THE SOLUTION OF THE TAME GENERATORS CONJECTURE ACCORDING TO SHESTAKOV AND UMIRBAEV

Arno van den Essen

Report No. 00309 (July 2003)
Introduction

One of the most fundamental questions in the study of invertible polynomial maps is: how do they all look like? For invertible linear maps over a field everyone knows from linear algebra that every such map is a finite composition of elementary maps. For invertible polynomial maps one also has a natural notion of an elementary map (see the next section) and the crucial question was: is every invertible polynomial map over a field a finite composition of such elementary maps? This problem is most widely known as the Tame Generators Problem. It remained open for more than 60 years and was recently solved by Shestakov and Umirbaev. The answer is no in dimension 3!

Their proof is very technical and complicated and is given in a series of two papers [6] and [7] and will appear in the J. of the AMS. Together these papers contain about 50 pages and still many details are left to the reader! Our aim here is to present the main ideas of their proof, which may be helpful in the reading of [7].

1 Some history and preliminaries

Let $k$ be any commutative ring. By $k^n$ or $k[x_1,\ldots,x_n]$ we denote the polynomial ring in $n$ variables over $k$. A polynomial map $F : k^n \to k^n$ is just an $n$-tuple $(F_1,\ldots,F_n)$ of polynomials over $k$. Such a map is called invertible over $k$ or a polynomial automorphism of $k^n$ if there exists a polynomial map $G = (G_1,\ldots,G_n)$ such that $F \circ G = I$, the identity map. Examples of invertible polynomial maps are the so-called elementary polynomial maps given by

\[ E_{i,c,a} := (x_1,\ldots,x_{i-1},cx_i+a, x_{i+1},\ldots,x_n) \]

where $c$ is a unit in $k$ and $a$ a polynomial in $k[[x]]$ not containing $x_i$. The inverse of $E_{i,c,a}$ is the elementary map $E_{i,-c, -a}$. Of course making finite compositions of such elementary polynomial maps we get much more examples of invertible ones: the

---

1 This paper is an extended version of lectures given in Nijmegen and Toruń
group we obtain in this way is called the **tame group** and its elements are called **tame**. Now the crucial question is: are there any other invertible polynomial maps over $k$? If $k$ contains non-zero nilpotent elements the answer is easily seen to be yes: namely consider the case $n = 1$ and choose $c \in k$, non-zero, such that $c^2 = 0$. Since tame maps are finite compositions of the affine maps $cx + a$, with $c \in k^*$ and $a \in k$, all tame maps are affine. However the map $F := x + ex^2$ is invertible over $k$, with inverse $G := x - ex^2$ and clearly $F$ is not affine, hence not tame. On the other hand if we assume that $k$ is a domain (in fact it suffices if $k$ is reduced) then one easily verifies that all invertible maps are affine, hence tame.

If $n = 2$ the situation is more complicated. In case $k$ is a field of characteristic zero Jung showed in 1942, [2], that there are no other invertible polynomial maps. In other words every invertible polynomial map over $k$ is tame. This result was extended by van der Kulk in 1953, [3] to the case of positive characteristic. Furthermore he showed that the tame group is a free amalgamated product of the groups $Aff(k, 2)$ and $J(k, 2)$ over their intersection, where $Aff(k, 2)$ is the **Affine group** consisting of all invertible affine maps and $J(k, 2)$ is the group of the **de Jonquières**, consisting of all invertible polynomial maps of the form $F = (a_1x + f_1(y), a_2y + f_2)$, where $a_1, a_2 \in k^*$, $f_2 \in k$ and $f_1(y) \in k[y]$. This last result also holds in case $k$ is a domain (see [1], 5.1.3). However if $k$ is a domain which is not a field, then there do exist wild i.e. non-tame invertible polynomial maps over $k$. Namely in 1972, [5], Nagata made the following observation: choose $0 \neq z \in k$ which is not a unit in $k$ and define $\sigma := s_1^{-1}s_2s_1$ where $s_1 := (x + z^{-1}y^2, y)$ and $s_2 := (x, y + z^2x)$ ($z^{-1}$ belongs to the quotient field of $k$). Then the map $\sigma$ has all its coefficients in $k$, namely

$$\sigma = (x - 2y(zx + y^2) - z(zx + y^2)^2, y + z(zx + y^2))$$

and one easily verifies that $\sigma$ is invertible over $k$. Furthermore it follows from the free amalgamated product structure that $\sigma$ is not tame over $k$! Applying this construction to the univariate polynomial ring $k := \mathbb{C}[z]$ Nagata conjectured that the corresponding map of 3-space given by

$$\sigma(x, y, z) = (x - 2y(zx + y^2) - z(zx + y^2)^2, y + z(zx + y^2), z)$$

is not tame over $\mathbb{C}$. Several papers appeared to give evidence to the conjectured wildness of $\sigma$, however Nagata’s conjecture remained open until the recent work [7] of Shestakov and Umirbaev. On the other hand it was shown by M. Smith in 1989,[8], that $\sigma$ is 1-tame i.e., the extended map $\tilde{\sigma} : \mathbb{C}^4 \to \mathbb{C}^4$ given by $\tilde{\sigma}(x, y, z, t) = (\sigma(x, y, z), t)$ is tame.

