Computer Algebra and Finite Groups

Gert-Martin Greuel*
Universität Kaiserslautern
Fachbereich Mathematik

Gerhard Pfister†
Universität Kaiserslautern
Fachbereich Mathematik

Contents

*Supported by DFG Grant, GR 640/9-2, GIF grant G-616-5.C/1999 and Stiftung Rheinland–Pfalz für Innovation

†Supported by Stiftung Rheinland–Pfalz für Innovation

1 The Problem

The problem we address in this article can simply be stated as: *characterise the class of finite solvable groups by 2–variable identities.*

To explain the problem, note that a group G is abelian if and only if $[x, y] = 1$ for all $x, y \in G$ where $[x, y] = xyx^{-1}y^{-1}$ is the commutator. Recall also that a finite group G is nilpotent if and only if it satisfies the Engel identity $[x, y]_n$ for some n and all $x, y \in G$ (here $[x, y]_1 = [x, y]$ and $[x, y]_{n+1} = \big[[x, y]_n, y\big]$). It has been conjectured that some Engel–like identities should characterise also the class of finite solvable groups. The following, more precise, conjecture is due to B. Plotkin (cf. [9], [10]).

For a given word w in the letters X, Y, X^{-1}, Y^{-1}, consider the sequence $U_n = U_n^w$ of words defined inductively by

$$\begin{aligned} U_1 &= w \\ U_{n+1} &= [XU_nX^{-1}, YU_nY^{-1}] . \end{aligned}$$

Conjecture 1.1 (B. Plotkin). There exists a word w such that a finite group G is solvable if and only if there exists an $n \geq 1$ satisfying $U_n^w(x, y) = 1$ for all $x, y \in G$.

Recall that the minimal finite non–solvable groups G (that is, all subgroups of G are solvable) were classified by J. Thompson [11] in 1968:

(1) $\mathrm{PSL}(2, p)$, p a prime number, $p = 5$ or $p > 5$ and $p = \pm 2 \mod 5$.

(2) $\mathrm{PSL}(2, 2^n)$, $n \geq 2$, a prime number.

(3) $\mathrm{PSL}(2, 3^n)$, n odd, a prime number.

(4) $\mathrm{PSL}(3, 3)$.

(5) $Sz(2^n)$, n odd.

In view of this result, Conjecture 1.1 is implied by

Conjecture 1.2. Let G be one of the groups in Thompson's list (1) – (5). Then there exists a word w in X, Y, X^{-1}, Y^{-1}, independent of G, such that for all n the equation $U_n(x, y) = 1$ has no solution in G.

Conjecture 1.2 for all cases except for the Suzuki groups in (5) has been proved by G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister, E. Plotkin, Y.Segev, cf. [8].

Theorem 1.3 ([8]). *Conjecture 1.2 holds for the word* $w = X^{-1}YXY^{-1}X$ *and the groups (1) – (4) in Thompson's list.*

The proof, in the spirit of [2], proceeds as follows: for any of the groups in (1) – (3), consider its standard linear representation, that is, consider the matrices

$$x = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}$$

as elements of $\mathrm{PSL}(2, p^n)$, p any prime number. (The case (4), $\mathrm{PSL}(3,3)$ is easy.) Then it is easy to see that $U_1(x, y) \neq 1$ for all x, y as above.

Consider the matrix equation $U_1(x, y) = U_2(x, y)$. If this has a solution for some x, y as above, then, by construction of the sequence U_n, $U_n(x, y) = U_1(x, y) \neq 1$ for all $n \geq 1$. Hence, it suffices to show that $U_1(x, y) = U_2(x, y)$ has a solution. We shall show this for $\mathrm{PSL}(2, p)$, $p \geq 5$, $\mathrm{PSL}(2, 2^n)$, $n \geq 2$ and $\mathrm{PSL}(2, 3^n)$, $n \geq 2$. Note that the groups $\mathrm{PSL}(2, 2)$ and $\mathrm{PSL}(2, 3)$ are solvable, hence $U_1(x, y) = U_2(x, y)$ cannot have a solution over the prime field in characteristic 2 and 3. Therefore, the groups in (2) and (3) have to be treated separately (by the same method as the groups in (1) for large characteristic).

