COLLOQUIUM MATHEMATICUM

VOL. 146 2017 NO. 1

A NEW FORMULATION OF THE JACOBIAN CONJECTURE IN CHARACTERISTIC p

BY

STEFAN MAUBACH (Rotterdam) and ABDUL RAUF (Bremen)

Abstract. The Jacobian Conjecture uses the equation $\det \mathrm{Jac}(F) \in k^*$, which is a very short way to write down many equations putting restrictions on the coefficients of a polynomial map F. In characteristic p these equations do not suffice to (conjecturally) force a polynomial map to be invertible. We describe how to construct the conjecturally sufficient equations in characteristic p forcing a polynomial map to be invertible. This provides a formulation of the Jacobian Conjecture in characteristic p, alternative to Adjamagbo's. We strengthen this formulation by investigating some special cases and by linking it to the regular Jacobian Conjecture in characteristic zero.

1. Introduction

1.1. Notation and definitions. All rings considered are commutative with 1. We denote by $R^{[n]} = R[x_1, \ldots, x_n]$ the polynomial ring in n variables over a ring R. A *polynomial map* (or *polynomial endomorphism*) F with coefficients in a ring R is a list of polynomials $(F_1, \ldots, F_n)$ where $F_i \in R^{[n]}$. Such a polynomial map provides an endomorphism of $R^{[n]}$ as well as a map $R^n \to R^n$. Since R can be a finite field/ring, we cannot identify these viewpoints. (A polynomial map can induce the identity map $R^n \to R^n$ while not being the identity endomorphism.)

We define $\mathrm{ME}_n(R)$ as the set of polynomial endomorphisms on $R^{[n]}$. This forms a monoid with respect to composition, and the subset of invertible elements in this monoid is denoted by $\mathrm{GA}_n(R)$ and is the group of polynomial automorphisms. We define

$$\deg(F) = \max(\deg(F_1), \ldots, \deg(F_n)) \quad \text{for } F \in \mathrm{ME}_n(R).$$

The set of affine automorphisms $\mathrm{Aff}_n(R)$ is $\{F \in \mathrm{GA}_n(R) \mid \deg(F) = 1\}$. A polynomial map $F \in \mathrm{ME}_n(R)$ is *triangular* if $F_i \in R[x_i, \ldots, x_n]$. If F is a triangular automorphism and R is a domain, then F turns out to be of the form $(r_1 x_1 + f_1, \ldots, r_n x_n + f_n)$ where $r_i \in R^*$ and $f_i \in k[x_{i+1}, \ldots, x_n]$.

2010 *Mathematics Subject Classification*: Primary 14R15; Secondary 13F20.
Key words and phrases: Jacobian Conjecture, positive characteristic, ideals.
Received 5 July 2015; revised 4 March 2016.
Published online 11 July 2016.

DOI: 10.4064/cm6692-3-2016

The set of triangular automorphisms is denoted by $\mathrm{BA}_n(R)$. Both $\mathrm{BA}_n(R)$ and $\mathrm{Aff}_n(R)$ turn out to be subgroups of $\mathrm{GA}_n(R)$. We define $\mathrm{TA}_n(R) := \langle \mathrm{BA}_n(R), \mathrm{Aff}_n(R) \rangle$, the *tame automorphism group*.

We set $\mathrm{SA}_n(R) = \{F \in \mathrm{GA}_n(R) \mid \det \mathrm{Jac}(F) = 1\}$. Similarly, $\mathrm{STA}_n(R) = \mathrm{SA}_n(R) \cap \mathrm{TA}_n(R)$ etc.

For each of these sets, we set $\mathrm{ME}_n^d(R) = \{F \in \mathrm{ME}_n(R) \mid \deg(F) \leq d\}$, $\mathrm{GA}^d(R) = \mathrm{GA}_n(R) \cap \mathrm{ME}_n^d(R)$ etc.

We use the notation $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ if $\alpha \in \mathbb{N}^n$.

1.2. The Jacobian Conjecture. The Jacobian Conjecture is a quite notorious conjecture in affine algebraic geometry. One formulation is:

JC(R, n): If $F \in \mathrm{ME}_n(R)$ where R is a domain of characteristic zero, then $\det \mathrm{Jac}(F) \in R^*$ implies that $F \in \mathrm{GA}_n(R)$.

For many details we can refer to the book [2]. The conjecture is widely open even in the case $n = 2$ (and trivial in dimension 1). Proving JC(R, n) for any R of characteristic zero yields JC(R, n) for all domains R of characteristic zero.

Naively translating the Jacobian Conjecture into characteristic p yields counterexamples, already in dimension 1: the map $x - x^p$ is not injective but has $\det \mathrm{Jac}(x - x^p) = 1$. Therefore, Adjamagbo [1] stated a possible version of the Jacobian Conjecture for fields k with $\mathrm{char}(k) = p$:

AJC(n, p): Let $F = (F_1, \ldots, F_n)$ where $F_i \in k[x_1, \ldots, x_n]$ and k is a field of characteristic p. Assume that $\det \mathrm{Jac}(F) \in k^*$ and additionally that p does not divide $[k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)]$. Then F has a polynomial inverse.

The "$\mathrm{char}(k) \nmid [k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)]$" requirement seems to exclude all pathological counterexamples, but adds another difficult requirement to the (deceptively simple looking but) difficult equation $\det \mathrm{Jac}(F) \in k^*$. Adjamagbo showed that knowing AJC(n, p) for all p implies JC(n, k) for all k.

We approach the JC in characteristic p from a different perspective. Let us write down a generic polynomial automorphism of degree 2, having affine part identity:

$$F = (x + a_1 x^2 + a_2 xy + a_3 y^2, y + b_1 x^2 + b_2 xy + b_3 y^2).$$

Then, in characteristic zero, the equation $1 = \det \mathrm{Jac}(F)$ yields several equations on the coefficients:

$$\begin{aligned}1 = \det \mathrm{Jac}(F) = 1 + {} & \\ & (2a_1 + b_2)x + \\ & (a_2 + 2b_3)y + \\ & (2a_1b_2 + 2a_2b_1)x^2 + \\ & (2b_2a_2 + 4a_1b_3 + 4a_3b_1)xy + \\ & (2a_2b_3 + 2a_3b_2)y^2.\end{aligned}$$

Apparently, the equations $2a_1 + b_2 = 0$, $a_2 + 2b_3 = 0$, etc. are exactly the equations one needs to ensure that F is invertible in characteristic zero. However, in characteristic 2 the above equations are not enough (in fact, some of them completely vanish), as the example $(x + x^2, y)$ shows. Therefore, one needs extra equations in characteristic p. In fact, thinking a little deeper, we *know* that such equations must exist. (Without going into detail, the set of automorphisms of determinant Jacobian 1 is a subset of $\mathrm{ME}_n^d(k)$ which is endowed with a so-called ind-topology, and its closure can be described by equations; see [6, 7, 8] for details). We only have to *find* them. In this article we claim that we have found them (at least conjecturally). In fact, what we are doing is refining the regular Jacobian Conjecture so that it makes sense in characteristic p as well.

We make a related remark on Adjamagbo's formulation: if there exists at least one counterexample F to the Jacobian Conjecture in characteristic zero, then $[k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)] = d > 1$. It might well be that F mod p is an interesting map for any prime p. But, if $p \,|\, d$, then Adjamagbo's formulation excludes this example, while one could argue that a formulation of the JC in characteristic p should not. One could say that in this case $p \nmid [k(x_1, \ldots, x_n) : k(F_1, \ldots, F_n)]$ adds *too many* equations, or perhaps adds *wrong* equations.

