A Problem in Group Theory solved by Computer Algebra

Gerhard Pfister

9th December 2002

I shall briefly report on how a problem in finite group theory could be translated to algebraic geometry and partially solved using computer algebra.

If G is a group and $x,\ y \in G$, we inductively define

$$e_1(x,y) := x^{-2} \cdot y^{-1} \cdot x,\ e_{n+1}(x,y) := [x \cdot e_n(x,y) \cdot x^{-1}, y \cdot e_n(x,y) \cdot y^{-1}]$$

where the commutator of $g,\ h \in G$ is defined by $[g,h] := ghg^{-1}h^{-1}$.

Theorem 1 (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavsky, G. Pfister, E. Plotkin). A finite Group G is solvable if and only if there is an $n \in \mathbb{N}$ such that $e_n(x,y) = 1$ 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 [8] 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.

To prove the theorem it is enough to show that for each group G in Thompson's list we have $x, y \in G$ with $e_1(x,y) = e_2(x,y)$ and $y \neq x^{-1}$. This implies $1 \neq e_1(x,y) = e_n(x,y)$ for all n.

We shall give an idea on how to prove the theorem for the group PSL(2,q). The case PSL(3,3) is easy but the case $S_z(2^n)$ is much more difficult.

Proposition 2. If $q = p^k$ for a prime p and $q \neq 2, 3$, then there are x, y in $\mathrm{PSL}(2, \mathbb{F}_q)$ with $y \neq x^{-1}$ and $e_1(x,y) = e_2(x,y)$.

The proof will use some explicit computations with the following matrices. Let R be a commutative ring with identity and define

$$x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix}, \quad y(b,c) := \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \in \mathrm{SL}(2,R)$$

for $t, b, c \in R$.

Let $I = \langle n_1, n_2, n_3, n_4 \rangle \subseteq \mathbb{Z}[b,c,t]$ be the ideal generated by the entries of the matrix $e_1(x,y) - e_2(x,y)$.

Using Singular we can obtain I as follows:

```
LIB"linalg.lib";

ring R = 0,(b,c,t),dp;

matrix X[2][2] = t, -1,
                 1, 0;

matrix Y[2][2] = 1, b,
                 c, 1+bc;

matrix iX = inverse(X);
matrix iY = inverse(Y);

matrix M=iX*Y*iX*iY*X*X-Y*iX*iX*iY*X*iY;
ideal I=flatten(M);

I;
I[1]=b3c2t2+b2c2t3-b2c2t2-bc2t3-b3ct+b2c2t+b2ct2+2bc2t2+bct3
     +b2c2+b2ct+bc2t-bct2-c2t2-ct3-b2t+bct+c2t+ct2+2bc+c2+bt
     +2ct+c+1;
I[2]=-b3ct2-b2ct3+b2c2t+bc2t2+b3t-b2ct-2bct2-b2c+bct+c2t+ct2
      -bt-ct-b-c-1;
I[3]=b3c3t2+b2c3t3-b2c2t3-bc2t4-b3c2t+b2c3t+2b2c2t2+2bc3t2
     +2bc2t3+b2c2t+2b2ct2+bc2t2-c2t3-ct4-2b2ct+bc2t+c3t+bct2
     +2c2t2+ct3-b2c-b2t+bct+c2t +bt2+3ct2+bc-bt-b-c+1;
I[4]=-b3c2t2-b2c2t3+b2c2t2+bc2t3+b3ct-b2c2t-b2ct2-2bc2t2-bct3
     -2b2ct+c2t2+ct3+b2t-bct-c2t-ct2+b2-bt-2ct-b-t+1;
```

To prove Proposition 2 above, it is enough to prove the following

Proposition 3. Let q be as in Proposition 2, then the variety $V^{(q)} = V(I\mathbb{F}_q[b,c,t]) \subset \mathbb{F}_q^3$ induced by I is not empty.

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 $\overline{C}$.

Proposition 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 $\overline{C}$.

Let L be the algebraic closure of $\mathbb{F}_q$. To apply the proposition, we have to prove that $IL[b,c,t]$ is a prime ideal.

Lemma 5. $IL(t)[b,c] = \langle f_1, f_2 \rangle$ with

$$\begin{aligned} f_1 &= t^2b^4 - t^3(t-2)b^3 + (-t^5+3t^4-2t^3+2t+1)b^2 \\ &\qquad + t^2(t^2-2t-1)(t-2)b + (t^2-2t-1)^2 \\ f_2 &= t(t^2-2t-1)c + t^2b^3 + (-t^4+2t^3)b^2 + (-t^5+3t^4-2t^3+2t+1)b \\ &\qquad + (t^5-4t^4+3t^3+2t^2)\,. \end{aligned}$$

Moreover, $IL[b,c,t] = \langle f_1, f_2 \rangle : h^2$, $h = t(t^2-2t-1)$.

