# Automorphisms and Coordinates of Polynomial and Free Associative Algebras – 2

Vesselin Drensky
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Sofia, Bulgaria
e-mail: drensky@math.bas.bg
and
Jie-Tai Yu
Department of Mathematics, University of Hong Kong
Hong Kong, China
e-mail: yujt@hku.hk

February 24, 2014

## Recall that:

$K$ is a field of any characteristic;
$X_n = \{x_1, \dots, x_n\}$,
$G(X_n)$, $L(X_n)$, $K\langle X_n\rangle$ – the free group, the free Lie algebra, and the free associative algebra freely generated by $X_n$.
When we speak about algorithms, we assume that the field is constructive and we may perform calculations there.

## Algorithmic problems

**Problem.** If $\varphi$ is an endomorphism of the algebra $K[X_n]$, how to decide whether $\varphi$ is an automorphism?

**Answer.** (Abhyankar and Li, van den Essen, Shannon and Sweedler, 1988-1990) Let $f_j = f_j(X_n) = \varphi(x_j)$, $j = 1, \ldots, n$. We work in the polynomial algebra $K[X_n, Y_n]$ in $2n$ variables and consider its ideal $I$ generated by the polynomials

$$y_j - f_j(X_n), \quad j = 1, \ldots, n.$$

The endomorphism $\varphi$ is an automorphism of $K[X_n]$ if and only if the ideal $I$ has a system of generators

$$x_j - g_j(Y_n), \quad j = 1, \ldots, n.$$

Then the inverse automorphism $\psi = \varphi^{-1}$ of the algebra $K[X_n]$ is determined by the equalities

$$\psi(x_j) = g_j(X_n), \quad j = 1, \ldots, n.$$

### Proof

($\Rightarrow$) Let $\varphi$ be an automorphism of $K[X_n]$ with inverse $\varphi^{-1} : x_j \to g_j(X_n)$. Consider the ideals of $K[X_n, Y_n]$

$$I = (y_j - f_j(X_n) \mid j = 1, \dots, n),\ J = (x_j - g_j(Y_n) \mid j = 1, \dots, n).$$

Since $y_j \equiv f_j(X_n) \pmod{I}$, we have $g_j(Y_n) \equiv g_j(F_n(X_n)) \pmod{I}$. But $x_j = \varphi\varphi^{-1}(x_j) = g_j(F_n(X_n))$. Hence $x_j - g_j(Y_n) \in I$ and $J \subseteq I$. Similarly $I \subseteq J$ and hence $I = J$.

($\Leftarrow$) Let $I = J$. Then $x_j \equiv g_j(Y_n) \pmod{J}$, $y_j \equiv f_j(X_n) \pmod{I}$, $I = J$ and hence $x_j \equiv g_j(F_n(X_n)) \pmod{I}$. The map

$$(X_n, Y_n) \to (x_1, \ldots, x_n, y_1 - f_1(X_n), \ldots, y_n - f_n(X_n))$$

defines an automorphism of $K[X_n, Y_n]$. Changing the coordinates $x_j \to x_j$, $y_j \to z_j = y_j - f_j(X_n)$, we obtain that $I$ is generated in $K[X_n, Z_n]$ by $Z_n$. Since $x_j - g_j(F_n(X_n)) \in I$ does not depend on $Z_n$, we derive that $x_j = g_j(F_n(X_n))$ in $K[X_n]$. Similarly $y_j = f_j(G_n(Y_n))$ in $K[Y_n]$. Hence $x_j = f_j(G_n(X_n))$ in $K[X_n]$ which means that the endomorphism $\psi$ of $K[X_n]$ defined by $x_j \to g_j(X_n)$ is the inverse of $\varphi$.

## For polynomial algebras:

The problem whether an endomorphism of $K[X_n]$ is an automorphism can be solved by Gröbner bases techniques. Hence it can be solved efficiently.