Consider the ideal I generated by the entries of the matrix $U_1(x, y) - U_2(x, y)$ which is an ideal in $\mathbb{Z}[b, c, t]$.

We are going to show that the variety $V(I)$ has a rational point $(b, c, t) \in (\mathbb{F}_{p^n})^3$ for all (p, n), $p \geq 5$ and $n = 1$ or $p = 2, 3$ and $n \geq 2$, which is equivalent to $U_1(x, y) = U_2(x, y)$ having a solution $x, y \in \mathrm{PSL}(2, p^n)$.

To show that $V(I)$ has a rational point, we use:

- the Hasse–Weil bound for the number of rational points on an absolutely irreducible curve and its generalisation to singular curves,
- simple facts from algebraic geometry and singularity theory,
- simple generalisations of basic results from the theory of standard bases,
- extensive computations, using Singular.

We should mention that there are other words satisfying the statement of Theorem 1.3 (we checked this for $w = x^{-2}y^{-1}x$). In this article we concentrate on those steps of the proof which require computer algebra. Full details, containing the group theoretical background as well as a description of special strategies which helped to speed up the computation, will appear in [8].

2 $\mathbb{F}_{p^n}$–rational Points

Let $w = x^{-1}yxy^{-1}x$ and define $U_1 = w$, $U_2 = [xU_1x^{-1}, yU_1y^{-1}]$ (with $[x,y] = xyx^{-1}y^{-1}$).

Theorem 2.1. *The equation $U_1 = U_2$ has a solution $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$, $y = \left(\begin{smallmatrix} 1 & b \\ c & 1+bc \end{smallmatrix}\right) \in \mathrm{PSL}(2,p)$ such that $U_1(x,y) \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for all prime numbers $p \geq 5$.*

Before we start with the proof of Theorem 2.1, let us mention the following lemma, which is easily proved by looking at the equations.

Lemma 2.2. *The equation $U_1(x,y) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has no solution.*

Let $I \subseteq \mathbb{Z}[b,c,t]$ be the ideal generated by the four polynomials defining $U_1 = U_2$. Denote by $I^{(p)} \subseteq \mathbb{F}_p[b,c,t]$ the ideal induced by I.

Theorem 1.3 for $\mathrm{PSL}(2,p)$, $p \geq 5$, is then a consequence of the following theorem.

Theorem 2.3. *For all prime numbers $p \geq 5$ the variety $V(I^{(p)}) \subset \mathbb{F}_p^3$ is not empty.*

For all prime numbers $5 \leq p \leq 2530$ this has been checked by a computer in the most trivial way, by substituting the points of $\mathbb{F}_p^3$ in the polynomial generating $I^{(p)}$ and stopping when a solution was found.

For the other prime numbers, we are going to apply the theorem of Hasse–Weil as generalised by Aubry and Perret to singular curves (cf. [1]) and using the fact that the affine curve C has, at most, $\deg(\overline{C})$ rational points less than the projective closure $\overline{C}$.

Theorem 2.4. *Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field $\mathbb{F}_q$ and $\overline{C} \subset \mathbb{P}^n$ the projective closure, then the number of $\mathbb{F}_q$–rational points of C is at least $q + 1 - 2p_a\sqrt{q} - d$ with $d =$ the degree and p_a the arithmetic genus of $\overline{C}$.*

Note that the Hilbert function of $\overline{C}$, $H(t) = dt - p_a + 1$, can be computed from the homogeneous ideal I_h of $\overline{C}$, hence we can compute d and p_a without any knowledge about the singularities of $\overline{C}$.

Now we use the following notations. Let $I_h \subset \mathbb{Z}[b,c,t,h]$ denote the homogenisation of I with respect to the homogenising variable h and $I_h^{(p)}$ the induced ideal in $\mathbb{F}_p[b,c,t,h]$ for a prime number p.

Let $X^{(p)}$ be the projective curve in $\mathbb{P}^3_{\mathbb{F}_p}$, defined by $I_h^{(p)}$.

Proposition 2.5.

(1) $X^{(p)}$ is absolutely irreducible for all prime numbers $p \geq 2530$.

(2) $X^{(2)}$ and $X^{(3)}$ are absolutely irreducible.

