since $d|b+1$ it follows that there exists a k_2 such that $b=d-1+k_2(a+1+t(b+1))$, so $\varrho^{k_2}\tau\varrho^{k_1}((d-1,d-1))=(a+t(b+1),b)$. So $\tau\varrho^{q^m-1-t}\tau\varrho^{k_2}\tau\varrho^{k_1}((d-1,d-1))=(a,b)$.

It remains to prove that we can reach $(d-1,d-1)$. Unfortunately this can not be done just using ϱ, τ. So we have to show that $\pi_{q^m}(E_{1,(d-1,d-1)})\in\pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$, where $d|q^m-1$. Now from the previous part it follows that $\pi_{q^m}(E_{1,(d-1,d)})=\pi_{q^m}((X+Y^{d-1}Z^d,Y,Z))\in\pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$, since $\gcd(d,d+1,q^m-1)=1$. Now let d_1 be the smallest divisor of q^m-1, then

$$\begin{aligned}&\pi_{q^m}((X+(p-1)Y^{d_1-1}Z^{d_1},Y,Z))\pi_{q^m}((X,Y,Z+p-1))\\&\qquad\pi_{q^m}((X+Y^{d_1-1}Z^{d_1},Y,Z))\pi_{q^m}((X,Y,Z+1))\\&\quad=\pi_{q^m}((X+(p-1)Y^{d_1-1}Z^{d_1}+Y^{d_1-1}(Z+1)^{d_1},Y,Z))\\&\qquad=\pi_{q^m}((X+Y^{d_1-1}(\binom{d_1}{1}Z^{d_1-1}+P(Z)),Y,Z)),\end{aligned}$$

with $\deg(P(Z))\leq d_1-2$. Since d_1 is the smallest divisor of q^m-1, it follows that p does not divide d_1 and that $\gcd(d_1,d_1-i,q^m-1)=1$ for $1\leq i\leq d_1$. From which it follows that $\pi_{q^m}((X+Y^{d_1-1}P(Z),Y,Z))\in\pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$. Thus

$$\begin{aligned}&\pi_{q^m}\Big(S_{1,d_1}\big(X+Y^{d_1-1}P(Z),Y,Z\big)\big(X+Y^{d_1-1}(\tbinom{d_1}{1}Z^{d_1-1}+P(Z)),Y,Z\big)\cdot S_{1,d_1^{-1}}\Big)\\&=\ \pi_{q^m}((X+Y^{d_1-1}Z^{d_1-1},Y,Z)).\end{aligned}$$

Now let d_2 be the second smallest divisor, we can repeat the procedure described above and since we have already made all smaller degrees we have that $\pi_{q^m}((X+Y^{d_2-1}Z^{d_2-1},Y,Z))\in\pi_{q^m}(\mathrm{DA}_3(\mathbb{F}_q))$. Now by induction we are done. □

Now we are ready to prove our main result, Theorem 3.1.

Proof. First of all note that it suffices to prove that $\pi_{q^m}(E_{1,\alpha})\in\pi_{q^m}(\mathrm{DA}_n(\mathbb{F}_q))$ for all $\alpha\in\{0,\dots,q^m-1\}^{n-1}$.

Let $\mathcal{X}=\mathbb{F}_{q^m}^n$ and $\mathcal{X}_i=\mathcal{X}\setminus\{u\in\mathbb{F}_q^n\mid u_i=0\}$, then define the permutation $\psi_i:\mathcal{X}_i\to\mathcal{X}_i$ by $\psi_i(u_1,\dots,u_n)=(u_1u_i^{-1},u_2u_i,u_3,\dots,u_n)$. Now Proposition 3.2 states that there exists a map $T_m\in\mathrm{DA}_n(\mathbb{F}_q)$, such that $\pi_{q^m}(T_m)|_{\mathcal{X}_n}=\psi_n$. Now define $T_{m,i}=R_{i,n}T_mR_{i,n}$. Since π_{q^m} is a group homomorphism, it follows that $\pi_{q^m}(T_{m,i})|_{\mathcal{X}_i}=\pi_{q^m}(R_{i,n}T_mR_{i,n})|_{\mathcal{X}_i}=\pi_{q^m}(R_{i,n})|_{\mathcal{X}_i}\pi_{q^m}(T_m)|_{\mathcal{X}_i}\pi_{q^m}(R_{i,n})|_{\mathcal{X}_i}=\psi_i$. Now let $\alpha=(\alpha_2,\dots,\alpha_n)\in\{0,\dots,q^m-1\}^{n-1}$, for $i=4,\dots,n$ write $\alpha_i=pk_i+r_i$, with $r_i\in\{0\dots,p-1\}$. Then Lemma 3.3 states that $\pi_{q^m}(E_{1,(p-1,p-1,r_4,\dots,r_n)})\in$

