Finite Solvable Groups and Finite Algebraic Geometry

(G.-M. Greuel)

Problem: Characterise the class of finite solvable groups G by 2–variable identities

Examples:

- G is **abelian** $\Leftrightarrow xy = yx \ \forall\ x, y \in G$

- (Zorn, 1930)

  A finite group G is **nilpotent** $\Leftrightarrow$
  $\exists\ n \geq 1$ s.t. $v_n(x, y) = 1 \ \forall\ x, y \in G$
  (**Engel identity**)

  $v_1 := [x, y] = xyx^{-1}y^{-1}$ (commutator)
  $v_{n+1} := [v_n, y]$

Theorem (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister, E. Plotkin)

A finite group G is **solvable** $\Leftrightarrow$
$\exists\, n \geq 1$ s.t. $U_n(x,y) = 1 \;\forall\, x, y \in G$.

$$w := x^{-2}y^{-1}x$$

$$U_1 = U_1(x,y) := w$$

$$U_{n+1} = U_{n+1}(x,y) := [xU_nx^{-1}, yU_ny^{-1}].$$

(quasi–Engel–identity)

Note:

(1) $U_1(x,y) = 1 \Leftrightarrow y = x^{-1}$

(2) $U_1(x,y) = U_2(x,y)$
$\Leftrightarrow x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}$

(3) If $x, y \in G$ satisfy $y \neq x^{-1}$ and
$U_1(x,y) = U_2(x,y) \Rightarrow U_n(x,y) \neq 1 \;\forall\, n \in \mathbb{N}$.

Open Problem: Does the theorem also hold for

$$w = [x,y]\ ?$$

Motivation for the problem

- **Conjecture**: A profinite prosolvable group can be defined by a finite number of (Engel-like) profinite identities.
  Our result implies a proof of the conjecture and, moreover, **one** profinite identity is enough.

- The **Margulis–Platanov conjecture** on the normal subgroup structure of the group of rational points of simple simply connected algebraic groups over algebraic number fields was established by Y. Segev and G. Seitz by using commuting graph of a finite group G (vertex set is $G \setminus \{1\}$, edges are pairs of commuting elements).

  It is hoped that our result can be used to generalise the Margulis–Platonov conjecture by using the solvability graph (edges are pairs (x, y) s.t. $U_n(x, y) = 1$ for some n)

- Using our method, we can prove **Engel–like identities for nilpotent groups** for many different words v_1.

Motivation for the choice of the word $\mathbf{w} = U_1$

(so far only possible with the help of a computer)

Consider, for any word w in the letters X, Y, X^{-1}, Y^{-1} the sequence U_n (depending on w):

$$U_1 = w$$
$$U_{n+1} = [XU_nX^{-1}, YU_nY^{-1}].$$

A computer search through 10,000 shortest words in X, X^{-1}, Y, Y^{-1} gave the following four words for which the solution set of the equation $U_1 = U_2$ has dimension 1 (and not 0) for all $p < 1000$:

$$w_1 = X^{-2}Y^{-1}X$$
$$w_2 = X^{-1}YXY^{-1}X$$
$$w_3 = Y^{-2}X^{-1}$$
$$w_4 = XY^{-2}X^{-1}YX^{-1}$$

Proof of the theorem

G solvable $\Rightarrow$ identity holds (look at central series).

Outline of $\Leftarrow$

Assume G is **not solvable** and let G denote a minimal counter example (that is, every proper subgroup of G is solvable).

Note: If identity holds for G it holds for subgroups and for quotient groups of G.

Theorem (Thompson, 1968)

Let G be minimally non–solvable. Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime ≥ 5
- $\mathbf{PSL}(2, \mathbb{F}_{2^n})$,
- $\mathbf{PSL}(2, \mathbb{F}_{3^n})$, n odd
- $\mathbf{PSL}(3, \mathbb{F}_3)$
- $\mathbf{Sz}(2^n)$, n odd

Enough to prove (for G from Thompson's list):

$\exists\, x, y \in G$, s.t. $y \neq x^{-1}$ and $U_1(x, y) = U_2(x, y)$.

Translation from algebra to geometry

In the spirit of **E. Bombieri**, Thompson's problem $\sigma^2 = 3$, Inv. Math. 58 (1980).