Before proving the proposition, we apply it to prove Theorem 2.3. Since $X^{(p)}$ is absolutely irreducible, we can apply Theorem 2.4 and get

$$\# X^{(p)} \geq p + 1 - 2p_a\sqrt{p} - d\,.$$

We compute the Hilbert function of $X^{(p)}$ (using SINGULAR) as $16t-24$. This implies $d = 16$ and $p_a = 25$.

We need $p + 1 - 50\sqrt{p} - 16 > 0$, which holds if $p \geq 2530$.

It remains to prove Proposition 2.5. Here it is sufficient to prove that a suitable projection of $X^{(p)}$ to a plane curve is absolutely irreducible. Elimination of the variable c (using SINGULAR) results in a polynomial f of degree $d = 12$, which defines the projection of $X^{(p)}$ (d drops from 16 to 12 since we project from a point of $X^{(p)}$).

To prove that f is absolutely irreducible, we write $f = f_1^{(n)} f_2^{(d-n)}$, f_1 a homogeneous polynomial of degree n in b, t, h with variables $a_1^{(n)}, \ldots, a_{s(n)}^{(n)}$ as coefficients and f_2 a homogeneous polynomial of degree $d-n$ in b, t, h with variables $b_1^{(n)}, \ldots, b_{\ell(n)}^{(n)}$ as coefficients, $d = 12$ and $n = 1, \ldots, 6$.

This gives six systems of equations defined by polynomials in $\mathbb{Z}[\{a_i^{(n)}\}, \{b_j^{(n)}\}]$. Let $I_n \subset \mathbb{Z}[\{a_i^{(n)}\}, \{b_j^{(n)}\}]$ be the corresponding ideal $n = 1, \ldots, 6$. We have to prove that over $\overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) none of these ideals has a common zero. This is equivalent to the fact that 1 is contained in the ideals $I_n (\operatorname{mod} p)$.

For the proof we use the following easy splitting lemma (cf. [9]).

Lemma 2.6. *Let $I \subset \mathbb{Z}[x_1, \ldots, x_n]$ be an ideal and assume that $f \cdot g \in I$ for some polynomials $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$. Then $\sqrt{I} = \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$.*

Now we want to apply Corollary 3.4 and Lemma 2.6 to prove that $1 \in I_k\mathbb{F}_p[\{a_\nu^{(k)}\}, \{b_\nu^{(k)}\}]$.

For a finite, not too large, set of primes this can be checked by computing a Gröbner basis of $I_k\mathbb{F}_p[\{a_\nu^{(k)}\}\{b_\nu^{(k)}\}]$. However, we are faced with the problem of checking this for infinitely many points. The idea is to compute a Gröbner basis over $\mathbb{Q}$, taking care of the coefficients.

To be specific, let $S^{(k)} \subseteq \mathbb{Z}[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}]$ be a Gröbner basis of $I_k\mathbb{Q}[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}]$. If $e \in \mathbb{Z}$ is in $S^{(k)}$ then, using Corollary 3.4 (2), we obtain $I_k\mathbb{F}_p[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}] = \mathbb{F}_p[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}]$ for all p not dividing e.

Unfortunately, this does not work straightforwardly, since e becomes too large. However, if $e \in S^{(k)}$ is too large, we can apply Lemma 2.6 to split the ideal and obtain for the components smaller integers in the standard basis. The splitting tool is used in the following way:

- We factorise the generators of the ideal and split the ideal if one of the generators has a nontrivial factor.
- If all generators are irreducible in $\mathbb{Q}[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}]$, we compute a Gröbner basis for suitable sub-ideals to obtain new generators which could have a nontrivial factorisation. In our application "suitable" is a mixture of the first 30 generators and the sub-ideal generated by the generators with few monomials.

