

THE LINEAR COORDINATE PRESERVING PROBLEM

SHENG-JUN GONG AND JIE-TAI YU

Abstract. We prove that every K -endomorphism of a rank two polynomial algebra over an algebraically closed field K of positive characteristic taking all linear coordinates to coordinates is an automorphism. We give a new characterization of coordinates of $K[t][x, y]$, where K is an algebraically closed field of any characteristic. We also explore the close connection between coordinates and permutation polynomials of finite fields.

1. Introduction and main results

Let R be a commutative ring. Recall a polynomial $p \in R[x_1, \dots, x_n]$ is a *coordinate* if there exists an R -automorphism ψ of $R[x_1, \dots, x_n]$ taking x_1 to p . A *linear coordinate* is a polynomial p with $\deg(p) = 1$.

In [6], van den Essen and Shpilrain raised the following natural

Problem 1.1 (Coordinate preserving problem). *Let P_n be the polynomial algebra of rank n over a field K . Is every K -endomorphism ϕ of P_n taking all coordinates of P_n to coordinates an automorphism?*

Problem 1.1 was solved affirmatively for $n = 2$ in [6]. Derksen (see [6]) observed that, for an algebraically closed field K , an endomorphism ϕ of P_n taking all linear coordinates to coordinates, has the property $\det J(\phi) \in K^*$. Based on that, Jelonek [7] gave a positive answer in any dimension to Problem 1.1 for algebraically closed fields of zero characteristic by means of algebraic geometry.

Motivated by Derksen's observation, Mikhalev, J.-T. Yu and Zolotykh [15], considered the following

2000 *Mathematics Subject Classification.* Primary 13B25, 13F20; Secondary 12E10, 12E20.

Key words and phrases. Coordinate preserving problem, linear coordinate preserving problem, Jacobian conjecture, endomorphism, automorphism, positive characteristic, permutation polynomial, finite fields.

Sheng-Jun Gong was partially supported by a University of Hong Kong Post-graduate Studentship.

Jie-Tai Yu was partially supported by an RGC-CERG Grant.

Problem 1.2 (Linear coordinate preserving problem). *Is every K -endomorphism of P_n taking all linear coordinates to coordinates an automorphism?*

By Derksen's observation, the Jacobian conjecture (see, for instance, [5], [14]) implies the positive answer for Problem 1.2 in zero characteristic.

In [15] the negative solution was given to Problem 1.2 for each $n > 2$ and all non-algebraically closed fields. For algebraically closed fields, Problem 1.2 remains open for $n > 2$.

For $n = 2$, the positive answer to Problem 1.2 was given in [2] for any field of zero characteristic. In [1], a negative answer was given by S.-T. Chan for all finite fields and $n = 2$. The negative solution in [1] was extended to some special kind of infinite fields of positive characteristic by X.-G. Liu [11].

In this paper, we give a positive solution for Problem 1.2 for all algebraically closed fields of positive characteristic when $n = 2$:

Theorem 1.3. *Let K be an algebraically closed field of positive characteristic, ϕ a K -endomorphism of $K[x, y]$ taking all linear coordinates to coordinates. Then ϕ is an automorphism.*

We also give a new characterization of coordinates of $K[t][x, y]$, where K is an algebraically closed field, based on the methodology of C.-M. Lam and J.-T. Yu [12]:

Theorem 1.4. *Let K be an algebraically closed field and $f(t, x, y) \in K[t][x, y]$. Then f is a coordinate of $K[t][x, y]$ if and only if the following two conditions are satisfied:*

- (1) $f(t, x, y)$ is a coordinate of $K(t)[x, y]$; and
- (2) For every $a \in K$, $f(a, x, y)$ is a coordinate of $K[x, y]$.

Finally, we explore the close connection between the linear coordinate preserving problem and permutation polynomials of finite fields and give an alternative proof of Theorem 1.3 for the 'purely algebraic' case.

2. Preliminaries

Lemma 2.1. *Let $R \subseteq S$ be commutative rings and φ be an R -endomorphism of $R[x, y]$ such that $\det J(\varphi) \in U(R)$. If φ is an S -automorphism of $S[x, y]$, then φ is also an R -automorphism of $R[x, y]$.*

See, for instance, van den Essen [5].

In the sequel all endomorphisms (automorphisms) are K -endomorphisms (K -automorphisms).

The following reduction result follows from the well-known theorem of Jung [8] and van der Kulk [9]: every automorphism of $K[x, y]$ is a product of elementary automorphisms (that is, the automorphisms preserving all variables except one).

Proposition 2.2. *Let f be a coordinate of $K[x, y]$. Suppose $\deg_x f = m$ and $\deg_y f = n$ with $n \geq m \geq 1$. Then: $d = n/m$ is an integer, and $f^{(d,1)} = \alpha(x + \beta y^d)^m$ for some $\alpha, \beta \in K^*$; Moreover, denote by $\phi = (x - \beta y^d, y)$, then $\deg_y(\phi(f)) < \deg_y f$ and $\deg_x(\phi(f)) = \deg_x f$.*

See, for instance, Drensky [3], for a proof.

