Compositio Math. 142 (2006) 734–764
doi:10.1112/S0010437X0500179X

Identities for finite solvable groups and equations in finite simple groups

Tatiana Bandman, Gert-Martin Greuel, Fritz Grunewald, Boris Kunyavskiĭ, Gerhard Pfister and Eugene Plotkin

To B. I. Plotkin on the occasion of his 80th birthday

Abstract

We characterise the class of finite solvable groups by two-variable identities in a way similar to the characterisation of finite nilpotent groups by Engel identities. Let $u_1 = x^{-2}y^{-1}x$, and $u_{n+1} = [xu_nx^{-1}, yu_ny^{-1}]$. The main result states that a finite group G is solvable if and only if for some n the identity $u_n(x, y) \equiv 1$ holds in G. We also develop a new method to study equations in the Suzuki groups. We believe that, in addition to the main result, the method of proof is of independent interest: it involves surprisingly diverse and deep methods from algebraic and arithmetic geometry, topology, group theory, and computer algebra (Singular and MAGMA).

Contents

Received 17 November 2004, accepted in final form 21 June 2005.
2000 Mathematics Subject Classification 20F16, 20F45, 20E18, 20D10, 13P10, 14G15, 14G10, 14-04.
Keywords: finite solvable group, identity, simple group, Gröbner basis, trace formula, Lang–Weil estimate.

Bandman, Kunyavskiĭ, and Plotkin were partially supported by the Ministry of Absorption (Israel), the Israeli Science Foundation founded by the Israeli Academy of Sciences – Center of Excellence Program, and the Minerva Foundation through the Emmy Noether Research Institute of Mathematics. Kunyavskiĭ and Plotkin were also supported by the RTN network HPRN-CT-2002-00287 and INTAS 00-566. Greuel and Pfister were partially supported by the DFG project 'Globale Methoden in der komplexen Geometrie' as well as by the Stiftung Rheinland–Pfalz für Innovation. Greuel was also supported by the German–Israeli Foundation for Scientific Research and Development, G-616-15.6/1999. Bandman and Kunyavskiĭ thank the Max-Planck-Institut für Mathematik (Bonn) which they visited when preparing this paper for publication.

1. Introduction

1.1 Statement of the problem and main results

In this paper we characterise solvable groups in the class of finite groups by identities in two variables. The starting point for this research is the following classical fact: the class of finite nilpotent groups is characterised by Engel identities. To be more precise, Zorn's theorem [Zor36] (see also [Hup79, Satz III.6.3]) says that a finite group G is nilpotent if and only if it satisfies one of the identities $e_n(x,y) = [y,x,x,\dots,x] = 1$ (here $[y,x] = yxy^{-1}x^{-1}$, $[y,x,x] = [[y,x],x]$, etc.).

Our goal is to obtain a similar characterisation of solvable groups in the class of finite groups. We say that a sequence of words $u_1,\dots,u_n,\dots$ is correct if $u_k \equiv 1$ in a group G implies that $u_m \equiv 1$ in a group G for all $m > k$. We have found an explicit correct sequence of words $u_1(x,y),\dots,u_n(x,y),\dots$ such that a group G is solvable if and only if for some n the word u_n is an identity in G.

B. Plotkin suggested some Engel-like identities that could characterise finite solvable groups (see [PPT99, GKNP00]). In the present paper we establish B. Plotkin's conjecture (in a slightly modified form).

Define

$$u_1(x,y) := x^{-2}y^{-1}x, \quad \text{and inductively} \quad u_{n+1}(x,y) := [xu_n(x,y)x^{-1}, yu_n(x,y)y^{-1}]. \tag{1.1}$$

Note that sequence (1.1) is correct.

Our main result is the following.

THEOREM 1.1. *A finite group G is solvable if and only if for some n the identity $u_n(x,y) \equiv 1$ holds in G.*

Theorem 1.1 provides an effectively presented, recursively defined, Engel-like identity $u_n(x,y) \equiv 1$ characterising solvable groups. The effective form of $u_n(x,y)$ is a crucial fact; it gives a way to find a counterpart of Engel-like notions in the theory of solvable groups and Lie algebras. As a result, the theorem:

- gives rise to a vast spectrum of Burnside-type problems for solvable groups and Lie algebras as Zorn's theorem does for nilpotent groups;
- yields an explicit profinite identity defining the class of prosolvable groups;
- leads to a conjectural description of the solvable radical of a finite group (cf. Baer's theorem for the nilpotent radical of a finite group [Bae57]).