2. Initial considerations. Let us consider the degree 2 example of the previous section. One of the equations is $2a_1b_2 + 2a_2b_2$. In characteristic zero, this implies the equation $a_1b_2 + a_2b_1$. Looking at it like this, it seems strange to exclude this latter equation in characteristic 2. Also, if we define the ideal

$$I = (2a_1 + b_2, a_2 + 2b_3, 2a_1b_2 + 2a_2b_1, 2b_2a_2 + 4a_1b_3 + 4a_3b_1, 2a_2b_3 + 2a_3b_2)$$

in the ring $\mathbb{Q}[a_1a_2, a_3, b_1, b_2, b_3]$, then any invertible polynomial map of degree 2 over $\mathbb{Q}$ will have coefficients which satisfy *any* equation of I. Even more, they satisfy any equation appearing in $\mathrm{rad}(I)$. Again, in the same vein as before, we can argue that any equation appearing in $\mathrm{rad}(I)$ should appear as an equation in characteristic p as well. Hence, in this way we can give some universal equations which should work in any characteristic.

This is essentially the formulation of the Jacobian Conjecture in characteristic p we introduce in the next section, but we have to use more formal language.

3. A new formulation of the Jacobian Conjecture in characteristic p. Given $F = (F_1, \ldots, F_n) \in \mathrm{ME}_n(R)$ where R is some ring, we can write $F_i = \sum_{\alpha \in \mathbb{N}^n} c_{i,\alpha} x^\alpha$. We can also define the infinitely generated ring $C_R := R[c_{i,\alpha} \mid 1 \leq i \leq n,\ \alpha \in \mathbb{N}^n]$ where the $c_{i,\alpha}$ are variables. One can now construct the universal polynomial map of degree $d \in \mathbb{N}$ by taking the polynomial map in $\mathrm{ME}_n(C_R)$ which has coefficients the variables $c_{i,\alpha}$. We say that $C_{R,d}$ is the finitely generated ring generated by the coefficients up to and including degree d. (That is, C_R is the union, or direct limit, of the rings $\cdots \subset C_{R,d} \subset C_{R,d+1} \subset \cdots$.)

Definition 3.1. Let $F[d] \in \mathrm{ME}_n(C_{\mathbb{Q},d})$ be the universal polynomial endomorphism of degree d having affine part identity. Then computing $\det \mathrm{Jac}(F[d]) - 1 = \sum_{\alpha \in \mathbb{N}^n} E_\alpha x^\alpha$ yields a polynomial in $x_1, \ldots, x_n$ with coefficients $E_\alpha \in C_{\mathbb{Q},d}$. Define the ideal $I^d_{\mathbb{Q}} = (E_\alpha \mid \alpha \in \mathbb{N}^n)$ in $C_{\mathbb{Q},d}$ generated by the equations found from the formula $\det \mathrm{Jac}(F[d]) = 1$. We define the ideal $I_{\mathbb{Q}}$ in $C_{\mathbb{Q}}$ as the inverse limit of the canonical chain $\cdots \to I^{d+1}_{\mathbb{Q}} \to I^d_{\mathbb{Q}} \to \cdots$. It coincides with the equations coming from $\det \mathrm{Jac}(F[\infty]) = 1$, where $F[\infty]$ is the power series with universal coefficients.

Definition 3.2. We define $J_{\mathbb{Z}} := \mathrm{rad}(I_{\mathbb{Q}}) \cap C_{\mathbb{Z}}$ as the "ideal of integer Keller equations". This ideal captures the universal equations described in the previous section. If R is a ring, we consider $J_R := J_{\mathbb{Z}} \otimes R$ as an ideal in the ring C_R. It is the ideal in C_R generated by those same equations (in characteristic zero) or by those equations modulo p (in characteristic p). In particular, we define $J_p := J_{\mathbb{F}_p} = J_{\mathbb{Z}} \bmod p$ as an ideal in $C_{\mathbb{F}_p}$. Similarly we define $J^d_{\mathbb{Z}} := \mathrm{rad}(I^d_{\mathbb{Q}}) \cap C_{\mathbb{Z},d}$, $J^d_R := J^d_{\mathbb{Z}} \otimes R$ and $J^d_p := J^d_{\mathbb{Z}} \bmod p$ where $d = \deg(F)$.

Let M_d be the number of variables in $F[d]$ (i.e. the dimension of the ring $C_{R,d}$). We say that $v \in R^{M_d}$ *satisfies* J^d_R if $f(v) = 0$ for all $f \in J^d_R$. We say that $v \in R^{M_d}$ *satisfies* J_R if $v \in R^{M_d}$ satisfies J^d_R.

We can identify $F \in \mathrm{ME}_n(R)$ by the vector of coefficients $v(F)$ of F; in particular, if $F \in \mathrm{ME}_n(R)$ we say that F *satisfies* J_R (resp. J^d_R) if $v(F)$ satisfies J_R (resp. J^d_R).

Throughout, we will write the elements of $J_R = J_{\mathbb{Z}} \otimes R$ as $\sum_i e_i h_i$ instead of $\sum_i e_i \otimes h_i$, where $e_i \in J_{\mathbb{Z}}$ and $h_i \in R$ for all i (for simplicity, we will omit the tensor notation in this manuscript).

Definition 3.3. We say that $F \in \mathrm{ME}_n(R)$ is a *strong Keller map* if F satisfies J_R (or equivalently $F \in \mathrm{ME}_n(R)$ is a *strong Keller map* if F

satisfies J_R^d where $\deg(F) = d$). We denote the set of strong Keller maps by $\mathrm{SKE}_n(R)$, and the set of Keller maps by $\mathrm{KE}_n(R)$.

CONJECTURE 3.4 (Jacobian Conjecture over any field (in particular, in positive characteristic), $\mathcal{JC}(\mathbf{k}, \mathbf{n})$). *Let k be a field (of characteristic p) and $F \in \mathrm{ME}_n(k)$ be a strong Keller map. Then $F \in \mathrm{GA}_n(k)$.*

So, an alternative definition of $\mathcal{JC}(k, n)$ is $\mathrm{SKE}_n(k) = \mathrm{GA}_n(k)$. We will use the caligraphic notation $\mathcal{JC}$ to represent the Jacobian Conjecture in characteristic p.

Of course, we still need to show that the above formulation coincides with the regular formulation if the field is of characteristic zero. However, this will follow directly from Lemma 4.3.

Note that we only defined the conjecture for fields of any characteristic, but with a slight modification one can define it for all domains (of any characteristic). However, we will stick to the above formulation in this first encounter.

Before we study the validity of this conjecture, we will introduce some facts and concepts we will use afterwards.

4. Basic facts. In the following remark some basic facts about the map $F \bmod p$ for $F \in \mathrm{ME}_n(\mathbb{Z})$ are gathered. They are used in various places without mention.