## Algorithm.

Consider the ideal of $K[X_n, Y_n]$ generated by

$$y_j - f_j(X_n), \quad j = 1, \dots, n.$$

Define a lexicographic order on $K[X_n, Y_n]$ assuming that $x_i > y_j$, $i, j = 1, \dots, n$. Apply the Buchberger algorithm to fing the Gröbner basis of $I$. Then $\varphi$ is an automorphism of $K[X_n]$ if and only if the Gröbner basis of $I$ consists of

$$x_j - g_j(Y_n), \quad j = 1, \dots, n.$$

### Free associative algebras:

An endomorphism $\varphi$ of $K\langle X_n\rangle$ is an automorphism if and only if the ideal

$$I = (y_j - \varphi(x_j) \mid j = 1, \dots, n) \lhd K\langle X_n, Y_n\rangle$$

has a system of generators

$$x_j - g_j(Y_n), \quad j = 1, \dots, n.$$

Then $\varphi^{-1}(x_j) = g_j(X_n)$, $j = 1, \dots, n$.
Gröbner bases exist also for free associative algebras but not always it is possible to find them effectively. (The Gröbner basis may be infinite even if the ideal is finitely generated.) Also, the word problem is not algorithmically solvable for free associative algebras.

### Free associative algebra:

The problem whether an endomorphism $\varphi$ of the algebra $K\langle X_n\rangle$ is an automorphism can be solved efficiently using the algorithm of Yagdzhev (1980).

### Face polynomials:

Let $f(X_n) \in K[X_n]$. The polynomials

$$f(0, x_2, \dots, x_n), f(x_1, 0, x_3, \dots, x_n), \dots, f(x_1, \dots, x_{n-1}, 0)$$

are called *faces* of the polynomial $f(X_n)$.

### Theorem

If $\varphi$ is an automorphism of $K[X_n]$ and $\varphi(x_i) = f_i(X_n)$, then $\varphi$ is uniquely determined by its $n^2$ face polynomials $f_i(x_i, \dots, x_{j-1}, 0, x_{j+1}, \dots, x_n)$.
If $\varphi$ is an endomorphism, there is an algorithm which decides, from the $n^2$ face polynomials, whether $\varphi$ is an automorphism and if "yes" reconstructs it.

Many contributions for parts of the theorem:

van den Essen (1986)
McKay and Wang (1986, 1988)
Moh, McKay, and Wang (1988)
Li (1989)
Dennis, Boo Barkee (1990)
van den Essen and Kwieciński (1992).

### Proof of the uniqueness:

Let $n = 3$ (for simplicity of the notation only) and let the automorphisms $\varphi$ and $\psi$ have the same face polynomials. Let

$$\varphi(x_i) = f_i, \varphi^{-1}(x_i) = g_i, \psi(x_i) = u_i, \psi^{-1}(x_i) = v_i.$$

We work in $K[X_3, Y_3]$ and consider ideals there:

$$(y_1 - f_1(X_3), y_2 - f_2(X_3), y_3 - f_3(X_3)) = (x_1 - g_1(Y_3), x_2 - g_2(Y_3), x_3 - g_3(Y_3))$$

Substituting $x_1 = 0$ we obtain

$$(y_1 - f_1(0, x_2, x_3), y_2 - f_2(0, x_2, x_3), y_2 - f_2(0, x_2, x_3))$$

$$= (g_1(Y_3), x_2 - g_2(Y_3), x_3 - g_3(Y_3)) \triangleleft K[x_2, x_3, Y_3].$$

Similar arguments for $\psi$ give

$$(y_1 - u_1(0,x_2,x_3), y_2 - u_2(0,x_2,x_3), y_2 - u_2(0,x_2,x_3))$$

$$= (v_1(Y_3), x_2 - v_2(Y_3), x_3 - v_3(Y_3)) \lhd K[x_2, x_3, Y_3].$$

Since the faces of $f_i$ and $u_i$ are equal, we obtain

$$(g_1(Y_3), x_2 - g_2(Y_3), x_3 - g_3(Y_3)) = (v_1(Y_3), x_2 - v_2(Y_3), x_3 - v_3(Y_3))$$

in $K[x_2, x_3, Y_3]$. Hence

$$g_1(Y_3) = a_1 v_1(Y_3) + a_2(x_2 - v_2(Y_3)) + a_3(x_2 - v_2(Y_3)),$$

$a_i \in K[x_2, x_3, Y_3]$. If we let $x_i = v_i(Y_3)$ we obtain

$$g_1(Y_3) = b_1(Y_3)v_1(Y_3), \quad b_1(Y_3) \in K[Y_3].$$

Similarly, $v_1(Y_3) = c_1(Y_3)g_1(Y_3)$, $c_1(Y_3) \in K[Y_3]$, and $b_1, c_1 \in K^*$.