$\pi_{q^m}(\mathrm{DA}_n(\mathbb{F}_q))$. Now from Proposition 3.7 it follows that

$$\pi_{q^m}(T_{m,i}^{-1}E_{1,(p-1,p-1,r_4,\ldots,r_n)}T_{m,i}) = \pi_{q^m}(E_{1,(p-1,p-1,r_4,\ldots,r_i+p,\ldots,r_n)}).$$

So $\pi_{q^m}(T_{m,4}^{-k_4}\cdots T_{m,n}^{-k_n}E_{1,(p-1,p-1,r_4,\ldots,r_n)}T_{m,n}^{k_n}\cdots T_{m,4}^{k_4}) = \pi_{q^m}(E_{1,(p-1,p-1,\alpha_4,\ldots,\alpha_n)})$ $\in \pi_{q^m}(\mathrm{DA}_n(\mathbb{F}_q)$. To prove the final step one can copy the proof of Proposition 3.10, and extend all automorphisms with $n-3$ variables. □

4. Tamizables versus Linearizables. In this section we will compare two subgroups of $\mathrm{GA}_n(k)$ (k a field), namely the group generated by the so called linearizables ($\mathrm{GLIN}_n(k)$) and the group generated by the tamizables ($\mathrm{GTAM}_n(k)$), both introduced in [11]. An automorphism $F \in \mathrm{GA}_n(k)$ is called linearizable if it is the conjugate of a linear automorphism, so if there exist an $L \in \mathrm{GL}_n(k)$ and a $G \in \mathrm{GA}(k)$, such that $F = G^{-1} \circ L \circ G$. Similarly, an automorphism is called tamizable if it is the conjugate of a tame automorphism.

Definition 4.1. *Let G be a group, and H a subgroup of G. We define $\mathcal{N}(H,G)$ to be the smallest normal subgroup of G that contains H, i.e.*

$$\mathcal{N}(H,G) = \langle g^{-1}hg \mid h \in H, g \in G\rangle.$$

Furthermore let $g,h \in G$ then we write the commutator as $[g,h] := g^{-1}h^{-1}gh$. Now we can define the following subgroups of $\mathrm{GA}_n(k)$:

$$\begin{aligned}\mathrm{GLIN}_n(k) &:= \mathcal{N}(\mathrm{GL}_n(k), \mathrm{GA}_n(k))\\ \mathrm{GTAM}_n(k) &:= \mathcal{N}(\mathrm{TA}_n(k), \mathrm{GA}_n(k))\\ \mathrm{TLIN}_n(k) &:= \mathcal{N}(\mathrm{GL}_n(k), \mathrm{TA}_n(k)).\end{aligned}$$

(Note that some "TTAM" would equal $\mathrm{TA}_n(k)$.) Then the following is obviously true:

$$\begin{tikzcd}
 & \mathrm{TA}_n(k) \arrow[r, phantom, "\subseteq"] & \mathrm{GTAM}_n(k) \arrow[dr, phantom, "\subsetneq" sloped] & \\
 & & & \mathrm{GA}_n(k) \\
\mathrm{GL}_n(k) \arrow[r, phantom, "\subseteq"] & \mathrm{TLIN}_n(k) \arrow[r, phantom, "\subseteq"] \arrow[uu, phantom, "\subseteq" sloped] & \mathrm{GLIN}_n(k) \arrow[uu, phantom, "\subseteq" sloped] \arrow[ur, phantom, "\subsetneq" sloped] &
\end{tikzcd}$$

One of the motivations of this section is in attacking the so-called *linearization problem*, which is the conjecture that if $F^s = I$, then F is linearizable. In particular, $F \in \mathrm{GLIN}_n(k)$. Note that in characteristic p one actually has non-linearizable automorphisms like $F := (X+Y^2, Y)$, for which $F^p = I$ and indeed

F is non-linearizable. (Or many an automorphism of an additive group action, for that matter.) This indicates that the linearization problem over characteristic p should be reformulated:

Linearization problem in characteristic p: let $F \in \mathrm{GA}_n(k)$ where k is a field of characteristic $p > 0$. Assume that $F^s = I$ where $\gcd(p, s) = 1$. Then F is linearizable.

Note Asanuma's result [1] stating that the linearization problem for the multiplicative group in positive characteristic is false. This may give indication that the Linearization Problem as stated above might still be false.

