# The conjugacy problem for two-by-two matrices over polynomial rings

Fritz J. Grunewald[1], Natalia K. Iyudu[2]

[1] Mathematisches Institut, Henrich Heine Universität,
40225 Düsseldorf, Germany,
[2] Department of Pure Mathematics, Queen's University Belfast,
Belfast BT7 1NN, U.K.

**e-mails:** n.iyudu@qmul.ac.uk, fritz@math.uni-duesseldorf.de

**Abstract**

We give an effective solution of the conjugacy problem for two by two matrices over the polynomial ring in one variable over a finite field.

## Contents

# 1 Introduction

We consider here the conjugacy problem in the ring of two by two matrices $M(2, \mathbb{F}[x])$ over the polynomial ring $\mathbb{F}[x]$, where $\mathbb{F}$ is a finite field. We say that two matrices $A$, $B \in \mathrm{M}_2(\mathbb{F}[x])$ are conjugate if there is a conjugating matrix $U$ in the group $\mathrm{GL}\,(2, \mathbb{F}[x])$ of invertible matrices over $\mathbb{F}[x]$, such that $U$ satisfies $B = UAU^{-1}$. In the following we write $\deg(p)$ for the degree of a polynomial $p \in \mathbb{F}[x]$ and $\deg(A)$ for the maximal degree of the entries of $A \in \mathrm{M}_2(\mathbb{F}[x])$. We prove:

**Theorem 1.1** *Let $\mathbb{F}$ be a finite field with $q$ elements and $A$, $B \in \mathrm{M}_2(\mathbb{F}[x])$. Let $\delta$ be the maximum of* $\deg(A)$, $\deg(B)$*. If $A, B$ are conjugate, then there is a conjugating matrix $U$ with* $\deg(U) \leq (1 + q)\delta q^{7\delta}$.

For certain pairs of matrices $A$, $B \in \mathrm{M}_2(\mathbb{F}[x])$ the estimate of the degrees of the entries of $U$ can be improved to be linear in $\delta$ not depending on $q$ (see Proposition 4.2). Theorem 1.1 shows that there is an algorithm which decides whether two matrices $A$, $B \in \mathrm{M}_2(\mathbb{F}[x])$ are conjugate or not. Hence we can state:

**Corollary 1.2** *Let $\mathbb{F}$ be a finite field, then the conjugacy problem in the group* $\mathrm{GL}\,(2, \mathbb{F}[x])$ *is effectively solvable.*

Corollary 1.2 should be compared with the solution of the conjugacy problem in an arithmetic group. The conjugacy problem for $\mathrm{GL}\,(n, \mathbb{Z})$ ($n \in \mathbb{N}$) was solved in [3]. But even in the case $n = 2$ no explicit estimates like those from Theorem 1.1 are known. Also the algorithms described in [4], which solve the conjugacy problem in any arithmetic group, do not give estimates for the degree of a conjugating matrix. The method of solution employed in [3] for the case of $\mathrm{GL}\,(n, \mathbb{Z})$ $(n \in \mathbb{N})$ can be extended (without giving any estimates) to the case of $\mathrm{GL}\,(n, \mathbb{F}[x])$ $(n \in \mathbb{N}$, $\mathbb{F}$ a finite field) when the characteristic of the field $\mathbb{F}$ does not divide the size $n$ of the matrices. Also our method in [3] provides extra difficulties in case $\mathbb{F}$ has characteristic 2. Further features of the conjugacy problem in $\mathrm{GL}\,(2, \mathbb{F}[x])$ are described in Section 7.

Given a matrix $A \in \mathrm{GL}\,(2, \mathbb{F}[x])$ we define

$$\mathrm{Z}(A) := \{\, U \in \mathrm{GL}\,(2, \mathbb{F}[x]) \;\mid\; UAU^{-1} = A \,\} \tag{1}$$

to be its centralizer. In case $A \neq \mathbf{1}$ is semisimple it is well known that $\mathrm{Z}(A)$ is either finite or the direct product of an infinite cyclic group by a finite group. By our methods we can give an estimate for the degrees of the entries of a generator of the infinite part:

**Theorem 1.3** *Let $\mathbb{F}$ be a finite field with $q$ elements and $A \in \mathrm{GL}\,(2, \mathbb{F}[x])$ a semisimple matrix, not equal to the identity matrix, such that Z(A) is infinite. Then there is a matrix $U \in \mathrm{Z}(A)$ which generates Z(A) up to a finite group with* $\deg(U) \leq \deg(A) q^{2\deg(A)}$.

Our method to prove Theorem 1.1 uses a reduction to a quadratic equation in two variables. As a special case Pell's equation

$$u^2 + Dv^2 = 1 \tag{2}$$

with $D \in \mathbb{F}[x]$ arises. Let us call $D \in \mathbb{F}[x]$ to be positive if it is neither constant nor a square, has even degree and highest coefficient a square. Let us furthermore call a solution $(u, v)$ of (2) trivial if $u$, $v \in \mathbb{F}$ holds. We prove:

**Theorem 1.4** *Let $\mathbb{F}$ be a finite field with $q$ elements and $D \in \mathbb{F}[x]$ a positive polynomial. Then (2) has a nontrivial solution $(u, v)$ with* $\deg(u)$, $\deg(v) \leq q^{\deg(D)}$.

Pell's equation (2) has been studied extensively in the paper of Emil Artin of 1924 [1]. He investigate Pell's equation through continued fraction expansions. But he assumed that the characteristic of $\mathbb{F}$ is not equal to 2. Our result in Theorem 1.4 follows straightforward from [1]. We then modify Artin's technique for the case of characteristic 2.

Following our reduction we have to analyze the solution of the general quadratic equation

$$au^2 + buv + cv^2 = d$$

where $a, \dots, d$ are polynomials in $\mathbb{F}[x]$. We use new degree function on certain quadratic extension rings of $\mathbb{F}[x]$ in the imaginary case and control the behavior of continued fraction expansion in the real case.

Note that as we will see while the case of characteristic 2 in some sense more difficult the estimations for algorithms in this case which we obtain turned out be better than in the case of the other finite fields.

It worth mentioning also that the reduction step itself gives quite noticeable impact to the whole estimate of the degree of conjugating matrix.

# 2 Reduction to a quadratic equation

Let $\mathbb{F}$ be a field. We consider here pairs of matrices

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(\mathbb{F}[x]),$$

which we call rationally conjugate if they are conjugate by an element of $\mathrm{GL}\,(2, \mathbb{F}(x))$, where $\mathbb{F}(x)$ is a field of rational functions over $\mathbb{F}$. Being rationally conjugate implies the conditions:

$$Tr(A) = Tr(B), det(A) = det(B).$$

Suppose we want to find a matrix

$$U = \begin{pmatrix} u & p \\ v & q \end{pmatrix} \in GL_2(\mathbb{F}[x]),$$

which conjugates $A$ to $B$. We are lead then to four linear equations given by the matrix entries of $UA - BU$ in the variables $u, p, v, q$, plus the quadratic equation $det(U) \in \mathbb{F}^* = \mathbb{F}\backslash\{0\}$. Elementary considerations of this system of equations proves:

**Lemma 2.1** *Suppose the matrices $A, B \in \mathrm{M}_2(\mathbb{F}[x])$ satisfy $a_{21} = b_{21} = 0$. Let $\delta$ be the maximum of the degrees of the entries of $A, B$. Then $A, B$ are conjugate by an element of $\mathrm{GL}\,(2, \mathbb{F}[x])$ if and only if they are conjugate by $U \in \mathrm{GL}\,(2, \mathbb{F}[x])$ with $deg(U) \leq \delta$.*

The above lemma proves Theorem 1.1 in the special case of upper triangular matrices $A, B$.

Let $char\,\mathbb{F} = 2$. The conjugating condition $UAU^{-1} = B$ for $U \in \mathrm{GL}\,(2, \mathbb{F}[x])$ is equivalent to the system

$$uq + pv \in \mathbb{F}^* \tag{3}$$

$$UA = BU \tag{4}$$

where $U = \left( \begin{array}{cc} u & p \\ v & q \end{array} \right)$, $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ is the multiplicative group of the field $\mathbb{F}$. Since the set of conjugating matrices is stable under multiplication by a nonzero constant and we have a unique square root in our field, the solvability of the system (3, 4) is equivalent to the solvability of the same system with (3) replaced by

$$uq + pv = 1 \tag{5}$$

The quadratic equation (5) with additional linear conditions (4) can be reduced to one quadratic equation in two different ways.

