

A Computer Algebra Solution to a Problem in Finite Groups

Gert-Martin Greuel

Abstract

We report on a partial solution of the conjecture that the class of finite solvable groups can be characterised by 2–variable identities. The proof requires pieces from number theory, algebraic geometry, singularity theory and computer algebra. The computations were carried out using the computer algebra system SINGULAR.

1. The Problem

The following problem has been communicated to me by B. Kunyavskii: *characterise the class of finite solvable groups by 2–variable identities.* The answer to this question would solve conjectures in the theory of finite and profinite groups and has potential applications to graph theory.

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 $[x, y]_{n+1} = [[x, y]_n, y]$). 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. [7]).

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

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

2000 Mathematics Subject Classification: 11, 13, 14, 20.

Keywords: Solvable groups, Engel identity, rational points on curves, computer algebra, SINGULAR.

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 $x, y \in G$.*

One may even conjecture that for *any* word w such that the sequence U_n^w does not contain the trivial word $U_n^w = 1$ for some n , the conclusion of Conjecture 1.1 holds.

The starting point for the proof is the following Theorem:

Theorem 1.2 (J. Thompson [8]) *The minimal finite non-solvable groups (that is, all subgroups are solvable) are:*

- (1) $\text{PSL}(2, p)$, p prime number, $p = 5$ or $p = \pm 2 \pmod{5}$, $p \neq 3$.
- (2) $\text{PSL}(2, 2^n)$, $n \geq 2$.
- (3) $\text{PSL}(2, 3^n)$, $n \geq 3$, odd.
- (4) $\text{PSL}(3, 3)$.
- (5) $\text{Sz}(2^n)$, $n \geq 3$.

In view of this result, Conjecture 1.1 is implied by

Conjecture 1.3 *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 there exists $x, y \in G$ satisfying $U_n(x, y) \neq 1$.*

Conjecture 1.3 has been proved for all cases except for the Suzuki groups in (5) by using, in particular, computer algebra computations.

Theorem 1.4 ([2]) *Conjecture 1.3 holds for the word $w = X^{-1}YXY^{-1}$ and the groups (1)-(4) in Thompson's list.¹*

While several attempts to prove the above conjectures by using the structure theory of finite groups failed, the following, completely different approach (in the spirit of [3]) leads to a proof of Theorem 1.4.

For any of the groups in (1)-(3), consider its standard linear representation, that is, consider the matrices

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

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

¹Meanwhile (October 2002), all cases, including the Suzuki case (5), have been settled by the authors, too, using the word $w_2 = X^{-2}Y^{-1}X$. Hence Conjecture 1.3 is proved with $w = w_2$.

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 definition 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.

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) occurring in (1)-(3) of Thompson's list. This is equivalent to $U_1(x, y) = U_2(x, y)$ having a solution $x, y \in \text{PSL}(2, p^n)$.

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.

Remark: The word w in Theorem 1.4 is the first of the following four words found by a computer search through about 10,000 shortest words in X, X^{-1}, Y, Y^{-1} , for which the equation $U_1 = U_2$ had a non-trivial solution in $\text{PSL}(2, p)$, $p < 1000$:

$$\begin{aligned} w_1 &= X^{-1}YXY^{-1}X, & w_2 &= X^{-2}Y^{-1}X, \\ w_3 &= Y^{-2}X^{-1}, & w_4 &= XY^{-2}X^{-1}YX^{-1}. \end{aligned}$$

Meanwhile we could verify that also w_2 satisfies the statement of Theorem 1.4.

Acknowledgements: The present paper is a report on joint work in preparation with T. Bandman, F. Grunewald, B. Kunyavskii, G. Pfister and E. Plotkin ([2]), which will appear elsewhere. I should particularly like to thank B. Kunyavskii for many interesting discussions on the subject. It is also a pleasure to thank the organisers of the conference in honour of J. L. Vicente for providing a stimulating atmosphere during the conference. Special thanks to H. Schönemann, who provided the necessary changes of the kernel of SINGULAR.

2. Principal Steps of the Proof

We present only the principal steps for proving Theorem 1.4 and the groups (1) in Thompson's list. The other cases are similar. The arguments which we present are valid for sufficiently large prime numbers $p \geq p_0$. The bound p_0 can be explicitly determined and is small enough so that the remaining cases can be checked case by case. For small p , a variety of different methods and tricks has been used for which we refer to [5]. Here we concentrate mainly on arguments from *singularity theory*, which helped to solve the problem for large p .