In the sequel we denote by p a prime number, q a power of p , \mathbb{F}_q the finite field with q elements, $\mathbf{\Gamma}_p$ the algebraic closure of \mathbb{F}_p .

Let $K \subseteq L$ be a field extension. By the definition, it is obvious that a coordinate of $K[x, y]$ is also a coordinate of $L[x, y]$. In general, the converse is not true. For example, $x^p + ty^p + x \in \mathbb{F}_p(t)[x, y]$ is a coordinate of $\mathbb{F}_p(t^{\frac{1}{p}})[x, y]$, but not a coordinate of $\mathbb{F}_p(t)[x, y]$. However, if K is perfect, this is indeed the case. Recall that a field K is perfect if $\text{char}(K) = 0$ or $K = K^p$ when $\text{char}(K) = p$.

Lemma 2.3. *Let $K \subseteq L$ be perfect fields, $f \in K[x, y]$ a coordinate of $L[x, y]$. Then f is also a coordinate of $K[x, y]$.*

Proof. Let $\deg_y f = n$ and $\deg_x f = m$. The case $n = 0$ or $m = 0$ is trivial. Say, $n \geq m \geq 1$. By Proposition 2.2, $d = n/m$ is an integer and $f^{(d,1)} = \alpha(x + \beta y^d)^m$ for some $\alpha, \beta \in L^*$. The condition $f \in K[x, y]$ implies that $\alpha(x + \beta y^d)^m \in K[x, y]$. Now there are two cases:

- (1) If $\text{char}(K) = 0$, then we have $\beta \in K$ and $\alpha \in K$;
- (2) If $\text{char}(K) = p > 0$, suppose $m = p^k s$ for some $k, p \nmid s$, we have $\beta^{p^k} \in K$ and $\alpha \in K$. As K is perfect, we conclude $\beta \in K$.

Therefore one gets x by acting a sequence of elementary automorphisms of $K[x, y]$ to f inductively. Hence, f is a coordinate of $K[x, y]$. \square

Lemma 2.4. *Let L be a field of $\text{char}(L) = p$, $f \in L[x, y]$ a coordinate of $L[x, y]$. Then there exists a field K , finitely generated over the prime field \mathbb{F}_p , such that f is a coordinate over any field containing K .*

Proof. Let K be the field generated over \mathbb{F}_p by all the coefficients of the polynomials appearing in the sequence of elementary automorphisms taking f to x . Of course K is finitely generated. The same argument in the proof of Lemma 2.3 concludes that f is a coordinate of $K[x, y]$. \square

Remark 2.5. In particular, let $L = \mathbf{\Gamma}_p$, the algebraic closure of \mathbb{F}_p , since every subfield of $\mathbf{\Gamma}_p$ is perfect, by Lemma 2.3, we can choose K to be generated by all the coefficients of f . Apparently K is a finite field.

Recall the derivation $\Delta_f : K[x, y] \rightarrow K[x, y]$, associated with a polynomial $f(x, y) \in K[x, y]$ is defined by: $\Delta_f(g) = f_x g_y - f_y g_x$.

Lemma 2.6. *Let K be a field, $\varphi = (f(x, y), g(x, y))$ an automorphism of $K[x, y]$. Then*

- (1) *If $\text{char}(K) = 0$, $\text{Ker}(\Delta_f) = K[f]$.*
- (2) *If $\text{char}(K) = p$, $\text{Ker}(\Delta_f) = K[f, g^p]$.*

Proof. Let $a := \det J(\varphi) \in K^*$. Direct calculation shows that $\Delta_f(h) = a\Delta_{\varphi^{-1}(f)}(\varphi^{-1}(h))$ for any $h \in K[x, y]$. Hence $\text{Ker}(\Delta_f) = \varphi(\text{Ker}(\Delta_{\varphi^{-1}(f)}))$. On the other hand, it is easy to see that $\Delta_x(h) = h_y$. Hence $\text{Ker}\Delta_x = K[x]$ if $\text{char}(K) = 0$ and $\text{Ker}(\Delta_x) = K[x, y^p]$ if $\text{char}(K) = p > 0$. Then the conclusion follows from that $\varphi^{-1}(f) = x$ and $\varphi^{-1}(g) = y$. \square

Let A be an algebra over K . Denote by $C_A(a)$ the algebraic closure of a in A , i.e. the subalgebra of all elements algebraically dependent with a over K .