First, using the procedure of construction of the generating system of syzygies module ([2]) for the linear system (4). Another way is a direct substitution of the solution in rational functions of the linear system (4). In both cases we obtain an equation of the type $au^2 + buv + cv^2 = d$, but in the first case with variables of different meaning, in the second case with some additional divisibility conditions. We will follow the second way. Let $A = \left( \begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right)$, $B = \left( \begin{array}{cc} b_{11} & b_{12} \\ b_{21} & b_{22} \end{array} \right) \in M_2(\mathbb{F}[x])$, substituting rational solutions

$$p = \frac{(a_{11} + b_{11})u + b_{12}v}{a_{21}}, q = \frac{b_{21}u + (a_{11} + b_{11})v}{a_{21}} \tag{6}$$

from (4) to (5) we obtain the equation

$$b_{21}u^2 + (b_{11} + b_{22})uv + b_{12}v^2 = a_{21}. \tag{7}$$

To ensure that $p$ and $q$ are polynomials, for the solutions $u, v$ of (7) we have to check that $a_{21}\Big|(a_{11} + b_{11})u + b_{12}v$ and $a_{21}\Big|b_{21}u + (a_{11} + b_{11})v$.

We can consider separately quite an easy case when one of matrices is diagonal. Matrices $A, B$ where B is diagonal are conjugate if and only if $\frac{a_{12}(b_{22}-b_{11})}{g.c.d.(a_{11}-b_{11},a_{12})g.c.d.(a_{11}-b_{22},a_{12})} \in \mathbb{F}^*$ (in case when $(a_{11} - b_{11}, a_{12}) \neq (0, 0)$ and $(a_{11} - b_{22}, a_{12}) \neq (0, 0)$). In case $(a_{11} - b_{11}, a_{12}) = (0, 0)$ the condition looks slightly different: $\frac{(b_{11}-a_{22})(b_{22}-a_{11})-a_{12}a_{21}}{g.c.d.(b_{11}-a_{22},a_{12})g.c.d.(a_{11}-b_{22},a_{12})} \in \mathbb{F}^*$.

After that we can restrict ourselves by the case $(a_{12}, a_{21}) \neq (0,0)$ and $(b_{12}, b_{21}) \neq (0,0)$. Since any matrix is conjugate with it's transposed, we can assume without loss of generality that $a_{21}$ and $b_{21}$ are non-zero.

# 3 Preliminary considerations for the solution of the quadratic equation $au^2 + buv + cv^2 = d$

We study here the equation $au^2 + buv + cv^2 = d$ with $a \neq 0$. Multiplying the equation by $a$ and making the change of variables $u_1 = au$, $v_1 = v$ we obtain the equation $u_1^2 + bau_1v_1 + cav_1^2 = da$ with the monic polynomial in the lefthand side. After we find a solution, we have to check whether $a$ divides $u_1$ and only in this case $a|u_1$ will give a solution of the initial equation.

We consider the following three cases determined by the nature of the roots of the equation

$$t^2 + bt + c = 0. \tag{8}$$

Case 1. Equation (8) is solvable in $\mathbb{F}(x)$. Note, that in fact it means that (8) is solvable in $\mathbb{F}[x]$. If $\frac{F}{Q}$ is a rational solution and g.c.d.$(F, Q) = 1$, then from $F^2 + bFQ + cQ^2 = 0$ follows $Q\Big|F^2$, hence $Q$ can be only constant and the solution is in fact polynomial. In this case $d = u^2 + buv + cv^2 = (u + \Delta v)(u + (b + \Delta)v)$ is a product of two polynomials. There exists a finite set of factorizations of $d$ into two multiples from $\mathbb{F}[x]$, hence we obtain a finite number of linear systems on $u, v$.

Let us mention that if $b = 0$ then we have a rational solutions (we are in case 1). Indeed, let $b = 0$: $u^2 + cv^2 = d$. We can just present the coefficients as follows: $c(x) = c_0(x^2) + xc_1(x^2), d(x) = d_0(x^2) + xd_1(x^2)$. If $u = \sum\limits_{i=0}^{n} u_i x^i$, let $\widetilde{u} = \sum\limits_{i=0}^{n} u_i^2 x^i$, then $u^2(x) = \widetilde{u}(x^2)$. Considering separately cases of even and odd degrees on $x$ we get two linear equations on $\widetilde{u}$ and $\widetilde{v}$:

$$\begin{cases} \widetilde{u} + c_0\widetilde{v} = d_0, \\ c_1\widetilde{v} = d_1. \end{cases}$$

If $c_1 = d_1 = 0$ there are infinitely many rational solutions: $\widetilde{u} = -\frac{d_0}{c_0}\widetilde{v}$. Otherwise, there is at most one rational solution. For any solution $\widetilde{u}$ and $\widetilde{v}$ we can uniquely determine $u$ and $v$: $u_i = \sqrt{\widetilde{u}_i}$ and $v_i = \sqrt{\widetilde{v}_i}$, — due to the existence and uniqueness of square roots in our field $\mathbb{F}$.

The other two cases are more essential and will compose our main treatment later on.

From this point we will suppose that the equation (8) has no rational solutions, particularly $b \neq 0$.

Let us define a *degree function on* $\mathbb{F}[x]$ as an ordinary degree on non-zero polynomials and $\deg(0) = -\infty$.

We deal with the completion of $\mathbb{F}[x]$ by the valuation $|p| = 2^n$, where $n = \deg\, p$ (valuation of zero is 1). This completion is the algebra of formal power series $K = \mathbb{F}((x)) = \{\sum_{i=-\infty}^{d} \alpha_i x^i, \alpha_i \in \mathbb{F}, d \in \mathbb{Z}\}$.

Here is an essential in what follows

**Definition.** *Let* $\rho = \sum_{-\infty}^{d} \alpha_n x^n$ *be a power series. We say that* $d$ *is a degree of* $\rho$ *if* $\alpha_d \neq 0$.

Case 2. If (8) is solvable in $K \backslash \mathbb{F}[x]$, we say that it is a *real* case.

Case 3. In case when the solution can not be presented as a power series, we say it is an *imaginary* case.

Let us consider now the ring (and corresponding function field) $R = \mathbb{F}[x,t]/f_x(t)$, where $f_x(t) = t^2 + bt + c$, $b, c \in \mathbb{F}[x]$. Obviously elements of $R$ can be uniquely presented as $u + \Delta v$, where $u, v \in \mathbb{F}[x]$ and $f_x(\Delta) = 0$. We can define the *norm* of an element $\omega = u + \Delta v$ as $N(u + \Delta v) = F(u,v) = u^2 + buv + cv^2$. Let define the *conjugate* element for $\omega$ as follows: $\omega' = u + (b + \Delta)v$.

It is easy to check that the introduced notions of norm and conjugate element satisfy the natural properties.

**Lemma 3.1** *a).* $N(\omega) = \omega\omega'$; *b).* $(\omega_1\omega_2)' = \omega_1'\omega_2'$. *c).* $N(\omega_1\omega_2) = N(\omega_1)N(\omega_2)$. *d).* $N(\omega^{-1}) = N(\omega)^{-1}$.

**Lemma 3.2** *An element* $\epsilon$ *is a unit of* $R$ *if and only if* $N(\epsilon) \in \mathbb{F}^*$.

**Proof**. If $\epsilon^{-1}$ does exist then by lemma 3.1 c). and d). $N(\epsilon\epsilon^{-1}) = N(\epsilon)N(\epsilon^{-1}) = N(\epsilon)N(\epsilon)^{-1} = 1$. Hence $N(\epsilon)$ is an invertible polynomial, i.e. $N(\epsilon) \in \mathbb{F}^*$. □

We treat real and imaginary cases in different ways, thus we need first to be able to distinguish these cases. The following proposition serve for this.

Our equation as earlier is

$$u^2 + buv + cv^2 = d. \tag{9}$$

**Proposition 3.3**

I. *If* $\deg \mathrm{c} > 2\deg \mathrm{b}$ *and* $\deg c$ *is odd then we are in the imaginary case.*

II. *If* $\deg c \geq 2\deg b$ *and* $\deg c$ *is even then there exists an invertible linear change of variables which turns the equation into new one* $u^2 + buv + \widetilde{c}v^2 = d$, *with* $\deg \widetilde{c} < \deg c$.