As observed above, an automorphism $F^s = I$, $\gcd(p, s) = 1$ for which $F \notin \mathrm{GLIN}_n(k)$, must be a counterexample to the above problem. However, in this section we show that such an approach cannot work except if $k = \mathbb{F}_2$: if $k \neq \mathbb{F}_2$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$, the latter being a good candidate of equalling $\mathrm{GA}_n(k)$. The main result of this section is the following:

Theorem 4.2. *If $n \geq 2$ and $k \neq \mathbb{F}_2$, then $\mathrm{TLIN}_n(k) = \mathrm{TA}_n(k)$, and hence $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. In case $k = \mathbb{F}_2$, then $\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$, and hence $\mathrm{TLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{TA}_n(\mathbb{F}_2)$.*

The proof of the theorem can be found near the end of this section. We first need to prove some lemmas:

Lemma 4.3. *If $k \neq \mathbb{F}_2$, then $\mathrm{TA}_n(k) = \mathrm{TLIN}_n(k)$.*

Proof. Only the inclusion "$\subseteq$" needs to be proven. Since $\mathrm{GL}_n(k) < \mathrm{TLIN}_n(k)$ it suffices to prove that $E_{1,\alpha} \in \mathrm{TLIN}_n(k)$ for all $\alpha \in \mathbb{N}^{n-1}$. Choose $c \neq 0, 1$ (which is possible since $k \neq \mathbb{F}_2$) and $d := (1-c)^{-1}$. Then an elementary computation shows that

$$S_{1,c}\left(S_{1,d}E_{1,\alpha}S_{1,d^{-1}}\right)^{-1} S_{1,c}^{-1}\left(S_{1,d}E_{1,\alpha}S_{1,d^{-1}}\right) \quad = \quad E_{1,\alpha}$$

Since $S_{1,c}$ and $\left(S_{1,d}E_{1,\alpha}S_{1,d^{-1}}\right)^{-1} S_{1,c}^{-1}\left(S_{1,d}E_{1,\alpha}S_{1,d^{-1}}\right)$ are in $\mathrm{TLIN}_n(k)$ by definition, it follows that $E_{1,\alpha} \in \mathrm{TLIN}_n(k)$. □

Let $\mathcal{A}_{2^n}$ be the alternating subgroup of the symmetric group $\mathcal{S}_{2^n} \cong \mathrm{Perm}(\mathbb{F}_2^n)$.

Lemma 4.4. $\pi_2(\mathrm{GLIN}_n(\mathbb{F}_2)) \subseteq \mathcal{A}_{2^n}$ *if $n \geq 2$.*

Proof. First remark that if $\pi_2(h) \in \mathcal{A}_{2^n}$, then also $\pi_2(g^{-1}hg) \in \mathcal{A}_{2^n}$. So all we have to do is to show that $\pi_2(\mathrm{GL}_n(\mathbb{F}_2)) \subseteq \mathcal{A}_{2^n}$. It suffices to prove that the following generators of $\mathrm{GL}_n(\mathbb{F}_2)$ are all even:

$$\begin{aligned} F_1 &:= (x_1 + x_2, x_3, \ldots, x_n) \\ F_i &:= R_{1,i} = (x_i, x_2, \ldots, x_{i-1}, x_1, x_{i+1}, \ldots, x_n) \ \text{ for } \ 2 \leq i \leq n. \end{aligned}$$

The set of fixed points for each map F_i can be easily counted: each one has 2^{n-1} fixed points. Since each map is an involution, the other 2^{n-1} points are interchanged by transpositions, so each map has 2^{n-2} transpositions, which is an even number since $n \geq 3$. This means that the sign of the permutation is even, which proves the claim. □

Proposition 4.5. $\mathrm{GTAM}_n(\mathbb{F}_2) \neq \mathrm{GLIN}_n(\mathbb{F}_2)$ *if* $n \geq 2$.

Proof. Case $n \geq 3$: Theorem 2.3 in [9] states that $\pi_2(\mathrm{TA}_n(\mathbb{F}_2)) = \mathrm{Perm}(\mathbb{F}_2^n)$, so $\pi_2(\mathrm{GTAM}_n(\mathbb{F}_2)) = \mathrm{Perm}(\mathbb{F}_2^n)$. Furthermore we have just shown in Lemma 4.4 that $\pi_2(\mathrm{GLIN}_n(\mathbb{F}_2)) \subseteq \mathcal{A}_{2^n}$, but $\mathcal{A}_{2^n} \neq \mathrm{Perm}(\mathbb{F}_2^n)$, so $\mathrm{GTAM}_n(\mathbb{F}_2) \neq \mathrm{GLIN}_n(\mathbb{F}_2)$.