- (1) Create the ideal $I \subset \mathbb{Z}[b, c, t]$ generated by the entries of $U_1(x, y) - U_2(x, y)$. Show that it defines a smooth curve C in $\mathbb{A}^3(\mathbb{C})$. Indeed, computing a Gröbner basis without any division² of the ideal defining the singular locus, we find a p such that C defines a smooth curve in $\mathbb{A}^3(\mathbb{F}_q)$ for all primes $q \geq p$.

We want to show: For p sufficiently large, C has a rational point, that is, a point in $(\mathbb{F}_p)^3$. Since $U_1(x, y) \neq 1$ for all x, y , this is equivalent to $U_1(x, y) = U_2(x, y)$ having a solution and, hence, proves Theorem 1.4 (1) for large p .

- (2) Compute the ideal $I^h \subset \mathbb{Z}[b, c, t, h]$ of the projective closure \overline{C} of C in \mathbb{P}^3 , h is the homogenising variable. Compute the Hilbert polynomial of I^h as $16t - 24$, hence \overline{C} is of degree $d = 16$ and arithmetic genus $p_a = 25$.
- (3) Compute the singular locus of \overline{C} . We obtain that \overline{C} has four singular points: $p_1 = (1 : 0 : 0 : 0)$, $p_2 = (1 : 0 : 1 : 0)$, $p_3 = (0 : 1 : 0 : 0)$, $p_4 = (0 : 1 : -1 : 0)$, lying on $H_\infty = \{h = 0\}$. We obtain these points by computing a primary decomposition of the ideal $\langle I^h, h \rangle$ defining $\overline{C} \cap H_\infty$.
- (4) Make a local analysis of the singularities by computing the tangent cone of \overline{C} at each singular point.

Compute, for each singular point, a primary decomposition of the ideal defining the tangent cone. We obtain that \overline{C} has four different smooth branches at p_1 and p_3 and two different smooth branches at p_2 and p_4 .

- (5) Compute the delta invariants $\delta_1, \dots, \delta_4$ of p_1, \dots, p_4 by analysing the tangent cone at these points further and computing intersection and Milnor numbers. We obtain $\delta_1 = \delta_3 = 4$, $\delta_2 = \delta_4 = 2$. Hence, the geometric genus of \overline{C} is $p_g = 13$.

²The result will not be a Gröbner basis over \mathbb{Z} but a *pseudo Gröbner basis*, which means that, for any prime number p such that p does not divide any leading coefficient, the result is a Gröbner basis over the field \mathbb{Z}_p (cf. [4], [5]).

- (6) Now we use the (generalised) Hasse–Weil bound for the number of rational points $N_q(\overline{C}) = \#\overline{C}(\mathbb{F}_q)$ of an absolutely irreducible projective curve \overline{C} , defined over a finite field \mathbb{F}_q :

$$N_q(\overline{C}) \geq q + 1 - 2p_g\sqrt{q} - \sum_{p \in \text{Sing}(\overline{C})} (r_p - 1)$$

where r_p denotes the number of local analytic branches of the germ (\overline{C}, p) . This is an easy improvement of the bound given in [1] (which involves δ_p instead of $r_p - 1$).

We want to show $N_p(C) > 0$ for large primes p .

Since $C = \overline{C} \setminus H_\infty \cap \overline{C}$ and $\#H_\infty \cap \overline{C} = 4$, we obtain

$$N_p(C) \geq p - 26\sqrt{p} - 11,$$

that is, $N_p(C) > 0$ if $p > 700$, provided \overline{C} is absolutely irreducible.

- (7) It remains to show that \overline{C} is absolutely irreducible. This is the hardest part.

Project $\overline{C} \subset \mathbb{P}^3$ from the point $p_3 = (0 : 1 : 0 : 0)$ to \mathbb{P}^2 by eliminating c from the ideal $\overline{I} \subset \mathbb{Z}[b, c, t, h]$. The result is a homogeneous polynomial f of degree 12.

Now we make an “Ansatz”

$$f = f_1 \cdot f_2,$$

with $1 \leq \deg f_1 \leq 12$, $\deg f_2 = 12 - \deg f_1$, where the coefficients of f_1 , resp. f_2 , are indeterminates a_1, \dots, a_N , resp. b_1, \dots, b_M , that is, $f_1 \in \mathbb{Z}[a_1, \dots, a_N, b, t, h]$, $f_2 \in \mathbb{Z}[b_1, \dots, b_M, b, t, h]$.