Outline for PSL$(2, \mathbb{F}_p)$, $p \geq 5$

(PSL$(2, \mathbb{F}_q)$, $q = 2^p$ or $q = 3^p$ is similar, PSL$(3, \mathbb{F}_3)$ easy, Sz(2^p) more difficult.)

We translate the conjecture to a problem on the **existence of rational points on an algebraic curve over a finite field:**

Fix $w_1 = x^{-2}y^{-1}x$ and consider the matrices

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

in $G =$ PSL$(2, \mathbb{F}_p)$.

Since $x^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$ we have $y \neq x^{-1}$ for all $(b, c, t) \in \mathbb{F}_p^3$.

Hence, it suffices to show that the matrix equation $U_1(x, y) = U_2(x, y)$ has a solution (b, c, t) in $\mathbb{F}_p^3$.

Consider the ideals
$I := \langle$ entries of $U_1(x,y) - U_2(x,y)\rangle \subset \mathbb{Z}[b,c,t]$;
$I^{(p)} := I \mod p \subset \mathbb{F}_p[b,c,t]$.

We show: the variety $V(I^{(p)})$ has a rational point $(b,c,t) \in \mathbb{F}_p^3$.

This implies that $U_1(x,y) = U_2(x,y)$ has a solution $x, y \in \mathrm{PSL}(2,p)$.

To show that $V(I^{(p)})$ 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**,
- simple generalisations of basic results from the **theory of standard bases**,
- computer algebra computations, using **SINGULAR**.

We concentrate on steps of the proof which require computer algebra.

The ideal I is given by the four polynomials in $\mathbb{Z}[b,c,t]$:

$$-b^4c^4t^4 - b^4c^3t^5 + 2b^3c^4t^5 + 2b^3c^3t^6 - b^2c^4t^6 - b^2c^3t^7 - b^4c^3t^3 - 2b^4c^2t^4 - 2b^3c^3t^4 - 2b^2c^4t^4 + b^3c^2t^5 + 3b^2c^3t^5 + 2bc^4t^5 + 2b^2c^2t^6 - bc^2t^7 - b^3c^3t^2 + b^2c^4t^2 - b^4ct^3 - 4b^3c^2t^3 + b^2c^3t^3 - bc^4t^3 - 2b^3ct^4 - b^2c^2t^4 - 4bc^3t^4 - c^4t^4 + 2b^2ct^5 + 2bc^2t^5 + c^3t^5 - b^3ct^2 - 4b^2c^2t^2 + bc^3t^2 + c^4t^2 - b^3t^3 - 4b^2ct^3 + 3bc^2t^3 + 3bct^4 - c^2t^4 - ct^5 - b^2ct - bc^2t - 2b^2t^2 - 6bct^2 - c^2t^2 + bt^3 + 4ct^3 - bct + ct^2 - 2bt - 2ct - b - 1$$

$$b^4c^3t^4 + b^4c^2t^5 - 2b^3c^3t^5 - 2b^3c^2t^6 + b^2c^3t^6 + b^2c^2t^7 + b^4c^2t^3 + 2b^4ct^4 + b^3c^2t^4 + 2b^2c^3t^4 - 2b^3ct^5 - b^2c^2t^5 - 2bc^3t^5 - bc^2t^6 + b^3c^2t^2 - b^2c^3t^2 + b^4t^3 + 3b^3ct^3 - 2b^2c^2t^3 + bc^3t^3 - b^2ct^4 + 4bc^2t^4 + c^3t^4 + bct^5 + b^3t^2 + 2b^2ct^2 - c^3t^2 - b^2t^3 - 2bct^3 - 2c^2t^3 - ct^4 + b^2t + c^2t + bt^2 + 3ct^2 - bc + ct - 1$$