Finally, we obtained the following list of prime numbers ≥ 2530 for which we checked directly that $1 \in I_n\mathbb{F}_p[\{a_\nu^{(n)}\},\{b_\nu^{(n)}\}]$ by computing a Gröbner basis separately:

n=2: 3463,7489
n=3: 7129,9041,10343,18413,20857
n=4: 2671,2693,3299,3373,3391,3517,3593,3701,3779,4111,4409,4423,4561, 4657,4793,5273,5399,5659,5987,6949,7487,8011,8243,8887, 9769,10159, 10177,12007,26347
n=6: 6151,6343,7823

It remains to study the equation $U_1 = U_2$ for $\mathrm{PSL}(2,2^n)$, $n \geq 2$, and $\mathrm{PSL}(2,3^n)$, $n \geq 3$ and odd. A direct computation of the Gröbner basis over $\mathbb{F}_2$ (resp. $\mathbb{F}_3$) of the corresponding ideals $I_k\mathbb{F}_p[\{a_\nu^{(k)}\},\{b_\nu^{(k)}\}]$, $p = 2,3$, shows that the curves $X^{(2)}$ and $X^{(3)}$ are also absolutely irreducible. Theorem 2.4 implies that $U_1 = U_2$ has a solution in $\mathrm{PSL}(2,2^n)$ (resp. $\mathrm{PSL}(2,3^n)$) if $n \geq 12$ (resp. $n \geq 8$).

For the remaining cases we checked directly by a computer, trying all matrices in $\mathrm{PSL}(2,2^n)$ resp. $\mathrm{PSL}(2,3^n)$ in order to show that $U_1 = U_2$ has a solution.

The computations were carried out on an AMD Athlon 700 with 256 MB, running Linux and using the computer algebra system Singular [4]. Finding rational points in Theorem 2.3 for $5 \leq p \leq 2530$ (the trivial way) took roughly six hours, showing absolute irreducibility in Proposition 2.5 (1) (except for the primes tested above) took about one day, while the computations for the primes listed above lasted about half a day. Finally, the computation for $\mathrm{PSL}(2,2^n)$ and $\mathrm{PSL}(3,3^n)$ lasted together about half a day.

3 Standard Bases and Specialisation

We recall and generalise some notions and results from the theory of standard bases which are used in the proof of Proposition 2.5.

A *monomial ordering* is a total ordering $>$ on the set of monomials $\mathrm{Mon}(x_1,\ldots,x_n)=\{x^\alpha=x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}\mid \alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{Z}^n_{\geq 0}\}$, satisfying: $x^\alpha>x^\beta\Rightarrow x^\gamma x^\alpha>x^\gamma x^\beta$, for all α,β,γ.

We do not assume $>$ to be a well–ordering, in particular, we allow $x_i<1$ for all i, which is used when we compute invariants of singularities in local rings.

Let R be a Noetherian integral domain and let $f\in R[x]=R[x_1,\ldots,x_n]$ be a nonzero polynomial. With respect to a fixed monomial ordering, write f as a sum of nonzero terms

$$f=a_\alpha x^\alpha+a_\beta x^\beta+\cdots+a_\gamma x^\gamma,\quad x^\alpha>x^\beta>\cdots>x^\gamma\,,$$

with $a_\alpha,a_\beta,\ldots,a_\gamma\in R$. We call

$\mathrm{LM}(f):=x^\alpha$ the *leading monomial* of f,
$\mathrm{LC}(f):=a_\alpha$ the *leading coefficient* of f,
$\mathrm{LT}(f):=a_\alpha x^\alpha$ the *leading term* of f,

and assume always that $f\neq 0$, if we use these notations.

Consider the multiplicatively closed set $S_>:=\{f\in R[x]\mid \mathrm{LT}(f)=1\}$ and define the localisation of $R[x]$ with respect to $S_>$ as

$$R[x]_>:=S_>^{-1}(R[x])=\left\{\frac{f}{g}\;\middle|\; f,g\in R[x],\ \mathrm{LT}(g)=1\right\}.$$

If $>$ is a global ordering (that is, $x_i>1$ for all i), then $R[x]_>=R[x]$. If $>$ is a local ordering ($x_i<1$ for all i), then $R[x]_>=R[x]_{\langle x_1,\ldots,x_n\rangle}$, the localisation of $R[x]$ at the prime ideal $\langle x_1,\ldots,x_n\rangle$.

For any ideal $I\subset R[x_1,\ldots,x_n]$, we set

$$L(I):=\langle \mathrm{LT}(f)\mid f\in I\rangle\,,$$

the ideal in $R[x_1,\ldots,x_n]$ generated by all leading terms of elements of I. Recall that a finite set $G\subset I$ is called a *standard basis* of I (over the ring

R) if $L(I) = \langle \mathrm{LT}(g) \mid g \in G\rangle$. If R is a field, we can use the leading monomials $\mathrm{LM}(g)$ instead of the leading terms in the above definition. If $>$ is a well–ordering, a standard basis is usually called a *Gröbner basis*.