Compute the ideal $H \subset \mathbb{Z}[a_1, \dots, a_N, b_1, \dots, b_M]$ generated by the coefficients of $f - f_1 \cdot f_2$.

- (8) Compute a Gröbner basis of H in $\mathbb{Q}[a_1, \dots, a_N, b_1, \dots, b_M]$ but without any division. That is, the result is defined over \mathbb{Z} and during the computation no division occurred (here we had to change the kernel of SINGULAR). It turns out that, in all cases, the result is an integer n , and hence the following holds:

For any prime p such that $p \nmid n$, the reduction of $H \bmod p$, that is the image of H in $\mathbb{Z}_p[a_1, \dots, a_N, b_1, \dots, b_M]$, has no solution over the algebraic closure $\overline{\mathbb{Z}}_p$ of \mathbb{Z}_p . This is an easy generalisation of the well-known corresponding result for Gröbner bases over fields (cf. [4], [5]).

Hence, for any $p \nmid n$, the decomposition $f = f_1 \cdot f_2$ is impossible over $\overline{\mathbb{Z}}_p$ and, therefore, the image of f in $\mathbb{Z}_p[b, t, h]$ is absolutely irreducible.

- (9) For the remaining finitely many primes p which divide n , we check by a direct computation that C has a point in $(\mathbb{Z}_p)^3$.
- (10) All computations were done by using the computer algebra system SINGULAR ([6]). To be able to compute a pseudo Gröbner basis, we had to change the kernel of SINGULAR slightly. This is available in SINGULAR-2-0-3 or higher by setting `option(contentsB)`. However, a straightforward Gröbner computation led to much too large integers n . Therefore, we invented a “divide and conquer” strategy to keep n small, for which we refer to [5], and to the SINGULAR code which is available from the authors.

3. SINGULAR Computations

In this section we present the SINGULAR computations for steps (1)-(5) which are needed for the computation of the geometric genus of the space curve \overline{C}^3 . We omit the computations for proving that \overline{C} is absolutely irreducible, which is much more involved (cf. [5]). The sequence of commands below may be used as a model to attack related problems.

We start by loading all SINGULAR libraries:

```
LIB "all.lib"; //load all libraries
```

Step (1)

Create the polynomial ring and the matrices X and Y representing elements of $\text{PSL}(2, p^n)$:

```
ring r = 0,(b,c,t),dp; //global (affine) ring
matrix X[2][2] = 0, -1,
                1, t;
matrix Y[2][2] = 1, b,
                c, 1+bc;
```

Create the word w :

```
matrix iX = inverse(X);
matrix iY = inverse(Y);
matrix U1 = iX*Y*X*iY*X; //the word w
matrix N = X*U1*iX;
matrix M = Y*U1*iY;
matrix iN = inverse(N);
matrix iM = inverse(M);
matrix U2 = N*M*iN*iM;
```

³New versions of SINGULAR (2-0-4 and higher) will contain a procedure `genus` which computes the geometric genus of a reduced curve automatically.