Lemma 2.7. *Let f be a coordinate of $K[x, y]$. Then for any $g \in K[f] \setminus K$, $C_{K[x, y]}(g) = K[f]$. In particular, for any $h(x) \in K[x] \setminus K$, we have $C_{K[x, y]}(h) = K[x]$.*

In the sequel we fix $K(t)$ to be a rational field over K . Let $f(x, y) \in K(t)[x, y]$ and write

$$f(x, y) = \sum_{i, j} \frac{a_{ij}(t)}{b_{ij}(t)} x^i y^j$$

where $a_{ij}(t), b_{ij}(t) \in K[t]$ and $b_{ij}(t) \neq 0$. We also assume that for any i, j , $(a_{ij}(t), b_{ij}(t)) = 1$.

We say an element $t_0 \in K$ is a *regular* point of $f(x, y)$ if t_0 is not a zero of any $b_{ij}(t)$, otherwise it is *irregular*. Moreover, we call t_0 is a *regular*

point of an endomorphism $\varphi = (f(x, y), g(x, y)) \in \text{Aut}(K(t)[x, y])$ if it is a regular point of both $f(x, y)$ and $g(x, y)$, otherwise it is called *irregular*.

Let t_0 be a regular point of a polynomial $f(x, y) \in K(t)[x, y]$, we use $f(t_0; x, y)$, or simply $f(t_0)$, to denote the substitution of $f(x, y)$ with $t = t_0$, which is a polynomial in $K[x, y]$. Similarly, denoted by $\varphi(t_0)$ for the endomorphism $(f(t_0; x, y), g(t_0; x, y))$ of $K[x, y]$ provided t_0 is a regular point of the endomorphism $\varphi = (f(x, y), g(x, y))$.

3. Technical lemmas

In this section, we prove several technical lemmas for coordinate substitution, which play crucial roles in the proofs of the main results.

Lemma 3.1. *Let K be an infinite perfect field and $f(x, y) \in K(t)[x, y]$, $f(a)$ a coordinate of $K[x, y]$ for infinitely many $a \in K$.*

- (1) *If $\text{char}(K) = 0$, then $f(x, y)$ is a coordinate of $K(t)[x, y]$.*
- (2) *If $\text{char}(K) = p$, then there exists some non-negative integer s such that $f(x, y)$ is a coordinate of $K(t^{\frac{1}{p^s}})[x, y]$.*

Proof. Let $\deg_y f = n$ and $\deg_x f = m$. The case $n = 0$ or $m = 0$ is trivial. So we may assume, say, $n \geq m \geq 1$. By the hypothesis, viewing $f(x, y)$ as a polynomial of x and y only, the leading coefficients belong to $K(t)$. And there are only finite possible values for a in which these two coefficients vanish or make no sense. So for infinitely many $a \in K$, $f(a)$ is a coordinate of $K[x, y]$ with $\deg_y f(a) = \deg_y f$ and $\deg_x f(a) = \deg_x f$. Denote by S the set of all the elements for a such that the substitution $t = a$ satisfies the above property. Clearly, S is an infinite set. Hence, by Proposition 2.2, $d = n/m$ is an integer and for all $a \in S$, $f(a)^{(d,1)} = \alpha(x + \beta y^d)^m$ with some $\alpha, \beta \in K^*$.

On the other hand, by the above arguments, we may write

$$f^{(d,1)} = a_0(t)(x^m + \sum_{i=1}^m b_i(t)x^{m-i}y^{di})$$

where $a_0(t), b_m(t) \in K(t) \setminus \{0\}$ and $b_i(t) \in K(t)$, $1 \leq i \leq m$. Comparing the coefficients of $f(a)^{(d,1)}$, $a \in S$, we get

$$a_0(a) = \alpha, b_i(a) = \binom{m}{i} \beta^i, 1 \leq i \leq m.$$

Observing for any $1 \leq i \leq m$,

$$\binom{m}{1}^i b_i(a) = \binom{m}{i} (b_1(a))^i.$$

Since S is infinite, this implies, as elements in $K(t)$,

$$\binom{m}{1}^i b_i(t) = \binom{m}{i} (b_1(t))^i$$

for any $0 \leq i \leq m$. Consider the following two cases:

(1) $b_1(t) \neq 0$. Since $\binom{m}{1}^m b_m(t) = (b_1(t))^m$, then we must have $\binom{m}{1} \neq 0$ and thus, $b_i(t) = (b_1(t))^i \binom{m}{i} / \binom{m}{1}^i$, $0 \leq i \leq m$. Hence $f^{(d,1)} = a_0(t)(x + b_1(t)/\binom{m}{1} y^d)^m$, where $a_0(t), b_1(t) \in K(t) \setminus \{0\}$.