III. *If* $\deg c = 2\deg b$, *we have two possibilities. In case if the equation* $b_0^2t^2 + b_0^2t + c_0 = 0$ *(* $b_0, c_0 \in \mathbb{F}$ *– coefficients near highest terms of* $b$ *and* $c$ *) is solvable in* $\mathbb{F}$, *there exists a change of variables which turns the equation into new one* $u^2 + buv + \widetilde{c}v^2 = d$, *with* $\deg \widetilde{c} < \deg c$. *Otherwise we are in the imaginary case.*

IV. *If* $\deg c < 2\deg b$ *we are in the real case.*

**Proof.** I. Suppose that $\omega = \sum\limits_{-\infty}^{m} a_n t^n \in K$ is a root of the equation $\omega^2 + b\omega + c = 0$, $a_n \neq 0$. It is necessary for the cancellation that the degrees of a pair of terms in this equation are equal and the degree of the third one is not grater than that. A priori there exist three possibilities.

1). $\deg \omega^2 = \deg b\omega$. Then $\deg(\omega^2 + b\omega) \leq 2\deg b < \deg c$ and cancellation is in fact impossible.

2). $\deg b\omega = \deg c$. Hence $\deg \omega = \deg c - \deg b$ and $\deg(b\omega + c) \leq \deg c < \deg \omega^2$ and cancellation is again impossible.

3). $\deg \omega^2 = \deg c$. This case is not possible because $\deg c$ have to be odd.

This means that there are no solutions of (9) in power series.

II.

We try to find desired change of variables in the form:

$$\begin{cases} u' = u + brv, \\ v' = v \end{cases}$$

In that case we have to find $r$ such that $\deg(b^2r^2 + b^2r + c) < \deg c$. Highest terms in this sum are $b^2r^2$ and $c$ ($\deg c > 2\deg b$, hence $\deg r \neq 0$). To provide their cancellation we take $\deg r = \frac{1}{2}(\deg c - 2\deg b)$. Coefficients near the highest terms also have to coincide: $b_0^2r_0^2 = c_0$. We ensure this due to the existence of a square root in the basic field $\mathbb{F}$: $r_0 = \frac{\sqrt{c_0}}{b_0}$. The desired $r$ is then for example $\frac{\sqrt{c_0}}{b_0}t^{\frac{1}{2}\deg c - \deg b}$.

III.

In the case deg$c = 2$deg$b$ we are again trying to find the change of variables of the same type like in II, such that $\deg(b^2r^2 + b^2r + c) <$ deg$c$. Now deg$r$ have to be zero and cancellation of the highest terms is possible if and only if the equation $b_0^2r^2 + b_0^2r + c_0 = 0$ solvable in $\mathbb{F}$. If so, after corresponding change of variables we get an equation with the free term $c$ of the smaller degree. Otherwise, let us show that we are in the imaginary case, i.e. there are no solutions of the equation $\Delta^2 + b\Delta + c = 0$ in $\mathbb{F}((x))$. If we suppose that such a solution does exist then deg$\Delta =$ deg$b$ and $\Delta_0^2 + b_0\Delta_0 + c_0 = 0$ ($\Delta_0 \in \mathbb{F}$ is a coefficient near the highest term of $\Delta$). But this means that the equation $b_0^2t^2 + b_0^2t + c_0 = 0$ is also solvable: $t = \frac{\Delta_0}{b_0}$. Thus we are in the imaginary case here if the equation is unsolvable in $\mathbb{F}$.

IV.

Let $\Delta \in K\backslash\mathbb{F}[x]$ be the root of (8): $\Delta^2 + b\Delta + c = 0$.

If $\deg \Delta^2 = \deg c$, then $\deg b\Delta$ is greater.

We construct now the root in case $\deg b\Delta = \deg c$, i.e. $\deg \Delta = \deg c - \deg b$. Denote $k = \deg\, \Delta$, $m = \deg b$, $\Delta = a_kt^k + ....$ From the equation $\Delta^2 = b\Delta + c$ we have $a_kt^{2k} + ... = a_kb_mt^{m+k} + ... + c_{m+k}t^{m+k} + ....$ Since $2k < m+k$, for cancellation it is necessary that $a_kb_m = c_{m+k}$, i.e. $a_k = \frac{b_m}{c_{m+k}}$. Denote by $\widetilde{\Delta} = \Delta - a_kt^k$. Then $\widetilde{\Delta}$ satisfies the equation $\widetilde{\Delta}^2 = b\widetilde{\Delta} + \widetilde{c}$, where $\widetilde{c} = a_k^2t^{2k} + ba_kt^k + c$. It is easy to see that $\deg \widetilde{c} < \deg c$. Hence we have to find the root of the equation satisfying the condition in III, and this root will have the degree smaller than $\mathbb{F}$. By such an inductive procedure we obtain a desired root as a power series.

In case $\deg \Delta^2 = \deg b\Delta$ we get a conjugate root $b + \Delta$.

□

Consideration of the case II leads us necessarily to the case I, III or IV. Cases I and IV are imaginary and real respectively. Consideration of the case III leads us either to the case I or IV, or we remain in the imaginary case.

# 4 Imaginary case

Now we will give a solution in the imaginary case. According to proposition 3.3 we can assume that either 1). $\deg c > 2\deg b$ and $\deg c$ is odd or 2). deg$c = 2$deg$b$ and the equation $b_0^2t^2 + b_0^2t + c_0 = 0$ unsolvable in the field $\mathbb{F}$.

Consider first the first case.

The main our tool here is a construction of the degree function on $R$, which respects the multiplication.

**Definition.** *Let define a function* $\mathrm{Deg} : R \to \mathbb{Q}_+ \cup \{-\infty\}$*, as follows:*

$$\mathrm{Deg}(u + \Delta v) = \max(\deg u, \deg v + \frac{1}{2}\deg c),$$

*where* deg *is the usual degree function on polynomials.*

**Theorem 4.1** *Let* $f(t) = t^2+bt+c$ *with* deg c *to be odd and* $R = \mathbb{F}[x,t]/f(t)$*, then for any* $\alpha, \beta \in R$*,*

$$\mathrm{Deg}(\alpha\beta) = \mathrm{Deg}\alpha + \mathrm{Deg}\beta.$$

**Proof.** Let $\alpha = u' + \Delta v'$, $\beta = u + \Delta v$. Consider four different possibilities for the degrees of $\alpha$ and $\beta$:

1) $\mathrm{Deg}\alpha = deg\, u'$, $\mathrm{Deg}\beta =$ deg $u$ (i.e. deg $u' > \frac{1}{2}$deg $c +$ deg $v'$ and deg $u > \frac{1}{2}$deg $c +$ deg $v$);

2) Deg $\alpha = \frac{1}{2}$deg $c+$deg $v'$, Deg $\beta =$ deg $u$ (i.e., deg $u' < \frac{1}{2}$deg $c+$deg $v'$ and deg $u > \frac{1}{2}$deg $c +$ deg $v$);

3) Deg $\alpha =$ deg $u'$, Deg $\beta = \frac{1}{2}$deg $c+$deg $v$ (i.e., deg $u' > \frac{1}{2}$deg $c+$deg $v'$ and deg $u < \frac{1}{2}$deg $c +$ deg $v$);

4) Deg $\alpha = \frac{1}{2}$deg $c+$deg $v'$, Deg $\beta =$ $frac12$deg $c+$deg $v$ (i.e., deg $u' < \frac{1}{2}$deg $c +$ deg $v'$ and deg $u < \frac{1}{2}$deg $c +$ deg $v$).

Note that by definition

$$\deg\ \alpha\beta = \max\{\deg\ (u'u + cv'v), \frac{1}{2}\deg\ c + \deg\ (u'v + v'u + bv'v)\}.$$

In case 1 from the inequalities deg $u' > \frac{1}{2}$deg $c+$deg $v'$, deg $u > \frac{1}{2}$deg $c+$ deg $v$ and deg $c >$ 2deg $b$ we have deg $u'u >$ deg $cv'v$, deg $u'u > \frac{1}{2}$deg $c +$ deg $u'v$, deg $u'u > \frac{1}{2}$deg $c +$ deg $v'u$, deg $u'u > \frac{1}{2}$deg $c +$ deg $bv'v$. Hence deg $\alpha\beta =$ deg $u'u =$ deg $u' +$ deg $u =$ deg $\alpha +$ deg $\beta$.