We know $g_i(Y_3) = b_i(Y_3)v_i(Y_3)$ (i.e., $\varphi^{-1}(x_i) = b_i\psi(x_i)$), $b_i \in K^*$, $i = 1, 2, 3$. Then (easy to see)

$$f_i(X_3) = \psi(x_i) = b_i\varphi(x_i), \text{ i.e., } u_i(x_1, x_2, x_3) = f_i(b_1x_1, b_2x_2, b_3x_3).$$

Since $\varphi$ is an automorphism, $f_i$ has the form

$$f_i(X_3) = \alpha_i + \sum_{j=1}^{3} \alpha_{ji}x_j + \tilde{f}_i(X_3), \alpha_i, \alpha_{ji} \in K, \text{mindeg}(\tilde{f}_i) \geq 2.$$

The matrix $(a_{ji})$ is invertible and some $a_{1i}$ is different from 0. Let $\alpha_{11} \neq 0$. From $u_1(x_1, x_2, x_3) = f_1(b_1x_1, b_2x_2, b_3x_3)$ we obtain

$$f_1(x_1, 0, x_3) = u_1(x_1, 0, x_3) = f_1(b_1x_1, 0, b_3x_3).$$

Letting $x_3 = 0$ we have $f_1(x_1, 0, 0) = f_1(b_1x_1, 0, 0)$ and $\alpha_{11} = \alpha_{11}b_1$. Hence $b_1 = 1$. Similarly $b_2 = b_3 = 1$ and $\varphi = \psi$.

(i) How to recognize whether an endomorphism of $(K[z])[x,y]$ is an automorphism? and (ii) if the answer is "YES", whether it is tame or wild?

(i) We apply the algorithm which works in $K[X_n, Y_n]$ (which holds also for $A[X_n]$)

$$I = (u - \varphi(x), v - \varphi(y))$$

$$= (x - g_1(u,v,z), y - g_2(u,v,z)) \lhd (K[z])[x,y,u,v],$$

$$\varphi^{-1}(x) = g_1(x,y,z), \quad \varphi^{-1}(y) = g_2(x,y,z).$$

## Lemma

Let $\varphi$ be an automorphism of $K(z)[x,y]$ such that $f=\varphi(x), g=\varphi(y)\in(K[z])[x,y]$. Then $\varphi$ is an automorphism of $(K[z])[x,y]$ if and only if its Jacobian matrix

$$J(\varphi)=\begin{pmatrix}\frac{\partial f}{\partial x} & \frac{\partial g}{\partial x}\\ \\ \frac{\partial f}{\partial y} & \frac{\partial g}{\partial y}\end{pmatrix}$$

is invertible in $GL_2(K[z][x,y])$, i.e., its Jacobian (determinant) is a nonzero constant.

## Answer to question (ii):

If $\varphi \in \mathrm{Aut}((K[z])[x,y])$ is a tame automorphism,

$$f = \varphi(x), g = \varphi(y),$$

then one of the degrees (with respect to $x$ and $y$) $\deg_{x,y}(f)$ and $\deg_{x,y}(g)$ divides the other. If $\deg_{x,y}(f) > \deg_{x,y}(g)$, then the homogeneous component (in $x$ and $y$) $\overline{f}$ is proportional to a power of $\overline{g}$, i.e., $\overline{f} = \alpha(z)\overline{g}^k$, $\alpha(z) \in K[z]$.
If $\deg_{x,y}(f) = \deg_{x,y}(g)$, then $\overline{f} = \alpha(z)h(x,y,z)$, $\overline{g} = \beta(z)h(x,y,z)$, $h(x,y,z) \in (K[z])[x,y]$, $\alpha(z), \beta(z) \in K[z]$, and $(\alpha(z), \beta(z)) = 1$.
Again, this gives an algorithm which presents $\varphi$ as a product of elementary automorphisms.