REMARK 4.1. Let $F \in \mathrm{ME}_n(\mathbb{Z})$. Then

$$(\det \mathrm{Jac}(F)) \bmod p = \det(\mathrm{Jac}(F) \bmod p) = \det \mathrm{Jac}(F \bmod p).$$

In particular:

- $\det \mathrm{Jac}(F) = 1 \bmod p \Leftrightarrow \det \mathrm{Jac}(F \bmod p) = 1 \bmod p$.
- If $F \in \mathrm{ME}_n(\mathbb{Z})$ is such that $F \bmod p \in \mathrm{SKE}_n(\mathbb{F}_p)$, then $\det \mathrm{Jac}(F) = 1 + pH$ for some $H \in \mathrm{ME}_n(\mathbb{Z})$.
- $(F \circ G) \bmod p = (F \bmod p) \circ (G \bmod p)$ and $\det \mathrm{Jac}(F \circ G) \bmod p = \det \mathrm{Jac}(F \bmod p \circ G \bmod p)$.

Proof. Writing out the equations $\det(\partial(F_i \bmod p)/\partial x_j)$ we see that checking the remark essentially comes down to checking that if $c_\alpha x^\alpha$ is a generic monomial where $\alpha \in \mathbb{N}^n$ and $c_\alpha \in \mathbb{Z}$, then

$$\frac{\partial c_\alpha x^\alpha}{\partial x_i} \bmod p = \frac{\partial c_\alpha x^\alpha \bmod p}{\partial x_i},$$

which is true (just check the case where p divides c_α or p divides α_i separately). ∎

LEMMA 4.2. *Let $F \in \mathrm{ME}_n(R)$. If F satisfies the ideal $I_{\mathbb{Q}}$, then it satisfies $J_{\mathbb{Z}}$.*

Proof. Consider $Q \in J_{\mathbb{Z}}$. Note that $J_{\mathbb{Z}} = \mathrm{rad}(I_{\mathbb{Q}}) \cap C_{\mathbb{Z}} = \mathrm{rad}(I_{\mathbb{Q}} \cap C_{\mathbb{Z}})$, thus there exists $n \in \mathbb{Z}$ such that $Q^n \in I_{\mathbb{Q}} \cap C_{\mathbb{Z}} \subset C_{\mathbb{Z}}$. Assume $I_{\mathbb{Q}}$ is generated by $\{e_i\}_{i\in\Omega}$; then $Q^n = \sum_i h_i e_i$ for $h_i \in C_{\mathbb{Z}}$ for all i. Thus $Q^n(\nu(F)) = \sum_i h_i(\nu(F))e_i(\nu(F)) = 0$ since F satisfies $e_i \in I_{\mathbb{Q}}$. Hence $Q(\nu(F)) = 0$ as $C_{\mathbb{Z}}$ is an integral domain. ∎

LEMMA 4.3. *Let R be a ring with* $\mathrm{char}(R) = 0$. *Then $F \in \mathrm{SKE}_n(R)$ if and only if $F \in \mathrm{KE}_n(R)$.*

Proof. Let $F \in \mathrm{SKE}_n(R)$; then for all $Q \in J_R$ we have $Q(\nu(F)) = 0$. Since $f \otimes 1 \in J_R$ for $f \in J_{\mathbb{Z}}$ and $1 \in R$, we see that $f(\nu(F)) = 0$ for all $f \in J_{\mathbb{Z}}$. As $I_{\mathbb{Q}} \cap C_{\mathbb{Z}} \subseteq J_{\mathbb{Z}}$, we get $f(\nu(F)) = 0$ for all $f \in I_{\mathbb{Q}} \cap C_{\mathbb{Z}}$. For any $e \in I_{\mathbb{Q}}$ we can find $f \in I_{\mathbb{Q}} \cap C_{\mathbb{Z}}$ such that $e = f/m$ for some $m \in \mathbb{Z}$. Thus $e(\nu(F)) = 0$ for all $e \in I_{\mathbb{Q}}$. Hence $F \in \mathrm{KE}_n(R)$.

Conversely, suppose that F is a Keller map; then F satisfies $I_{\mathbb{Q}}$. Thus by Lemma 4.2 we have $e(\nu(F)) = 0$ for all $e \in J_{\mathbb{Z}}$. Now for any $\sum_i e_i r_i \in J_R$ we get $\sum_i e_i r_i(\nu(F)) = \sum_i e_i(\nu(F))r_i(\nu(F)) = 0$, where $r_i \in R$ and $e_i \in J_{\mathbb{Z}}$ for all i. Thus F is strong Keller map. ∎

LEMMA 4.4. $\mathrm{SKE}_n(k) \subset \mathrm{SKE}_n(\acute{k})$ *for any fields $k \subset \acute{k}$ of positive characteristic.*

Proof. Let $F \in \mathrm{SKE}_n(k)$. Consider k_0 to be the subfield of k generated by the coefficients of F. Then $F \in \mathrm{SKE}_n(k_0)$, and so F satisfies the ideal J_{k_0}. Since $J_{k_0} \subset J_{\acute{k}}$, it is obvious to see $q(\nu(F)) = 0$ for any $q \in J_{\acute{k}} \setminus J_{k_0}$ (as q does not involve any coefficient of F by definition of $J_{\acute{k}}$). Thus F satisfies the ideal $J_{\acute{k}}$, and so $F \in \mathrm{SKE}_n(\acute{k})$. ∎

5. Two surjectivity conjectures. Given $F \in \mathrm{GA}_n(\mathbb{Z})$ we can define F mod p for any prime p, yielding an element of $\mathrm{GA}_n(\mathbb{F}_p)$. If we additionally assume that $p \nmid \det(\mathrm{Jac}(F))$ then $F \bmod p \in \mathrm{GA}_n(\mathbb{F}_p)$, even. This yields the natural map $\pi : \mathrm{SA}_n(\mathbb{Z}) \to \mathrm{SA}_n(\mathbb{F}_p)$. The following fact is not difficult to prove:

REMARK 5.1. $\pi(\mathrm{STA}_n(\mathbb{Z})) = \mathrm{STA}_n(\mathbb{F}_p)$.

The reason for this is that (1) any affine or triangular map having determinant Jacobian 1 has a preimage under π, (2) any tame automorphism of determinant Jacobian 1 can indeed be written as a composition of affine and triangular automorphisms of determinant Jacobian 1. (See [4, Lemma 3.4].)

Now an obvious question is whether the map $\pi : \mathrm{SA}_n(\mathbb{Z}) \to \mathrm{SA}_n(\mathbb{F}_p)$ is surjective or not; this question is interesting as non-surjectivity would yield non-tame maps due to the above remark. This is part of the topic of [4, 3, 5].

DEFINITION 5.2. Let R be a $\mathbb{Z}$-algebra and k be a field such that we have a surjective ring homomorphism $R \to k$. We can extend it naturally as $\mathrm{ME}_n(R) \to \mathrm{ME}_n(k)$. We denote this extended map by π.

We notice that corresponding to each automorphism $F \in \mathrm{SA}_n(\mathbb{Z})$ we have $F \bmod p \in \mathrm{SA}_n(\mathbb{F}_p)$, but there may exist some automorphisms $f \in \mathrm{SA}_n(\mathbb{F}_p)$ such that $\pi^{-1}(f) \subset \mathrm{SA}_n(\mathbb{Z})$. We conjecture the following for a $\mathbb{Z}$-algebra R and a field k:

CONJECTURE 5.3. *Let R be a $\mathbb{Z}$-algebra and k be any field. If there is a surjective ring homomorphism $R \to k$, then:*

(1) $\pi(\mathrm{SA}_n(R)) = \mathrm{SA}_n(k)$.
(2) $\pi^{-1}(\mathrm{SA}_n(k)) \cap \mathrm{KE}_n(R) = \mathrm{SA}_n(R)$.