(2) $b_1(t) = 0$. This can only happen when $\text{char}(K) = p > 0$ and $p \mid m$ since $\binom{m}{1}^m b_m(t) = (b_1(t))^m$. Write $m = p^l m_1$, where $l > 0$ and $p \nmid m_1$. Then for any $a \in S$, $f(a)^{(d,1)} = \alpha(x + \beta y^d)^m = \alpha(x^{p^l} + \beta^{p^l} y^{dp^l})^{m_1}$. Using the same arguments, we obtain that

$$b_i(t) = 0 \text{ for any } p^l \nmid i, \text{ and}$$

$$b_{p^l k}(t) = (b_{p^l}(t))^k \binom{m_1}{k} / \binom{m_1}{1}^k \neq 0, 0 \leq k \leq m_1.$$

Hence

$$f^{(d,1)} = a_0(t)(x^{p^l} + b_{p^l}(t)/\binom{m_1}{1} y^{dp^l})^{m_1} = a_0(t)(x + b'_{p^l}(t)^{\frac{1}{p^l}} y^d)^m,$$

where $b'_{p^l}(t) \in K(t) \setminus \{0\}$ satisfies $(b'_{p^l}(t)^{\frac{1}{p^l}})^{p^l} = b_{p^l}(t)/\binom{m_1}{1}$. Note here we need to use the condition that K is perfect (hence $K^p = K$).

Combining the above two cases, $f^{(d,1)}$ is of the form $A(t)(x + B(t)y^d)^m$ or $A(t)(x + B(t)^{\frac{1}{p^l}} y^d)^m$ for some $l \geq 0$ and $A(t), B(t) \in K(t) \setminus \{0\}$. Denote by $\phi = (x - B(t)y^d, y)$ or $(x - B(t)^{\frac{1}{p^l}} y^d, y)$ and we consider the polynomial $\phi(f)$ instead. Repeating the same arguments, eventually we will get x after a sequence of elementary automorphisms. This implies that $f(x, y)$ is a coordinate of $K(t)[x, y]$ or $K(t^{\frac{1}{p^s}})[x, y]$ for some non-negative integer s . \square

For $R = K, K(t), K[t]$, denote by $R^0[x, y]$ the augmentation ideal of $R[x, y]$, i.e., the sets of polynomials without constant terms. Similarly, we use $\text{Aut}^0 R[x, y]$ to denote the subgroup of augmentation preserving automorphisms of $\text{Aut}(R[x, y])$, that is, automorphisms of the form

$(f(x, y), g(x, y))$ where the polynomials $f(x, y)$ and $g(x, y)$ have zero constant terms. It is easy to see that every automorphism ψ of $R[x, y]$ can be decomposed as $\tau \circ \varphi$, where $\tau = (x + a, y + b)$ for some $a, b \in R$ and $\varphi = (f, g) \in \text{Aut}^0 R[x, y]$. Hence, it is sufficient to study the automorphisms and coordinates in this form.

Recall that a polynomial $0 \neq f(x, y) \in K[t]^0[x, y]$ is *primitive* if the coefficients of f are relatively prime in $K[t]$.

In the sequel we call $f(x, y) \in K[t]^0[x, y]$ a *primitive coordinate* of $K(t)[x, y]$ if it is a coordinate in $K(t)^0[x, y]$ and a primitive polynomial in $K[t]^0[x, y]$. Moreover, we call an automorphism $\varphi = (f(x, y), g(x, y))$ a *primitive automorphism* if both $f(x, y)$ and $g(x, y) \in K[t]^0[x, y]$ are primitive coordinates.

Lemma 3.2. *Let K be a field, $\varphi = (f(x, y), g(x, y))$ a primitive automorphism of $K(t)^0[x, y]$, t_0 an element in K such that $\det J(f, g)(t_0) = 0$. Then $f(t_0)$ and $g(t_0)$ are algebraically dependent over K .*

Proof. We may assume $t_0 = 0$ and $\det J(f, g) \in K[t] \setminus \{0\}$. Let the inverse automorphism of $\varphi = (f, g)$ be $\psi = (p(x, y), q(x, y))$ with

$$p(x, y) = (\sum_{i \geq 1} b_i(x, y)t^i + b_0(x, y))/(t^a h(t))$$

for some $a \geq 0$, where $b_i(x, y) \in K^0[x, y]$, $i \geq 0$ and $p(t) \in K[t]$, $p(0) \neq 0$. We may assume the right side of the above equality is reduced, hence a is uniquely determined. Now we have two cases:

- (a) $a = 0$, then 0 is a regular point of $p(x, y)$;
- (b) $a > 0$, since $(p, q) \circ (f, g) = (x, y)$, $b_0(f, g)(0) = b_0(f(0), g(0)) = 0$. We claim that $b_0(x, y)$ involves both x and y : If $b_0(x, y) \in K[x]$, then $b_0(f, g)(0) = b_0(f(0)) \neq 0$, by reducibility it forces $a = 0$. Similarly $b_0(x, y) \notin K[y]$. Therefore $b_0(f(0), g(0)) = 0$ implies that $f(0)$ and $g(0)$ are algebraically dependent.