$$b^4c^4t^5 + b^4c^3t^6 - 2b^3c^4t^6 - 2b^3c^3t^7 + b^2c^4t^7 + b^2c^3t^8 - b^4c^4t^3 + 2b^3c^4t^4 + 2b^4c^2t^5 + 4b^3c^3t^5 + b^2c^4t^5 - b^3c^2t^6 - 4b^2c^3t^6 - 2bc^4t^6 - 2b^2c^2t^7 + bc^2t^8 - b^4c^3t^2 + b^3c^4t^2 - 2b^4c^2t^3 - 4b^2c^4t^3 + b^4ct^4 + 5b^3c^2t^4 + b^2c^3t^4 + 3bc^4t^4 + 2b^3ct^5 + 3b^2c^2t^5 + 4bc^3t^5 + c^4t^5 - 2b^2ct^6 - 3bc^2t^6 - c^3t^6 - b^4ct^2 - 2b^3c^2t^2 + 2b^2c^3t^2 + bc^4t^2 - b^3ct^3 + 3b^2c^2t^3 - 5bc^3t^3 - 2c^4t^3 + b^3t^4 + 6b^2ct^4 - 2bc^2t^4 + c^3t^4 - 3bct^5 + c^2t^5 + ct^6 - 2b^2c^2t - b^3t^2 - b^2ct^2 + 5bc^2t^2 + c^3t^2 + 2b^2t^3 + 8bct^3 - bt^4 - 5ct^4 + bct^2 - ct^3 - b^2t - 4bct - c^2t + 3bt^2 + 5ct^2 + bt + ct + 1$$

$$-b^4c^3t^5 - b^4c^2t^6 + 2b^3c^3t^6 + 2b^3c^2t^7 - b^2c^3t^7 - b^2c^2t^8 + b^4c^3t^3 - 2b^3c^3t^4 - 2b^4ct^5 - 3b^3c^2t^5 - b^2c^3t^5 + 2b^3ct^6 + 2b^2c^2t^6 + 2bc^3t^6 + bc^2t^7 + b^4c^2t^2 - b^3c^3t^2 + 2b^4ct^3 - b^3c^2t^3 + 4b^2c^3t^3 - b^4t^4 - 5b^3ct^4 + 2b^2c^2t^4 - 3bc^3t^4 + b^2ct^5 - 5bc^2t^5 - c^3t^5 - bct^6 + b^4t^2 + b^3ct^2 - 2b^2c^2t^2 - bc^3t^2 - b^3t^3 - 2b^2ct^3 + 3bc^2t^3 + 2c^3t^3 + b^2t^4 + 3bct^4 + 2c^2t^4 + ct^5 + b^2ct + bc^2t - 2b^2t^2 - 2bct^2 - 3c^2t^2 - bt^3 - 4ct^3 + bct - ct^2 + 2bt + 2ct + c + t - 1$$

To prove the $V(I^{(p)}) \subset \mathbb{F}_p^3$ is non–empty for **all** $p \geq 5$ we perform **two main steps**:

Step 1: We use the theorem of Hasse–Weil to find an explicit bound $p(= 593)$ so that $V(I^{(p)}) \neq \emptyset$ for all primes $> p$. Check for each prime $p \leq 5 \leq 593$ directly with a computer that $V(I^{(p)}) \neq \emptyset$.

Step 2: We prove (using **SINGULAR**) that the assumptions of the Hasse–Weil theorem are satisfied.

Step 1

Theorem of Hasse–Weil (generalised by Aubry and Perret to singular curves):

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 $\Rightarrow$

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

(d = degree, p_a = arithmetic genus of $\overline{C}$).

The Hilbert polynomial of $\overline{C}$, $H(t) = d \cdot t - p_a + 1$, can be computed from the homogeneous ideal I_h of $\overline{C}$:
We compute $H(t) = 10t - 11 \Rightarrow d = 10$, $p_a = 12$.

Since $p + 1 - 24\sqrt{p} - 10 > 0$ if $p > 593$, step 1 follows from a direct check.

Note: To compute I_h we have to compute a degree standard basis **without division** and then homogenise.

Step 2

Proposition: $V(I^{(p)})$ is absolutely irreducible for all primes $p \geq 5$.

Proof:

- Use the `lift` command of **SINGULAR** to show: $I \subset K$, K generated by the following two polynomials in $\mathbb{Z}[b,c,t]$:
  $bct - t^2 + 2t + 1$
  $bt^3 - ct^3 - t^4 + b^2t + c^2t - 2bt^2 + 2ct^2 + 3t^3 - bc - 2t^2 + t$

  `lift(K,I);` returns a 2×4–matrix M with entries in $\mathbb{Z}[b,c,t]$, so that $\text{matrix}(K) * M = I$.

