DEMONSTRATIO MATHEMATICA
Vol. XLV No 4 2012

Zbigniew Jelonek

SOLVING POLYNOMIAL EQUATIONS

Abstract. Let k be a field and $f : k^n \to k^n$ be a polynomial isomorphism. We give a formula for f^{-1}. In particular we show how to solve the equation $f = 0$.

1. Introduction

Many processes in economy, engineering, or biological sciences are described by real or complex polynomial equations. Moreover, such equations (over fields of positive characteristic) play important role in a modern cryptography.

From this point of view it is interesting and important to have an algorithm to solve a system of such equations. Let us fix a field k and number $n \in \mathbb{N}$. Here we consider a system of polynomials $f = (f_1, \ldots, f_n) : k^n \to k^n$ with additional assumption that f is a polynomial isomorphism. Such systems are important in cryptography. There is a well known formula based on Gröbner basis to compute the inverse of f (see e.g. [2], p. 66), however this kind of formulas are not convenient for effective computations.

Here, we give a different formula (which seems to be effective in many cases) to invert f and to solve equation $f = 0$. Such a formula was well-known in the characteristic zero (see e.g. [1]). The new ingredient is a proof that this formula is still valid in positive characteristic.

2. Polynomial isomorphisms.

Here, we recall basic properties of polynomial isomorphisms. If f is a polynomial isomorphism and $g = f^{-1}$ is a polynomial inverse of f, then $f \circ g = identity$. Consequently $Jac(f)Jac(g) = 1$. Since we can extend both mappings f and g to algebraic closure of k, we see that $Jac(f) = const$. Now

2000 *Mathematics Subject Classification*: 12, 14.
Key words and phrases: polynomial mappings, polynomial equations, polynomial isomorphis.
This paper is supported by the research project 0 R 00 0043 07, 2009–2011.

it is easy to compute $Jac(f)$ – it is enough to compute Jacobian of linear parts of f_i. If $Jac(f) = 1$ we say that f is normalized. For our purposes we can always assume that f is normalized. Now we show how to estimate the degree of f^{-1}. We start with the Perron Theorem (see [4], Satz 57, p. 129, for the classical version and [3] for short modern proof):

Theorem 2.1. (Perron Theorem) *Let k be a field and let $Q_1, \ldots, Q_{n+1} \in k[x_1, \ldots, x_m]$ be non-constant polynomials with $\deg Q_i = d_i$. If the mapping $Q = (Q_1, \ldots, Q_{n+1}) : k^{n+1} \to k^{n+1}$ is generically finite, then there exists a non-zero polynomial $W(T_1, \ldots, T_{n+1}) \in k[T_1, \ldots, T_{n+1}]$ such that*

(a) $W(Q_1, \ldots, Q_{n+1}) = 0$,
(b) $\deg W(T_1^{d_1}, T_2^{d_2}, \ldots, T_{n+1}^{d_{n+1}}) \leq \prod_{j=1}^{n+1} d_j$.

Now we have the following basic and well-known fact:

Theorem 2.2. *Let $f : k^n \to k^n$ be a polynomial isomorphism. Let $\deg f_i = d_i$, where $d_1 \geq d_2 \geq \cdots \geq d_n$. If $g = (g_1, \ldots, g_n) = f^{-1}$, then $\max_{i=1}^{n} \deg g_i \leq \prod_{j=1}^{n-1} d_j$.*

Proof. For the sake of completeness we give a proof of this theorem. Fix a number $1 \leq i \leq n$. Apply Theorem 2.1 to the polynomials $f_1, \ldots, f_n$ and x_i. Thus there exists a non-zero polynomial $W(X, T_1, \ldots, T_n) \in k[X, T_1, \ldots, T_n]$ such that

$$W(x_i, f_1, \ldots, f_n) = 0 \quad \text{and} \quad \deg W(X, T_1^{d_1}, T_2^{d_2}, \ldots, T_n^{d_n}) \leq \prod_{j=1}^{n} d_j.$$