Similarly, we write $q(x, y) = (\sum_{i \geq 1} b'_i(x, y)t^i + b'_0(x, y))/(t^b h'(t))$ as above. Note that, if $a = b = 0$, then 0 is a regular point of both $p(x, y)$ and $q(x, y)$. Therefore $(p(0), q(0))$ and $(f(0), g(0))$ are both automorphisms of $K[x, y]$. If $\det J(f, g)(0) = 0$, then obviously $\varphi(0) = (f(0), g(0))$ is not an automorphism. So we must have $a > 0$ or $b > 0$. Without loss of generality, we may assume that $a > 0$. Then the polynomial $b_0 \in K[x, y]$ gives an algebraic dependence of $f(0)$ and $g(0)$. Hence $f(0)$ and $g(0)$ are algebraically dependent. \square

Lemma 3.3. *Let K be an arbitrary field, $f \in K[x, y]$ such that $f + t^m x$ is a coordinate of $K[t][x, y]$ for some positive integer m . Then (f, x) is an automorphism of $K[x, y]$.*

Proof. We may assume that $f(x, y) \in K^0[x, y]$. Let ψ be a primitive automorphism of $K[t]^0[x, y]$ such that $\psi(x) = f(x, y) + t^m x$. Write

$$\psi(y) = g_0(x, y) + g_1(x, y)t + \cdots + g_n(x, y)t^n,$$

where $g_i(x, y) \in K^0[x, y]$, $0 \leq i \leq n$. We claim $g_i(x, y) \in K[x, f(x, y)]$ for any $0 \leq i \leq n$.

To see that, we consider the endomorphism $\phi = (f', g')$, where

$$\begin{aligned} f' &= t^m f(x, y) + x, \text{ and} \\ g' &= t^n g_0(x, y) + t^{n-1} g_1(x, y) + \cdots + t g_{n-1}(x, y) + g_n(x, y). \end{aligned}$$

Observe that it is a primitive automorphism of $K(t)^0[x, y]$ (which can be obtained by replacing t by $1/t$ in $\psi(x)$, then multiplying the first coordinate by t^m , and the second coordinate by t^n) and $t^{n+m} \mid \det J(\phi(t))$ in $K[t]$. So $\det J(\phi(0)) = 0$ and by Lemma 3.2, $f'(0)$ and $g'(0)$ are algebraically dependent. By Lemma 2.7, $g_n(x, y) \in C_{K[x, y]}(x) = K[x]$. Hence $g_n(x, y) = h(x)$ for some $h(x) \in K[x]$ and consider the endomorphism $\phi' = (f', \frac{g' - h(f')}{t})$. Write

$$\frac{g' - h(f')}{t} = \cdots + t^{n-1} g'_0(x, y) + t^{n-2} g'_1(x, y) + \cdots + g'_{n-1}(x, y).$$

Here the first ‘ \cdots ’ denote the terms whose degrees, respect to t , are greater than $(n-1)$. Similarly $g'_{n-1}(x, y) \in C_{K[x, y]}(x) = K[x]$. Observe that

$$\begin{aligned} g'_{n-1}(x, y) - g_{n-1}(x, y) &= \left\{ \frac{[g' - h(f')] - [g' - h(x)]}{t} \right\} (t = 0) \\ &= \frac{h(x) - h(f')}{t} (t = 0) \in K[x, f(x, y)]. \end{aligned}$$

Hence $g_{n-1}(x, y) \in K[x, f(x, y)]$. By inductive arguments, eventually we obtain that $g_i(x, y) \in K[x, f(x, y)]$ for all $0 \leq i \leq n$. In particular, $g_0(x, y) \in K[x, f(x, y)]$. On the other hand, as ψ is an automorphism of $K[t][x, y]$, $\psi(0) = (f(x, y), g_0(x, y))$ is an automorphism of $K[x, y]$. Therefore $K[f(x, y), g_0(x, y)] = K[x, y]$. We have $K[x, y] = K[f(x, y), g_0(x, y)] \subseteq K[x, f(x, y)] \subseteq K[x, y]$. It follows that $K[x, f(x, y)] = K[x, y]$. Therefore, $(f(x, y), x)$ is an automorphism of $K[x, y]$. \square

Remark 3.4. The above proof, as well as the proof of Theorem 1.4 in the next section, is motivated by the methodology of C.-M. Lam and J.-T. Yu [12] where it is used to produce an algorithm to determine coordinates of $\mathbb{Z}[x, y]$.

4. Proof of the main results

Proof of Theorem 1.4. The ‘only if’ part is obvious. For the ‘if’ part, we may assume that $f(x, y) \in K[t]^0[x, y]$ is primitive. Since $f(x, y)$ is a coordinate of $K(t)[x, y]$, then there exists a polynomial $g(x, y) \in K[t]^0[x, y]$ to be a coordinate mate of $f(x, y)$.