In case 2 we similarly have deg $\alpha\beta = \frac{1}{2}$deg $c+$deg $u'v =$ deg $u' + \big(\frac{1}{2}$deg $c+$ deg $v\big) =$ deg $\alpha +$ deg $\beta$.

Case 3 is equivalent to case 2. One just has to replace $u'$ by $u$, $u$ by $u'$, $v'$ by $v$ and $v$ by $v'$.

In case 4 we have deg $\alpha\beta =$ deg $cv'v = (\frac{1}{2}$deg $c +$ deg $v') + (\frac{1}{2}$deg $c +$ deg $v) =$ deg $\alpha +$ deg $\beta$. □

The existence of this degree function allows us to solve the equation $u^2 + buv + cv^2 = d$, since it is equivalent to $(u + \Delta v)(u + (b + \Delta)v) = d$ and therefore the degrees of $u$ and $v$ (which are non-negative) are bounded by the degree of $d$.

Now we shell give a solutions in the second case. and show that there are also a finite number of them.

Suppose that there exists a solution of (9) such that $\deg u > \frac{1}{2}\deg d$ or $\deg v > \frac{1}{2}(\deg d - \deg c)$. In this case degree of $d$ is not maximal, hence among $u^2, buv, cv$ there are terms of the same degree. We show that if degrees of two of them are coincide then the third has also the same degree. It is easy calculations in three possible cases using $\deg c = 2\deg b$. Hence the highest terms of $u^2, buv$ and $cv$ are cancelled and $u_0^2 + b_0u_0v_0 + c_0v_0^2 = 0$ holds for $u_0, v_0, b_0, c_0 \in \mathbb{F}$ – coefficients near the highest terms of polynomials $u, v, b, c$. But it means that the equation $b_0^2t^2 + b_0^2t + c_0 = 0$ is solvable: $t = u_0/v_0b_0$. Therefore we have a bound for the degrees of $u, v$ also in this case.

We will use later on the following denotation:

$$r_{A,B} = \min_{U \in \mathrm{GL}\,(2): UAU^{-1}=B} \deg U.$$

In both variants of the imaginary case we get the following linear estimation.

**Proposition 4.2** *An estimation for the degree of elements of the conjugating matrix in imaginary case is linear: $r_{A,B} \leq 2\delta$, where as earlier $\delta$ is a maximum of* $\deg(A)$ *and* $\deg(B)$*.*

**Proof.** To obtain the estimation we have to take into account that before we turn out to be in real or imaginary case we have to make a change of variables of the type

$$\begin{cases} u' = u + qv, \\ v' = v \end{cases}$$

where $\deg q \leq \frac{1}{2}\deg c$.

Then in imaginary case of type I (proposition 3.3) we estimate degrees of $u'$ and $v'$ from the equality $(u' + \Delta v')(u' + (b + \Delta)v') = d$ using introduced above degree function Deg on $R$. We get $\deg u' \leq \delta/2$, $\deg v' \leq \delta/2$ and $\deg u \leq \delta$, $\deg v \leq \delta$.

In imaginary case of type III (proposition 3.3) as was shown above we have bounds: $\deg u \leq \frac{1}{2}\deg d$ or $\deg v \leq \frac{1}{2}(\deg d - \deg c)$. Hence, also $\deg u \leq \delta$ and $\deg v \leq \delta$.

Now taking into account (6) we have an estimation for the degree of entries of conjugating matrix: $r_{A,B} \leq 2\delta$. □

# 5 Real case

## 5.1 Units (equation $u^2 + buv + cv^2 = 1$)

We start in real case ($\deg c < 2\deg b$) with the solution of our equation with $d = 1$:

$$u^2 + buv + cv^2 = 1. \tag{10}$$

If $(u, v)$ is a solution of our equation we say also that $\omega = u + \Delta v \in R$ is a solution. Denote by $U(R)$ the set of all solutions $\omega \in R$ of the equation (10), $U(R)$ becomes a group with the multiplication by that of $R$.
**Definition.** *We say that $p \in R$ is reduced if* $\deg p > 0$ *and* $\deg p' < 0$, *where $p'$ is the conjugate element (defined in section 3).*

**Theorem 5.1** *The set $U(R)$ of solutions of (10) is an infinite cyclic group. The generator of $U(R)$ is an element with minimal positive degree. Moreover $R^* = U(R) \times \mathbb{F}^*$, where $R^*$ is the group of units of $R$.*

**Proof**. Show first that $R^* = U(R) \times \mathbb{F}^*$. The equation (10) means that $N(\omega) = 1$, hence lemma 3.1 c). and d). implies that $U(R)$ is a subgroup of $R^*$. Let $\omega \in R^*$. According to lemma 3.2 $N(\omega) \in \mathbb{F}^*$. Since $\mathbb{F}$ is finite field of characteristic 2 there exists a unique $\alpha \in \mathbb{F}^*$ such that $N(\omega) = \alpha^2$. Therefore $N(\omega/\alpha) = 1$, i.e. $\omega/\alpha \in U(R)$ and $\alpha$ is uniquely determined.

Now we prove that $U(R)$ is an infinite cyclic group and its generator is an element with minimal positive degree.

**Lemma 5.2** *If $\epsilon \in R^*$ and $|\epsilon| = 1$, than $\epsilon$ is a nonzero constant.*

**Proof**. According to lemma 3.2 $|N(\epsilon)| = 1$. Hence $|\epsilon'| = 1$ follows from $|N(\epsilon)| = |\epsilon\epsilon'| = |\epsilon||\epsilon'| = 1$. Comparing the corresponding power series we can see that $|\epsilon| = 1$ and $|\epsilon'| = 1$ together imply that $bv \in \mathbb{F}$. Hence there are three possibilities: $b = 0$; $v = 0$; or $b, v \in \mathbb{F}^*$. The case $b = 0$ was considered in section 3, $v = 0$ means that $\epsilon$ is a polynomial but it was a unit, so it is actually a constant. From $b \in \mathbb{F}^*$ and $v \in \mathbb{F}^*$ it follows that $c = 0$ (since $\deg c < 2\deg b$) and we are in the case when the equation is factorizable over $\mathbb{F}[x]$, which again was considered in section 3. □

**Lemma 5.3** *If $\epsilon_1$ and $\epsilon_2$ are units and $|\epsilon_1| = |\epsilon_2|$, than $\epsilon_1$ and $\epsilon_2$ coincide up to a constant: $\epsilon_1 = \alpha\epsilon_2, \alpha \in \mathbb{F}^*$.*

**Proof**. Obviously $\frac{\epsilon_1}{\epsilon_2}$ is also a unit and $|\frac{\epsilon_1}{\epsilon_2}| = \frac{|\epsilon_1|}{|\epsilon_2|} = 1$, hence by lemma 5.2 $\frac{\epsilon_1}{\epsilon_2} \in \mathbb{F}^*$. □

Let $\epsilon_0$ be the unit with minimal valuation $|\epsilon| > 1$ (with minimal positive degree).

**Lemma 5.4** *Any unit $\epsilon \in R^*$ has the form $\epsilon = \alpha\epsilon_0^n, \alpha \in \mathbb{F}^*$*

**Proof**. Suppose that it is not true. There exists $n \in N$ such that $|\epsilon_0|^n < |\epsilon| < |\epsilon_0|^{n+1}$. The equality is impossible, because if $|\epsilon| = |\epsilon_0|^n$ than by lemma 5.3 $\epsilon = \alpha\epsilon_0^n$. We then multiply previous inequalities by $|\epsilon_0|^{-n}$ and get a contradiction with minimality of $|\epsilon_0|$: $1 < |\epsilon_0^{-n}\epsilon| < |\epsilon_0|$. □

By this the proof of the theorem is completed.

□

We find the generator of $U(R)$ in two steps. First, we construct some nontrivial element of $U(R)$.

Let us denote by $[A_0; A_1, A_2, ...]$ where $(A_i \in \mathbb{F}[x])$ the continued fraction expansion $A_0 + \frac{1}{A_1 + \frac{1}{A_2 + ...}}$. We shall say that this expansion is *purely* periodical if the periodicity of the sequence $A_0; A_1, A_2, ...$ starts from $A_0$.