- Compute a lexicographical standard basis of K in the ring $\mathbb{Q}(t)[b,c]$ (without division). It is contained in $\mathbb{Z}[b,c,t]$ and called J:
  $t^2b^4 + (t^4 - 2t^3 - 2t^2)b^3 - (t^5 - 2t^4 - t^2 - 2t - 1)b^2 - (t^5 - 4t^4 + t^3 + 6t^2 + 2t)b + (t^4 - 4t^3 + 2t^2 + 4t + 1)$
  $(t^3 - 2t^2 - t)c + t^2b^3 + (t^4 - 2t^3 - 2t^2)b^2 - (t^5 - 2t^4 - t^2 - 2t - 1)b - (t^5 - 4t^4 + t^3 + 6t^2 + 2t)$

  Since $J[2]$ is linear in c, J is absolutely irreducible if $J[1] \in \mathbb{Z}[b,t]$ is absolutely irreducible. (Geometrically: $V(J[2])$ is the projection of $V(I)$ onto the (b,t)–plane and this projection is birational.)

Make $J[1] \in \mathbb{Z}(t)[b]$ monic by setting
$P(x) := t^2 J[1]|_{b=x/t}$.
We obtain a polynomial of degree 4 in x:

$$x^4 + (t^3 - 2t^2 - 2t)x^3 - (t^5 - 2t^4 - t^2 - 2t - 1)x^2 - (t^6 - 4t^5 + t^4 + 6t^3 + 2t^2)x + (t^6 - 4t^5 + 2t^4 + 4t^3 + t^2).$$

We show that the image $P \in \mathbb{F}_p[t, x]$ is absolutely irreducible for all primes $p \geq 2$.
(This is equivalent to P being irreducible in $\overline{\mathbb{F}}_p(t)[x]$ by the lemma of Gauß.)

- To show that P is not divisible by any factor of degree 1 in x, we make an **Ansatz**:

$$P = (x^3 + ax^2 + bx + c)(x + d).$$

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

(*) $$P = (x^2 + ax + b)\,(x^2 + gx + d),$$

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

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

Hence $V(I^{(p)})$ is absolutely irreducible for all primes $\neq 2$.

The Suzuki groups Sz(q)

Let $n = 2m+1$, $q = 2^n$ and consider the automorphism

$$\pi : \mathbb{F}_q \longrightarrow \mathbb{F}_q, \qquad \pi(a) = a^{2^{m+1}}.$$

Note that $\pi^2(a) = a^2$, i.e. π^2 is the Frobenius.

$$\mathrm{Sz}(q) = \left\langle U(a,b), M(c), T \mid a,b,c \in \mathbb{F}_q, c \neq 0 \right\rangle$$

$$U(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ a\pi(a)+b & \pi(a) & 1 & 0 \\ a^2\pi(a)+ab+\pi(b) & b & a & 1 \end{pmatrix}$$

$$M(c) = \begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Recall that

$$U_1(x,y) = U_2(x,y)$$

if and only if

$$x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}.$$

Fix two matrices

$$x = TU(a,b), y = TU(c,d) \in \ \mathrm{Sz}(q).$$

The equations of the variety $V(n)$ for $U_1 = U_2$ will depend on n $(q = 2^n)$.

Goal: Show that the variety $V(n) \subset \mathbb{F}_q^4$ is not $\{0\}$.

Problem: We cannot treat infinitely many systems of equations.

To make the equations independent of n we replace the expressions $\pi(a), \pi(b), \pi(c), \pi(d)$ by indeterminates a_0, b_0, c_0, d_0.

$$S(a,b,a_0,b_0) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ aa_0+b & a_0 & 1 & 0 \\ a^2a_0+ab+b_0 & b & a & 1 \end{pmatrix}$$

then

$$U(a,b) = S\big(a,b,\pi(a),\pi(b)\big).$$

Consider the matrices

$$x = TS(a,b,a_0,b_0)$$
$$y = TS(c,d,c_0,d_0)$$

then the matrix equation

$$U_1(x,y) = U_2(x,y)$$

leads to a system of equations defining a variety $V = V(I) \subset \mathbb{F}_2^8$, not depending on n (I: 16 polynomials in 8 variables).