If $\det J(f, g) \in K^*$. By Lemma 2.1, (f, g) is an automorphism of $K[t][x, y]$ and hence, f is a coordinate of $K[t][x, y]$. So we may assume $\Delta_f(g) = \det J(f, g) \in K[t] \setminus K$.

As K is algebraically closed, there exists a zero $t_0 \in K$, of $\Delta_f(g)$. We claim that there exists a polynomial $h(x) \in K[x]$ such that $g(t_0) = h(f(t_0))$. The hypothesis implies that $f(t_0)$ is a coordinate of $K[x, y]$. Let $v(x, y) \in K[x, y]$ be a coordinate mate of $f(t_0)$. Since $\Delta_{f(t_0)}(g(t_0)) = \det J(f(t_0), g(t_0)) = 0$, by Lemma 2.6, we have $g(t_0) = h(f(t_0), v(x, y)^p)$ for some polynomial $h(x, y) \in K[x, y]$. On the other hand, by Lemma 3.2, $f(t_0)$ and $g(t_0)$ are algebraically dependent. This forces that $g(t_0) = h(f(t_0))$ for some $h(x) \in K[x]$.

Set $g_1 := \frac{g-h(f)}{t-t_0}$. Then $g_1 \in K[t][x, y]$ and $\det J(f, g_1) = \frac{\Delta_f(g)}{t-t_0}$. Repeating the same process inductively, eventually we would obtain some $g_m \in K[t][x, y]$ such that $\det J(f, g_m) \in K^*$ and hence, by Lemma 2.1, (f, g_m) is an automorphism. Therefore f is a coordinate of $K[t][x, y]$ \square .

Remark 4.1. The condition that ‘ K is algebraically closed’ is essential for the above theorem since the conclusion no longer holds for non-algebraically closed fields. For example, let \mathbb{R} be the real number field, then $x^2 + (t^2 + 1)y$ is coordinate of $\mathbb{R}(t)[x, y]$ and for any $a \in \mathbb{R}$, $x^2 + (a^2 + 1)y$ is a coordinate of $\mathbb{R}[x, y]$. However, it is not a coordinate of $\mathbb{R}[t][x, y]$.

Note that for $\text{char}(K) = 0$, Drensky and J.-T. Yu ([4]) obtained another characterization for the coordinates of $K[t][x, y]$.

Proof of Theorem 1.3. Let $\varphi = (f, g)$ be an endomorphism of $K[x, y]$ taking each linear coordinate to a coordinate. After acting an automorphism, we may assume that $g = x$.

Since algebraically closed fields are infinite and perfect, by Lemma 3.1, $f(x, y) + tx$ is a coordinate of $K(t^{\frac{1}{p^s}})[x, y]$ for some $s \geq 0$. Hence $f(x, y) + t^{p^s}x$ is a coordinate of $K(t)[x, y]$. As K is algebraically closed, and $f(x, y) + c^{p^s}x$ is a coordinate of $K[x, y]$ for all $c \in K$ by hypothesis,

by Theorem 1.4, $f(x, y) + t^p x$ is a coordinate of $K[t][x, y]$. By Lemma 3.3, $\varphi = (f(x, y), x)$ is an automorphism of $K[x, y]$ \square .

5. Coordinates and permutation polynomials

In this section, we explore the close connection between coordinate preserving problem and permutation polynomials of finite fields, and give an alternative proof of Theorem 1.3 for the ‘purely algebraic’ case. First we need some backgrounds about permutation polynomials. We follow the standard reference Lidl and Niederreiter [10].

A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of \mathbb{F}_q if the associated polynomial function $f : c \mapsto f(c)$ from \mathbb{F}_q into \mathbb{F}_q is a permutation of \mathbb{F}_q . Obviously, if f is a permutation polynomial of \mathbb{F}_q , then the equation $f(x) = a$ has exactly one solution in \mathbb{F}_q for each $a \in \mathbb{F}_q$. Thus we are led to the following definition of permutation polynomials in several variables:

Definition 5.1. Let $n \geq 1$ and $\mathbb{F}_q[x_1, \dots, x_n]$ be the ring of polynomials in n variables over \mathbb{F}_q . A polynomial $f \in \mathbb{F}_q[x_1, \dots, x_n]$ is called a permutation polynomial in n variables over \mathbb{F}_q if the equation $f(x_1, \dots, x_n) = a$ has q^{n-1} solutions in \mathbb{F}_q^n for each $a \in \mathbb{F}_q$.

In the case $n > 1$ we cannot use the interpretation that a permutation polynomial $f(x_1, \dots, x_n)$ over \mathbb{F}_q induces a permutation of \mathbb{F}_q^n , because the associated mapping is not a mapping from \mathbb{F}_q^n into itself. The next definition, however, enables us to consider functions from \mathbb{F}_q^n into \mathbb{F}_q^n induced by systems of polynomials in several variables.