To conclude this section we introduce some notation and give some results which will be used in the sequel.

From now on $k$ will denote a field. If $f \in k^{[n]}$ the homogeneous part of the highest degree of $f$ will be denoted by $\overline{f}$. Now let $F := (f_1, \ldots, f_n)$ be a polynomial map. If $F$ is invertible over $k$, then it is well-known that its Jacobian determinant is a unit in $k$ i.e. $detJ(f_1, \ldots, f_n) \in k^*$. It follows (see [1], 1.2.9) that

$$f_1, \ldots, f_n \text{ are algebraically independent over } k.$$
On the other hand if $F$ is non-linear it follows that $\det J(f_1,\ldots,f_n) = 0$, which implies that

\begin{equation}
(1.2) \quad f_1,\ldots,f_n \text{ are algebraically dependent over } k.
\end{equation}

Furthermore we define $\deg F := \deg f_1 + \ldots + \deg f_n$.

Now let $F$ and $G$ be polynomial maps over $k$. If there exists an elementary map $E$ such that $G = E \circ F$ we write $F \rightarrow_E G$ or $F \rightarrow G$. If furthermore $\deg G < \deg F$ we say that $F$ admits an elementary reduction to $G$ and write $F \rightarrow_{\text{red}} G$. More precisely we say that $f_i$ is elementary reducible if there exists a polynomial $a \in k[n]$ not containing $x_i$ such that $\deg(f_i - a(f_1,\ldots,f_{i-1},f_{i+1},\ldots,f_n)) < \deg f_i$.

Finally, if $f_1,\ldots,f_s$ are some elements of $k[n]$ then the $k$-subalgebra of $k[n]$ generated by the $f_i$'s is denoted by $\langle f_1,\ldots,f_s \rangle$.

2 The two-dimensional case: Jung's theorem

Throughout this and the next sections $k$ denotes a field of characteristic zero.

To understand the work of Shestakov and Umirbaev we first consider the two dimensional case i.e. we prove

**Theorem 2.1 (Jung, 1942)** Every automorphism $F = (f,g)$ of $k^2$ is tame.

**Proof.** The theorem follows by induction on $\deg F$ if we can show that

\begin{equation}
(2.2) \quad F \text{ admits an elementary reduction if } \deg F > 2.
\end{equation}

First we prove (2.2) for the special case that $\mathcal{F} \in \langle \mathcal{F} \rangle$: namely then $\mathcal{F} = c \mathcal{F}'$ for some $c \in k^*$ and $r \geq 1$. Consequently $\deg (f - cg^r) < \deg f$. So if we put $E := \langle x - cy^r, y \rangle$, then $\deg E \circ F < \deg F$. i.e. $F$ admits an elementary reduction. Similarly (2.2) holds if $\mathcal{G} \in \langle \mathcal{G} \rangle$. So taking into account (1.1) and (1.2) we need to study pairs $(f,g)$ which have the following properties:

1) $f$ and $g$ are algebraically independent over $k$.
2) $\mathcal{F}$ and $\mathcal{G}$ are algebraically dependent over $k$.
3) $\mathcal{F} \notin \langle \mathcal{G} \rangle$ and $\mathcal{G} \notin \langle \mathcal{F} \rangle$.

Such pairs are called $\ast$-reduced. They were studied by Shestakov and Umirbaev in [6]. As a consequence of their main result (on these pairs), it follows that $f,g$ cannot form a $\ast$-reduced pair(see 3.4). In other words, using (1.1) and (1.2) again, condition 3) is not satisfied. So either $\mathcal{F} \notin \langle \mathcal{G} \rangle$ or $\mathcal{G} \notin \langle \mathcal{F} \rangle$. Hence we are done by the observations made above $\Box$

3 Poisson algebras and $\ast$-reduced pairs

**Definition 3.1** Let $A := k[x_1,\ldots,x_n]$ and $f, g \in A$. Then $f, g$ is called $\ast$-reduced if

1) $f, g$ are algebraically independent over $k$.
2) $\mathcal{F}, \mathcal{G}$ are algebraically dependent over $k$.
3) $\mathcal{F} \notin \langle \mathcal{G} \rangle$ and $\mathcal{G} \notin \langle \mathcal{F} \rangle$. 

3
The crucial idea of [6] to study these pairs is to embed the polynomial ring $k[x_1, \ldots, x_n]$ in the so-called free Poisson algebra in $x_1, \ldots, x_n$ over $k$.

**Definition 3.2** A Poisson algebra $B$ is a $k$-vector space endowed with two bilinear operations: $(x, y) \to x \cdot y$ (multiplication) and $(x, y) \to [x, y]$ (Poisson bracket) such that

i) $B$ is commutative and associative with respect to "$ \cdot "$.

ii) $B$ is a Lie-algebra with respect to $[,]$.

iii) $[a, bc] = b[a, c] + [a, b]c$ for all $a, b, c \in B$ (Leibniz’ rule).