The ideal of an irreducible component $V(J)$ of V:

```
J[1]=d2+adv+cdv+a2v2+c2v2+abx+bcx+wx+c2x2+vy+xy+c2;
J[2]=a2b+acd+a2cv+aw+a3x+a2cx+ac2x+ay+av+cx;
J[3]=bcw+acvw+w2+a2wx+acwx+b2+bd+d2+abv+bcv+c2v2+bcx+adx+a4+a3c
     +vx+x2+ac+1;
J[4]=adv2+cdv2+d2x+abvx+bcvx+advx+cdvx+vwx+abx2+bcx2+wx2+c2x3+v2y
     +vxy+x2y+ab+cd+acv+c2v+w+a2x+acx+c2x+y;
J[5]=abd+abcv+bc2v+a2dv+dw+avw+cvw+bc2x+c2dx+ac2vx+awx+a2cx2+ac2x2
     +c3x2+by+cxy+dv+av2+cv2+bx+cx2+ac2+a+c;
J[6]=bcd+cd2+a2bv+abcv+a2dv+c2dv+bw+avw+cvw+a2dx+c2dx+c3vx+a3x2
     +a2cx2+ac2x2+by+dy+cvy+axy+bv+dv+cv2+dx+cvx+ax2+a3+a+c;
J[7]=a3v2+a2cv2+c2dx+a3vx+ac2vx+a2cx2+ac2x2+c3x2+cxy+cx2;
J[8]=d2v+acv3+c2v3+cdvx+a2vx2+acvx2+a2bc+ac2d+ac3v+acw+a3cx+vx2
     +acy+a2v+acx+v;
J[9]=advx+cdvx+a2v2x+c2v2x+abx2+bcx2+a2vx2+c2vx2+wx2+vxy+c3d+a3cv
     +a2c2v+a3cx+a2c2x+c4x+c2y+cd+a2v+c2v+c2x+y;
J[10]=a2vw+acvw+c2vw+w2+ac2dx+c3dx+a3cvx+ac3vx+acwx+c2wx+a3cx2+c4x2
      +aby+acxy+c2xy+a2v2+acv2+abx+adx+cdx+a2vx+acvx+c2vx+a2x2+c2x2
      +a4+a2c2+v2+1;
```

As in the PSL(2)–case, we show that this component is absolutely irreducible.

Problem: V is a surface, not a curve.

Proof: $\dim(std(I)) = 2$ (using SINGULAR)

On $V \subset \mathbb{F}_2^8$ consider the endomorphism

$$\theta : V \longrightarrow V$$
$$\theta(a,b,c,d,a_0,b_0,c_0,d_0) = (a_0,b_0,c_0,d_0,a^2,b^2,c^2,d^2).$$

Then θ^2 is the Frobenius.

Using Gröbner bases and SINGULAR, we show that $\theta(V) = V$.

The following holds obviously for $p = (a,b,c,d) \in \overline{\mathbb{F}}_2^4$:

$p \in V(n) \subset \mathbb{F}_q^4$

$\Updownarrow$

(1) $(a,b,c,d,a^{2^{m+1}},b^{2^{m+1}},c^{2^{m+1}},d^{2^{m+1}}) \in V \times_{\mathbb{F}_2} \bar{\mathbb{F}}_2$

(2) $a^q = a, \ldots, d^q = d$

We use these conditions describing $V(n)$ to define $V(n)$ as the fixed point set of the nth power of θ.

Note: these conditions hold for the word w_1, but not for the other words.

Let $(a, b, c, d, a_0, b_0, c_0, d_0) \in V \subset \overline{\mathbb{F}}_2^8$. Then

$$\begin{aligned} & \theta^n(a, \ldots, d_0) = (a, \ldots, d_0) \\ \Rightarrow \quad & \begin{cases} a_0 = a^{2^{m+1}}, \ldots, d_0 = d^{2^{m+1}} \\ a = a^q, \ldots, d^q = d. \end{cases} \\ \Rightarrow \quad & (a, b, c, d) \in V(n) \end{aligned}$$

(recall: $n = 2m + 1, q = 2^m$)

Hence:

If $(a, b, c, d, a_0, b_0, c_0, d_0) \in V$ is fixed point of θ^n, then $(a, b, c, d) \in V(n)$.

Problem:

Prove that for every odd n, that θ^n has a non–zero fixed point on V.

The existence of rational fixed points of the (power of the) Frobenius follows from generalisations of the Hasse–Weil formula to higher dimensions using a Lefschetz trace formula.