Definition 5.2. A system of polynomials $\{f_1, \dots, f_n\} \subset \mathbb{F}_q[x_1, \dots, x_n]$, is called orthogonal in \mathbb{F}_q if the systems of equations

$$f_1(x_1, \dots, x_n) = a_1, \dots, f_n(x_1, \dots, x_n) = a_n$$

has exact one solution in \mathbb{F}_q^n for each $(a_1, \dots, a_n) \in \mathbb{F}_q^n$.

In [10] a necessary and sufficient condition for a system of polynomials to be orthogonal is given:

Proposition 5.3. *The system $\{f_1, \dots, f_n\} \in \mathbb{F}_q[x_1, \dots, x_n]$, is orthogonal in \mathbb{F}_q if and only if for all $(b_1, \dots, b_n) \in \mathbb{F}_q^n$ with $(b_1, \dots, b_n) \neq (0, \dots, 0)$, the polynomial $b_1 f_1 + \dots + b_n f_n$ is a permutation polynomial over \mathbb{F}_q .*

Lemma 5.4. *Let $\{f(x_1, \dots, x_n), x_1, \dots, x_{n-1}\}$ be an orthogonal system of \mathbb{F}_q . Then for any $(a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{n-1}$, $f(a_1, \dots, a_{n-1}, y)$ is a permutation polynomial in one variable in \mathbb{F}_q .*

Proof. According to the definition of orthogonal systems, for any $b \in \mathbb{F}_q$, the system of equations

$$f(x_1, \dots, x_n) = b, x_1 = a_1, \dots, x_{n-1} = a_{n-1}$$

has one solution in \mathbb{F}_q^n . It implies that the equation $f(a_1, \dots, a_{n-1}, y) = b$ has exactly one solution in \mathbb{F}_q . Therefore, $f(a_1, \dots, a_{n-1}, y)$ is a permutation polynomial in one variable over \mathbb{F}_q . \square

In terms of permutation polynomials, we have following necessary (but not sufficient) condition for coordinates.

Lemma 5.5. *Every coordinate of $\mathbb{F}_q[x_1, \dots, x_n]$ induces a permutation polynomial of \mathbb{F}_q .*

Proof. Let f be a coordinate of $\mathbb{F}_q[x_1, \dots, x_n]$, then there exists an automorphism φ such that $\varphi(f) = x_1$. It is easy to see that φ , as an induced mapping from \mathbb{F}_q^n to itself, is bijective. For any $a \in \mathbb{F}_q$, there is a one-to-one corresponding between the solutions of the equation $f = a$ and of the equation $\varphi(f) = a$. Indeed, if (x_1, \dots, x_n) is a solution of the equation $f = a$, then $(\varphi^{-1}(x_1), \dots, \varphi^{-1}(x_n))$ is a solution of $\varphi(f) = a$. Therefore the number of the solutions of $f = a$ in \mathbb{F}_q equals to that of $\varphi(f) = x_1 = a$, which is exactly q^{n-1} . This implies that f is a permutation polynomial of \mathbb{F}_q . \square

Obviously, a coordinate f of $\mathbb{F}_q[x_1, \dots, x_n]$ is also a coordinate of the polynomial algebra over any finite extension of \mathbb{F}_q . Thus, by Lemma 5.5, we obtain the following

Lemma 5.6. *A coordinate of $\mathbb{F}_q[x_1, \dots, x_n]$ induces a permutation polynomial of every finite extension of \mathbb{F}_q .*

The polynomials of one variable over \mathbb{F}_q that are permutation polynomials of all finite extensions of \mathbb{F}_q are characterized by the following result in [10], which is crucial in this section.

Proposition 5.7. *A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of all finite extensions of \mathbb{F}_q if and only if it is of the form $f(x) = ax^{p^h} + b$, where $a \neq 0$, and h is a non-negative integer.*

The following lemma, which demonstrates the close connection between permutation polynomials and the linear coordinate preserving problem, is a consequence of Proposition 5.3 and Lemma 5.5.

Lemma 5.8. *Let $\varphi = (f_1, \dots, f_n)$ be an endomorphism of $\mathbb{F}_q[x_1, \dots, x_n]$ taking all linear coordinates to coordinates. Then $\{f_1, \dots, f_n\}$ form an orthogonal system of \mathbb{F}_q .*

Now we are ready to present

An alternative proof of Theorem 1.3 for the algebraic closure Γ_p of \mathbb{F}_p .

(1) Let $\phi = (f, g)$ be an endomorphism of Γ_p which takes all linear coordinates to coordinates. After acting an automorphism, we may assume that $g = x$.