Since the mapping $f = (f_1, \ldots, f_n)$ is an isomorphism with inverse g, we have $x_i = g_i(f_1, \ldots, f_n)$. Hence a polynomial $P(X, T) = X - g_i(T_1, \ldots, T_n)$ is a minimal polynomial of x_i over $k[f_1, \ldots, f_n]$. By the minimality of P, we have $P(X, T) | W(X, T)$, in particular

$$\deg P(X, T_1^{d_1}, T_2^{d_2}, \ldots, T_n^{d_n}) \leq \prod_{j=1}^{n} d_j.$$

Since $P(X, T) = X - g_i(T_1, \ldots, T_N)$ we conclude that

$$\deg g_i(T_1^{d_1}, T_2^{d_2}, \ldots, T_n^{d_n}) \leq \prod_{j=1}^{n} d_j$$

and consequently $\deg g_i \leq \prod_{j=1}^{n-1} d_j$. ∎

3. Derivations

We start with:

Definition 3.1. Let L be a k-linear operator $L : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$. We say that L is a derivation if $L(fg) = L(f)g + fL(g)$.

It is easy to see that a derivation is determined by its values on variables $x_1, \dots, x_n$. Moreover derivations $\frac{\partial}{\partial x_i}$ generate the module of derivations over $k[x_1, \dots, x_n]$, i.e., every derivation L has the form

$$L = \sum_{i=1}^{n} A_i(x) \frac{\partial}{\partial x_i},$$

where A_i are polynomials. Now consider the derivation $S_i = \frac{\partial}{\partial x_i}$. Note that

$$S_i^a(x_i^m) = \frac{m!}{(m-a)!} x_i^{m-a} = a! C_m^a x_i^{m-a}.$$

Take $S_i^a/a!(x_i^m) = C_m^a x_i^{m-a}$ and $S_i^a/a!(x_j^m) = 0$ for $j \neq i$. In this way we can define the operator $S_i^a/a!$ over every field. We have the following:

Theorem 3.2. (Taylor formula) *Let k be a field of any characteristic. Let $F \in k[x_1, \dots, x_n]$. Then for $b = (b_1, \dots, b_n) \in k^n$ we have*

$$F(x_1, \dots, x_n) \\ = \sum_{|\alpha| \leq \deg\ F} \frac{S_1^{\alpha_1}}{\alpha_1!} \frac{S_2^{\alpha_2}}{\alpha_2!} \dots \frac{S_n^{\alpha_n}}{\alpha_n!} (F)(b)(x_1 - b_1)^{\alpha_1} (x_2 - b_2)^{\alpha_2} \dots (x_n - b_n)^{\alpha_n},$$

where $|\alpha| = \alpha_1 + \dots + \alpha_n$.

Proof. If $\operatorname{char} k = 0$, the result is well-known. Assume that $\operatorname{char} k = p > 0$. Let

$$F(x_1, \dots, x_n) = \sum_{|\alpha| \leq \deg F} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

and let $\mathbb{F}_p(\{a_\alpha\}_{|\alpha| \leq \deg F})$ be a field generated by all coefficients of F. Now choose real numbers $\{b_\alpha\}_{|\alpha| \leq \deg F}$ and $b'_1, \dots, b'_n$, which form purely transcendental system over $\mathbb{Q}$. We have an epimorphism

$$\pi : \mathbb{Z}[\{b_\alpha\}_{|\alpha| \leq \deg F}, \{b'_k\}] \to \mathbb{F}_p(\{a_\alpha\}_{|\alpha| \leq \deg F}, \{b_k\}),$$

which induces the epimorphism

$$\pi' : \mathbb{Z}[\{b_\alpha\}_{|\alpha| \leq \deg F}, \{b'_k\}][x_1, \dots, x_n] \to \mathbb{F}_p(\{a_\alpha\}_{|\alpha| \leq \deg F}, \{b_k\})[x_1, \dots, x_n].$$

It is easy to see that π' commutes with every derivation $D^a/a!$. Now take

$$F'(x_1, \dots, x_n) = \sum_{|\alpha| \leq \deg F} b_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}.$$

Note that $\pi'(F') = F$ and $\pi'(b') = b$. Over $\mathbb{R}$ we have a classical Taylor formula:

$$F'(x_1,\dots,x_n) = \sum_{|\alpha|\le \deg F} \frac{S_1^{\alpha_1}}{\alpha_1!}\frac{S_2^{\alpha_2}}{\alpha_2!}\dots\frac{S_n^{\alpha_n}}{\alpha_n!}(F')(b')(x_1-b_1')^{\alpha_1}(x_2-b_2')^{\alpha_2}\dots(x_n-b_n')^{\alpha_n}.$$