We do not need standard bases over rings but something weaker, which we call pseudo standard bases and which we explain now.

Definition 3.1. Let $\mathcal{G}$ denote the set of finite ordered sets (or lists) $G \subset R[x] = R[x_1, \ldots, x_n]$. A function

$$\mathrm{NF} : R[x] \times \mathcal{G} \to R[x], \quad (f, G) \mapsto \mathrm{NF}(f|G)\ ,$$

is called a *pseudo normal form* on $R[x]$ if the following holds:

(1) $\mathrm{NF}(f|G) \neq 0 \Rightarrow \mathrm{LM}\big(\mathrm{NF}(f|G)\big)$ is not divisible by $\mathrm{LM}(g)$ for all $g \in G$.

(2) For all $f \in R[x]$ and $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$ there exists a $u \in R[x]$ with $\mathrm{LT}(u)$ a product of some $\mathrm{LC}(g_i)$, such that $r := uf - \mathrm{NF}(f|G)$ has a *standard representation* with respect to G. This means either $r = 0$, or

$$r = \sum_{i=1}^{s} a_i g_i,\ a_i \in R[x]\ ,$$

such that $\mathrm{LM}(r) \geq \mathrm{LM}(a_i g_i)$ for all i with $a_i g_i \neq 0$.

If in (2) we have $u = 1$, respectively u a unit in $R[x]_>$, then NF is called a normal form, respectively a weak normal form, (cf. [6], [7]).

We define the *s–polynomial* of two polynomials $f, g \in R[x] \smallsetminus \{0\}$, $\mathrm{LT}(f) = ax^\alpha$ with $\mathrm{LT}(g) = by^\beta$ as

$$\mathrm{spoly}(f, g) := bx^{\gamma-\alpha} f - ax^{\gamma-\beta} g\ ,$$

where $\gamma = (\gamma_1, \ldots, \gamma_n),\ \gamma_i = \max\{\alpha_i, \beta_i\},\ i = 1, \ldots, n$. If $\mathrm{LM}(g) \mid \mathrm{LM}(f)$, then $\gamma = \alpha$ and we have

$$\mathrm{spoly}(f, g) = bf - ax^{\alpha-\beta} g\ .$$

In our application, we need the following result, which is the reason why we introduced pseudo normal forms (notations from above).

Proposition 3.2. *Let $I \subset R[x]_>$ be an ideal, NF a pseudo normal form on $R[x]_>$ and $G = \{g_1, \ldots, g_s\} \subset I$ satisfying*

(1) G generates $IR[x]_>$;

(2) $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ for all $1 \leq i < j \leq s$.

Then, for any maximal ideal $\mathfrak{m} \subset R$ such that $\mathrm{LC}(g_i) \notin \mathfrak{m}$ for all i, the set $\{\bar{g}_1, \dots, \bar{g}_s\}$ is a standard basis of $I \cdot (R/\mathfrak{m})[x]_>$. Here $\bar{g}_i$ denotes the residue class of g_i in $(R/\mathfrak{m})[x]$.

The proof is the same as in [6] or [7].

If R is a field and $\mathfrak{m} = \langle 0 \rangle$, this is just Buchberger's criterion for a standard basis (cf. [3]).

Definition 3.3. We call G, satisfying (1) and (2) of Proposition 3.2, a *pseudo standard basis* of I (note that this is *not* a standard basis of I over the ring R).

Corollary 3.4. *(1) Let $R = K[t]$, $t = (t_1, \dots, t_r)$, K a field and let $\{g_1, \dots, g_s\} \subset (K[t])[x]$, $x = (x_1, \dots, x_n)$, be a pseudo standard basis of I. Set $h_i = \mathrm{LC}(g_i)$ and $h = h_1 \cdot \ldots \cdot h_s \in K[t]$. Then, for any $t_0 \in K^s$ such that $h(t_0) \neq 0$, $\{g_1(t_0, x), \dots, g_s(t_0, x)\}$ is a standard basis of $I|_{t=t_0} \subset K[x]$.*

(2) Let $R = \mathbb{Z}$, $\{g_1, \dots, g_s\} \subset \mathbb{Z}[x]$ a pseudo standard basis of I, let $h_i = \mathrm{LC}(g_i)$ and set $h = h_i \cdot \ldots \cdot h_s \in \mathbb{Z}$. Then, for any prime p so that $p \nmid h$, $\{\bar{g}_1, \dots, \bar{g}_s\}$ is a standard basis of $\overline{I}$ in $\mathbb{F}_p[x]$.