**Theorem 5.5** *Let $\rho \in R$ be a reduced root of (8). Then the continued fraction expansion $\rho = [A_0; A_1, A_2, ...]$ $(A_i \in \mathbb{F}[x])$ is purely periodical with a period $T \leq q^{2m}$, where $q = |\mathbb{F}|, m = \deg b$.*

**Proof**. One can present the series $\rho_n = [A_n; A_{n+1}, ...]$ which appears in the process of construction of a continued fraction, as obtained by operations $\varphi_1 : \rho \to u + \rho$ (cutting a polynomial part of the series) and $\varphi_2 : \rho \to 1/\rho$ (taking an inverse).

It is easy to see that $\varphi_1$ and $\varphi_2$ act on the set $\mathcal{U} = \{$solutions of the equations $\widetilde{a}x^2 + bx + \widetilde{c} = 0 \;\; |\deg \;\; \widetilde{c} < \deg b, \;\; \deg \widetilde{a} < \deg b\}$.

Indeed, let $x \in \mathcal{U}$, $y = \varphi_1(x) = x + u$, where $u \in \mathbb{F}[x]$, $\deg y < 0$. Since $\widetilde{a}x^2 + bx + \widetilde{c} = 0$, we have that $\widetilde{a}y^2 + by + c' = 0$, where $c' = au^2 + bu + \widetilde{c}$. From the latter equation $c' = \widetilde{a}y^2 + by$, and $\deg y < 0$. Hence for the degree of $c'$ we have $\deg c' < \deg (\widetilde{a}y + b) \leq \deg b$, therefore $y \in \mathcal{U}$.

Let now $x \in \mathcal{U}$ and $y = \varphi_2(x) = 1/x$. Since $\widetilde{a}x^2 + bx + \widetilde{c} = 0$, we have that $\widetilde{c}y^2 + by + \widetilde{a} = 0$, therefore $y \in \mathcal{U}$. Thus $\varphi_1(x)$ and $\varphi_2(x)$ acts on $\mathcal{U}$.

Hence the number of steps to obtain the same $\rho$ is less then $|\mathcal{U}| = 2q^{2m}$, where $m = \deg b, q$ — number of elements of the field.

Put now $\mathcal{U}_+ = \{x \in \mathcal{U}, \deg x \geq 0\}$. Note that $\rho_{n+1} = \varphi_2\varphi_1(\rho_n)$. Purely periodicity follows from the fact that $\varphi_2\varphi_1$ is a permutation of $\mathcal{U}_+$. Indeed, $\varphi_2\varphi_1(\rho_n)$ acts on $\mathcal{U}_+$ and it can be easily checked that it is an injection.

The estimation $T < q^{2m}$ follows from the equality $|\mathcal{U}_+| = q^{2m}$.

□

For $n = T$ we have $\rho = \rho_T$, and

$$\rho = \frac{P_n\rho + P_{n-1}}{Q_n\rho + Q_{n-1}},$$

where

$$P_{n+1} = P_nA_n + P_{n-1}, P_0 = 1, P_1 = A_0 \tag{11}$$

$$Q_{n+1} = Q_nA_n + Q_{n-1}, Q_0 = 0, Q_1 = 1 \tag{12}$$

This means that $\rho$ satisfies the quadratic equation $Q_n\rho^2 + (P_n + Q_{n-1})\rho + P_{n-1} = 0$. Since $\rho$ satisfies also the equation $\rho^2 + b\rho + c = 0$ and the latter equation does not have solutions in rational functions (this case was considered separately in the section 3), these two equations are proportional. Denote the coefficient of proportionality by $V$. Then $Q_n = V$, $P_{n-1} = cV$, $P_n + Q_{n-1} = bV$. Denote $P_n = U$. From the known equation $P_nQ_{n-1} + Q_nP_{n-1} = 1$ we obtain that $\epsilon = U + \Delta V = P_T + \Delta Q_T$ is a solution of the equation (10).

**Lemma 5.6** *When we live in the real case (*$\deg c < 2\deg b$*), there exists an invertible linear change of variables which turns the equation* $u^2 + buv + cv^2 = d$ *into* $u^2 + buv + \widetilde{c}v^2 = d$ *with* $\deg \widetilde{c} < \deg b$.

**Proof**. We have $u^2 + buv + cv^2 = d$, $\deg b \leq \deg c < 2\deg b$. Let us divide $c$ by $b$: $c = bq + r, \deg r < \deg b$ and consider the change of variables:

$$\begin{cases} u' = u + qv, \\ v' = v \end{cases}$$

New equation is: $u^2 + buv + (q^2 + r)v^2 = d$. Denote $\widetilde{c} = q^2 + r$. Note that $\deg \widetilde{c} < \deg c$. Indeed, $\deg r < \deg b \leq \deg c$ and $\deg q = \deg c - \deg b$, hence

$\deg q^2 = 2\deg c - 2\deg b < \deg c$, this means that we can keep making changes of variables of such a type until we get $\deg b > \deg \widetilde{c}$. □

Note that the composition of changes of variables of the type $u' = Qu, v' = v$, with $deg\, Q \leq \alpha$ has the same form.

In proposition 3.3 III we proved that the case $\deg c < 2\deg b$ is real by the construction of the root $\Delta$ of the equation (8) as a power series. It follows from this construction that in the case $\deg c < \deg b$ one of the roots of our equation is reduced. Hence we have obtained the following lemma.

**Lemma 5.7** *If* $\deg c < \deg b$ *then the element* $\Delta + b$ *is reduced and* $\epsilon = P_T + \Delta Q_T$ *is a nontrivial element of the group* $U(R)$*, where* $T$ *is the period of the continued fraction expansion of* $\Delta + b$*.*

**Lemma 5.8** *The estimation for the degree of this element* $\epsilon$ *of the group* $U(R)$ *is the following:* $\deg \epsilon \leq \delta q^{2\delta}$*.*

**Proof**. We have to estimate first $\deg u' = \deg P_T$ and $\deg v' = \deg Q_T$. Here $u'$ and $v'$ are the same as at the proof of proposition 4.2. Recall that $\rho = [A_0; A_1, A_2, ...]$ is a continued fraction expansion of the reduced root of (8). Note that $\deg A_n \leq \deg b$. Indeed, it is a positive part of an element $\rho_n = [A_n; A_{n+1}, ...] \in \mathcal{U}$ ($\mathcal{U}$ is the set constructed above in the proof of 5.5) and $\deg \rho_n = \deg b - \deg \widetilde{c} \leq \deg b$. From the recurrent formulas (11) and (12) for $P_n$ and $Q_n$ it follows that $\deg u' \leq \deg b\, T \leq \delta q^{2\delta}$ and $\deg v' \leq \deg b\,(T-1) \leq \delta(q^{2\delta} - 1)$. Then we get estimations for $\deg u$, $\deg v$ and $\deg \epsilon = \deg(u + \Delta v) \leq \delta q^{2\delta}$. □

Now we have to construct the generator of U(R), from a nontrivial element of U(R), we just have found using the continued fraction expansion.

**Lemma 5.9** *Let* $\epsilon_0 = x_0 + \Delta y_0$ *be any generator of the group* $U(R)$*. Then* $y_0 = g.c.d.(Y)$*, where* $Y = \{y : x + \Delta y \in U(R)\}$*.*

**Proof**. Let $\omega \in U(R), \omega = x + \Delta y, \omega^n = x_n + \Delta y_n$. It is enough to check the following recursive formula: $y_{n+2} = y_n + byy_{n+1}$. □

Hence we can just consider all divisors $y_i$ of $y$ where $\epsilon = x + \Delta y$ is an element of $U(R)$, we have constructed. Then find $x_i$, such that $x_i^2 + bx_iy_i +$

$cy_i^2 = 1$, for those $y_i$ for which it is possible. From the constructed in this way finite set of $\epsilon_i \in U(R)$ we select those with minimal positive degree. This is the desired $\epsilon_0$.

We can summarize the results of this section in the following

**Proposition 5.10** *The group $U(R)$ is an infinite cyclic group and there exists an algorithm for constructing of its generator.*

## 5.2 General case $d \neq 1$

Now we consider a general equation (9): $u^2 + buv + cv^2 = d, d \neq 1$.

Let $\epsilon_0$ be the generator of the group $U(R)$ with a positive degree. Denote $k = \deg \epsilon_0$.