To show that θ^n has fixed points, we use the **Lefschetz(–Weil–Grothendieck–Verdier) trace formula** as generalised by Deligne–Lusztig, T. Zink, Pink, Katz and Adolphson–Sperber:

We find an open, smooth and θ–invariant and absolutely irreducible subset U of V for which the trace formula gives

Theorem: For any odd $n > 1$

$$| \# \text{ Fix } (\theta^n, U) - 2^n | \leq b_1(U) \cdot 2^{\frac{3}{4}n} + b_2(U) \cdot 2^{\frac{1}{2}n},$$

$b_i(U) = \dim H^i_{\acute{e}t}(U, \bar{Q}_l)$ l–adic Betti number.

A quite involved computation gives the following estimates for the Betti numbers b_1 and b_2:

$$b_1(U) \leq 2^{10}, \quad b_2(U) \leq 2^{22}.$$

To guarantee a fixed point we need

$$2^n > 2^{10} \cdot 2^{\frac{3}{4}n} + 2^{22} \cdot 2^{\frac{n}{2}}$$

which holds for $n \geq 48$.

Steps of the proof

- $I \subset \mathbb{Z}[a,b,c,d,v,w,x,y]$ ideal of coefficients of $U_1 - U_2$ (is reducible)
- $J = I : a^3x^2$ defines a component $V(J)$ of $V(I)$ (several hours computation)
- $\dim(\mathrm{std}(J)) = 2$, i.e. $V(J)$ is a surface

Show that $\mathbf{V(J)}$ is irreducible in $\bar{\mathbb{F}}^{\mathbf{8}}$

- Show that std $(J) \cap \mathbb{F}_2(a,c)[b] =< h >$ (several hours of computation)
- $V(J)$ irreducible $\Leftrightarrow$ $h \in \bar{\mathbb{F}}_2(a,c)[b]$ irreducible (theoretical)
- To show that h is absolutely irreducible we
  - analyse the coefficients of h in $\mathbb{F}_2[a.c]$ ($\deg h = 12$)
  - show $\widetilde{h}(b,c) = h(1,b,c)$ irreducible $\Rightarrow$ h irreducible
  - reduce this by some coordinate change to a polynomial g of degree 6
  - analyse (by hand) that g has no linear, quadratic, cubic factor

Find a nonsingular invariant open set $U \subset V(J)$

- Show that Sing $(V(J)) \subset V(xc)$ by computer
  $U := V(J) - V(xc)$

Trace Formula

- Translate general theorems of Deligne, Lusztig, Zink, Pink, Katz ... to show for $n > 1$ odd

$$\#\mathrm{Fix}(\theta^n, U) = \sum_{i=0}^{4} (-1)^i \mathrm{tr}(\theta^n | H_c^i(U, \bar{\mathbb{Q}}_l))$$

- By general results of Deligne and Katz
  $b_c^i = b_{4-i}$
  (Poincaré duality between compact and ordinary Betti numbers)
  $b_i = 0, i > 2$
  (Katz, since U is affine)
  $b_0 = 1$
  (since U is absolutely irreducible)
  $\mathrm{tr}\ (\theta^n | H_c^4(U, \bar{\mathbb{Q}}_l)) = 2^n$ (directly)
  $|\ \mathrm{tr}\ (\theta^n | H_c^3(U, \bar{\mathbb{Q}}_l)\ | \leq b_1 2^{3n/4}$
  $|\ \mathrm{tr}\ (\theta^n | H_c^2(U, \bar{\mathbb{Q}}_l)\ | \leq b_2 2^{n/2}$

Last inequalities follow from Deligne, Weil II, as estimates for eigenvalues of Frobenius.

Estimates of l–adic Betti numbers

Analysis of $V(J)$ by looking at equations, and use

- Hyperplane sections
- Stratification of from $U = W \setminus L$, (Mayer–Vietoris)
- Projection
- Use weak Lefschetz theorem on hyperplane sections (Katz)
- compute $b_1(U) \leq 675, (< 2^{10})$
- Estimate of Euler characteristics $\chi(U)$ by a polynomial in the degrees of the defining equations (Adolphson–Sperber, Katz)
- Poincaré duality, $\chi(U)$ and $b_1(U)$ give $b_2(U) \leq 2^{22}$

All this is obtained by a mixture of computer computation (e.g. primary decomposition of sections) and hand–analysis of the equations.