Note two obvious properties of the initial word $w = x^{-2}y^{-1}x$: (1) if a group G satisfies the identity $w \equiv 1$, then $G = \{1\}$; (2) the words w and x generate the free group $F = \langle x,y\rangle$. Thus, w can also be used as the initial term of a sequence characterising finite nilpotent groups, see Proposition A.1. We shall discuss the choice of the initial word below. We conjecture after long computer experiments that Theorem 1.1 holds for any sequence formed as in (1.1) from any initial word not of the form $w = (x^{-1}y)^k$ ($k \in \mathbb{N}$).

Historical remarks. Our results can be viewed as a natural development of the classical Thompson–Flavell theorem [Tho68, Fl95], stating that if G is a finite group in which every two elements generate a solvable subgroup, then G is solvable. Of course, Theorem 1.1 immediately implies this theorem (see Corollary A.16 for an analogous statement in the pro-finite setting). As mentioned in [BW88], the Thompson–Flavell theorem, together with [Bra81, Satz 2.12], implies that finite solvable groups can be characterised by a countable set of two-variable identities. (This fact also follows from [Neu67, Lemma 16.1 and Theorem 16.21] saying that an n-generator group G belongs to a variety V if and only if all n-variable identities from V are fulfilled in G.) However, this does not

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

provide explicit two-variable identities for finite solvable groups. Furthermore, in [BW88], Brandl and Wilson constructed a countable set of words $w_n(x,y)$ with the property that a finite group G is solvable if and only if for almost all n the identity $w_n(x,y) \equiv 1$ holds in G. As in their construction there is no easily described relationship between terms of $w_n(x,y)$, the question whether one can characterise finite solvable groups by sequences of identities fitting into a simple recursive definition remained open.

Recently, Lubotzky proved that for any integer $d \geqslant 2$ the free pro-solvable group $\hat{F}_d(S)$ can be defined by a *single* pro-finite relation [Lub01, Proposition 3.4]. Using this proposition and Thompson's theorem, one can derive the existence of a needed sequence of identities characterising finite solvable groups (Lubotzky's result does not give, however, any candidate for such a sequence).[1]

One can mention here some more cases where certain interesting classes of finite groups were characterised by two-variable commutator identities [Bra81, BP91, BN86, Gup66, GH67, Nik83, Nik85]; see [GKNP00] or the above cited papers for more details.

Although Theorem 1.1 is a purely group-theoretic result, its proof involves surprisingly diverse methods of algebraic geometry, arithmetic geometry, group theory, and computer algebra (note, however, a paper of Bombieri [Bom80] that served for us as an inspiring example of such an approach). We want to emphasise a special role played by problem-oriented software (in particular, the packages Singular and MAGMA): not only proofs but even the precise statements of our results would hardly have been found without extensive computer experiments.

We believe that some of the above techniques yield outcomes which are of interest in their own right. For example, the geometry of solutions of certain equations in Suzuki groups leads to a new presentation for Sz(8), see § 1.4 below; results on fixed points of fractional powers of Frobenius acting on an open variety may have more applications, etc.

The results of this paper were announced in the note [BGGKPP03].

Clearly, in every solvable group the identities $u_n(x,y) \equiv 1$ are satisfied from a certain $n \in \mathbb{N}$ onward. We shall deduce the non-trivial 'if' part of the theorem from the following.

Theorem 1.2. *Let G be one of the following groups:*

(1) $G = \mathrm{PSL}(2, \mathbb{F}_q)$ *where* $q \geqslant 4$ *($q = p^n$, p a prime);*

(2) $G = \mathrm{Sz}(2^n)$, $n \in \mathbb{N}, n \geqslant 3$ *and odd;*

(3) $G = \mathrm{PSL}(3, \mathbb{F}_3)$.

Then there are $x, y \in G$ such that $u_1(x,y) \neq 1$ and $u_1(x,y) = u_2(x,y)$.

Here $\mathrm{PSL}(n, \mathbb{F}_q)$ denotes the projective special linear group of degree n over $\mathbb{F}_q$. For $q = 2^m$ we denote by $\mathrm{Sz}(q)$ the Suzuki group (the twisted form of ${}^2B_2$, see [HB82, XI.3]).