Now it is enough to apply π to both sides of this equation. ∎

Proposition 3.3. *Let $f=(f_1,\dots,f_n)$ be a normalized polynomial isomorphism. Then*

$$\frac{\partial}{\partial f_i} = \sum A_{ij}\frac{\partial}{\partial x_j},$$

where

$$A_{ij} = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \dots & \frac{\partial f_1}{\partial x_{j-1}} & 0 & \frac{\partial f_1}{\partial x_{j+1}} & \dots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \dots & \frac{\partial f_2}{\partial x_{j-1}} & 0 & \frac{\partial f_2}{\partial x_{j+1}} & \dots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ \frac{\partial f_i}{\partial x_1} & \frac{\partial f_i}{\partial x_2} & \dots & \frac{\partial f_i}{\partial x_{j-1}} & 1 & \frac{\partial f_i}{\partial x_{j+1}} & \dots & \frac{\partial f_i}{\partial x_n} \\ \vdots & \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \dots & \frac{\partial f_n}{\partial x_{j-1}} & 0 & \frac{\partial f_n}{\partial x_{j+1}} & \dots & \frac{\partial f_n}{\partial x_n} \end{vmatrix}.$$

Proof. Let $D_i = \frac{\partial}{\partial f_i}$. Derivation D_i is uniquely determined by conditions

$$D_i(f_j) = \delta_{ij}$$

where δ_{ij} is the Kronecker delta. This leads to the following system of linear equations:

$$\sum A_{ik}\frac{\partial f_j}{\partial x_k} = \delta_{ij},$$

$j=1,\dots,n$. Now it is enough to solve this system using the Cramer rules (note that the Jacobian of f is one). ∎

In the sequel we need a generalized version of this Proposition. We have:

Proposition 3.4. *Let k be a domain. Let $(f_1,\dots,f_n)\subset k[x_1,\dots,x_n]$ be a system of algebraically independent polynomials. Let $\delta = det[\frac{\partial f_i}{\partial x_k}]$. Then there exists a derivation D_i' on the ring $k[x_1,\dots,x_n]_\delta$, which coincides on the subring $k[f_1,\dots,f_n]$ with $D_i = \frac{\partial}{\partial f_i}$. Moreover we have*

$$D_i' = 1/\delta\sum A_{ij}\frac{\partial}{\partial x_j},$$

where

$$A_{ij} = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_{j-1}} & 0 & \frac{\partial f_1}{\partial x_{j+1}} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_{j-1}} & 0 & \frac{\partial f_2}{\partial x_{j+1}} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ \frac{\partial f_i}{\partial x_1} & \frac{\partial f_i}{\partial x_2} & \cdots & \frac{\partial f_i}{\partial x_{j-1}} & 1 & \frac{\partial f_i}{\partial x_{j+1}} & \cdots & \frac{\partial f_i}{\partial x_n} \\ \vdots & \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_{j-1}} & 0 & \frac{\partial f_n}{\partial x_{j+1}} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix}.$$

Proof. Exactly as in Proposition 3.3 we get:

$$D_i' = \frac{\partial}{\partial f_i} = 1/\delta \sum A_{ij}' \frac{\partial}{\partial x_j},$$

where

$$A_{ij}' = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_{j-1}} & 0 & \frac{\partial f_1}{\partial x_{j+1}} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_{j-1}} & 0 & \frac{\partial f_2}{\partial x_{j+1}} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ \frac{\partial f_i}{\partial x_1} & \frac{\partial f_i}{\partial x_2} & \cdots & \frac{\partial f_i}{\partial x_{j-1}} & 1 & \frac{\partial f_i}{\partial x_{j+1}} & \cdots & \frac{\partial f_i}{\partial x_n} \\ \vdots & \vdots & \cdots & \vdots & 0 & \vdots & \cdots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_{j-1}} & 0 & \frac{\partial f_n}{\partial x_{j+1}} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix}$$

and $\delta = \det[\frac{\partial f_i}{\partial x_k}]$. The derivation D_i' is the derivation of the ring $k[x_1, \ldots, x_n]_\delta$. Moreover, we have $D_i'(f_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta. Since a derivation is uniquely determined by its values on generators, we have that D_i' on $k[f_1, \ldots, f_n]$ coincides with $D_i = \frac{\partial}{\partial f_i}$. ∎