**Example 1** One easily verifies that the polynomial ring $k[x, y]$ together with the usual multiplication and Poisson bracket given by

$$[f, g] := fxgy - fgyx$$

is a Poisson algebra. Observe that the (two-dimensional) Jacobian Conjecture in terms of this bracket gets the following form: if $[f, g] = [x, y]$, then $k[f, g] = k[x, y]$.

**Example 2** The Free Poisson algebra $P < x_1, \ldots, x_n >$ on the variables $x_1, \ldots, x_n$ is the $k$-algebra generated by the variables $x_1, \ldots, x_n, [x_i, x_j], 1 \leq i < j \leq n, [x_i, [x_j, x_k]]$ etc. It becomes a graded ring by putting $\deg(x_i) = 1, \deg([x_i, x_j]) = 2, \ldots$. It follows that

$$[f, g] = \sum_{1 \leq i < j \leq n}(fxgy - fgyx)[x_i, x_j] \text{ for all } f, g \in k^n.$$ 

This formula implies the following two facts

- $\deg([f, g]) \leq \deg(f) + \deg(g)$ and
- $[f, g] = 0$ iff $f, g$ are algebraically independent over $k$.

In particular

If $f, g$ are algebraically independent over $k$, then $\deg([f, g]) \geq 2$.

Now let $f, g$ be a $*$-reduced pair. Then $f$ and $g$ are algebraically dependent over $k$. So by Gordan’s lemma there exists a polynomial $h$ such that $f, g \in < h >$. Since $f$ and $g$ are homogeneous it follows that $h$ is homogeneous, $f = c_1h^p$ and $g = c_2h^s$ for some natural numbers $p, s$ and $c_1, c_2 \in k^*$. We can choose $h$ in such a way that $(p, s) = 1$. We may furthermore assume that $n := \deg(f) \leq m := \deg(g)$. Observe that 3) of 3.1 implies that $n < m$. So $m \geq 2$. Furthermore $n = p.(n, m)$ i.e. $p = \frac{m}{(n, m)}$ and $m = s.(n, m)$ i.e. $s = \frac{n}{(n, m)}$. Instead of saying that $f, g$ is a $*$-reduced pair we sometimes call it a $p$-reduced pair. Also $p \geq 2$, namely if $p = 1$ then $g \in < f >$, contradicting 3) of 3.1). Consequently, if we put

$$N(f, g) := pm - m - n + \deg([f, g])$$

then
(1) $N(f,g) > \deg[f,g]$.

Now we can formulate the main theorem of [6].

**Theorem 3.3** Let $G(x,y) \in k[x,y]$ with $\deg_y G = pq + r$, where $0 \leq r < p$. Then

\[ \deg G(f,g) \geq qN(f,g) + mr. \]

Furthermore, if $\deg_y G(x,y) = q_1s + r_1$, with $0 \leq r_1 < s$, then $\deg G(f,g) \geq q_1N(f,g) + nr_1$.

It is this theorem which plays a crucial role in the understanding of tame maps in dimension 3. To demonstrate the power of this theorem we show how it implies the result used in the proof of Jung’s theorem which asserts that there do not exist non-linear invertible polynomial maps of $k^2$ whose components form a *-reduced pair.

More precisely

**Corollary 3.4** If $F = (f,g)$ is invertible over $k$ with $\deg F > 2$, then

\[ \mathcal{F} \in \langle \mathcal{F} \rangle \text{ or } \mathcal{G} \in \langle \mathcal{G} \rangle. \]

**Proof.** If the conclusion is not true then $(f,g)$ is a *-reduced pair (by (1.1) and (1.2)). Let $(G_1, G_2)$ be the inverse of $(f,g)$. Then $x = G_1(f,g)$. Let $\deg_y G_1 = qp + r$, with $0 \leq r < p - 1$. Then by 3.3 we get

\[ \deg x = \deg G_1(f,g) \geq qN(f,g) + mr. \]

Since, as observed above $\deg[f,g] \geq 2$ it follows from (1) that $N(f,g) > 2$. Since also $m \geq 2$ it follows from (2) that $q = r = 0$. So $\deg_y G_1 = 0$ i.e. $G_1 = G_1(x)$. Hence $x = G_1(f)$, which implies that $f = f(x)$ and $\deg(f) = 1$. So $\mathcal{F} = cx$ for some $c \in k^*$.

But $\mathcal{F}$ and $\mathcal{G}$ are algebraically dependent over $k$ (by (2) of 3.1)). So $\mathcal{G}$ only depends on $x$. Hence $\mathcal{F} \in \langle x \rangle = \langle \mathcal{F} \rangle$, contradicting 3) of 3.1. $\Box$

To conclude this section we give some useful results concerning *-reduced pairs which will be used in section 6. With the notation introduced above we have

**Lemma 3.5** Let $f, g$ be a *-reduced pair. Then the elements $f^i g^j$ with $j < p$ all have different degrees.

**Proof.** If $\deg f^i g^j = \deg f^i g^j$ with $j_1 \leq j_2 < p$, then $i_1n + j_1m = i_2n + j_2m$, whence $(i_1 - i_2)n = (j_2 - j_1)m$. Since $(p,s) = 1$ it follows that $p$ divides $j_2 - j_1$.