Create the ideal I of entries of the matrix $U_1 - U_2$:

```

ideal I = ideal(U1-U2);
I;
/--> I[1]=-b6c4+b5c5-b6c3t+4b5c4t-2b4c5t+3b5c3t2-5b4c4t2+b3c5t2
/-->      -3b4c3t3+2b3c4t3+b3c3t4-b6c2-4b5c3+3b4c4+2b3c5-b5c2t
/-->      +12b4c3t-2b3c4t-2b2c5t+7b4c2t2-11b3c3t2-b2c4t2-7b3c2t3
/-->      +3b2c3t3+2b2c2t4-3b5c-8b4c2+4b3c3+5b2c4+bc5+3b4ct+12b3c2t
/-->      +2b2c3t-2bc4t+2b3ct2-3b2c2t2-4bc3t2-2b2ct3-bc2t3-2b4
/-->      -10b3c+2b2c2+4bc3+c4+2b3t+6b2ct+c3t+2bct2-b2c-b2t+bct
/-->      +bt2-5b2-2bc+c2+bt-ct-b-c-1
/--> I[2]=b6c3-b5c4+b6c2t-4b5c3t+2b4c4t-3b5c2t2+5b4c3t2-b3c4t2
/-->      +3b4c2t3-2b3c3t3-b3c2t4+b6c+3b5c2-3b4c3-2b3c4-10b4c2t
/-->      +2b3c3t+2b2c4t-5b4ct2+10b3c2t2+b2c3t2+6b3ct3-3b2c2t3
/-->      -2b2ct4+2b5+4b4c-6b3c2-5b2c3-bc4-4b4t-8b3ct+2bc3t+2b3t2
/-->      +3b2ct2+4bc2t2+bct3-b2c2-2b2ct+bc2t-b2t2+2bct2+bt3+3b3
/-->      -7b2c-5bc2-c3-4b2t+2bct-c2t+bt2-2bc-c2-2bt-ct-2b-2c-1
/--> I[3]=-b6c5+b5c6-b6c4t+4b5c5t-2b4c6t+3b5c4t2-5b4c5t2+b3c6t2
/-->      -3b4c4t3+2b3c5t3+b3c4t4-b6c3-5b5c4+4b4c5+2b3c6-2b5c3t
/-->      +16b4c4t-4b3c5t-2b2c6t+10b4c3t2-16b3c4t2-10b3c3t3+5b2c4t3
/-->      +3b2c3t4-4b5c2-11b4c3+6b3c4+7b2c5+bc6+3b4c2t+20b3c3t
/-->      +2b2c4t-4bc5t+6b3c2t2-9b2c3t2-6bc4t2-6b2c2t3+bc2t4-4b4c
/-->      -16b3c2+5b2c3+7bc4+2c5+4b3ct+14b2c2t+c4t+b2ct2-c3t2-bct3
/-->      -b3-11b2c-bc2+3c3+b2t+4bct-2c2t+ct2+b2-bt-2b-2c+1
/--> I[4]=b6c4-b5c5+b6c3t-4b5c4t+2b4c5t-3b5c3t2+5b4c4t2-b3c5t2
/-->      +3b4c3t3-2b3c4t3-b3c3t4+b6c2+4b5c3-4b4c4-2b3c5+b5c2t
/-->      -14b4c3t+4b3c4t+2b2c5t-8b4c2t2+15b3c3t2+9b3c2t3-5b2c3t3
/-->      -3b2c2t4+3b5c+6b4c2-8b3c3-7b2c4-bc5-5b4ct-14b3c2t+4bc4t
/-->      +8b2c2t2+6bc3t2+3b2ct3-bct4+b4+6b3c-12b2c2-8bc3-2c4-2b3t
/-->      -10b2ct+4bc2t-c3t+b2t2+4bct2+c2t2+b2c+b2t-bct-bt2+b2-6bc
/-->      -5c2-bt+ct+b+c+t-1

```

We now have to show that I defines a curve and that its reduction mod p has rational points for sufficiently large p .

We start by computing the dimension and singular locus of the variety defined by I :

```

ideal sI = groebner(I);      //compute a Groebner basis
dim(sI);                    //compute the dimension of I
/--> 1                        //I defines a curve

dim_slocus(I);              //the singular locus is empty
/--> -1

```

Step (2)

Compute the projective closure \overline{C} of C by homogenising I :

```
ring rh = 0,(b,c,t,h),dp;    //h is the homogenizing variable
ideal I = imap(r,I);
ideal sI = groebner(I);
ideal hI = homog(sI,h);      //the projective closure is given
                               //by a homogenized standard basis
ideal shI =std(hI);         //a Groebner basis of hI
```

Compute the Hilbert polynomial, the degree and arithmetic genus of the projective curve \overline{C} :

The command `hilb(shI)`; displays the first and the second Hilbert series of \overline{C} . The second Hilbert series is used to compute the Hilbert polynomial of \overline{C} . It is coded in the integer vector `v=hilb(shI,2)`.

```
intvec v = hilb(shI,2);
v;
/--> 1,2,3,4,5,4,-1,-2,0
```

To compute the Hilbert polynomial we need a small procedure:

```
poly hp;
for(int i=1; i<=size(v); i++)
{
  hp=hp+v[i]*(t-i+2);    (t)^(-i+2)
}
hp;
/--> 16t-24              //the Hilbert polynomial
```

The Hilbert polynomial of \overline{C} is $16t - 24$. Hence \overline{C} is a curve of degree 16 and arithmetic genus 25.