Remark 3.5. The crucial point here is that even if a polynomial $g \in k[f_1, \ldots, f_n]$ is given as a sum (of polynomials from $k[x_1, \ldots, x_n]$) $g = g_1 + g_2$, where $g_i \notin k[f_1, \ldots, f_n]$ we have still $D_i(g) = D_i'(g_1) + D_i'(g_2)$.

We also need a following obvious observation:

Proposition 3.6. *Let k be a domain of characteristic zero. Assume that $I \subset k$ is an ideal. If D is a k-linear derivation of the ring $R = k[a_1, \ldots, a_n]$ then $D^a/a!(IR) \subset IR$.*

Now we show how to compute $D_i^a/a!$ effectively. Of course, it is complicated only for a fields of positive characteristic. We assume that $D_i = \frac{\partial}{\partial f_i}$, where f_i is a component of a polynomial automorphism.

Definition 3.7. The method of computing $D_i^a/a!(h)$: First, we compute operator D_i in a formal way, i.e., we leave all integral coefficients which appear unchanged. Next, we compute D_i “a” times also in a formal way, we receive the operator N. Then we compute formally $N(h)$ and then divide all formal coefficients by $a!$. Finally, we compute the impression in the field.

We show that this definition is stated in a correct way (i.e., fractions do not appear in this constructions). Let

$$f_i(x_1, \dots, x_n) = \sum_{|\alpha| \le \deg F} a_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

and $h = H(f_1, \dots, f_n)$, where $H = \sum_{|\alpha| \le \deg H} b_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$.

Take $\mathbb{F}_p(\{a_{i,\alpha}, b_\alpha\})$. Now choose real numbers $\{a'_{i,\alpha}\}, \{b'_\alpha\}$, which form purely transcendental system over $\mathbb{Q}$. We have the epimorphism

$$\pi : \mathbb{Z}[a'_{i,\alpha}, \{b'_\alpha\}] \to \mathbb{F}_p(\{a_{i,\alpha}\}, \{b_\alpha\}),$$

which induces the epimorphism

$$\pi' : R = \mathbb{Z}[\{a'_{i,\alpha}\}, \{b'_{\alpha\}}][x_1, \dots, x_n] \to S = \mathbb{F}_p(\{a_{i,\alpha}\}, \{b_{\alpha\}})[x_1, \dots, x_n].$$

If I denotes ker π, then ker $\pi' = I[x_1, \dots, x_n]$. It is easy to see that π' commutes with every derivation $D^a/a!$. Now take

$$f'_i(x_1, \dots, x_n) = \sum_{|\alpha|} a_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

and

$$H'(x_1, \dots, x_n) = \sum_{|\alpha|} b'_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}.$$

Let $f' = (f'_1, \dots, f'_n)$. Note that $\pi'(f') = f$. If we take $h' = H'(f'_1, \dots, f'_n)$ then $\pi(h') = h$. Now if we compute $D_i'^a/a!(h')$ fractions do not appear and it is enough to use π - ${D_i}^a/a!(h) = \pi(D_i'^a/a!(h'))$.

Example 3.8. Let $k = \mathbb{F}_2$ and let (formally) $D = 3x^2 \frac{\partial}{\partial y} - \frac{\partial}{\partial x}$. Then formally $D^2 = 9x^2 \frac{\partial}{\partial y}^2 - 6x^2 \frac{\partial}{\partial x} \frac{\partial}{\partial y} - 6x \frac{\partial}{\partial y} + \frac{\partial}{\partial x}^2$ and consequently

$$D^2/2! = x^2 \frac{\partial}{\partial y}^2 /2! + x^2 \frac{\partial}{\partial x} \frac{\partial}{\partial y} + x \frac{\partial}{\partial y} + \frac{\partial}{\partial x}^2 /2!.$$

4. A formula

In this section we give a formula for the inverse of polynomial automorphism. We have:

Theorem 4.1. *Let $f = (f_1, \dots, f_n)$ be a normalized polynomial isomorphism. Assume that* $\deg f_i = d_i$ *and $d_1 \ge d_2 \dots \ge d_n$. Take $b = (b_1, \dots, b_n)$*

$= f(0)$. *Let* $D_i = \frac{\partial}{\partial f_i}$ *be derivations as in Proposition* 3.3. *Let* $g = (g_1, \ldots, g_n)$ $= f^{-1}$. *Then*

$$g_j(y_1, \ldots, y_n) = \sum_{|\alpha| \le Q} \frac{D_1^{\alpha_1}}{\alpha_1!} \frac{D_2^{\alpha_2}}{\alpha_2!} \ldots \frac{D_n^{\alpha_n}}{\alpha_n!}(x_j)(0)(y_1 - b_1)^{\alpha_1}(y_2 - b_2)^{\alpha_2} \ldots (y_n - b_n)^{\alpha_n},$$

where $Q = \prod_{j=1}^{n-1} d_j$.

Proof. First assume that $\operatorname{char} k = 0$. Let us note that $g_i(f_1, \ldots, f_n) = x_i$. Now develop a function x_i considered as a function of variables $f_1, \ldots, f_n$ in a Taylor series in a center b (note that for every polynomial h we have $h(b) = h(f)(0)$).

Now assume that char $k = p > 0$. In fact, we could repeat the previous proof, but it does not suggest a way how to compute derivations in effective way. Hence we use different method. Let $g = f^{-1}$ and $g = (g_1, \ldots, g_n)$. Let

$$f_i(x_1, \ldots, x_n) = \sum_{|\alpha| \le \deg F} a_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

and

$$g_i(x_1, \ldots, x_n) = \sum_{|\alpha| \le \deg F} b_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Take $\mathbb{F}_p(\{a_{i,\alpha}, b_{i,\alpha}\}, b_1, \ldots, b_n)$ to be a field generated by all coefficients of components of automorphisms f, g and by $b_1, \ldots, b_n$. Now choose real numbers $\{a'_{i,\alpha}\}, \{b'_{i,\alpha}\}, \{b'_i\}$, which form purely transcendental system over $\mathbb{Q}$. We have the epimorphism

$$\pi : \mathbb{Z}[a'_{i,\alpha}, \{b'_{i,\alpha}\}, \{b'_i\}] \to \mathbb{F}_p(\{a_{i,\alpha}\}, \{b_{i,\alpha}\}, \{b_i\}),$$

which induces the epimorphism

$$\pi' : R = \mathbb{Z}[\{a'_{i,\alpha}\}, \{b'_{i,\alpha\}}, \{b'_i\}][x_1, \ldots, x_n] \\ \to S = \mathbb{F}_p(\{a_{i,\alpha}\}, \{b_{i,\alpha}\}, \{b_i\})[x_1, \ldots, x_n].$$

If I denotes ker π, then ker $\pi' = I[x_1, \ldots, x_n]$. It is easy to see that π' commutes with every derivation $D^a/a!$. Now take

$$f'_i(x_1, \ldots, x_n) = \sum_{|\alpha|} a_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

and

$$g'_i(x_1, \ldots, x_n) = \sum_{|\alpha|} b'_{i,\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Let $f' = (f'_1, \ldots, f'_n)$ and $g' = (g'_1, \ldots, g'_n)$. Note that $\pi'(f') = f$ and $\pi'(g') = g$. Over $\mathbb{R}$ we have $g'_i(f'_1, \ldots, f'_n) = x_i + H_i$, where $H_i \in I[x_1, \ldots, x_n]$. Now we compute $D'_i = \frac{\partial}{\partial f'_i}$. By Proposition 3.4 we get:

$$D'_i = \frac{\partial}{\partial f'_i} = 1/\delta \sum A'_{ij} \frac{\partial}{\partial x_j},$$