A similar conjecture is (see also Lemma 7.8 and Corollary 7.9):

CONJECTURE 5.4. *Let R be a $\mathbb{Z}$-algebra and k be any field of characteristic p. If there is a surjective ring homomorphism $R \to k$, then the map $\pi : \mathrm{KE}_n(R) \to \mathrm{ME}_n(k)$ has $\mathrm{SKE}_n(k)$ in its image.*

If the above conjecture is *not* true, it could mean that $\mathcal{JC}(k, n)$ is not true (or should be reformulated), or that there exist non-tame automorphisms over k.

Assuming $\mathcal{JC}(k, n)$ is true, Conjecture 5.3 implies 5.4, but no other implications can be made, nor does $\mathcal{JC}(k, n)$ imply any of the above conjectures.

Justification of the above conjectures. The conjectures are not made to "match exactly what we need in our proofs". They capture the essence of whether characteristic p is *truly* different from characteristic zero. If one or more of these conjectures are wrong, then characteristic p is in its core different from characteristic zero (for example, there might exist $\mathbb{F}_p$-automorphisms of $\mathbb{F}_p^{[n]}$ which are of a completely different nature than one can find in characteristic zero), while if both of them are correct, then characteristic p is not too dissimilar from characteristic zero and both are intricately linked.

The tendency is to believe the conjectures (hence the name "conjecture" and not "problem" or "question"): it would be really surprising if any counterexamples were easily constructible in low degree and dimension, whereas it can be easily imagined that the conjectures are true but hard to prove. For example, due to the fact that we do not even have a (parametrized) list of generators for the automorphism group $\mathrm{GA}_n(k)$ (unlike for $\mathrm{GL}_n(k), \mathrm{TA}_n(k)$), we can understand that Conjecture 5.4, if true, is very hard to prove ([1]).

([1]) Note that with a little change, *some people* would agree on the same text for the Jacobian Conjecture.

6. Some computations indicating the correctness of $\mathcal{JC}(k,n)$. We should check this conjecture for some non-trivial cases, in order to point out that it might do what it claims. Therefore, in this subsection we considered polynomial endomorphisms of degree ≤ 3 with coefficients in a field of characteristic p, and having affine part identity. We will check if $\mathcal{JC}(k,2)$ is true for these maps for fields k of characteristic p. Let us write down such a polynomial map with generic coefficients:

$$T = (x,y) + \big(Ax^2 + By^2 + Cxy + Dx^3 + Ey^3 + Fx^2y + Gxy^2, \\ A_1x^2 + B_1y^2 + C_1xy + D_1x^3 + E_1y^3 + F_1x^2y + G_1xy^2\big).$$

Let us take the determinant of the Jacobian and equal it to 1:

$$\begin{aligned} 1 = \det \mathrm{Jac}(T) &= 1 + (C_1 + 2A)x + (2B_1 + C)y \\ &+ (F_1 + 3D + 2AC_1 - 2A_1C)x^2 + (2G_1 + 2F + 4AB_1 - 4A_1B)xy \\ &+ (3E_1 + G + 2CB_1 - 2BC_1)y^2 \\ &+ (6AE_1 - 6A_1E + 4B_1F - 4BF_1 + CG_1 - C_1G)xy^2 \\ &+ (6DB_1 - 6D_1B + 4AG_1 - 4A_1G + FC_1 - F_1C)x^2y. \end{aligned}$$

This gives us generators of the ideal $I_{\mathbb{Q}} = (C_1 + 2A, 2B_1 + C, \ldots)$ in the ring $\mathbb{Q}[A, B, \ldots, E_1]$. By some elementary manipulations it is clear that the following equations are also in $I_{\mathbb{Q}}$:

$$\begin{aligned} &F_1+3D, AC_1-A_1C, G_1+F, AB_1-A_1B, 3E_1+G, CB_1-BC_1, \\ &AE_1-A_1E, B_1F-BF_1, CG_1-C_1G, DB_1-D_1B, AG_1-A_1G, FC_1-F_1C, \\ &DE_1-D_1E, FG_1-F_1G, FA_1-F_1A, DC_1-D_1C, CE_1-C_1E, B_1G-BG_1, \\ &DG_1-GD_1, FE_1-EF_1, DF_1-D_1F, C_1+2A, C+2B_1, GE_1-EG_1 \in I_{\mathbb{Q}}. \end{aligned} \tag{6.1}$$

Moreover, it can be checked by any computer algebra package (we used `singular`) that

$$A^3E_1^2 - B^3D_1^2, A^3E^2 - B^3D^2 \in \mathrm{rad}(I_{\mathbb{Q}}), \tag{6.2}$$

where these equations do not belong to $I_{\mathbb{Q}}$.

As before, we define $J_{\mathbb{Z}} := \mathrm{rad}(I_{\mathbb{Q}}) \cap \mathbb{Z}[A, B, \ldots, E_1]$ and $J_p := J_{\mathbb{Z}} \bmod p$. It is now possible to use a computer algebra system to show that (6.1) and (6.2) generate J_p, but this can be quite a strain on the computer system, which we can avoid in this case: We will show that (Part 1) assuming these equations forces T to be invertible for any p, and (Part 2) if T is assumed to be invertible, then it satisfies (6.1) and (6.2) (meaning we show that these equations might not generate J_p, but the radical of the ideal generated by them does).

Part 1: *the equations yield invertibility.* We first assume that A, A_1, E are all non-zero. Then solving (6.1) and (6.2) yields

$$C_1 = -2A, \quad C = -\frac{2A^2}{A_1}, \quad B_1 = \frac{A^2}{A_1}, \quad B = \frac{A^3}{{A_1}^2},$$
$$G = -\frac{3A_1E}{A}, \quad G_1 = -\frac{3{A_1}^2E}{A^2},$$
$$D = -\frac{{A_1}^3E}{A^3}, \quad D_1 = \frac{{A_1}^4E}{A^4},$$
$$F_1 = -3D, \quad G = -3E_1, \quad F = -G_1.$$

Thus

$$T = (x,y) + \Big(Ax^2 + \frac{A^3}{{A_1}^2}y^2 - \frac{2A^2}{A_1}xy - \frac{{A_1}^3E}{A^3}x^3 + Ey^3 + \frac{3{A_1}^2E}{A^2}x^2y - \frac{3A_1E}{A}xy^2,$$
$$A_1x^2 + \frac{A^2}{A_1}y^2 - 2Axy - \frac{{A_1}^4E}{A^4}x^3 + \frac{A_1E}{A}y^3 + \frac{3{A_1}^3E}{A^3}x^2y - \frac{3{A_1}^2E}{A^2}xy^2 \Big).$$

This can be rewritten as

$$T = \begin{pmatrix} x + A\big(x - \frac{A}{A_1}y\big)^2 - \frac{A^3E}{A_1^3}\big(x - \frac{A}{A_1}y\big)^3 \\ y + A_1\big(x^2 - \frac{A}{A_1}y\big)^2 - \frac{A_1^4E}{A^4}\big(x - \frac{A}{A_1}y\big)^3 \end{pmatrix}.$$

Regardless of characteristic, T is a tame map of the form

$$T = \Big(x + \frac{A}{A_1}y, y\Big)\Big(x, y + A_1x^2 - \frac{EA_1^3}{A^3}x^3\Big)\Big(x - \frac{A}{A_1}y, y\Big)$$

meaning that T is invertible.