## Coordinate polynomials

A polynomial $f(X_n) \in K[X_n]$ is called a *coordinate* if there is an automorphism $\varphi \in \mathrm{Aut}(K[X_n])$ such that

$$f(X_n) = \varphi(x_1).$$

In the same way one can define coordinates in $A[X_n]$ ($A$ a commutative algebra), in $K\langle X\rangle$, in the free group, in the free Lie algebra, etc.

## Problem

If $f(X_n)$ is a polynomial, how to determine whether is it a coordinate? If the answer is "YES", how to find an automorphism $\varphi$ such that $f(X_n) = \varphi(x_1)$?

## Partial results

**Answer for** $n = 2$, $\mathrm{char}(K) = 0$: (Shpilrain and J.-T. Yu, 1998):
**Theorem.** Let $f(x, y) \in K[x, y]$ and let

$$p(x, y) = f_x = \frac{\partial f}{\partial x}, \quad q(x, y) = f_y = \frac{\partial f}{\partial y}.$$

Then $f(x, y)$ is a coordinate polynomial if and only if the vector-column $(p(x, y), q(x, y))^t$ is the first column of some matrix in $GE_2(K[x, y])$. An equivalent form of this statement is that $(p(x, y), q(x, y))$ can be brought to $(1, 0)$ by the Euclidean algorithm.

The proof contains an algorithm how to find an automorphism which maps $x$ to the coordinate $f(x, y)$.

### Answer for $(K[z])[x,y]$, $\mathrm{char}(K) = 0$:

$f(X_n) \in A[X_n]$ has a unimodular gradient, if the ideal

$$\left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right)$$

generated by its partial derivatives is equal to the whole algebra $A[X_n]$ ($A$ a commutative algebra).

### Theorem

Drensky and J.-T. Yu (2000):
The polynomial $f(x,y) \in K[z][x,y]$ is a coordinate in $K[z][x,y]$ if and only if $f(x,y)$ is a coordinate in $K(z)[x,y]$ with unimodular gradient in $K[z][x,y]$.

## Example

For the Nagata automorphism of $K[z][x,y]$

$$\nu(x) = x - 2(y^2+xz)y - (y^2+xz)^2 z, \nu(y) = y + (y^2+xz)z, \nu(z) = z$$

the partial derivatives of $f(x,y) = \nu(y)$ are

$$p(x,y) = \frac{\partial f}{\partial x} = z^2, \quad q(x,y) = \frac{\partial f}{\partial y} = 1 + 2yz.$$

Since $z$ is invertible in $K(z)[x,y]$, the Euclidean algorithm gives that $q - 2yp/z = 1$. Hence $f(x,y)$ is a coordinate in $K(z)[x,y]$. Now

$$-2yp + zq = z \in (p,q) \triangleleft K[z][x,y], 1 = q - 2y(-2yp + zq) \in (p,q),$$

$f(x,y)$ has unimodular gradient and hence is a coordinate in $K[z][x,y]$.

Theorem.

(Drensky and Yu, 2000) The following statements for $f(x, y) \in K[z][x, y]$ are equivalent:
(i) The polynomial $f(x, y)$ is a tame coordinate in $K[z][x, y]$;
(ii) There exists a matrix $g \in GE_2(K[x, y, z])$ such that

$$(f_x \ f_y)g = (1 \ 0),$$

i.e., $(f_x \ f_y)$ can be brought to $(1 \ 0)$ by elementary transformations;
(iii) Applying the Euclidean algorithm to $f_x$ and $f_y$, the result is equal to 1.

Again, there is an algorithm to find a tame automorphism which sends $x$ to the tame coordinate $f(x, y)$.

## Example

The Nagata automorphism again:

$$f(x,y)=\nu(y),\quad f_x=z^2,\quad f_y=2yz+1.$$

We cannot apply the Euclidean algorithm in $K[x,y,z]$ because the leading monomials of $f_x$ and $f_y$ do not divide each other. Hence $f(x,y)$ is a wild coordinate in $K[z][x,y]$.