**Lemma 5.11** *The set of all solutions of (9) has the form $\{\omega\epsilon_0^l : l \in \mathbb{Z}$, $\omega$ is a solution of (9) with $\deg \omega = 0, \ldots, k-1\}$.*

**Proof**. If $\omega$ is an arbitrary solution of (9): $N(u, v) = u^2 + buv + cv^2 = d$, then any $\omega\epsilon_0^l, l \in Z$ is also a solution (lemma 3.1 c). Hence we can rewrite the set of solutions of (9) in the following way: $\{\omega\epsilon_0^l : l \in \mathbb{Z}, \omega$ is a solution of (9) with $\deg \omega = 0, 1, ..., k-1\}$. □

**Theorem 5.12** *Let $\omega = u+\Delta v$ be a solution of (9) with $\deg \omega = 0, \ldots, k-1$. Then $\deg v \leq \max\{\deg d, k\} - \deg b$.*

**Proof**. As we said at the beginning of the section 5.1 $\omega = u + \Delta v$ is a solution of (9) means that $(u, v)$ is a solution of (9), i.e. $N(\omega) = \omega\omega' = d$. On the other hand $\omega\omega' = \omega^2 + b\omega v$. Hence the solution $\omega$ satisfies the equation

$$\omega^2 + (bv)\omega + d = 0. \tag{13}$$

Let us consider two cases:

Case 1. $\deg bv \leq \deg d$,

For this case $\deg v \leq \deg d - \deg b$.

Case 2. $\deg bv > \deg d$,

Here a priori there exist three possibilities for the degrees of terms in the equation.

a). $\deg \omega^2 = \deg d$. This is impossible because it implies $\deg bv > \deg \omega^2 = \deg d$ and the highest term $(bv)\omega$ can not be cancelled.

b). $\deg \omega^2 = \deg bv\omega$. It means that $\deg \omega = \deg bv$. Since we are interested in the solutions $\omega$ with $\deg \omega \leq k-1$, we have $\deg bv \leq k-1$, and $\deg v \leq k-1-\deg b$. This proves the theorem in this case.

c). $\deg bv\omega = \deg d$. Hence $\deg \omega < 0$. Which is incompatible with the hypothesis.

We can conclude that for any solutions $\omega$ of (9) we have $\deg v \leq \max(\deg d - \deg b, k-1-\deg b)$.

□

According to the theorem 5.12 we can find all solutions of (9) by a finite procedure.

The last step is to choose from the set of solutions $\omega\epsilon_0^l = u_l + \Delta v_l$ those for which $b_{21}$ is a divisor of $u_l$, and $a_{21}$ is a divisor of both $(a_{11}+b_{11})u_l + b_{12}v_l$ and $b_{12}u_l + (a_{11}+b_{22})v_l$. It is possible to describe all such solutions due to the following fact.

**Lemma 5.13** *Let $\omega\epsilon_0^l = u_l + \Delta v_l$, $P$ be a polynomial and $r_l$, $\deg r_l < \deg P$, be the sequence of residues of $P_1u_l + P_2v_l$ for some polynomials $P_1, P_2$ with respect to $P$. Then this sequence is periodical: $r_{l+T_0} = r_l$ for some period $T_0$.*

*The estimation for the period is the following: $T_0 \leq q^{\deg P}$.*

**Proof.** It is enough to show the periodicity of residues of $x_n$ and $y_n$, where $\epsilon_0 = x + \Delta y$, $\epsilon_0^n = x_n + \Delta y_n$. Let $\mathrm{res}(Q,P)$ denote the residue of $Q$ with respect to $P$. It is clear that $\mathrm{res}(Q(x_n,y_n),P) = \mathrm{res}Q(res(x_n,P),\mathrm{res}(y_n,P))$. We will show that $\mathrm{res}(x_n,P)$ and $\mathrm{res}(y_n,P)$ are periodical with the period $T_0$. Then periodicity of $x_n$ and $y_n$ will follow, because $\omega\epsilon_0^n = u_0x_n + cv_0y_n + \Delta(u_0y_n + v_0x_n + bv_0y_n)$, where $\omega = u_0 + \Delta v_0$. Let $r_n = \mathrm{res}(y_n,P)$, $s_n = \mathrm{res}(x_n,P)$. Just from $(x_n + \Delta y_n)(x + \Delta y) = x_{n+1} + \Delta y_{n+1}$, we have the following recurrent formulas:

$$x_{n+1} = x_nx + cy_ny, y_{n+1} = x_ny + y_nx + by_ny.$$

We shell consider the sequence of pairs of the residues: $(r_n, s_n)$. It is recurrent of length one since

$$s_{n+1} = \mathrm{res}(s_nx + cr_ny), r_{n+1} = \mathrm{res}(s_ny + r_nx + br_ny).$$

This sequence belongs to the finite set $M^2$ of pairs of polynomials of degree $< \deg P$, hence it is periodical with a period $T_0 \leq q^{\deg P}$. □

As a corollary we see that the estimation for the period $T_0$ in our situation is the following: $T_0 \leq q^{2\delta}$, where $\delta$ is a maximum of degrees of entries of initial matrices.

Summarizing above statements of lemma 5.11, theorem 5.12 and lemma 5.13 we end up with a construction of the set $\widetilde{\mathfrak{S}}_{A,B}$ which describes the set of all conjugating matrices for the pair $A$, $B$.

$$\widetilde{\mathfrak{S}}_{A,B} = \{\omega\epsilon_0^{l+nT_0} | \deg\omega = 0, ..., k-1, \quad l = 0, \dots T_0 - 1,$$
$$b_{21}\Big| u_l; \quad a_{21}\Big|(a_{11}+b_{11})u_l + b_{12}v_l; \quad \text{and} \quad a_{21}\Big| b_{12}u_l + (a_{11}+b_{22})v_l\}.$$

For any element $\omega \in \widetilde{\mathfrak{S}}_{A,B}$ one can obtain a conjugating matrix

$$U = \begin{pmatrix} u & p \\ v & q \end{pmatrix},$$

where $\omega = u + \Delta v$ and $p, q$ found from (6).

Moreover from $\widetilde{\mathfrak{S}}_{A,B}$ we can also choose a finite subset which characterize the conjugacy of matrices $A$ and $B$.

**Corollary.** *Put*

$$\mathfrak{S}_{A,B} = \{\omega\epsilon_0^{l} | \deg\omega = 0, ..., k-1, \quad l = 0, \dots T_0 - 1,$$
$$b_{21}\Big| u_l; \quad a_{21}\Big|(a_{11}+b_{11})u_l + b_{12}v_l; \quad \text{and} \quad a_{21}\Big| b_{12}u_l + (a_{11}+b_{22})v_l\}.$$

*then* $\mathfrak{S}_{A,B} \neq \emptyset \iff A$ *is conjugate with* $B$.

**Proposition 5.14** *The estimation for the degree $r_{A,B}$ of the entries of conjugating matrix in real case is the following: $r_{A,B} \leq 2\delta q^{6\delta}$.*

**Proof.** We will estimate first degree of the solution $\widetilde{\omega} = \omega\epsilon_0^l$ where $\deg\omega \leq k-1$, $l \leq T_0 - 1$.

Let $\omega\epsilon_0^l = u_l + \Delta v_l, T_0 = \text{l.c.m}(T_1, T_2, T_3)$, where $T_1, T_2$ and $T_3$ are periods of the residues (as they defined in lemma 5.13) of sequences $u_l$, $(a_{11}+b_{11})u_l + b_{12}v_l$ and $b_{12}u_l + (a_{11}+b_{22})v_l$ relative to $b_{12}, a_{21}$ and $a_{21}$ respectively. Using proposition 5.13 we can estimate $l.c.m(T_2, T_3)$ by $q^{2\deg a_{21}}$, $T_1$ by $q^{2\deg b_{12}}$, hence $T_0 \leq q^{4\delta}$. Then $\deg\widetilde{\omega} = \deg\omega\epsilon_0^l \leq \delta q^{6\delta} - 1$. Using the equation (13) we can obtain: $\deg u \leq \delta q^{6\delta} + \delta - 1$ and $\deg v \leq \delta q^{6\delta} + \delta$. (Note that in real case it is impossible that $\delta = 0$.) □

Combining together all estimations obtained above separately in the following cases: when one of the matrices is diagonal, $b = 0, \Delta \in \mathbb{F}(x)$, real case and imaginary case, we get the estimation for the degree of conjugating matrix in case of $char = 2 : \quad r_{A,B} \leq \delta(q^{6\delta} + 2)$.