The case that one or more of A, A_1, E are zero is easier (many coefficients are forced to be zero) and we leave it to the reader.

PART 2: *invertibility implies the equations.* Since we have a map in dimension 2, it is tame, and we can use the Jung–van der Kulk theorem. Since the degree is three or less, it is a map of the form $\alpha(x, y + f(x))\beta$ where α, β are affine invertible maps, and $\deg(f) \leq 3$. (There can only be one triangular map involved, as the degree is prime.) We can assume that $\beta = (ax + by + c, y)$ as we can put anything occurring in the second component of f. Also, we can assume f is of degree 2 or 3, and also that $f(0) = 0$ as we can put any constant added in α. Adding in the requirement that the affine part of $\alpha(x, y + f(x))\beta$ must be the identity yields requirements on α given β and $f(x)$. Working this out yields a generic map that is actually very similar to the formula of T above; it can be easily checked that it satisfies the equations.

REMARK. It is very hard to check this conjecture for specific degrees, even for $n = 2$, as there is no shortcut other than doing hard-core computations. In fact, *en passant* one is proving the conjecture, and the computations are very similar to proving the Jacobian Conjecture in characteristic zero—which is (we hope the reader agrees) a difficult task...

Of course, we also checked the conjecture for many specific examples (which we do not list here, though we specifically mention that we could rule out "obvious" examples like $(x + x^p, y)$).

7. Implications of the Jacobian Conjecture for various fields. In this section we will see, for $k, \acute{k}$ two arbitrary fields of characteristic p, what is the connection between $\mathcal{JC}(k, n)$ and $\mathcal{JC}(\acute{k}, n)$ for all $n \geq 1$. Recall we denote the Jacobian Conjecture over all domains having characteristic zero by $\mathrm{JC}(n, 0)$, and the Jacobian Conjecture over all fields of characteristic p by $\mathcal{JC}(n, p)$. In characteristic zero we have the following theorem [2, Theorem 1.1.18]).

THEOREM 7.1. *Let $R, \acute{R}$ be commutative rings contained in a $\mathbb{Q}$-algebra. If $\mathrm{JC}(R, n)$ is true for all $n \geq 1$, then $\mathrm{JC}(\acute{R}, n)$ is true for all $n \geq 1$.*

For the characteristic p equivalent we have to assume part of our conjectures:

THEOREM 7.2. *Assume that Conjectures* 5.3(2) *and* 5.4 *are true. Let $k, \acute{k}$ be two fields contained in an $\mathbb{F}_p$-algebra such that $\mathcal{JC}(k, n)$ is true for all $n \geq 1$. Then $\mathcal{JC}(\acute{k}, n)$ is true for all $n \geq 1$. In particular, it is enough to verify $\mathcal{JC}(\mathbb{F}_p, n)$.*

It is very hard to prove the statement of Theorem 7.2 without making any assumption. To mention the main hurdle: let k be infinite field and $k_1 \subset k$ a finite Galois extension, let $a_1, \ldots, a_n$ be a k_1-basis of k and denote by $\alpha : k_1^m \to k$ the map defined by $\alpha(y_1, \ldots, y_n) = y_1 a_1 + \cdots + y_n a_n$. The obvious extension $(k_1^m)^n \to k^n$, which we also denote by α, is clearly bijective. Let $F = (F_1, \ldots, F_n) : k^n \to k^n$ be a polynomial map. Conjugating F with α we get the map $F^\alpha := \alpha^{-1} F \alpha : k_1^{mn} \to k_1^{mn}$. In the characteristic zero proof of Theorem 7.1 we know that $\det \mathrm{Jac}(F) \in k^*$ if and only if $\det \mathrm{Jac}(F^\alpha) \in k_1^*$ [2, (1.1.26)]. In characteristic p we should have a similar statement that F satisfies J_k if and only if F^α satisfies J_{k_1}, but the proof of this is very difficult. This equivalence is needed to prove Theorem 7.2 if we do not assume that Conjectures 5.3(2) and 5.4 are true.

The remaining part of this section is devoted to proving Theorem 7.2. We begin with some definitions and lemmas.

Let $\Omega :=$ algebraic closure of $\mathbb{F}_p(\{x_i \mid i \in \mathbb{N}\})$. Then Ω is a field with infinite transcendence degree over $\mathbb{F}_p$.

DEFINITION 7.3. Let R, S be commutative rings. Let $\phi : R \to S$ be a ring homomorphism. If $F \in R[X]^n$, then F^ϕ denotes the element of $S[X]^n$ obtained by applying ϕ to the coefficients of the F_i.

We use the notation $X = (x_1, \ldots, x_n)$. The following result is [2, Proposition 1.1.7]. Let η be the nilradical of R.

PROPOSITION 7.4 (Invertibility under base change). *Let $\phi : R \to S$ be a ring homomorphism with $\ker\phi \subset \eta$. Let $F \in R[X]^n$ with $\det JF(0) \in R^*$. Then F is invertible if and only if F^ϕ is invertible over S.*

We use this to show that proving the $\mathcal{JC}$ for Ω is universal, in the sense that it proves the Jacobian Conjecture for all fields of the same characteristic:

PROPOSITION 7.5. *Let $n \geq 1$. If $\mathcal{JC}(\Omega, n)$ is true then $\mathcal{JC}(k, n)$ is true for any field k of characteristic p.*

Proof. Let $F \in k[X]^n$ satisfy $J_\mathbb{Z} \otimes k$. Let k_0 be the subfield of k generated over $\mathbb{F}_p$ by the coefficients of F (i.e. $k_0 = \mathbb{F}_p(x_1, \ldots, x_m)$ for some $x_1, \ldots, x_m \in k$). Then F satisfies $J_\mathbb{Z} \otimes k_0$. By the definition of Ω it is trivial that we get an embedding $\phi : k_0 \to \Omega$. Since F satisfies $J_\mathbb{Z} \otimes k_0$ we see that F^ϕ satisfies $J_\mathbb{Z} \otimes \phi(k_0)$, and by Lemma 4.4 we find that F^ϕ satisfies $J_\mathbb{Z} \otimes \Omega$. This shows F^ϕ is invertible over Ω since we assume that $\mathcal{JC}(\Omega, n)$ is true. Thus F is invertible over k_0 by Proposition 7.4 and hence over k. ∎

COROLLARY 7.6 (of Lemma 4.4). *Let $n \geq 1$ and let $k_0 \subset k$ be fields of characteristic p. If $\mathcal{JC}(k, n)$ is true then $\mathcal{JC}(k_0, n)$ is true.*

Proof. Let $F \in \mathrm{SKE}_n(k_0)$. Then by Lemma 4.4 we have $F \in \mathrm{SKE}_n(k)$. Since we assume that $\mathcal{JC}(k, n)$ is true, we deduce F is invertible over k. Hence F is invertible over k_0 by Proposition 7.4. ∎

DEFINITION 7.7. Let k be any countable field of characteristic p. Write $k = \{a_1, a_2, \ldots\}$ where $a_i \neq a_j$ for $i \neq j$. We can also assume that k is an ordered set. Corresponding to each element a_i in k consider the indeterminate x_i. Define a polynomial ring over $\mathbb{Z}$ by $\Lambda_k := \mathbb{Z}[x_1, x_2, \ldots]$. Define a map $\tau : \Lambda_k \to k$ by $x_i \mapsto a_i$ and $m \mapsto m \bmod p$ for any $m \in \mathbb{Z}$. It is clearly a well defined surjective ring homomorphism.