## Applications to $K\langle x, y, z\rangle$

(Shpilrain and Yu, Drensky and Yu):
There is an algorithm which determines whether a polynomial $f(x, y)$ in the free associative algebra $K\langle x, y\rangle$ is a coordinate. Similarly, one can decide whether $f(x, y) \in K[z]\langle x, y\rangle$ is a tame coordinate.
In both the cases, if the answer is affirmative, the algorithm produces a concrete tame automorphism sending $x$ to $f(x, y)$.

## Tame and wild coordinates in $K[x, y, z]$ and $K\langle x, y, z\rangle$:

**Problem** If $\varphi$ is a wild automorphism of $K[x, y, z]$, does there exist a tame automorphism $\psi$ of $K[x, y, z]$ such that $\varphi(x) = \psi(x)$. If such a tame automorphism does not exist, $\varphi(x)$ is called *a wild coordinate*. One defines *wild coordinates* in $K\langle x, y, z\rangle$ similarly.

### Theorem

(Umirbaev and Yu, 2004).
Let $\mathrm{char}(K) = 0$. Then the polynomial algebra $K[x, y, z]$ has wild coordinates. In particular, the two nontrivial coordinates $\nu(x)$ and $\nu(y)$ of the Nagata automorphism are wild.

This result may be considered as a stronger form of the Nagata conjecture because it implies the Nagata conjecture but not vice versa. In any case the existing proof uses essentially the methods of Shestakov and Umirbaev for the proof of the Nagata conjecture.

### Theorem

(Drensky and Yu, 2006).
Let $\mathrm{char}(K) = 0$. Then the free associative algebra $K\langle x, y, z\rangle$ has wild coordinates. In particular, the two nontrivial coordinates $\alpha(x)$ and $\alpha(y)$ of the Anick automorphism are wild.

Again, this result may be considered as a stronger form of the Anick conjecture because it implies the Anick conjecture but not vice versa. The proof uses essentially the methods of Umirbaev for the proof of the Anick conjecture although it covers some automorphisms of $K\langle x, y, z\rangle$ whose wildness do not follow from the proof of Umirbaev.

## Test polynomials

Let $\mathfrak{E}$ be a class of endomorphisms of $K[X_n]$. The polynomial $p(X_n) \in K[X_n]$ is a *test polynomial* in the class $\mathfrak{E}$ if any endomorphism $\varphi \in \mathfrak{E}$ which fixes $p(X_n)$ is an automorphism.
If $\mathfrak{E}$ is the class of all endomorphisms, we speak simply about test polynomials.
Test elements can be defined also for other free objects – for free groups, free Lie algebras, free associative algebras, etc. At first test elements were introduced by Shpilrain (1993) in the case of free groups.

## Example – the commutator test

(Dicks, 1982)
The commutator $[x, y]$ is a test polynomial for the free algebra $K\langle x, y\rangle$.

## Related notions

The subalgebra $S$ of the algebra $R$ is a *retract* if the identity map $\iota : S \to S$ can be extended to a homomorphism (called a projection or a retraction) $\pi : R \to S$.
**Trivial example:** $m < n$ and $S = K[X_m]$, $R = K[X_n]$.

## Relation with test elements

For free objects, the test elements do not belong to any proper retract and there is a conjecture that any element which is not in a proper retract is a test element.

### Test, elements, retracts, and elements of maximal outer rank

The *outer rank* of a element $p(X_n)$ in $K[X_n]$ (or in $K\langle X_n\rangle$, or in the free group $G(X_n)$, etc.) is the minimal number of generators $x_i$ on which an automorphic image of $p$ can depend.

(Turner, 1996): An element of the free group $G(X_n)$ is a test element if and only if it is not contained in any proper retract. An element of $G(X_n)$ is of maximum outer rank if and only if it is a test element for automorphisms in the class of all monomorphisms.