This can be tested in Singular as follows

```
ring S=(0,t),(c,b),lp;
ideal I=imap(R,I);
ideal J=std(I);
J;
J[1]=(t2)*b4+(-t4+2t3)*b3+(-t5+3t4-2t3+2t+1)*b2+(t5-4t4+3t3+2t2)
     *b+(t4-4t3+2t2+4t+1)
J[2]=(t3-2t2-t)*c+(t2)*b3+(-t4+2t3)*b2+(-t5+3t4-2t3+2t+1)
     *b+(t5-4t4+3t3+2t2)
```

Now $IL(t)[b,c] \cap L[b,c,t] = \langle f_1, f_2 \rangle : h^2 = IL[b,c,t]$. Therefore, it is enough to prove that $IL(t)[b,c]$ is a prime ideal which is equivalent to proving that f_1 is irreducible in $L(t)[b]$. This is equivalent to proving that f_1 is irreducible in $L[t,b]$.

Let $P(x) := t^2 f_1(x/t)$, then

$$\begin{aligned} P(x) = x^4 - t^2(t-2)x^3 + (-t^5+3t^4-2t^3+2t+1)x^2 + t^3(t-2)(t^2-2t-1) \\ x + t^2(t^2-2t-1)^2\,. \end{aligned}$$

It suffices to prove that $P \in L[x,t]$ is irreducible.

To show that P is not divisible by any factor of degree 2 in x we make the following**Ansatz:**

$$p = (x^2 + ax + b)\,(x^2 + gx + d), \tag{*}$$

a, b, g, d polynomials in t with indeterminates `a(i)`, `b(i)`, `g(i)`, `d(i)` as coefficient. It is easy to see that we can assume

$$\deg(b) \leq 5, \deg(a) \leq 3, \deg(d) \leq 3, \deg(g) \leq 2\,.$$

Then a decomposition (*) with `a(i)`, `b(i)`, `g(i)`, `d(i)` $\in \overline{\mathbb{F}}_p$ does not exist if and only if the ideal `co` of the coefficients in x, t of $P-(x^2+ax+b)(x^2+gx+d)$ has no solution in $\overline{\mathbb{F}}_p$; i.e., if a Gröbner basis of `co` contains $1 \in \mathbb{F}_p$. The ideal of coefficients `co`:

```
co[1]=-b(5)*d(3)
co[2]=-b(5)*g(2)
co[3]=-b(4)*d(3)-b(5)*d(2)
co[4]=-b(4)*g(2)-b(5)*g(1)-d(3)-1
co[5]=-b(3)*d(3)-b(4)*d(2)-b(5)*d(1)+1
co[6]=-b(5)-g(2)-1
co[7]=a(0)*b(5)-a(2)*d(3)-b(3)*g(2)-b(4)*g(1)-d(2)+4
co[8]=-a(0)^2*b(5)+b(0)*b(5)-b(2)*d(3)-b(3)*d(2)-b(4)*d(1)-b(5)-4
co[9]=-a(2)*g(2)-b(4)-g(1)+2
co[10]=a(0)*b(4)-a(1)*d(3)-a(2)*d(2)-b(2)*g(2)-b(3)*g(1)-d(1)-1
co[11]=-a(0)^2*b(4)+b(0)*b(4)-b(1)*d(3)-b(2)*d(2)-b(3)*d(1)-b(4)+2
co[12]=a(0)-a(1)*g(2)-a(2)*g(1)-b(3)-d(3)
co[13]=-a(0)^2+a(0)*b(3)-a(0)*d(3)-a(1)*d(2)-a(2)*d(1)+b(0)
       -b(1)*g(2)-b(2)*g(1)-7
co[14]=-a(0)^2*b(3)+b(0)*b(3)-b(0)*d(3)-b(1)*d(2)-b(2)*d(1)-b(3)+4
co[15]=-a(2)-g(2)-2
co[16]=a(0)*a(2)-a(0)*g(2)-a(1)*g(1)-b(2)-d(2)+1
co[17]=-a(0)^2*a(2)+a(0)*b(2)-a(0)*d(2)-a(1)*d(1)+a(2)*b(0)-a(2)
       -b(0)*g(2)-b(1)*g(1)-2
co[18]=-a(0)^2*b(2)+b(0)*b(2)-b(0)*d(2)-b(1)*d(1)-b(2)+1
co[19]=-a(1)-g(1)-2
co[20]=a(0)*a(1)-a(0)*g(1)-b(1)-d(1)+2
co[21]=-a(0)^2*a(1)+a(0)*b(1)-a(0)*d(1)+a(1)*b(0)-a(1)-b(0)*g(1)
co[22]=-a(0)^2*b(1)+b(0)*b(1)-b(0)*d(1)-b(1)
co[23]=-a(0)^3+2*a(0)*b(0)-a(0)
co[24]=-a(0)^2*b(0)+b(0)^2-b(0)
```