Let us show that Theorem 1.2 implies Theorem 1.1.

Assume that Theorem 1.2 holds, and suppose that there exists a non-solvable finite group in which the identity $u_n \equiv 1$ holds. Denote by G a minimal counterexample, that is, a finite non-solvable group of the smallest order with identity $u_n \equiv 1$. Such a G must be simple. Indeed, if H is a proper normal subgroup of G, then both H and G/H are solvable (because any identity remains true in the subgroups and the quotients). However, the list of groups in Theorem 1.2 contains

[1] After this paper was finished J. N. Bray *et al.* proved that the sequence $\{s_n\}$ defined by the rule $s_1 = x$, $s_{n+1} = [s_n^{-y}, s_n]$ also characterizes the class of finite solvable groups [BWW05]. Their method is also based on reducing to Thompson's list of minimal non-solvable groups, but instead of solving the equation $s_1 = s_2$ in each group G from that list, as in our Theorem 1.2, they prove that for each such G there is $y \in G$ such that the map $\varphi_y \colon G \to G$ defined by $\varphi_y(x) = [x^{-y}, x]$ has a non-trivial periodic point.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Thompson's list of finite simple groups all of whose subgroups are solvable [Tho68], hence G is one of the groups (1)–(3). As sequence (1.1) is correct, the assumption $u_1(x,y) = u_2(x,y)$ implies that $u_2(x,y) = u_3(x,y) = \cdots$. From $u_1 \neq 1$ it follows that the identity $u_n \equiv 1$ does not hold in G, a contradiction.

Theorem 1.2 admits a generalisation which can easily be deduced from the classification of finite simple groups.

COROLLARY 1.3. *Let G be a finite non-abelian simple group. Then there are $x, y \in G$ such that $u_1(x,y) \neq 1$ and $u_1(x,y) = u_2(x,y)$.*

For small groups from the above list it is an easy computer exercise to verify Theorem 1.2. Altogether, for example, there are 44 928 suitable pairs x, y in the group $\mathrm{PSL}(3, \mathbb{F}_3)$; here is one of them:

$$x = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

The general idea of our proof can roughly be described as follows. For a group G in the list of Theorem 1.2, using its standard matrix representation over $\mathbb{F}_q$, we regard the entries of the matrices corresponding to x and y in this representation as variables, and thus interpret solutions of the equation $u_1(x,y) = u_2(x,y)$ as $\mathbb{F}_q$-rational points of an algebraic variety. Lang–Weil type estimates [LW54] for the number of rational points on a variety defined over a finite field guarantee in appropriate circumstances the existence of such points for big q. Small values of q are checked case by case. Of course, we are faced here with the extra difficulty of having to ensure that $u_1(x,y) \neq 1$ holds. This is achieved by taking the x, y from appropriate Zariski-closed subsets only. In the next two sections we discuss more details.

1.2 The case $G = \mathrm{PSL}(2, \mathbb{F}_q)$

Here we explain a more general setup which will also shed some light on the somewhat peculiar choice of the word u_1 in (1.1).

Let w be a word in x, x^{-1}, y, y^{-1}. Let G be a group and $x, y \in G$. Define

$$u_1^w(x,y) := w, \quad \text{and inductively} \quad u_{n+1}^w(x,y) := [x u_n^w(x,y) x^{-1}, y u_n^w(x,y) y^{-1}].$$

Let $R := \mathbb{Z}[t, z_1, z_2, z_3, z_4]$ be the polynomial ring over $\mathbb{Z}$ in five variables. Consider further the two following 2×2 matrices over R.

$$x(t) = \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix}, \quad y(z_1, \ldots, z_4) = \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}.$$

Let $\mathfrak{a}$ be the ideal of R generated by the determinant of y and by the four polynomials arising from the matrix equation $u_1^w(x,y) = u_2^w(x,y)$, and let $\mathcal{V}^w \subset \mathbb{A}^5$ be the corresponding closed set of five-dimensional affine space. Further, let $\mathfrak{a}_0$ be the ideal of R generated by the determinant of y and by the matrix entries arising from the equation $u_1^w(x,y) = 1$, and let $\mathcal{V}_0^w \subset \mathbb{A}^5$ be the corresponding closed set. Our approach aims at showing that $\mathcal{V}^w \setminus \mathcal{V}_0^w$ has points over finite fields. We have therefore searched for words w satisfying $\dim(\mathcal{V}^w) - \dim(\mathcal{V}_0^w) \geqslant 1$ and also $\dim(\mathcal{V}^w) \geqslant 1$. We have only found the following words with this property:

$$x^{-2}y^{-1}x, \quad y^{-1}xy, \quad yx^{-1}y^{-1}, \quad yxy^{-1}, \quad x^{-1}yxy^{-1}x, \quad x^{-1}yx^{-1}y^{-1}x. \tag{1.2}$$