Notice that we can naturally extend τ to a map $\mathrm{ME}_n(\Lambda_k) \to \mathrm{ME}_n(k)$. We denote this extended map by π as in Definition 5.2.

LEMMA 7.8. *Let k be a countable field of characteristic p. Then $\pi(\mathrm{KE}_n(\Lambda_k)) \subseteq \mathrm{SKE}_n(k)$ for every $n \geq 1$.*

Proof. Let $F \in \mathrm{KE}_n(\Lambda_k)$. Then $\det \mathrm{Jac}(F) = 1$ and so F satisfies $I_\mathbb{Q}$. We want to show $\pi(F) \in \mathrm{SKE}_n(k)$. Let $\bar{J}_\mathbb{Z}$ be the ideal of integer Keller equations for the polynomial $\pi(F)$ and $J_k := \bar{J}_\mathbb{Z} \otimes k$ (see Definition 3.2). Let $q \in J_k$. Then $q = \sum_i \tilde{e}_i h_i$ for $\tilde{e}_i \in \bar{J}_\mathbb{Z}$, and $h_i \in k$ for all i (here $\tilde{e}_i h_i = \tilde{e}_i \otimes h_i$, but we omit the tensor notation). Since $h_i \in k$ there exist $H_i \in \Lambda_k$ such that $\tau(H_i) = h_i$. We can define a surjective homomorphism $J_{\Lambda_k} := J_\mathbb{Z} \otimes \Lambda_k \to \bar{J}_\mathbb{Z} \otimes k$ by $a \otimes b \mapsto \tau(a) \otimes \tau(b)$ where $a \in J_\mathbb{Z}$ and $b \in \Lambda_k$. Thus there exists $Q \in J_{\Lambda_k}$ defined by $Q = \sum_i e_i H_i$ such that $\tau(Q) = q$, i.e. $\sum_i \tau(e_i)\tau(H_i) = \sum_i \tilde{e}_i h_i$ where $e_i \in J_\mathbb{Z}$ is such that $\tau(e_i) = \tilde{e}_i$ for all i. By

Lemma 4.2 we have $e_i(\nu(F)) = 0$ for all i (since F satisfies $I_{\mathbb{Q}}$). If we identify x_i with a_i as in the definition of τ, then $\tilde{e_i}(\nu(\pi(F))) = e_i(\nu(F)) \bmod p = 0 \bmod p$ for all i. Thus $q(\nu(\pi(F))) = \sum_i \tilde{e_i}(\nu(\pi(F)))h_i(\nu(\pi(F))) = 0 \bmod p$. This shows that $\pi(F)$ satisfies J_k. Hence $\pi(F) \in \mathrm{SKE}_n(k)$. ∎

Of course, the above lemma slightly reformulates Conjecture 5.4:

Corollary 7.9. *Assume Conjecture* 5.4 *is true and let k be a countable field of characteristic p. Then $\pi(\mathrm{KE}_n(\Lambda_k)) = \mathrm{SKE}_n(k)$.*

We are now ready to link $\mathrm{JC}(n, 0)$ to $\mathcal{JC}(n, p)$.

Proposition 7.10.

(1) *Assume Conjecture* 5.4 *is true. Then*

$$\mathrm{JC}(n, 0)\ \forall n \in \mathbb{N}^* \ \Rightarrow\ \mathcal{JC}(n, p)\ \forall n \in \mathbb{N}^*.$$

(2) *Assume Conjectures* 5.3(2) *and* 5.4 *are true. Then*

$$\mathrm{JC}(n, 0)\ \forall n \in \mathbb{N}^* \ \Leftrightarrow\ \mathcal{JC}(n, p)\ \forall n \in \mathbb{N}^*.$$

In fact, it is enough to prove or disprove $\mathrm{JC}(n, \mathbb{Z})$ for all n to prove or disprove $\mathcal{JC}(k, n)$ for all n and for any field k.

Proof. (1) Let K be an arbitrary field of characteristic p and $f \in \mathrm{SK}_n(K)$. Let k be a subfield of K generated over $\mathbb{F}_p$ by the coefficients of f. Since k is at most countable, we have a surjective ring homomorphism $\tau : \Lambda_k \to k$ (Definition 7.7). By Corollary 7.9 there exists $F \in \mathrm{KE}_n(\Lambda_k)$ such that $\pi(F) = f$. Thus F is invertible since we assume that $\mathrm{JC}(n, 0)$ is true, so there exists $G \in \mathrm{ME}_n(\Lambda_k)$ such that $F \circ G = I$. Applying π we have $\pi(F) \circ \pi(G) = \pi(I) = I \bmod p$. Thus $\pi(G)$ is an inverse of $f = \pi(F)$. This shows that f is invertible over k and hence over K.

(2) Let K be an arbitrary field of characteristic p, and consider a countable field $k \subseteq K$ (if K is itself countable then take $k = K$). By Corollary 7.9 we have $\pi(\mathrm{KE}_n(\Lambda_k)) = \mathrm{SKE}_n(k)$ (where Λ_k is defined in 7.7). Let $F \in \mathrm{KE}_n(\Lambda_k)$. Then $\pi(F)$ satisfies J_k. Suppose $\mathcal{JC}(K, n)$ is true; then so is $\mathcal{JC}(k, n)$ by Corollary 7.6. Thus $\pi(F) \in \mathrm{SA}_n(k)$ and so $F \in \pi^{-1}(\mathrm{SA}_n(k))$. By Conjecture 5.3(2) we have $F \in \mathrm{SA}_n(\Lambda_k)$. Theorem 7.1 tells us that $\mathrm{JC}(n, 0)$ is true. ∎

Proof of Theorem 7.2. This is a direct consequence of Proposition 7.10. ∎

8. Some results related to $\mathcal{JC}(k, n)$. In this section we present some basic results related to our formulation of the Jacobian Conjecture in characteristic p.

8.1. Invertible polynomial maps and $\mathcal{JC}(k, n)$. In this subsection we will discuss a natural question which can come to mind when studying the previous. If $\mathrm{char}(k) = 0$, we know that if $F \in \mathrm{SA}_n(k)$ then F satisfies

the Keller condition $\det \mathrm{Jac}(F) = 1$ (the only condition for $\mathrm{JC}(k,n)$). This is due to the fact that the determinant of the Jacobian has the property $\det \mathrm{Jac}(G \circ F) = \det \mathrm{Jac}(F) \cdot (\det \mathrm{Jac}(G) \circ F)$. If $\mathrm{char}(k) = p$, it is not easy to prove that if $F \in \mathrm{SKE}_n(k)$ then F satisfies J_k (the universal equations).

Nevertheless, assuming Conjectures 5.3(1) and 5.4 we can prove that if $F \in \mathrm{SA}_n(k)$ then $F \in \mathrm{SKE}_n(k)$.