However $0 \leq j_2 - j_1 < p$, so $j_2 - j_1 = 0$. Hence $i_1 - i_2 = 0$ i.e. $i_1 = i_2$ and $j_1 = j_2$. $\Box$

**Corollary 3.6** Situation as in lemma. If $h = G(f,g)$ with $\deg_y G < p$, then $\mathcal{H} \in \langle \mathcal{F}, \mathcal{G} \rangle$. 5
4 Automorphisms admitting a reduction of type I-IV and the main results

In the previous section we saw that Jung’s theorem is a consequence of (2.2) i.e. the assertion that every automorphism of \( k^2 \) admits an elementary reduction. This immediately leads to the following question

**Question.** Does every non-linear tame automorphism of \( k^3 \) admit an elementary reduction?

For several years the authors of [7] believed that the answer to this question was affirmative. However in 2001 they discovered the following "exotic" tame automorphism of \( k^3 \) i.e. one which does not admit an elementary reduction. It was this discovery which formed the real starting point of their solution of the tame generators problem. Here is their example.

**Example.** Let \( h_1 = x_1, h_2 = x_2 + x_1^2, h_3 = x_3 + 2x_1x_2 + x_1^3, g_1 = 4h_2 + h_3^2, g_2 = 6h_1 + 6h_1h_2 + h_3^3, g_3 = h_3. \) Then \( h := (h_1, h_2, h_3) \) and \( g := (g_1, g_2, g_3) \) are tame. Let \( f = g_2^3 - g_1^3. \) Finally put \( f_1 = g_1, f_2 = g_2 + (g_3 + f), f_3 = g_3 + f \) and \( F = (f_1, f_2, f_3). \) Then \( F \) is tame, but does not admit an elementary reduction.

Namely one easily verifies that \( \mathcal{F}_1 = x_1^6, \mathcal{F}_2 = x_1^3 \) and \( \mathcal{F}_3 = 12x_1^2x_3 - 12x_1^3x_2. \) If \( f_1 \) is elementary reducible then \( \mathcal{F}_1 \in < f_2, f_3 > \) which, since \( f_2 \) and \( f_3 \) are algebraically independent over \( k \) implies that \( f_1 \in < f_2, f_3 > \), but this is clearly not the case. Similarly \( f_2 \notin < f_1, f_3 > \) i.e. \( f_2 \) is not elementary reducible. It remains to see that \( f_3 \) is not elementary reducible. So suppose it is. Then there exists \( G(f_1, f_2) \) such that \( f_3 = G(f_1, f_2). \) Observe that \( f_1, f_2 \) is a 2-reduced pair. So by 3.3 we get

\[
8 = \deg(f_3) = \deg(G(f_1, f_2)) \geq q(2.9 - 9 - 6 + \deg(f_1, f_2)) + 9r.
\]

Since \( \deg(f_1, f_2) = 18 \) we get \( 8 \geq 6.21 + 9r, \) so \( q = r = 0 \) i.e. \( \deg G = 0. \) So \( f_3 = G(f_1, f_2) \in < f_1 >, \) a contradiction.

In fact this example is a special case of the following class of "exotic" automorphisms of \( k^3 \) introduced in [7], which all do not admit an elementary reduction.

**Definition 4.1** Let \( F = (f_1, f_2, f_3) \in Aut_k k^3. \) We say that \( F \) admits a reduction of type I (with active element \( f_3 \)) if the following conditions are verified

a) \( \deg(f_1) = 2n, \deg(f_2) = sn, s \text{ odd } s \geq 3, 2n < \deg(f_3) \leq sn \) and \( f_3 \notin < f_1, f_2 >. \)

b) There exists \( \alpha \in k^n \) such that \( g_1 := f_1 \) and \( g_2 := f_1 - \alpha f_3 \) satisfy

i) \( g_1, g_2 \) is a \( \alpha \)-reduced pair with \( \deg(g_1) = 2n \) and \( \deg(g_2) = sn. \)

ii) \( (g_1, g_2, f_3) \to_{\text{red}} (g_1, g_2, g_3) \) with \( \deg(g_1, g_3) < sn + \deg(g_1, g_2). \)

Observe that each \( f_i \) has degree > 1. Furthermore such a map \( F \) has the property that after a preliminary linear transformation \( L \) of the form \( L = (x_1, x_2 - \alpha x_3, x_3) \) with \( \alpha \in k^n \) the map \( L \circ F = (g_1, g_2, g_3) \) admits an elementary reduction where \( \deg(g_1) = \deg(f_1) \) and \( \deg(g_2) = \deg(f_2). \) More precisely there exists \( \alpha \in < g_1, g_2 > \) such that \( \deg(g_3 - \alpha(g_1, g_2)) < \deg(g_3). \) In other words, if \( E = (x_1, x_2, x_3 - \alpha(x_1, x_2)) \)
then $degE \circ L \circ F < degF$. So if $F$ admits a reduction of type I, then it admits a reduction to an automorphism of lower degree (than $F$) by a sequence of two elementary transformations.

Now the next question is: does every non-linear automorphism of $k^3$ admit either an elementary reduction or a reduction of type I?