Case $n = 2$: It follows from Jung–van der Kulk theorem, that $\mathrm{TA}_2(\mathbb{F}_2) = \mathrm{GTAM}_2(\mathbb{F}_2) = \mathrm{GA}_2(\mathbb{F}_2)$. A not too difficult computation (we used the computer algebra program MAGMA, for details we refer to [15, Chapter 5]) one can show that $[\pi_4(\mathrm{GLIN}_2(\mathbb{F}_2)) : \pi_4(\mathrm{GA}_2(\mathbb{F}_2))] = 2$, meaning that the groups are different. (Note that $\pi_2(\mathrm{GLIN}_2(\mathbb{F}_2)) = \pi_2(\mathrm{GTAM}_2(\mathbb{F}_2))$.) □

Proof of Theorem 4.2. The theorem follows directly from Lemma 4.3 and Proposition 4.5, and the implication "If $\mathrm{TLIN}_n(k) = \mathrm{TA}_n(k)$ then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$" and its opposite formulation "$\mathrm{GLIN}_n(k) \subsetneq \mathrm{GTAM}_n(k)$ then $\mathrm{TLIN}_n(k) \subsetneq \mathrm{TA}_n(k)$". □

We can now actually use the above work to show that some maps are not linearizable using almost zero effort (where normally at least some hard work is necessary):

Example 4.6. Let $F := (x + yz, y, z) \in \mathrm{TA}_3(\mathbb{F}_2)$. Then $\pi_2(F)$ is a transposition (of $(0, 1, 1)$ and $(1, 1, 1)$), and hence is odd. Lemma 4.4 now yields that F is not linearizable.

This example has an interesting corollary, which is to our knowledge the easiest proof of this fact:

Corollary 4.7. *Let* $F := (x + yz, y, z) \in \mathrm{TA}_3(\mathbb{Z})$. *Then* F *is not linearizable in* $\mathrm{TA}_3(\mathbb{Z})$.

REFERENCES

[1] T. Asanuma. Non-linearizable algebraic k^*-actions on affine spaces. *Invent. Math.* **138**, *2* (1999), 281–306.

[2] J. Berson. Prime power polynomial maps over finite fields. `arXiv:1201.1137v1`.

[3] Y. Bodnarchuk. On generators of the tame invertible polynomial maps group. *Int. J. Algebra Comput.* **15**, *5–6* (2005), 851–867.

[4] V. Drensky, J.-T. Yu. Automorphisms of polynomial algebras and Dirichlet series. *J. Algebra* **321**, *1* (2009), 292–302.

[5] A. van den Essen. Polynomial Automorphisms and the Jacobian Conjecture, volume of Progress in Mahtematics, vol. **190**, Basel, Birkhäuser, 2000.

[6] J.-Ph. Furter, S. Maubach. Locally finite polynomial endomorphisms. *J. Pure Appl. Algebra* **211**, *2* (2007), 445–458.

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

[8] W. van der Kulk. On polynomial rings in two variables. *Nieuw Arch. Wiskd., III. Ser.* **1** (1953), 33–41.

[9] S. Maubach. The automorphism group over finite fields. *Serdica Math. J.* **27**, *4* (2001), 343–350.

[10] S. Maubach. A problem on polynomial maps over finite fields. `arXiv:0802.0630v1`.

[11] S. Maubach, P.-M. Poloni. The Nagata automorphism is shifted linearizable. *J. Algebra* **321**, *3* (2009), 879–889.

[12] I. Shestakov, U. Umirbaev. The tame and the wild automorphisms of polynomial rings in three variables. *J. Amer. Math. Soc.* **17**, *1* (2004), 197–227.

[13] I. Shestakov, U. Umirbaev. Poisson brackets and two-generated subalgebras of rings of polynomials. *J. Amer. Math. Soc.* **17**, *1* (2004), 181–196.

[14] U. Umirbaev. Defining relations of the tame automorphism group of polynomial algebras in three variable. *J. Reine Angew. Math.* **600** (2006), 203–235.

[15] R. Willems. Polynomial Automorphisms and Mathieu Spaces. Ph.D. Thesis, Radboud University Nijmegen, 2011, ISBN:9789491211584.

Stefan Maubach
Jacobs University
28759 Bremen, Germany
e-mail: `s.maubach@jacobs-university.de`

Roel Willems
Callatay and Wouters
Brussels, Belgium
e-mail: `roelwill@gmail.com`

Received January 20, 2012