(2) Write $f = f_n y^n + f_{n-1} y^{n-1} + \dots + f_1 y + f_0$, where $f_i \in \Gamma_p[x]$ for all i and $f_n \neq 0$. Then $f + cx$ is a coordinate of $\Gamma_p[x, y]$ for any $c \in \Gamma_p$. It follows that $n = \deg_y f > 0$ and by McKay and S.S.-S.Wang [13], $f_n \in K^*$.

(3) Let K_0 be the finite field in Remark 2.5. We claim that:

For any $c \in \Gamma_p$, $f(c, y)$ is a permutation polynomial of finite extension of the finite field $K_0(c)$.

To see this, let K_1 be any finite extension of $K_0(c)$, then $b_1 f + b_2 x$ is a coordinate of $K_1[x, y]$ for any $b_1, b_2 \in K_1$, $(b_1, b_2) \neq (0, 0)$. By Lemma 5.8, $\{f, x\}$ is an orthogonal system in K_1 and thus, by Lemma 5.4, $f(c, y)$ is a permutation polynomial of K_1 . Applying Proposition 5.7, we obtain that

$$f(c, y) = f_n y^n + f_{n-1}(c) y^{n-1} + \dots + f_1(c) y + f_0(c) = ay^{p^h} + b,$$

for some $a \neq 0$, $b \in K_0(c)$ and some non-negative integer h . It implies that

$$n = p^h, f_n = a, \text{ and } f_{n-1}(c) = \dots = f_1(c) = 0$$

for any $c \in \Gamma_p$. Since Γ_p is infinite, we must have $f_{n-1}(x) = \dots = f_1(x) \equiv 0$. Hence $f = ay^{p^h} + f_0(x)$. The condition $f + cx$ is a coordinate for any $c \in \Gamma_p$ forces that $h = 0$ and, thus, $f = ay + f_0(x)$. Therefore, $\phi = (ay + f_0(x), x)$ is an automorphism. \square

6. Acknowledgements

Jie-Tai Yu is grateful to the Tata Institute for Fundamental Research, the University of California at San Diego, the University of Science and Technology of China, Chinese Academy of Sciences, Peking University, and the Institut des Hautes Études Scientifiques for warm hospitality during his visit when he spent some time for this work. The authors

also thank V. Drensky, L. Makar-Limanov and V. Shpilrain for helpful comments and suggestions.

REFERENCES

- [1] S. -T. Chan, M.Phil Thesis, The University of Hong Kong, 2001.
- [2] C. C. Cheng, A. Van den Essen, *Endomorphisms of the plane sending linear coordinates to coordinates*, Proc. Amer. Math. Soc. **128** (2000), 1911-1915.
- [3] V.Drensky, *Free Algebras and PI-Algebras: Graduate Course in Algebra*, Springer-Verlag, Singapore, 2000.
- [4] V.Drensky, J. -T. Yu, *Tame and wild coordinates of $K[z][x, y]$* , Trans. Amer. Math. Soc. **353** (2001), 519-537.
- [5] A.van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Mathematics **190**, Birkhäuser-Verlag, Basel-Boston-Berlin, 2000.
- [6] A.van den Essen, V. Shpilrain, *Some combinatorial questions about polynomial mappings*, J. Pure Appl. Algebra **119** (1997), 47-52.
- [7] Z. Jelonek, *A solution of the problem of van den Essen and Shpilrain*, J. Pure Appl. Algebra **137** (1999), 49-55.
- [8] H.W.E.Jung, *Über ganze birationale Transformationen der Ebene*, J. Reine Angew. Math. **184** (1942), 161–174.
- [9] W. van der Kulk, *On polynomial rings in two variables*, Nieuw Arch. Wisk **1** (1995), 33-41.
- [10] R.Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [11] X.-G. Liu, Private communication, 2004.
- [12] C.-M.Lam, J.-T.Yu, *Tame and wild coordinates of $\mathbb{Z}[x, y]$* , J. Algebra **279** (2004), 425-436.
- [13] J. H. McKay, S. S. -S. Wang, *An inversion formula for two polynomials in two variables*, J. Pure Appl. Algebra **40** (1986), 245-257.
- [14] A. A. Mikhalev, V. Shpilrain, J. -T. Yu, *Combinatorial Methods: Free Groups, Polynomials, and Free Algebras*, CMS Books in Mathematics, Springer New York, 2004.
- [15] A. A. Mikhalev, J. -T. Yu, A. A. Zolotykh, *Images of coordinate polynomials*, Algebra Colloquium **4** (1997), 159-162.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF HONG KONG, POKFULAM ROAD, HONG KONG SAR, CHINA
E-mail address: `sjgong@hkusua.hku.hk`

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF HONG KONG, POKFULAM ROAD, HONG KONG SAR, CHINA
E-mail address: `yujt@hkucc.hku.hk`, `yujietai@yahoo.com`