It turned out that the situation is much more complicated: in their paper Shestakov and Umirbaev introduce 3 more classes of "exotic" automorphisms: automorphisms which admit a reduction of type II, resp. type III, resp. type IV. Just as in the type I case the components $f_i$ of these automorphisms have very special restrictions on their degrees. In particular it follows that $deg(f_i) > 1$ for all $i$. Furthermore, without going into too much detail we just like to mention that if an automorphism $F$ admits a reduction of type II it can be reduced to an automorphism $G$ with $degG < degF$ by a sequence of three elementary transformations, two of which are linear. Similarly $F$'s admitting a reduction of type III can also be reduced to an automorphism $G$ with $degG < degF$ by a sequence of three elementary transformations, one of which is linear and an other is of the form $(x_1, x_2, x_3) \rightarrow (x_1, x_2 - \gamma x_3 - \alpha x_2^2, x_3)$ i.e. quadratic.

The type IV reduction is even more complicated since it consists of a sequence of four elementary transformations one of which is linear and two of them are quadratic. During the reduction process in the type III and IV cases the degree may go up in the intermediate steps, but finally becomes lower than $degF$. Now the main theorem of [7] asserts

**Theorem 4.2** Every non-linear automorphism of $k^3$ admits either an elementary reduction or a reduction of one of the types I-IV.

**Corollary 4.3** Let $F = (f_1, f_2, f_3)$ be a non-linear tame automorphism with $f_3 = x_3$.

Then $F$ admits an elementary reduction.

**Proof.** If $F$ admits a reduction of one of the types I-IV then, as observed before, $deg(f_i) > 1$ for all $i$. Since $deg(f_3) = 1$ theorem 4.2 implies that $F$ admits an elementary reduction. $\square$

**Corollary 4.4** Let $F$ be as in 4.3. Then $F$ is tame iff $(f_1, f_2)$ is tame over $k[x_3]$.

**Corollary 4.5** The Nagata automorphism $\sigma : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ is not tame.

5 Sketch of the proof of theorem 4.2

To prove theorem 4.2 we introduce the class of so-called simple automorphisms.

**Definition 5.1** By induction on $degF$ we define simple automorphisms of $k^3$. First all automorphisms of degree 3 i.e. linear ones are simple and if $degF > 3$ then $F$ is called simple if it admits either an elementary reduction or a reduction of one of the types I-IV to a simple automorphism $G$ (with $degG < degF$).
Theorem 4.2 can then be reformulated as

**Theorem 5.2** If $F$ is tame, then $F$ is simple.

The converse is obvious since every reduction is done by a sequence of elementary transformations.

We are going to prove this theorem by contradiction. So suppose that there exists a tame automorphism $F$ of $k^3$ which is not simple. Then we have a sequence

$$F_0 := F ightarrow F_1 ightarrow \ldots ightarrow F_l = I$$

where $F_0$ is not simple, but $F_1$ is simple. Let $r$ be maximal such that $F_r$ is not simple, but $F_{r+1}$ is simple. Hence $F_{r+1} \rightarrow_{E} F_r$. So $\theta := F_{r+1}$ and $\tau := F_r$ are tame automorphisms, which satisfy 1) $\theta \rightarrow \tau$ 2) $\theta$ is simple and 3) $\tau$ is not simple.

Amongst all pairs $\theta, \tau$ satisfying 1), 2) and 3) we choose (once and for all) one pair $\theta_0, \tau_0$ such that $\deg \theta_0$ is minimal and we write $\theta_0 = (f_1, f_2, f_3)$. Since $\theta_0 \rightarrow \tau_0$ we have 3 cases namely

1. $\tau_0 = (f_1 + a(f_2, f_3), f_2, f_3)$
2. $\tau_0 = (f_1, f_2 + a(f_1, f_3), f_3)$
3. $\tau_0 = (f_1, f_2, f_3 + a(f_1, f_2))$.

Since $\theta_0$ is simple there are 5 cases for $\theta_0$, namely $\theta_0$ admits either an elementary reduction or a reduction of one of the types I-IV to a simple automorphism.

The whole proof consists of showing that in each of the 15 cases $\tau_0$ is simple, which is a contradiction since by definition $\tau_0$ is not simple!

To get an idea of how the simplicity of $\tau_0$ is obtained, we consider from these 15 cases only a relatively easy case, namely when $\tau_0$ is of the form (2) and $\theta_0$ admits a reduction of type I to a simple automorphism. More precisely we show

**Proposition 5.3** If $\theta_0 = (f_1, f_2, f_3)$ admits a reduction of type I and $\tau_0 = (f_1, f_2 + a(f_1, f_3), f_3)$, then $\tau_0$ is simple.

**Proof.** First we claim

$$\deg(a) \leq \deg(f_2).$$

Namely, suppose $\deg(a) > \deg(f_2)$. Then $\deg \tau_0 > \deg \theta_0$. Also $\theta_0 \rightarrow_{E} \tau_0$, whence $\tau_0 \rightarrow_{E-1} \theta_0$. So $\theta_0$ admits an elementary reduction to the simple automorphism $\theta_0$ which has lower degree. So by the definition of simpleness this implies that $\tau_0$ is simple, a contradiction. So (5.3.1) holds.