The extra freedom one might get by introducing variables for the entries of x does not lead to more suitable results. Indeed, elements of $\mathrm{GL}(2)$ act on the corresponding varieties by conjugation, and every matrix of determinant 1 except ± 1 is conjugate (over any field) to a matrix with entries as in $x(t)$.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

For the last five words in (1.2), the corresponding closed sets $\mathcal{V}^w$ have no absolutely irreducible components outside $\mathcal{V}_0^w$ and, in fact, the analogue of Theorem 1.2 does not hold for them. For the first word $w = x^{-2}y^{-1}x$ the closed set $\mathcal{V}^w$ has two irreducible components. One of them is $\mathcal{V}_0^w$, the second, which we call $\mathcal{S}$, has dimension 2 and is absolutely irreducible. The map $\varphi\colon \mathcal{S} \to \mathbb{A}^1\setminus\{0\}$, $\varphi(x,y) = z_1$, is a fibration with curves of genus 8 as fibres. We now consider the fibre $\varphi^{-1}(1)$ and thus arrive at the matrices of the form

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

Note that the obtained curve does not intersect $\mathcal{V}_0^w$ (indeed, $\mathcal{V}_0^w$ is given by the equation $w = 1$, which implies that $y(b,c) = x(t)^{-1}$, and this is impossible with the above choice of $x(t)$ and $y(b,c)$).

To give the precise form of this curve which is used in computations, we write the equation $u_1(x,y) = u_2(x,y)$ in an equivalent form

$$x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}. \tag{1.3}$$

On substituting $x(t)$ instead of x and $y(b,c)$ instead of y, we obtain a matrix equation giving rise to the following.

Definition 1.4. We denote by $I \subset \mathbb{Z}[b,c,t]$ the ideal generated by the four polynomials arising after equating the matrix entries in (1.3), and let C be the corresponding algebraic set.

The following theorem will be proved in § 2:

Theorem 1.5. *For any prime p the reduction of C modulo p is an absolutely irreducible curve.*

We now use the classical Hasse–Weil bound (in a slightly modified form adapted for singular curves, cf. [FJ86, Theorem 3.14], [AP96] and [LY94]).

Lemma 1.6. *Let D be an absolutely irreducible projective algebraic curve defined over a finite field $\mathbb{F}_q$, and let $N_q = \#D(\mathbb{F}_q)$ denote the number of its rational points. Then $|N_q-(q+1)| \leqslant 2p_{\mathrm{a}}\sqrt{q}$, where p_{a} stands for the arithmetic genus of D (in particular, if D is a plane curve of degree d, $p_{\mathrm{a}} = (d-1)(d-2)/2$).*

In fact, we need an affine version of the lower estimate of Lemma 1.6 (cf. [FJ86, Theorem 4.9 and Corollary 4.10]) based on the fact that an affine curve C has at most $\deg(\overline{C})$ rational points less than the projective closure $\overline{C}$.

Corollary 1.7. *Let $C \subset \mathbb{A}^n$ 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 $q+1-2p_{\mathrm{a}}\sqrt{q}-d$ where d is the degree and p_{a} the arithmetic genus of $\overline{C}$.*

To apply Lemma 1.6 (or Corollary 1.7) we have to compute the arithmetic genus of the curve C (or the degree of some plane projection of C) and to prove that the curve is absolutely irreducible (which is the most technically difficult part of the proof, see § 2 for more details). Computations give $d = 10$ and $p_{\mathrm{a}} = 12$. This implies that for $q > 593$ there exist enough $\mathbb{F}_q$-rational points on C to prove Theorem 1.2 in the case of the groups PSL(2).