# 6 Note on the case of characteristic $\neq 2$

The case of positive characteristic $\neq 2$ was considered in Artin's paper [1]. We will obtain here only an estimations which comes not always from the procedure described in [1]. We also have to make precise here the reduction of the conjugacy problem to a quadratic equation in this case.

Let $char\mathbb{F} \neq 2$. The conjugating condition $UAU^{-1} = B$ for $U \in \mathrm{GL}\,(2, \mathbb{F}[x])$ is equivalent to the system

$$uq - pv \in \mathbb{F}^*$$

$$UA = BU$$

where $U = \begin{pmatrix} u & p \\ v & q \end{pmatrix}$, $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ is the multiplicative group of the field $\mathbb{F}$.

To check the solvability of the system for an arbitrary coefficient $\alpha \in \mathbb{F}^*$ we need to check it only in two cases: $\alpha = 1$ and $\alpha$ is an element of $\mathbb{F}^*$ which is not a square. (Other solutions can be obtained from them because $\alpha/\beta$ is a square if $\alpha$ and $\beta$ are not.) We will obtain then a quadratic equation of the type $u^2 + buv + v^2 = d$ in the similar way as earlier, and since $char \neq 2$ we are able to reduce it to the Pell's equation: $u^2 - cv^2 = d$.

So we can use here the conventional notions of real and imaginary case and usual rule to distinguish them:

**Proposition 6.1**

*I. If* $\deg c$ *is odd or* $\deg c$ *is even but the highest term of polynomial* $c : c_n$ *is not a square, then we are in the imaginary case.*

*II. If* $\deg c$ *is even and* $c_n$ *is a square then we are in the real case.*

To obtain the estimations in these cases we will treat them separately.

In the imaginary case the highest terms of $c$ is not a square of a monomial (with coefficient). If we suppose that there exists a solution with $\deg u^2 >$

$\deg d$ or $\deg cv^2 > \deg d$ then the highest terms of $u^2$ and $cv^2$ have to be cancelled, but it would mean that highest term of $c$ is a square of a monomial (with a coefficient). Hence for any solution $\deg u < \frac{1}{2}\deg d$ and $\deg v < \frac{1}{2}(\deg d - \deg c)$. And we have got the following estimation.

**Theorem 6.2** *In the imaginary case always there exist only a finite number of solutions, and estimation for the degree of entries of conjugating matrix is linear:* $r_{A,B} \leq 2\delta$, *where* $\delta$ *is a maximum of* $\deg(A)$ *and* $\deg(B)$.

Now consider the real case. In Artin's paper it was proved (in case of *char* $\neq 2$) that there exists a reduced root $\rho$ (the root with $\deg\rho > 0$ and $\deg\rho' < 0$ for the conventional definition of $\rho'$) of the equation $t^2 + bt + c = 0$ and the continued fraction expansion of this reduced root is purely periodical. Also he proved that if continued fraction expansion is purely periodical then some unit can be constructed. He does not give an estimation of the period. We get it here now by methods similar to those we have used above, with only few essential changes. Namely, we present the process of continued fraction construction via an actions on the finite set. The set $\mathcal{U}$ we have to take to deal with the case *char* $\neq 2$ is different from one appeared in the proof of the Theorem 5.11. Estimation for the size of this set gives an estimation of the period.

**Lemma 6.3** *Let* $\rho \in R$ *be a reduced root of the equation* $at^2 + bt + c = 0$ *with the condition:* $\deg a \leq \delta, \deg b \leq \delta$ *and* $\deg c \leq \delta$, *where* $\delta$ *is as earlier a maximum of degrees of elements of initial matrices* $A$ *and* $B$. *Then the continued fraction expansion* $\rho = [A_0; A_1, A_2, ...]$ $(A_i \in \mathbb{F}[x])$ *is periodical with a the period* $T \leq q^{3\delta}$.

**Proof**. One can present the series $\rho_n = [A_n; A_{n+1}, ...]$ which appears in the process of construction of a continued fraction expansion, as obtained by the operations $\varphi_1 : \rho \to \rho - p$ (cutting a polynomial part of the series) and $\varphi_2 : \rho \to 1/\rho$ (taking an inverse).

We show that $\varphi_1$ and $\varphi_2$ act on the set $\mathcal{U}_r$ of reduced roots of the following equations: $\mathcal{U}_r = \{$reduced roots of the equations $at^2 + bt + c = 0 \ \mid \ \deg a \leq \delta, \ \deg b \leq \delta, \ \deg c \leq \delta\}$. But the root can be reduced only if $\deg b - \deg a < 0$ and $\deg c - \deg b < 0$ hence in fact $\mathcal{U}_r = \{$reduced roots of the equations $at^2 + bt + c = 0 \ \mid \ \deg a < \delta, \ \deg b \leq \delta, \ \deg c < \delta\}$. It is known ([1]) that if in the process of continued fraction expansion we get reduced root $\rho_n$, then all $\rho_{n+k}$ for $k \in \mathbb{Z}$ will be also reduced roots.

Hence we have to show only that if we take $\rho \in \mathcal{U}_r$, then $\varphi_1(\rho)$ and $\varphi_2(\rho) \in \mathcal{U}$, here $\mathcal{U} = \{$solutions of the equations $at^2 + bt + c = 0 \mid \deg a \leq \delta, \ \deg b \leq \delta, \ \deg c \leq \delta\}$.

It is obvious for $\varphi_2$. Let $\rho \in \mathcal{U}$ and $y = \varphi_2(\rho) = 1/\rho$. Since $a\rho^2+b\rho+c = 0$, we have $cy^2 + by + a = 0$ and $y \in \mathcal{U}$.

To prove the same property for $\varphi_1$ find first how the equation changes. If $\varphi_1(\rho) = \rho - p = y$ then for $y$ we have: $ay^2 + (2ap + b)y + (ap^2 + bp + c) = 0$. A priori there are three possibilities: 1). $\deg a\rho^2 = \deg c > \deg b\rho$; 2). $\deg a\rho^2 = \deg b\rho > \deg c$; 3). $\deg b\rho = \deg c > \deg a\rho^2$, but only the second one could actually exist. In this case $\deg{(2ap + b)} = \deg b$ and $\deg{(ap^2 + bp + c)} \leq \delta$. The latter follows from $ap^2 + bp + c = a(\rho - y)^2 + b(\rho - y) + c = a\rho^2 + b\rho + c + 2a\rho y - by + ay^2$ and $\deg y < 0$. Hence we have the equation on $y$ of the same type and $y \in \mathcal{U}$.

Notice that the highest terms of $b$ (middle coefficient) are the same for all elements of $\mathcal{U}_r$. Hence we can estimate the number of elements of $\mathcal{U}_r$ as follows: $|\mathcal{U}_r| \leq q^{3\delta}$. It is an estimation for the period of continued fraction expansion. □

Now we shall obtain the final estimation of $r_{A,B}$ in the case of $char \neq 2$ based on the estimation of the period.

**Theorem 6.4** *In the real case the estimation for the degree of entries of the conjugating matrix is the following:* $r_{A,B} \leq (q+1)\delta q^{7\delta}$*, where* $\delta$ *is a maximum of* $\deg(A)$ *and* $\deg(B)$.