Now the point is that the estimation (5.3.1) gives a very strong restriction on the form of the polynomial $a(f_1, f_3)$. More precisely we get

**Lemma 5.4** $a(f_1, f_3) = \beta f_3 + T(f_1), \beta \in k^*, \deg T(f_1) < \deg(f_2)$.

The proof of this lemma is the most technical part. Therefore we postpone its proof until the next section.

Now let us show how lemma 5.4 enables us to prove proposition 5.3.
First, since \( \theta_0 \) admits a reduction of type I we have
\[
\theta_0 = (f_1, f_2, f_3) \rightarrow (f_1, f_2 - \alpha f_3, f_3) \rightarrow (g_1, g_2, f_3 - g(g_1, g_2))
\]
with \( g_1 := f_1 \), \( \deg(g_2) = \deg(f_2) \), \( \deg(g_3) < \deg(f_3) \), \( g_1, g_2 \) is a \( * \)-reduced pair, \( G := (g_1, g_2, g_3) \) is simple and \( \deg[g_1, g_3] < sn + \deg[g_1, g_2] \). By lemma 5.4 we have that \( \tau_0 = (f_1, f, f_3) \), where \( f := f_2 + \beta f_3 + T(f_1) \) with \( T(f_1) < \deg(f_2) \). Now we distinguish two cases.

**Case 1.** \( \alpha + \beta \neq 0 \). We show that \( \tau_0 \) admits a reduction of type I to a simple automorphism (hence \( \tau_0 \) is simple) namely
\[
\tau_0 = (f_1, f, f_3) \rightarrow (f_1, f - (\alpha + \beta)f_3, f_3) = (f_1, (f_2 - \alpha f_3) + T(f_1), f_3)
\]
\[
= (g_1, g_2 + T(g_1), f_3) \rightarrow (g_1, g_2', f_3 - g(g_1, g_2)) = (g_1, g_2, f_3 - \bar{g}(g_1, g_2))
\]
To see that \( \tau_0 = (f_1, f, f_3) \rightarrow (f_1, f - (\alpha + \beta)f_3, f_3) \rightarrow (g_1, g_2', g_3) \) is a reduction of type I one also needs to check that \( \deg(g_2) = \deg(f) \), \( (g_1, g_2') \) is a \( * \)-reduced pair and \( \deg[g_1, g_3] < sn + \deg[g_1, g_2] \). We leave this easy verification to the reader. It remains to see that \( G' := (g_1, g_2, g_3) \) is simple. Assume that \( G' \) is not simple. Since \( \theta_0 \) admits a reduction of type I to the simple automorphism \( G = (g_1, g_2, g_3) \) we have (obviously) that \( G' = (g_1, g_2, g_3) \) is simple and \( \deg G < \deg \theta_0 \). Also \( G \rightarrow G' \), since \( g_2 = g_2 + T(g_1) \). But \( G \) is simple and \( G' \) is not simple. Since \( \deg G < \deg \theta_0 \) this gives a contradiction with the minimal choice of \( \theta_0 \). So \( G' \) is simple, which completes the proof of case 1.

**Case 2.** \( \alpha + \beta = 0 \) i.e. \( \beta = -\alpha \). Now we will show that \( \tau_0 \) admits an elementary reduction to a simple automorphism (hence \( \tau_0 \) is simple). Namely we get
\[
\tau_0 = (f_1, f, f_3) = (f_1, f_2 - \alpha f_3 + T(f_1), f_3)
\]
\[
= (g_1, g_2', f_3 - g(g_1, g_2)) = (g_1, g_2', f_3 - \bar{g}(g_1, g_2')).
\]
So \( \tau_0 = (f_1, f, f_3) \rightarrow (g_1, g_2', g_3) \) is an elementary reduction. By the same argument as above \( g_1, g_2, g_3 \) is simple, which completes the proof of proposition 5.3 \( \Box \)

6 The proof of lemma 5.4

The aim of this section is to give the complete proof of lemma 5.4, thereby clearly demonstrating how the fundamental estimations given in theorem 3.3 play a crucial role. So it suffices to show

**Theorem 6.1** Let \((f_1, f_2, f_3)\) be an automorphism of \( k^3 \) which admits a reduction of type I. If \( a \in (f_1, f_3) \) satisfies \( \deg(a) \leq sn \), then \( a = \beta f_3 + T(f_1) \), for some \( \beta \in k^* \) and \( T(f_1) \in (f_1) > \) with \( \deg T(f_1) < sn \).

The main ingredient in the proof is
Proposition 6.2 Let \((f_1, f_2, f_3)\) be as in 6.1. Then

i) \(\deg(f_1, f_3) > s_n\).

ii) If \(a \in < f_1, f_3 >\), then either \(\pi \in < \overline{f_1, f_3} >\) or \(\deg(a) > s_n\).

It is the second statement which gives sufficient control over the highest degree part of a polynomial in \(< f_1, f_3 >!\) Before we prove this result let us first show how it implies 6.1.