Remark 1.8. Consider the initial word $w = [x,y]$. The ideal $\mathfrak{a}$ corresponding to the variety $\mathcal{V}^w$ contains the polynomial $(-tz+v-w)(v+w)$. Let $\mathcal{V}_1^w$ be the closed set defined by the ideal generated by $\mathfrak{a}$ and $v+w$. This variety has five components: one is two-dimensional and equals $\mathcal{V}_0^w$, and four others are of dimension 0; each of them decomposes into four absolutely irreducibles components over a splitting field of the polynomial $5z^4+20z^3+36z^2+32z+16$. Let $\mathcal{V}_2^w$ be the closed set defined by the

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

ideal generated by $\mathfrak{a}$ and $-tz+v-w$. This variety also has five components, all of dimension 1; one of them is contained in $\mathcal{V}_0^w$ and each other decomposes into three absolutely irreducibles components over the splitting field of the polynomial t^2+t-1. As none of the components, except for that corresponding to trivial solutions of $u_1 = u_2$, is absolutely irreducible, our method fails for the initial word $w = [x, y]$. In fact, the analogue of Theorem 1.2 does not hold for this word.

1.3 The case $G = \mathrm{Sz}(q)$

To prove Theorem 1.2, the Suzuki groups $G = \mathrm{Sz}(q)$ ($q = 2^n, n$ odd) provide the most difficult case. This is due to the fact that although $\mathrm{Sz}(q)$ is contained in $\mathrm{GL}(4, \mathbb{F}_q)$, it is not a Zariski-closed set. In fact the group $\mathrm{Sz}(q)$ is defined with the help of a field automorphism of $\mathbb{F}_q$ (the square root of the Frobenius), and hence the standard matrix representation for $\mathrm{Sz}(q)$ contains entries depending on q. We shall describe now how our problem can still be treated by methods of algebraic geometry.

Let $R := \mathbb{F}_2[a, b, c, d, a_0, b_0, c_0, d_0]$ be the polynomial ring over $\mathbb{F}_2$ in eight variables. Let $\pi\colon R \to R$ be its endomorphism defined by $\pi(a) = a_0, \pi(a_0) := a^2, \ldots, \pi(d) := d_0, \pi(d_0) := d^2$. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_2$ and consider $a, \ldots, d_0$ as the coordinates of eight-dimensional affine space $\mathbb{A}^8$ over $\mathbb{F}$. The endomorphism π defines an algebraic bijection $\alpha : \mathbb{A}^8 \to \mathbb{A}^8$. The square of α is the Frobenius automorphism on $\mathbb{A}^8$ (note that a similar operator appears in [DL76, § 11]). Let $p \in \mathbb{A}^8$ be a fixed point of α^n, then its coordinates are in $\mathbb{F}_{2^n}$ if n is odd and in $\mathbb{F}_{2^{n/2}}$ if n is even.

Consider further the two following matrices in $\mathrm{GL}(4, R)$:

$$x = \begin{pmatrix} a^2a_0 + ab + b_0 & b & a & 1 \\ aa_0 + b & a_0 & 1 & 0 \\ a & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} c^2c_0 + cd + d_0 & d & c & 1 \\ cc_0 + d & c_0 & 1 & 0 \\ c & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{1.4}$$

The matrices x, y also define maps from $\mathbb{A}^8$ to $\mathrm{GL}(4, \mathbb{F})$. It can easily be checked that the matrices corresponding to a fixed point of α^n (n odd and $n \geqslant 3$) lie in $\mathrm{Sz}(2^n)$.

DEFINITION 1.9. Let $\mathfrak{a}$ be the ideal of R generated by the 16 polynomials arising from the matrix equation (1.3), where x and y are taken from (1.4), let $\mathfrak{a}' = \mathfrak{a} : a^3c_0^2$, and let V (respectively V') denote the closed set in $\mathbb{A}^8$ corresponding to $\mathfrak{a}$ (respectively $\mathfrak{a}'$). Let $U = V' \setminus S$ where S is defined by the equation $cc_0 = 0$.

The varieties V' and U are needed to understand the geometric structure of V. In fact, V' is the unique top-dimensional component of V, and U is a smooth open subset of V'. Note that detecting the varieties V' and U as well as proving its properties required in an essential way the computational power of SINGULAR. The following theorem will be proved in § 3.

THEOREM 1.10. *We have:*

(1) $\dim(V) = \dim(V') = 2$;
(2) $\pi(\mathfrak{a}) = \mathfrak{a}$, $\pi(\mathfrak{a}') = \mathfrak{a}'$.