## Free Lie (super)algebras

(Mikhalev and Zolotykh, 1995): An element in a free Lie (super)algebra is a test polynomial in the class of all monomorphisms if and only if it has the maximum rank.
(Shpilrain, 1995): A homogeneous element of a free Lie algebra is a test element if and only if it has the maximum rank.
(A.A. Mikhalev and Yu, 1997): Test elements of a finitely generated free Lie algebra are exactly those elements which are not contained in any proper retract of the algebra.

These results heavily rely on the fact that every subgroup of a free group is free and on a similar result for free Lie algebras and subalgebras.

## Description of retracts for $\mathbb{C}[x,y]$:

(Costa, 1977): Every proper retract of $\mathbb{C}[x,y]$ (i.e. different from $\mathbb{C}[x,y]$ and $\mathbb{C}$) is of the form $\mathbb{C}[p]$ for some $p(x,y) \in \mathbb{C}[x,y]$.

(Shpilrain and Yu, 1999):

If $\mathbb{C}[p(x,y)]$ is a proper retract of $\mathbb{C}[x,y]$, then there exists an automorphism of $\mathbb{C}[x,y]$ which brings $p(x,y)$ to the form $x + yq(x,y)$, $q(x,y) \in \mathbb{C}[x,y]$, and every polynomial of the form $x + yq(x,y)$ generates a proper retract of $\mathbb{C}[x,y]$.

The polynomial $p(x,y)$ generates a retract of $\mathbb{C}[x,y]$ if and only if there is an endomorphism of $\mathbb{C}[x,y]$ which takes $p(x,y)$ to $x$.

(Drensky and Yu, 2002): The polynomial $p(x,y) \in \mathbb{C}[x,y]$ belongs to a proper retract of $\mathbb{C}[x,y]$ if and only if $p(x,y)$ is fixed by some endomorphism of $\mathbb{C}[x,y]$ with nontrivial kernel. (This removes the essential requirement for idempotence of the projection in the definition of retracts.)

(van den Essen and Shpilrain, 1997): Any test polynomial $p(X_n) \in \mathbb{C}[X_n]$ is of maximal outer rank, namely $n$.
(Drensky and Yu, 2002): A polynomial of positive degree $p(x, y) \in \mathbb{C}[x, y]$ does not belong to a proper retract if and only if it recognizes monomorphisms in the class of all endomorphisms.
(Drensky and Yu, 1998): Many examples of test polynomials for $K[X_n]$ and $K\langle X_n\rangle$.

(Drensky and Yu, 1998):
Exponential automorphisms of $K[X_n]$ ($\mathrm{char}(K) = 0$) have no test polynomials.
The polynomial $p(x, y, z) = y^2 + xz$ is not a test polynomial: It is fixed by the endomorphisms $\psi$ of $K[x, y, z]$ the form

$$\psi(x) = x - 2yu - zu^2, \psi(y) = y + zu, \psi(z) = z,$$

where $u = u(x, y, z) \in K[x, y, z]$ is an arbitrary polynomial.
Clearly, $u$ may be chosen in such a way that $\psi$ is a monomorphism and not an automorphism.

## Definitions

A polynomial $p(X_n) \in \mathbb{C}[X_n]$ of degree $d$ is called a *generic polynomial* in $\mathbb{C}[X]$ if the coefficients $a_{i_1 \dots i_n}$ of all monomials $x_1^{i_1} \cdots x_n^{i_n}$ with $0 \leq i_1 + \cdots + i_n \leq d$ in

$$p(X_n) = \sum_{0 \leq i_1 + \cdots + i_n \leq d} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

are nonzero and algebraically independent over $\mathbb{Q}$.
(J.-T. Yu, 1997): An *identity polynomial* of $K[X_n]$ is defined as a polynomial $p(X_n) \in K[X_n]$ such that if $\varphi(p) = p(X_n)$, where $\varphi$ is an automorphism of $K[X_n]$, then $\varphi = \iota$ is the identity automorphism.

### Theorems

(J.-T. Yu, 1997): Every generic polynomial $p(X_n) \in \mathbb{C}[X_n]$ of degree $d \geq n > 2$ is an identity polynomial.
(Jelonek 2000): A “generic” polynomial $p(x, y)$ of degree $\geq 4$ is a test polynomial but the only automorphism which $p(x, y)$ recognizes is the identity automorphism.