where

$$A'_{ij} = \begin{vmatrix} \frac{\partial f'_1}{\partial x_1} & \frac{\partial f'_1}{\partial x_2} & \ldots & \frac{\partial f'_1}{\partial x_{j-1}} & 0 & \frac{\partial f'_1}{\partial x_{j+1}} & \ldots & \frac{\partial f'_1}{\partial x_n} \\ \frac{\partial f'_2}{\partial x_1} & \frac{\partial f'_2}{\partial x_2} & \ldots & \frac{\partial f'_2}{\partial x_{j-1}} & 0 & \frac{\partial f'_2}{\partial x_{j+1}} & \ldots & \frac{\partial f'_2}{\partial x_n} \\ \vdots & \vdots & \ldots & \vdots & 0 & \vdots & \ldots & \vdots \\ \frac{\partial f'_i}{\partial x_1} & \frac{\partial f'_i}{\partial x_2} & \ldots & \frac{\partial f'_i}{\partial x_{j-1}} & 1 & \frac{\partial f'_i}{\partial x_{j+1}} & \ldots & \frac{\partial f'_i}{\partial x_n} \\ \vdots & \vdots & \ldots & \vdots & 0 & \vdots & \ldots & \vdots \\ \frac{\partial f'_n}{\partial x_1} & \frac{\partial f'_n}{\partial x_2} & \ldots & \frac{\partial f'_n}{\partial x_{j-1}} & 0 & \frac{\partial f'_n}{\partial x_{j+1}} & \ldots & \frac{\partial f'_n}{\partial x_n} \end{vmatrix}$$

and $\delta = \det[\frac{\partial f'_i}{\partial x_k}]$. Note that $\delta = 1 \bmod I[x_1, \ldots, x_n]$ and hence, we can extend the mapping $\pi' : R \to S$ to the mapping $\pi' : R_\delta \to S$. Now develop a function $x_i + H_i$ considered as a function of variables $f'_1, \ldots, f'_n$ in a Taylor series in a center b' (note that for every polynomial h we have $h(b') = h(f')(0)$). Using rules of differentiation and facts that $H_i, D'_j(\delta) = 0 \bmod I[x_1, \ldots, x_n]$ and $\delta = 1 \bmod I[x_1, \ldots, x_n]$, (see Proposition 3.6) we get after application of π' that

$$\begin{aligned} &g_j(y_1, \ldots, y_n) \\ &\quad = \sum_{|\alpha| \le Q} \frac{D_1^{\alpha_1}}{\alpha_1!} \frac{D_2^{\alpha_2}}{\alpha_2!} \ldots \frac{D_n^{\alpha_n}}{\alpha_n!} (x_j)(0)(y_1 - b_1)^{\alpha_1}(y_2 - b_2)^{\alpha_2} \ldots (y_n - b_n)^{\alpha_n}. \ \blacksquare \end{aligned}$$

Now we are able to solve equation $f = 0$:

Corollary 4.2. *If $f(\gamma_1, \ldots, \gamma_n) = 0$, then*

$$\gamma_j = \sum_{|\alpha| \le Q} \frac{D_1^{\alpha_1}}{\alpha_1!} \frac{D_2^{\alpha_2}}{\alpha_2!} \ldots \frac{D_n^{\alpha_n}}{\alpha_n!} (x_j)(0)(-b_1)^{\alpha_1}(-b_2)^{\alpha_2} \ldots (-b_n)^{\alpha_n}.$$

Proof. We have $f(g) = identity$ hence $f(g(0)) = 0$. This means that $g(0)$ is a zero of f. ∎

Corollary 4.3. *Let S be the set of all coefficients of polynomials f_1, $\ldots, f_n$ (notations as in Theorem 4.1). Then all coefficients of polynomials $g_1, \ldots, g_n$ (where $g = f^{-1}$) belong to the ring $\mathbb{F}_p[S]$ (where $\mathbb{F}_0 = \mathbb{Z}$).*

References

[1] H. Bass, E. Connell, D. Wright, *The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse,* Bull. AMS 7 (1982), 287–330.
[2] A. Van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progress in Math., 190, Birkhäuser Verlag, Boston-Basel-Berlin, 2000.
[3] Z. Jelonek, *On the effective Nullstellensatz*, Invent. Math. 162 (2005), 1–17.
[4] O. Perron, *Algebra I (Die Grundlagen)*, Walter de Gruyter & Co., Berlin und Leipzig, 1927.

INSTYTUT MATEMATYCZNY PAN
ul. Śniadeckich 8
00-950 WARSZAWA, POLAND
E-mail: najelone@cyf-kr.edu.pl

Received December 12, 2010.