PROPOSITION 8.1. *Assume Conjectures* 5.3(1) *and* 5.4 *are true and let k be a field of characteristic p. If $f \in \mathrm{SA}_n(k)$ then $f \in \mathrm{SKE}_n(k)$.*

Proof. Let $f \in \mathrm{SA}_n(k)$. Consider $k_0 \subset k$ generated over $\mathbb{F}_p$ by the coefficients of f. By Conjecture 5.3(1) there exists some $F \in \mathrm{SA}_n(\Lambda_{k_0})$ such that $\pi(F) = f$, and thus F satisfies $\mathrm{KE}_n(\Lambda_{k_0})$. Assuming Conjecture 5.4 we have $\pi(\mathrm{KE}_n(\Lambda_{k_0})) = \mathrm{SKE}_n(k_0)$ by Corollary 7.9. Thus $f \in \mathrm{SKE}_n(k_0)$ and hence $f \in \mathrm{SKE}_n(k)$ by Lemma 4.4. ∎

8.2. Closure property of $\mathrm{SKE}_n(k)$. The set $\mathrm{KE}_n(R)$ is closed under composition for any ring R, and also for $R = k$ a field of characteristic p, even though it does not consist of automorphisms only. One would expect that $\mathrm{SKE}_n(\mathbb{F}_p)$ is also closed under composition. However, trying to prove this turns out to be an incredibly difficult task. If $F \in \mathrm{SKE}_n(\mathbb{F}_p)$ then the coefficients of F satisfy certain equations that can be found in J_p. For two such maps $F, G \in \mathrm{SKE}_n(\mathbb{F}_p)$, the coefficients of $F \circ G$ (denoted $v(F \circ G)$) are polynomials in the coefficients of F and G, i.e. $v(F \circ G) = P(v(F), v(G))$ for some polynomial map P. To check if $F \circ G$ is in $\mathrm{SKE}_n(\mathbb{F}_p)$ we need to see if $v(F \circ G)$ satisfy (the equations in) J_p; however, this has turned out to be extremely difficult.

In characteristic zero, we know a priori due to the "magical" equation $\det \mathrm{Jac}(F \circ G) = \det \mathrm{Jac}(G) \cdot (\det \mathrm{Jac}(F) \circ G)$ that $\mathrm{KE}_n(\mathbb{Z})$ is closed under composition. As a corollary, "$v(F)$ satisfies $J_{\mathbb{Z}}$ and $v(G)$ satisfies $J_{\mathbb{Z}}$" implies "$v(F \circ G)$ satisfies $J_{\mathbb{Z}}$", but exactly *how* is very complicated.

Nevertheless, under some assumption we can prove that $\mathrm{SKE}_n(\mathbb{F}_p)$ is closed under composition.

PROPOSITION 8.2. *Assume Conjecture* 5.4 *is true. Then* $\mathrm{SKE}_n(k)$ *is closed under composition, where k is any field of characteristic p.*

Proof. Let $f, g \in \mathrm{SKE}_n(k)$. Let k_1 be the subfield of k generated over $\mathbb{F}_p$ by the coefficients of f and g. Then k_1 is countable, thus by Corollary 7.9 there exist $F, G \in \mathrm{KE}_n(\Lambda_{k_1})$ such that $\pi(F) = f$ and $\pi(G) = g$. Now $F \circ G \in \mathrm{KE}_n(\Lambda_{k_1})$ as $\mathrm{KE}_n(\Lambda_{k_1})$ is closed under composition. Thus $f \circ g = \pi(F) \circ \pi(G) = \pi(F \circ G) \in \mathrm{SKE}_n(k_1)$ by Corollary 7.9. Hence $f \circ g \in \mathrm{SKE}_n(k)$ (Lemma 4.4). ∎

8.3. Connection between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathrm{JC}(\mathbb{Z}, n)$. In this subsection we will see how we can move back and forth between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathrm{JC}(\mathbb{Z}, n)$. We quote [2, Theorem 10.3.13]; we will need this theorem to build the connection between $\mathcal{JC}(\mathbb{F}_p, n)$ and $\mathrm{JC}(\mathbb{Z}, n)$.

THEOREM 8.3. *Let $F \in \mathbb{Z}[x_1, \ldots, x_n]^n$. If $F \bmod p : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is injective for all but finitely many primes p and $\det \mathrm{Jac}(F) \in \mathbb{Z} \setminus \{0\}$, then F is invertible over $\mathbb{Z}$.*

LEMMA 8.4. *If $\mathcal{JC}(\mathbb{F}_p, n)$ is true for all but finitely many primes p, then $\mathrm{JC}(\mathbb{Z}, n)$ is true.*

This is a slight variation on Proposition 7.10 but without any requirements.

Proof of Lemma 8.4. Let $F \in \mathrm{ME}_n(\mathbb{Z})$ be such that $\det \mathrm{Jac}(F) = 1$. Then $F \bmod p$ satisfies J_p by Lemma 7.8. Thus $F \bmod p$ is invertible for almost all p by the assumptions. By Theorem 8.3 we conclude that F is invertible. ∎

For the converse of this lemma we need to assume Conjecture 5.4. This again resembles Proposition 7.10.

LEMMA 8.5. *Suppose Conjecture 5.4 and $\mathrm{JC}(\mathbb{Z}, n)$ are true. Then $\mathcal{JC}(\mathbb{F}_p, n)$ is true.*

Proof. Let $f \in \mathrm{ME}_n(\mathbb{F}_p)$ satisfy J_p. By Corollary 7.9 there exists $F \in \mathrm{KE}_n(\mathbb{Z})$ such that $F \bmod p = f$. By assumption, F is invertible, so there exists $G \in \mathrm{ME}_n(\mathbb{Z})$ such that $F \circ G = I$. Thus $(F \bmod p) \circ (G \bmod p) = I \bmod p$ and hence $G \bmod p =: g$ is the inverse of f. ∎

8.4. Boundedness. In this subsection we explore what happens if we assume that the degree d, or the degree and the coefficents, of a polynomial map are small with respect to p. In some sense, the results say that if p is "large enough" with respect to some formula depending on d and n, then the situation is exactly the same as in characteristic zero. We fix n in this section, but note that the constant N_d below depends also on n. Let $\mathrm{ME}_n^d(\mathbb{F}_p)$ be the set of polynomial endomorphisms of degree at most d. Similarly we can define $\mathrm{KE}_n^d(\mathbb{Z})$, $\mathrm{SKE}_n^d(\mathbb{F}_p)$ etc.

LEMMA 8.6. *Let $F \in ME_n^d(\mathbb{F}_p)$ and $I_Q^d = (E_1, \ldots, E_m)$ then there exists a positive integer N_d such that for $p > N_d$ we have $J_R^d = \mathrm{rad}(E_1, \ldots, E_m)$ for $R := \mathbb{Z}[1/N_d]$.*

Proof. Consider the ideals

$$I_{\mathbb{Q}}^d = (E_1, \ldots, E_m) \quad \text{and} \quad I_{\mathbb{Q}}^d \cap C_{R,d} = (E_1, \ldots, E_m, Q_1, \ldots, Q_r),$$

where $Q_i = P_i(E_1, \ldots, E_m)/n_i$, and $P_i(X)$ are polynomials with integer coefficients. Let $N_d = \mathrm{lcm}(n_1, \ldots, n_r)$. Then for $p > N_d$ we have $I_{\mathbb{Q}}^d \cap C_{R,d} =$

$(E_1, \ldots, E_m)$ where $R := \mathbb{Z}[1/N_d]$. Hence

$$J_R^d := \operatorname{rad}(I_{\mathbb{Q}}^d \cap C_{R,d}) = \operatorname{rad}(E_1, \ldots, E_m). \blacksquare$$

In the rest of this section we will use the same definition of the constant N_d as given in the above proof.