Step (3)

By Step (1) we know that C is non-singular. To check whether \overline{C} is singular, we compute the dimension of the singular locus of the affine cone of \overline{C} :

```
dim_slocus(shI);
/--> 1                    //curve is singular at infinity
```

Now compute the singular points of \overline{C} at infinity:

```
ideal I0 = subst(hI,h,0); //intersection with line
                               //at infinity
list pr = primdecGTZ(I0); //make a primary decomposition
```

To locate the intersection points of \overline{C} with the hyperplane at infinity, we make a primary decomposition of the ideal I_0 which defines the affine cone over these points.

The primary decomposition is displayed by typing `pr;`. The list consists of five entries `pr[1], ..., pr[5]`, we omit the entry `pr[5]` of the list, describing the embedded component corresponding to the vertex of the affine cone. Each list entry `pr[i]` consists of two ideals `pr[i][1]`, and `pr[i][2]`, where the first is the ideal of the primary component, while the second is the ideal of the associated prime ideal. The SINGULAR output is slightly changed to save space:

```
pr;
//-->[1]:                               //-->[2]:
//-->  [1]:                               //-->  [1]:
//-->    _[1]=c2                          //-->    _[1]=t5
//-->    _[2]=b-t                         //-->    _[2]=ct2
//-->  [2]:                               //-->    _[3]=c2+ct
//-->    _[1]=c                           //-->    _[4]=b2ct+t4
//-->    _[2]=b-t                         //-->  [2]:
                                           //-->    _[1]=t
                                           //-->    _[2]=c
//-->[3]:                               //-->[4]:
//-->  [1]:                               //-->  [1]:
//-->    _[1]=c+t                          //-->    _[1]=t5
//-->    _[2]=b2                           //-->    _[2]=bt2
//-->  [2]:                               //-->    _[3]=bc2t-t4
//-->    _[1]=c+t                          //-->    _[4]=b2-bt
//-->    _[2]=b                           //-->  [2]:
                                           //-->    _[1]=t
                                           //-->    _[2]=b
```

Hence we see that \overline{C} has four points at infinity: $p_1 = (1 : 0 : 0 : 0)$, $p_3 = (1 : 0 : 1 : 0)$, $p_2 = (0 : 1 : 0 : 0)$, $p_4 = (0 : 1 : -1 : 0)$, the coordinates are $(b : c : t : h)$.

Step (4)

Make a local analysis of the points at infinity. We consider only the affine chart $(b = 1)$ which contains the points $p_1 = (0, 0, 0)$ and $p_3 = (0, 1, 0)$ in affine coordinates:

```
ideal I1 = subst(hI,b,1); //set b=1
```

Make a local analysis in p_1 :

```
ideal T1 = tangentcone(I1); //the tangent cone of C at p1
list pr = primdecGTZ(T1); //primary decomposition
//of the tangent cone
```

```

pr;
/-->[1]:          /-->[2]:          /-->[3]:
/--> [1]:          /--> [1]:          /--> [1]:
/-->   _[1]=t-2h  /-->   _[1]=t+h    /-->   _[1]=h
/-->   _[2]=c+h   /-->   _[2]=c2-ch+h2 /-->   _[2]=c
/--> [2]:          /--> [2]:          /--> [2]:
/-->   _[1]=t-2h  /-->   _[1]=t+h    /-->   _[1]=h
/-->   _[2]=c+h   /-->   _[2]=c2-ch+h2 /-->   _[2]=c

```

Hence, we obtain four different smooth branches because the second list entry `pr[2]` defines two (non-rational) points. Moreover, we see from `pr[1]` and `pr[3]` that the branches 1 and 4 have rational tangent directions, and from `pr[2]` that branches 2 and 3 have irrational tangent directions. Therefore, two of the preimage points in the normalisation are rational and two are irrational.

Step (5)

To compute the delta invariant of the singular point p_1 , we note that $(C_1, 0)$, the union of branches 1 and 4, as well as $(C_2, 0)$, the union of the two branches with irrational tangents, define both an A_1 -singularity. Since $\delta(A_1) = 1$ and since $\delta((C_1, 0) \cup (C_2, 0)) = \delta(C_1, 0) + \delta(C_2, 0) + (C_1 * C_2, 0)$ we have to compute the intersection multiplicity of $(C_1 * C_2, 0)$ of C_1 and C_2 at 0, which coincides with the intersection multiplicities of the tangents.

```

ring s = 0,(c,t,h),ds;          //create a local ring
list pr = imap(rh,pr);
ideal i1, i2 = pr[1][2], pr[3][2];
ideal C1 = intersect(i1,i2);
ideal C2 = pr[2][2];
option(prot);
vdim(std(C1+C2));              //intersection multiplicity of C1 and C2
/--> 2                          //intersection multiplicity is 2

```

Hence $\delta(\overline{C}, p_1) = 1 + 1 + 2 = 4$.