Hence, we obtain an effective way to determine parameters t_0, respectively prime numbers p, for which $\{g_1, \dots, g_s\}$ induces a standard basis of $I|_{t=t_0}$ (t substituted by t_0), respectively of $\overline{I}$ (the reduction of $I \mod p$). However, these conditions are only sufficient, not necessary (and depend on the strategy of pair selection in the Buchberger algorithm). Indeed, the strategy in Section 2 was chosen to keep $\mathrm{LC}(g_i)$ small.

To see that nontrivial pseudo normal forms exist, we generalise `NFBuchberger` and `NFMora` from [5], [7] to the present situation. As before, R denotes a Noetherian integral domain.

Algorithm 3.5 (NFBuchberger). Assume $>$ to be a global monomial ordering.

Input: $f \in R[x_1, \dots, x_n]$, $G = \{g_1, \dots, g_s\} \in \mathcal{G}$.

Output: $h \in R[x_1, \dots, x_n]$, a pseudo normal form of f with respect to G, having a standard representation

$$cf - h = \sum_{i=1}^{s} a_i g_i$$

with c a product of leading coefficients of elements of G.

`NFBuchberger` is essentially the same as the following algorithm `NFMora` applied to global orderings.

Algorithm 3.6 (NFMora). Let $>$ be any monomial ordering.
Input: $f \subset R[x_1, \dots, x_n]$, $G = \{g_1, \dots, g_s\} \in \mathcal{G}$.

Output: $h \in R[x_1, \dots, x_n]$, a pseudo normal form of f with respect to G, having a standard representation

$$uf - h = \sum_{i=1}^{s} a_i g_i$$

with $\mathrm{LM}(u) = 1$ and $\mathrm{LC}(u)$ a product of leading coefficients of elements of G.

- $h = f$;
- $T = G$;
- while $h \neq 0$ and $T_h = \{g \in T \mid \mathrm{LM}(g) \mid \mathrm{LM}(h)\} \neq \emptyset$

  choose $g \in T_h$ with $\mathrm{ecart}(g)$ minimal;

  if $(\mathrm{ecart}(g) > \mathrm{ecart}(h))$

    $T = T \cup \{h\}$,

  $h = \mathrm{spoly}(h, g)$;
- $\mathrm{return}(h)$;

Proof. Termination of `NFMora` can be seen as in [7, Algorithm 1.7.6].

To see correctness, consider the ν–th turn in the while loop. There we have $(h_0 := f)$

$$\begin{aligned}
&h_\nu = \mathrm{spoly}(h_{\nu-1}, g'_\nu) = c'_\nu h_{\nu-1} - m_\nu g'_\nu \,, \\
&\mathrm{LM}(h_{\nu-1}) = \mathrm{LM}(m_\nu)\,\mathrm{LM}(g'_\nu) \,, \\
&\mathrm{LM}(h_{\nu-1}) > \mathrm{LM}(h_\nu) \,,
\end{aligned}$$

where $c'_\nu = \mathrm{LC}(g'_\nu)$, m_ν is a term and for g'_ν we have two possibilities:

(a) $g'_\nu = g_j \in \{g_1, \dots, g_s\} = G$ for some j, or

(b) $g'_\nu = h_j \in T \smallsetminus G = \{h_0, \dots, h_{\nu-3}, h_{\nu-2}\}$.

Suppose, by induction, that at the end of step $\nu - 1$ we have constructed a standard representation $(u_0 := 1, a_i^{(0)} := 0)$

$$(*) \qquad u_{\nu-1} f = \sum_{i=1}^{s} a_i^{(\nu-1)} g_i + h_{\nu-1},\ a_i^{(\nu-1)} \in R[x_1, \dots, x_n]\,,$$

with $\mathrm{LM}(u_{\nu-1}) = 1$ and $\mathrm{LC}(u_{\nu-1})$ a product of leading coefficients of elements of G.