COROLLARY 8.7. *Suppose that $F \in \mathrm{ME}_n^d(\mathbb{F}_p)$ and $I_{\mathbb{Q}}^d = (E_1, \ldots, E_m)$. Then there exists a positive integer N_d such that for $p > N_d$ we have $J_p^d = \operatorname{rad}(E_1 \bmod p, \ldots, E_m \bmod p) = J_R^d \bmod p$ for $R := \mathbb{Z}[1/N_d]$.*

Proof. By definition $J_p^d = J_{\mathbb{Z}}^d \bmod p = J_{\mathbb{Z}}^d \otimes_{\mathbb{Z}} \mathbb{F}_p$. Since for $p > N_d$ we have $R \otimes_R \mathbb{F}_p = \mathbb{F}_p$, it follows that

$$J_p^d = J_{\mathbb{Z}}^d \otimes_{\mathbb{Z}} (R \otimes_R \mathbb{F}_p) = (J_{\mathbb{Z}}^d \otimes_{\mathbb{Z}} R) \otimes_R \mathbb{F}_p = J_R^d \otimes_R \mathbb{F}_p = J_R^d \bmod p.$$

By Lemma 8.6 we get $J_p^d = J_R^d \bmod p = \operatorname{rad}(E_1 \bmod p, \ldots, E_m \bmod p)$ for $R := \mathbb{Z}[1/N_d]$ and $p > N_d$. $\blacksquare$

COROLLARY 8.8. *There exists a positive integer N_d such that*

$$\mathrm{KE}_n^d(\mathbb{Z}) \bmod p \subset \mathrm{SKE}_n^d(\mathbb{F}_p) \quad \textit{for } p > N_d.$$

Proof. A direct consequence of Corollary 8.7. $\blacksquare$

The following lemma is intuitively clear: if you have a polynomial map with coefficients which are small (in $\mathbb{Z}$), then knowing that the map modulo p is a (special) Keller map implies that it was a Keller map to start with.

LEMMA 8.9. *Let $f \in \mathrm{SKE}_n^d(\mathbb{F}_p)$ have coefficients bounded by some constant C. Pick $F \in \mathrm{ME}_n^d(\mathbb{Z})$ such that $f = F \bmod p$ and the coefficients of F are in the interval $[-C, C]$. Then there exists a positive integer $N_d(C)$ such that for $p > N_d(C)$ we have $F \in \mathrm{KE}_n^d(\mathbb{Z})$.*

Proof. By definition for $f \in \mathrm{SKE}_n^d(\mathbb{F}_p)$ we have $s(\nu(f)) = 0 \bmod p$ for all $s \in J_p^d$. By Corollary 8.7 there exists a positive integer N_d such that for $p > N_d$ we have $J_p^d = \operatorname{rad}(E_1 \bmod p, \ldots, E_m \bmod p) = J_R^d \bmod p$ for $R := \mathbb{Z}[1/N_d]$. Thus for given $F \in \mathrm{ME}_n^d(\mathbb{Z})$ such that $F \bmod p = f$ we have $S(\nu(F)) \bmod p = 0 \bmod p$ for all $S \in J_R^d$ with $p > N_d$. In particular, for $p > N_d$ we have $E_i(\nu(F)) \bmod p = 0 \bmod p$ for all $1 \le i \le m$. Define

$$N_i := \max\{|E_i(\eta)| \mid \eta \in [-C, C]^l,\ l = \text{the number of coefficients of the generic polynomial } F\}$$

and $N_d(C) := \max\{N_d, N_1, N_2, \ldots, N_m\}$. Then for $p > N_d(C)$ we have $|E_i(\nu(F))| < p$ for all $1 \le i \le m$. Thus for $p > N_d(C)$ we get $E_i(\nu(F)) = 0$ for all $1 \le i \le m$. Hence $F \in \mathrm{KE}_n^d(\mathbb{Z})$ for $p > N_d(C)$. $\blacksquare$

Under some *very stringent conditions* we can now show closedness under composition of some elements in $\mathrm{SKE}_n(\mathbb{F}_p)$. Let $\mathrm{ME}_n^{d,C}(\mathbb{Z})$ be the set of polynomial endomorphisms of degree at most d with coefficients bounded

by C. Similarly, let $\mathrm{KE}_n^{d,C}(\mathbb{Z})$ be the set of Keller maps of degree at most d with coefficients bounded by C, and $\mathrm{SKE}_n^{d,C}(\mathbb{F}_p)$ be the set of strong Keller maps of degree at most d with coefficients bounded by C.

COROLLARY 8.10. *There exists a positive integer $N_{d^2}(C)$ such that if $f, g \in \mathrm{SKE}_n^{d,C}(\mathbb{F}_p)$ with $p > N_{d^2}(C)$ then $f \circ g \in \mathrm{SKE}_n^{d^2,C}(\mathbb{F}_p)$.*

Proof. Let $F, G \in \mathrm{ME}_n^{d,C}(\mathbb{Z})$ be such that $F \bmod p = f$ and $G \bmod p = g$. By Lemma 8.9 there exists a positive integer $N_d(C)$ such that for $p > N_d(C)$ we have $F, G \in \mathrm{KE}_n^{d,C}(\mathbb{Z})$. Since $\mathrm{KE}_n(\mathbb{Z})$ is closed under composition, we get $F \circ G \in \mathrm{KE}_n^{d^2,C}(\mathbb{Z})$. Hence by Corollary 8.8 there exists a positive integer N_{d^2} such that for $p > N_{d^2}(C) := \max\{N_{d^2}, N_d(C)\}$ we have $f \circ g \in \mathrm{SKE}_n^{d^2,C}(\mathbb{F}_p)$. ∎

The generic case eludes us:

CONJECTURE 8.11. *Let k be a field of characteristic p. Then $\mathrm{SKE}_n(k)$ is closed under composition.*

Acknowledgements. This research was supported by DAAD grant (funding program ID 57076385).

REFERENCES

[1] K. Adjamagbo, H. Derksen and A. van den Essen, *On polynomial maps in positive characteristic and the Jacobian conjecture*, report 9208, Univ. of Nijmegen, 1992.

[2] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progr. Math. 190, Birkhäuser, Basel, 2000.

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

[4] S. Maubach and A. Rauf, *The profinite polynomial automorphism group*, J. Pure Appl. Algebra 219 (2015), 4708–4727.

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

[6] I. R. Shafarevich, *On some infinite-dimensional groups*, Rend. Mat. e Appl. (5) 25 (1966), 208–212.

[7] I. R. Shafarevich, *On some infinite-dimensional groups. II*, Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), 214–226 (in Russian).

[8] I. Stampfli, *On the topologies on ind-varieties and related irreducibility questions*, J. Algebra 372 (2012), 531–541.

Stefan Maubach
Radboud University Nijmegen
Postbus 9010
6500 GL Nijmegen, The Netherlands
E-mail: S.Maubach@math.ru.nl

Abdul Rauf
Department of Mathematics
Jacobs University Bremen
Bremen, Germany
E-mail: a.rauf@jacobs-university.de