Now let us compute δ of \overline{C} at the point p_3 :

```

setring rh;
map phi = rh,b,c,t+1,h;
ideal I3 = phi(I1);
ideal T3= tangentcone(I3);
primdecGTZ(T3);
/-->[1]:
/--> [1]:
/-->   _[1]=c2
/-->   _[2]=t
/--> [2]:
/-->   _[1]=c
/-->   _[2]=t

```

Hence we have a singularity of multiplicity 2 with one tangent, it must be an A_k singularity with $k > 1$.

```

setring s;
ideal I3 = imap(rh,I3);
option(prot);
I3 = std(I3);
I3;
/--> I3[1]=t-c2+2ct+4t2+ch+th-2h2-c3-2c2t+4ct2+6t3+4cth+3t2h
/--> -7ch2-7th2-c3t-c2t2+3ct3+4t4+2c2th+6ct2h+4t3h-2c2h2
/--> -13cth2-11t2h2-4ch3-th3-3h4+ct4+t5+c3th+3c2t2h+4ct3h+2t4h
/--> +c3h2-4ct2h2-5t3h2-2c2h3-5cth3-3t2h3+ch4-2th4-2h5
/--> I3[2]=c2-ct-2ct2-cth+6ch2-2th2-c2t2-ct3-c2th-ct2h+5cth2
/--> -3t2h2+2ch3-2th3+7h4+c2th2-t3h2-2cth3-2t2h3-2ch4+5th4+4h5

```

We see that I_3 is a complete intersection and we can compute its Milnor number (using the Greuel-Lê formula implemented in SINGULAR):

```

milnor(I3);
/--> 3

```

The curve \overline{C} has at p_3 an A_3 -singularity, hence $\delta(\overline{C}, p_3) = 2$.

Similarly, we compute $\delta(\overline{C}, p_2) = 4$, $\delta(\overline{C}, p_4) = 2$. Altogether, the total δ invariant is 12 and we can compute the geometric genus of the projective closure of C as $p_g(\overline{C}) = p_a(\overline{C}) - \delta(\overline{C}) = 25 - 12 = 13$.

References

- [1] AUBRY, Y. AND PERRET, M.: A Weil theorem for singular curves. In *Arithmetic, Geometry and Coding Theory (Luminy, 1993)*, 1–7. De Gruyter, Berlin-New York, 1996.
- [2] BANDMAN, T., GREUEL, G.-M., GRUNEWALD, F., KUNYAVSKII, B., PFISTER, G. AND PLOTKIN, E.: Engel-like identities characterising finite solvable groups. Available at <http://arxiv.org/abs/math.GR/0303165>.
- [3] BOMBIERI, E.: Thompson's problem $\sigma^2 = 3$. *Invent. Math.* **58** (1980), 77–100.
- [4] GREUEL, G.-M. AND PFISTER, G.: *A SINGULAR Introduction to Commutative Algebra*. With contributions by O. Bchmann, C. Lossen and H. Schönemann. Springer Verlag Berlin, Heidelberg, New York, 2002.
- [5] GREUEL, G.-M. AND PFISTER, G.: Computer Algebra and Finite Groups. In *Mathematical software (Beijing, 2002)*, 4–14. World Sci. Publishing, River Edge, NJ, 2002.

- [6] GREUEL, G.-M., PFISTER, G. AND SCHÖNEMANN, H.: SINGULAR, 2-0-3. *A Computer Algebra System for Polynomial Computations*. Centre for Computer Algebra, University of Kaiserslautern, 2001. <http://www.singular.uni-kl.de>.
- [7] PLOTKIN, B., PLOTKIN, E. AND TSURKOV, A.: Geometrical equivalence of groups. *Comm. Algebra* **27** (1999), 4015–4025.
- [8] THOMPSON, J.: Non-solvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.

Recibido: 9 de abril de 2002

Gert-Martin Greuel
Fachbereich Mathematik
Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern, Germany
greuel@mathematik.uni-kl.de