**Proof.** First we consider the root $\Delta$ of the equation $t^2 = c$. We can construct it as a power series by usual recursive procedure. It is not a reduced root, since here $\deg\Delta = \deg\Delta'$. Note that it is different from the case of $char = 2$ where one of two roots of the initial equation had to be reduced. But in process of the construction of the continues fraction expansion of $\Delta = [A_0; A_1, ...]$ in some step $\Delta_n = [A_n; A_{n+1}, ...]$ the reduced root have to appear ([1]). For this root $\rho = \Delta_{n_0}$ we will have $\rho = \frac{P_n\rho+P_{n-1}}{Q_n\rho+Q_{n-1}}$. Let $\rho$ satisfy the equation: $A\rho^2+B\rho+C = 0$. Then from the proportionality of two quadratic equations (which can not have a rational solutions) for the reduced root, we get a formulas for nontrivial unit $X+\Delta Y$: $P_n+Q_{n-1} = 2X$, $P_n-Q_{n-1} = 2Yb$, where $n = T$, $T$ is a period of the continued fraction expansion of $\rho$. Hence we can estimate degrees of $X$ and $Y$ as $\deg X \leq \deg B\,T$, $\deg Y \leq \deg B\,T$. Let us convince that $\deg B \leq \delta$ and $T \leq q^{3\delta+1}$, for $\delta$ being as earlier maximal degree of entries of given matrices. It will follow from lemma 6.3. But we have to note the following: if we start the process of continued fraction expansion with $\Delta$, the root of $t^2 = c$, $\deg c \leq 2\delta$, then already at the first step, we get an equation $\Delta_1^2 - 2p\Delta_1 - c + p^2 = 0$ with $\deg(c-p^2) \leq \delta, \deg(2p) \leq \delta$. At the next steps degrees of the coefficients of the equations can not become bigger any more.

Hence we can estimate $\deg X$ and $\deg Y$ by $\delta q^{3\delta+1}$. If we take into account the change of variables, we get $\delta q^{3\delta+1} + \delta$.

Then the estimation for $k = \deg \epsilon_0, \epsilon_0 = X + \Delta Y$ will be: $k \leq \delta q^{3\delta+1} + 2\delta$.

Let $\omega\epsilon_0^l = u_l + \Delta v_l, T_0 = \text{l.c.m}(T_1, T_2, T_3)$, where $T_1, T_2$ and $T_3$ are periods of the residues (as they defined in lemma 5.13) of sequences $u_l$, $(a_{11}+b_{11})u_l + b_{12}v_l$ and $b_{12}u_l + (a_{11}+b_{22})v_l$ relative to $b_{12}, a_{21}$, and $a_{21}$ respectively. By the estimation from the proposition 5.13 we have $T_0 \leq q^{4\delta}$.

Consider an arbitrary root of $u^2 + cv^2 = d$ : $\widetilde{\omega} = \omega\epsilon_0^l = u + \Delta v$ of degree $\leq k-1$. Estimate first $\deg\widetilde{\omega}$ as a series. After checking divisibility we get: $\deg\widetilde{\omega} = \omega\epsilon_0^l \leq k - 1 + k(T_0 - 1) = kT_0 - 1 = \delta q^{7\delta+1} + 2\delta q^{4\delta}$. Now using this estimation we can get the estimation for $u, v$, it gives us $r_{A,B} \leq \delta q^{7\delta+1} + 2\delta q^{4\delta} + \delta$. Since $q \leq 3$ we can estimate the latter as follows: $r_{A,B} \leq (q+1)\delta q^{7\delta}$. $\Box$.

Let us note that using the same idea we can get an estimation for the degree of the generator of an infinite part of centralizer of a given matrix $A$. We omit here details, they are similar but easier then those were discussed above. The resulting estimation presented in the Theorem 1.3.

# 7 Conjugacy separability of $\mathrm{GL}(2, \mathbb{F}[x])$

In this section we would like to note that $\mathrm{GL}(2, \mathbb{F}[x])$ is conjugacy separable group, but it does not immediately lead to any algorithm which decides conjugacy in $\mathrm{GL}(2, \mathbb{F}[x])$, because it is not finitely generated (see for example [7]) and the finite images together with the homomorphisms onto them can not be constructed. We mean here Maltsev's algorithm [8] for the decision of the conjugacy problem for finitely presented conjugacy separable groups. Note moreover that Maltsev's algorithm does not allow to give any estimations. To be precise let us show here the conjugacy separability of the group $\mathrm{GL}(2, \mathbb{F}[x])$.

**Proposition 7.1** $\mathrm{GL}(2, \mathbb{F}[x])$ *is conjugacy separable group.*

**Proof.** It is known due to Serre [7] and Nagao [6] that $\mathrm{GL}(2, \mathbb{F}[x]) = T(\mathbb{F}[x]) \times_{T(\mathbb{F})} \mathrm{GL}(2, \mathbb{F})$ is an amalgamated free product of subgroup of upper triangular matrices $T(\mathbb{F}[x])$ and $\mathrm{GL}\,(2,\mathbb{F})$ through the upper triangular matrices over $\mathbb{F}$.

There exists the result of J.L.Dyer [5] saying that conjugacy separable groups amalgamating along the finite subgroup is conjugacy separable.

We have only to verify that the subgroup $T(\mathbb{F}[x])$ of upper triangular matrices in $\mathrm{GL}\,(2,\mathbb{F}[x])$ is conjugacy separable.

**Lemma 7.2** *Two elements* $e_1 = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix}$, $e_2 = \begin{pmatrix} \alpha' & c' \\ 0 & \beta' \end{pmatrix}$ *from* $T(\mathbb{F}[x])$ *are not conjugate if and only if*

*I.* $(\alpha,\beta) \neq (\alpha',\beta')$ *or*

*II.*$(\alpha,\beta) = (\alpha',\beta')$ *with* $\alpha = \beta$*, and* $c$*,* $c'$ *are non-proportional.*

Let us show that for any pair $e_1 \not\sim e_2$, $e_1, e_2 \in T(\mathbb{F}[x])$ we can find normal subgroup $H_{(e_1,e_2)} \triangleleft T(\mathbb{F}[x])$, such that $\bar{e}_1 \not\sim \bar{e}_2$, where $\bar{e}_i$ is image of $e_i$ in the finite quotient $T(\mathbb{F}[x])/H_{(e_1,e_2)}$.

Note first that subgroups of the type

$$H_n = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a = \alpha x^n + \dots, \alpha \in \mathbb{F}^* \right\}$$

are normal in $T(\mathbb{F}[x])$.

Indeed, $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^e = \begin{pmatrix} 1 & \frac{\alpha}{\beta}a \\ 0 & 1 \end{pmatrix}$, where $e = \begin{pmatrix} \alpha & d \\ 0 & \beta \end{pmatrix}$.

To separate non-conjugate elements of the type I it is enough to take a subgroup $H_0$. Pick two non-conjugate elements of the type II: $h_1 = \begin{pmatrix} \gamma & c \\ 0 & \gamma \end{pmatrix}$ and $h_2 = \begin{pmatrix} \gamma & c' \\ 0 & \gamma \end{pmatrix}$. Note that $\begin{pmatrix} \gamma & c \\ 0 & \gamma \end{pmatrix}^e = \begin{pmatrix} \gamma & c' \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$ if and only if $\frac{\alpha}{\beta}c + c' = \gamma f$. Hence if we take $H_{(h_1,h_2)} = H_n$ with $n > \max\{\deg c, \deg c'\}$ then non-conjugates $h_1$ and $h_2$ in the quotient $T(\mathbb{F}[x])/H_{(h_1,h_2)}$ remain non-conjugate. □

# 8 Acknowledgments

This work has been done during the stay of the second named author in the University of Düsseldorf supported by DFG and in the Max-Planck-Intitüt für Mathematik in Bonn, who is grateful to these institutions for their hospitality and encouraging research atmosphere.

# References

[1] E.Artin *Quadratische Körper im Gebiet der höheren Kongruenzen I*, Math. Zeitschrift 19(1924), pp.153-206.

[2] W.Adams, P.Loustaunau *An introduction to Gröbner bases*, Graduate Studies in Math., Vol 3, (1994).

[3] F. Grunewald, *Solution of the conjugacy problem in certain arithmetic groups*, in Word Problems II, ed. Adian, Boone and Higman, Amsterdam, North-Holland, 1980, p.101-139.

[4] F. Grunewald, D. Segal, *Some general algorithms 1: Arithmetic groups.* Annals of Math., **112**, 531–583, (1980)

[5] J.L.Dyer, *Separating conjugates in amalgamated free products and HNN-extensions.* J.Austral.Math.Soc., **A29, N1**, 35–51, (1980)

[6] H. Nagao *On* $\mathrm{GL}\,(2, \mathbb{F}[x])$. J. Inst.Polytech. Osaka City Univ, Ser.A, 10, 117–121.(1959)

[7] J.P. Serre, *Trees*, Springer, (1980).

[8] A.I.Maltsev *On the homomorphisms onto finite groups.* Sci. notices of Ivanovo State Pedagogical University (Uch. zapiski Ivanovskogo ped. instituta; in russian), 1958, 18, N5, p.49-60.