In case (a), multiply both sides of $(*)$ with $c_j = \mathrm{LC}(g_j)$ and replace $c_j h_{\nu-1}$ with $h_\nu + m_\nu g_j$. We obtain an expression $u_\nu f = \sum a_i^{(\nu)} g_i + h_\nu$ with $u_\nu = c_j u_{\nu-1}$ and $a_i^{(\nu)} \in R[x_1, \dots, x_n]$, hence, $\mathrm{LM}(u_\nu) = 1$, $\mathrm{LC}(u_\nu)$ a product of leading coefficients of elements of G.

In case (b), multiply both sides of $(*)$ with $c'_\nu = \mathrm{LC}(h_j)$ and replace $c'_\nu h_{\nu-1}$ with $h_\nu + m_\nu h_j$, where $j < \nu - 1$.

By induction,

$$-h_j = \sum_{j=1}^{s} a_i^{(j)} g_j - u_j f, \quad \mathrm{LM}(u_j) = 1$$

with $\mathrm{LM}(u_j) = 1$, $\mathrm{LC}(u_j)$ a product of leading coefficients of elements of G. Hence, $(c'_\nu u_{\nu-1} - m_\nu u_j) f = \sum_{i=1}^{s} a_i^{(\nu)} g_i + h_\nu$, $a_i^{(\nu)} \in K[x_1, \dots, x_n]$.

Since $\mathrm{LM}(m_\nu)\,\mathrm{LM}(g'_\nu) = \mathrm{LM}(h_{\nu-1}) < \mathrm{LM}(h_j)$ (since $j < \nu - 1$), we obtain $\mathrm{LM}(m_\nu) < 1$ and, hence, $\mathrm{LM}(m_\nu u_j) < 1$.

By induction, $\mathrm{LC}(u_{\nu-1})$ is a product of leading coefficients of G and $\mathrm{LM}(u_{\nu-1}) = 1$, hence $\mathrm{LM}(c'_\nu u_{\nu-1}) = 1$ and setting $u_\nu = c'_\nu u_{\nu-1} - m_\nu u_j$, we obtain the result. $\square$

Acknowledgement: We should like to thank B. Kunyavskii for communcating the problem to us and for continuous discussions. Moreover, we are grateful to the Deutsche Forschungsgemeinschaft, the German-Israeli Foundation for Scientific Research and Development and the Stiftung Rheinland–Pfalz für Innovation for financial support.

References

[1] Aubry, Y.; Perret, M.: A Weil theorem for singular curves. Arithmetic, Geometry and Coding Theory. Eds.: R. Pellikaan, M. Perret and S.G. Vladut, Walter de Gruyter, Berlin-New York, 1–7 (1996).

[2] Bombierei, E.: Thompson's problem $\sigma^2 = 3$. Invent. Math. **58**, 77–100 (1980).

[3] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, University of Innsbruck, Austria (1965).

[4] Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 2.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2001). `http://www.singular.uni-kl.de`.

[5] Greuel, G.-M.; Pfister, G.: Advances and Improvements in the Theory of Standard Bases and Syzygies. Arch. Math. 66, 163–176 (1996).

[6] Greuel, G.-M.; Pfister, G.: Gröbner Bases and Algebraic Geometry. In: B. Buchberger and F. Winkler (ed.): Gröbner Bases and Applications. LNS 251, 109–143, CUP 1998.

[7] Greuel, G.-M.; Pfister, G.: A SINGULAR Introduction to Commutative Algebra. To appear, Springer (2002).

[8] Greuel, G.-M.; Grunewald, F.; Kunyavskii, B.; Pfister, G.; Plotkin, E.; Segev, Y.: On Equations in Finite Linear Groups. To appear.

[9] Grunewald, F.; Kunyavskii, B.; Nikolova, D.; Plotkin, E.: Two–variable identities in groups and Lie algebras. Zap. Nauch. Semin. POMI **272**, 161–176 (2000).

[10] Plotkin, B.; Plotkin, E.; Tsurkov, A.: Geometrical equivalence of groups. Comm. Algebra **27**, 4015–4025 (1999).

[11] Thompson, J.: Non–solvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. **74**, 383–437 (1968).