Proof of Theorem 6.1. Since \(\deg(a) \leq s_n\) it follows from 6.2 ii) that \(\pi \in < \overline{f_1, f_3} >\), so \(\pi = \sum c_i \overline{f_1, f_3}^i\) with

\((6.1.1)\) \(\text{ideg}(f_1) + j \text{ideg}(f_3) \leq s_n\).

First we show that terms \(\overline{f_1, f_3}^j \) with \(j \geq 2\) cannot appear in \(\pi\); namely if \(j \geq 2\) then \(\text{deg} f_1 \overline{f_3}^j \geq \text{deg} f_3^j > \text{deg}(f_1) + \text{deg}(f_3)\) (since \(\text{deg}(f_3) > 2n = \text{deg}(f_1)) \geq \text{deg} f_1 f_3 > s_n\) (by 6.2 i), which contradicts (6.1.1).

Also the terms with \(j = 1\) and \(i \geq 1\) cannot appear in \(\pi\); namely for such a term we have \(\text{deg} f_1 \overline{f_3}^j \geq \text{deg}(f_1) + \text{deg}(f_3) \geq \text{deg} f_1 f_3 > s_n\) (by 6.2 i), contradicting (6.1.1) again.

So \(\pi = \beta \overline{f_3} + \lambda \overline{f_1}^i\) with \(2r \leq s_n\). Now observe that \(2r\) is even and \(s\) is odd, so \(2rn < s_n\). Then consider \(a_1 := a - \beta \overline{f_3} - \lambda \overline{f_1}^i\). So \(\deg(a_1) < \deg(a)\). Repeating the above argument with \(a_1\) instead of \(a\) we obtain that \(a_1 = a_1(f_1)\) and \(\deg(a_1) < s_n\).

Hence \(a = \beta \overline{f_3} + T(f_1)\) with \(\deg T(f_1) < s_n\). \(\Box\)

Proof of Proposition 6.2. Since \(f_3\) is reducible by \(g_1, g_2\) there exists \(G(g_1, g_2)\) such that \(g_3 := f_3 - G(g_1, g_2)\) satisfies \(\deg(g_3) < \deg(f_3)\). So \(\overline{f_3} = \overline{G(g_1, g_2)}\).

Claim. \(\overline{f_3} \notin < \overline{g_1, g_2} >\) (so \(G(g_1, g_2) \notin < \overline{g_1, g_2} >\)).

Case 1. \(\deg(f_3) = s_n\). Then \(\deg(\overline{f_3}) = \deg(\overline{f_2}) = \deg(\overline{g_2}) = s_n\). So \(\overline{g_2} = \overline{f_2} - \overline{a \overline{f_3}}\).

Now suppose that \(\overline{f_3} \in < \overline{g_1, g_2} >\). Then \(\deg(\overline{f_3}) = \deg(\overline{f_2}) - \deg(\overline{a \overline{f_3}})\) (by 6.2 i), which contradicts the hypothesis that \(\overline{f_3} \notin < \overline{g_1, g_2} >\).

Case 2. \(\deg(f_3) < s_n\). Then \(\overline{g_2} = \overline{f_2}\), so \(\overline{g_1, g_2} \gg \overline{f_1, f_2}\). Since by hypothesis \(\overline{f_3} \notin < \overline{f_1, f_2} >\) we get \(\overline{f_3} \notin < \overline{g_1, g_2} >\), which completes the proof of the claim.

i) Observe that \(g_1, g_2\) is 2-reduced. Write \(\text{deg} G = q + r\) with \(0 \leq r \leq 1\). If \(q = 0\) then \(\deg G = r \leq 1 < 2(= p)\). So it follows from 3.6 that \(\overline{G} \in < \overline{g_1, g_2} >\), which contradicts the claim. So \(q \geq 1\). Then by 3.3 we get

\[ s_n \geq f_3 = \deg G(g_1, g_2) \geq q^2(s_n - s_n - 2n + \deg(g_1, g_2)) + sn.r.\]

Since \(q \geq 1\) it follows that \(r = 0\). So \(\deg G = 2q\) is even. Hence \(\deg G(\overline{g}) = 2(q - 1) + 1\).

So applying 3.3 to \(\overline{G} \overline{g}\) (whose \("r" = 1\)) we get

\(6.2.1)\) \(\deg G(\overline{g}) \geq (q - 1)N(g_1, g_2) + sn.1 \geq s_n\).

Now observe that

\(\overline{[f_1, f_3]} = [g_1, g_3 + G(g_1, g_2)] = [g_1, g_3] + \overline{G}(g_1, g_2)[g_1, g_2].\)

Since \(\deg([g_1, g_3]) < \deg([g_1, g_2]) + s_n\), by 4.1 b ii), and \(\deg G(\overline{g_1, g_2})[g_1, g_2] \geq s_n + \deg(g_1, g_2)\) (by (6.2.1)) we get