Use the `lift` command of SINGULAR to show that (over $\mathbb{Z}$) $4 \in$ `co`

```
matrix M=lift(co,4);
M;
M[1,1]=-a(0)+8*b(0)*b(3)-8*b(0)*b(4)-16*b(0)*g(1)*g(2)-...
M[2,1]=-a(0)^2+6*a(0)*b(3)-30*a(0)*b(5)*d(1)+200*a(0)*b(5)*d(2)-...
```

```
M[3,1]=-8*b(0)*g(1)-8*b(0)*g(2)+8*b(1)*g(2)+8*b(1)-...
M[4,1]=-16*b(0)*g(2)*d(3)-18*b(0)*g(2)+8*b(0)*d(2)-8*b(0)*d(3)-...
M[5,1]=8*a(2)*b(0)+142*a(2)*d(1)*d(3)+41*a(2)*d(1)-...
M[6,1]=a(0)^2*g(2)+8*a(0)*b(0)*d(3)-6*a(0)*b(3)*g(2)+5*a(0)*b(3)+...
M[7,1]=8*b(0)*d(3)+5*b(3)-15*b(5)*d(1)+100*b(5)*d(2)-...
M[8,1]=0
M[9,1]=a(0)^2-6*a(0)*b(3)+30*a(0)*b(5)*d(1)-...
M[10,1]=-6*b(3)+30*b(5)*d(1)-200*b(5)*d(2)+32*b(5)-56*d(2)-79*d(3)+27
M[11,1]=-1
M[12,1]=5*a(0)*g(1)-a(0)*g(2)+16*a(0)*d(2)*d(3)+8*a(0)*d(2)-...
M[13,1]=16*d(2)*d(3)+8*d(2)-15*d(3)-15
M[14,1]=0
M[15,1]=-a(0)^2*g(2)+12*a(0)*b(3)*g(2)-...
M[16,1]=6*b(3)*g(2)-30*b(5)*g(2)*d(1)+200*b(5)*g(2)*d(2)-...
M[17,1]=0
M[18,1]=0
M[19,1]=4*a(0)^2-4*a(0)*b(3)-5*a(0)*g(1)*g(2)+a(0)*g(2)^2-...
M[20,1]=-4*b(3)+31*g(2)+16*d(2)*d(3)+8*d(2)-18*d(3)+8;
M[21,1]=-4
M[22,1]=0
M[23,1]=0
M[24,1]=0
```

We have

$$4 = \sum_{i=1}^{24} M[i,1] \cdot \texttt{ co } [i].$$

This implies that over $\overline{\mathbb{F}_p}$, $p \neq 2$ the polynomial P has no quadratic factor. Similarly, one can show that it has no linear factor. This implies that P is absolutely irreducible in $\mathbb{F}_p[t,x]$ for all $p \neq 2$. The case $p = 2$ can be treated similarly.

Now we can apply Proposition 4 to prove Proposition 3.

We compute the Hilbert polynomial $H(t)$ of the projective curve corresponding to K. We obtain $H(t) = 10t - 11$. The corresponding SINGULAR session is:

```
ring S=0,(b,c,t,w),dp;
option(contentSB);
ideal I=imap(R,I);
ideal J=std(I);
J;
J[1]=bct-t2+2t+1
J[2]=bt3-ct3+t4-b2t+bct-c2t-2bt2+2ct2-3t3+bc+t2+t+1
J[3]=b2c2-b2ct+bc2t-bct2+b2+2bc+c2-b+c-t+2
```

```
J[4]=c2t3-ct4+c3t-2c2t2+3ct3-t4-bc2+bt2-2ct2+4t3-2bt+ct-3t2
      -b-2t
```

It can easily be seen that J induces a Gröbner basis in $\mathbb{F}_p[b,c,t,w]$ for all p, because `option(contentSB)` forces Singular to avoid divisions by integers.

We homogenise J with respect to w and obtain again a Gröbner basis, cf. [6], with respect to the degree reverse lexicographical ordering. Therefore, the Hilbert polynomial is the same in any characteristic.

```
J=homog(J,w);
hilbPoly(J);

-11,10
```

From the Hilbert polynomial, we read the degree $d = 10$ and the arithmetic genus $p_a = 12$. Using Proposition 3, we obtain:

$$\#V^{(q)} \geq q + 1 - 24\sqrt{q} - 10.$$

This implies that $V^{(q)}$ is not empty if $q > 593$.

For the remaining cases, we check explicitly by computer that $V^{(q)}$ is not empty.

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

[3] 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`

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

[5] 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.

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

[7] Greuel, G.-M.; Pfister, G.: Computer Algebra and Finite Groups. In: Proc. of the ICMS Beijing, 2002, 4–14.

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