\(10\)
$\deg[f_1, f_3] \geq sn + \deg[g_1, g_2] > sn.$

ii) Now let $a \in <f_1, f_3>$, say $a = G(f_1, f_3)$. If $\overrightarrow{f_1}, \overrightarrow{f_3}$ are algebraically independent over $k$, then $\overrightarrow{a} \in <\overrightarrow{f_1}, \overrightarrow{f_3}>$. So assume that $\overrightarrow{f_1}, \overrightarrow{f_3}$ are algebraically dependent over $k$. Then $f_1, f_3$ is a 2-reduced pair (use that $\deg(f_1) = 2n$ and $\deg(f_3) = sn$, with $s$ odd). Write $\deg G_q = q.2 + r$ with $0 \leq r < 1$. If $q = 0$ then $\deg G = r \leq 1 < 2(= p)$, so by 3.6 $\overrightarrow{a} \in <\overrightarrow{f_1}, \overrightarrow{f_3}>$. So let $q \geq 1$. Then by 3.3

$$\deg(a) = \deg G_q(f_1, f_3) \geq qN(f_1, f_3) + sn.r \geq N(f_1, f_3) > \deg[f_1, f_3]$$

(by (1) in section 3). Since by i) $\deg[f_1, f_3] > sn$ this completes the proof of 6.2 □

7 Final comments

The method described in [7] even gives an algorithm to decide if a given polynomial automorphism of $k^3$ is tame. More precisely it decides if a given automorphism $F$ admits an elementary reduction or a reduction of one of the types I-IV. To decide if $F$ admits a reduction of one of the types I-IV one needs various technical parts of the proof. So we only show how one can decide if $F$ admits an elementary reduction.

So let $F = (f_1, f_2, f_3)$. We show how to decide if $f_3$ is elementary reducible by $f_1, f_2$. If $\overrightarrow{f_1}, \overrightarrow{f_2}$ are algebraically independent over $k$, then $f_3$ is reducible iff $\overrightarrow{f_3} \in <\overrightarrow{f_1}, \overrightarrow{f_2}>$ and this question is easy to decide either by Gröbner basis methods or using the homogeneity of the $\overrightarrow{f_i}$. So assume that $\overrightarrow{f_1}, \overrightarrow{f_2}$ are algebraically dependent over $k$. If $\overrightarrow{f_2} \in <\overrightarrow{f_1}>$, then $\overrightarrow{f_2} = cf_1^t$ for some $c \in k^*$ and $t \geq 1$. Observe that $f_3$ is reducible in $F$ iff it is reducible in $F' := (f_1, f_2 - cf_1^t, f_3)$. Since $\deg F' < \deg F$ the desired result follows by induction on the degree. A similar argument holds if $\overrightarrow{f_1} \in <\overrightarrow{f_2}>$. So we may assume that $f_1, f_2$ is a $*$-reduced pair and that $\deg(f_1) < \deg(f_2)$.

Now suppose that $f_3$ is reducible by $f_1$ and $f_2$. Then there exists a polynomial $G(x, y) \in k[x, y]$ such that $\overrightarrow{f_3} = G(f_1, f_2)$. Write $\deg G = qp + r$ with $0 \leq r < p$. Then by 3.3 and the fact that $N(f_1, f_2) \geq 1$ we get

$$\deg(f_3) = \deg G_q(f_1, f_2) \geq qN(f_1, f_2) + mr \geq q$$

So $q \leq \deg(f_3)$. Also $r < p \leq \deg(f_1)$. So $\deg G = qp + r \leq C := \deg(f_3)\deg(f_1) + \deg(f_1)$. Similarly using the second degree estimation in 3.3 involving $\deg G$ we get $\deg G \leq C$. Hence $G(f_1, f_2)$ belongs to the finite dimensional $k$-vector space $V$ generated by the monomials $f^i f^j$ with $i, j \leq C$. So if we define $\overrightarrow{V}$ to be the finite dimensional $k$-vector space generated by the highest degree homogeneous parts of the elements of $V$, then we get that $f_3$ is reducible by $f_1$ and $f_2$ iff $\overrightarrow{f_3}$ belongs to $\overrightarrow{V}$ and this question is easily to decide by linear algebra.

To conclude this paper let us mention some interesting open problems.

**Problem 1.** Do there exist tame automorphisms of type II-IV ?

**Problem 2.** What happens if $k$ has positive characteristic? Do there exist non-tame automorphisms of $k^3$ ?
In this respect the following result of Stefan Maubach [4], 2001, is interesting. If \( k \) is a finite field and \( F \) an automorphism of \( k^n \), then obviously it induces a bijection on \( k^n \), which we denote by \( E(F) \). So this bijection has a sign i.e. this bijection is either odd or even.

**Theorem 7.1** Let \( k = \mathbb{F}_{2^m} \) with \( m \geq 2 \). If \( F \in \text{Aut}_k k^n \) is tame, then \( E(F) \) is even!

This leads to the following problem

**Problem 3.** Let \( k = \mathbb{F}_{2^m} \), with \( m \geq 2 \). Does there exist \( F \in \text{Aut}_k k^3 \) with \( E(F) \) is odd ?

To formulate the last problem we make the following observations: in 1942 Jung proved the 2-dimensional case of the tame generators problem, in 1972 Nagata constructed his candidate counterexample and finally in 2002 Shestakov and Umirbaev solved the 3-dimensional case. This leads to

**The 30-years cycle problem.** What happens in 2032 ?

**References**


Author’s address:
Department of Mathematics
Postbus 9010
6500 GL Nijmegen
THE NETHERLANDS