We thus see that α defines an algebraic map $\alpha\colon V \to V$. Our task now becomes to show that α^n (n odd and $n \geqslant 3$) has a non-zero fixed point on the surface V. Our basic tool is the Lefschetz trace formula resulting from Deligne's conjecture proved by Fujiwara [Fu97]. To apply this formula, we replace V by U.

THEOREM 1.11. *The variety U is a smooth, affine, absolutely irreducible surface invariant under α. We have $b^1(U) \leqslant 675$ and $b^2(U) \leqslant 2^{22}$.*

Here $b^i(U) = \dim H^i_{\text{ét}}(U, \overline{\mathbb{Q}}_\ell)$ stand for the ℓ-adic Betti numbers of U. We use results of Adolphson–Sperber [AS88] and Ghorpade–Lachaud [GL02] to get the above estimates.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

As U is non-singular, the ordinary and compact Betti numbers of U are related by Poincaré duality, and we have $b^i_{\mathrm{c}}(U) := \dim H^i_{\mathrm{c}}(U, \overline{\mathbb{Q}}_\ell) = b^{4-i}(U)$. As U is affine, $b^i(U) = 0$ for $i > 2$. As U is absolutely irreducible, $b^0(U) = 1$ and the Frobenius acts on the one-dimensional vector space $H^0_{\text{ét}}(U, \overline{\mathbb{Q}}_\ell)$ as multiplication by 4. The operator α induces linear self-maps of all these cohomology groups. The above properties of U imply that the Lefschetz trace formula holds in the form

$$\#\operatorname{Fix}(U, n) = \sum_{i=0}^{4} (-1)^i \operatorname{tr}(\alpha^n \mid H^i_{\mathrm{c}}(U, \overline{\mathbb{Q}}_\ell)),$$

where $\operatorname{Fix}(U, n)$ is the set of fixed points of α^n acting on U ($n > 1$ is an odd integer).

Note that α acts on $H^0_{\text{ét}}(U, \overline{\mathbb{Q}}_\ell)$ as multiplication by 2. (Indeed, if it were multiplication by (-2), for a sufficiently large power of α the right-hand side of the trace formula would be negative.) Hence, α^n acts as multiplication by 2^n. Thus $\operatorname{tr}(\alpha^n \mid H^4_{\mathrm{c}}(U, \overline{\mathbb{Q}}_\ell)) = 2^n$.

We infer from Deligne's estimates for the eigenvalues of the endomorphism induced by α on étale cohomology the following inequality:

$$|\#\operatorname{Fix}(U, n) - 2^n| \leqslant b^1(U) 2^{3n/4} + b^2(U) 2^{n/2}.$$

An easy estimate then shows that $\#\operatorname{Fix}(U, n) \neq 0$ for $n > 48$. The cases $n < 48$ are checked with the help of MAGMA, and this finishes the proof of Theorem 1.2 (and hence Theorem 1.1). More details can be found in § 3.

Remark 1.12. As a by-product of these computations, we found the first terms of the zeta-function of the operator α acting on the set U. This is a rational function defined by

$$Z_U(\alpha, T) := \exp\Bigg(-\sum_{n=1}^{\infty} \frac{\#\operatorname{Fix}(U, n)}{n} T^n \Bigg).$$

We have found that $Z_U(\alpha, T)$ equals

$$\frac{(1-2T)(1-T)(1-T^2)^8(1+T^2)^3(2T^4+2T^2+1)(4T^8+2T^4+1)(2T^2+2T+1)(8T^6+4T^5+T+1)}{(1-2T^2)^3}$$

up to terms of order T^{33}. Note that the absolute values of the zeros and poles of this rational function are all equal to 1, $1/2$, $1/\sqrt{2}$, or $1/\sqrt[4]{2}$, as general theory predicts. This formula suggests heuristic values $b^4_c(U) = 1$, $b^3_c(U) = 6$, $b^2_c(U) = 43$.

1.4 Analogues, problems, and generalisations

First, let us mention the following analogue of Levi–van der Waerden's problems for nilpotent groups (cf. [Hup79, § 3.6]).

Problem 1.13. Fix $n \in \mathbb{N}$ and assume that a finite group G satisfies the identity $u_n(x, y) \equiv 1$. What can be said about the solvability length of G?

If $n = 1$, then $G = \{1\}$. If $n = 2$, then G is nilpotent of class at most 3.

Further on, Theorem 1.1 admits some natural analogues in Lie-algebraic and group-schematic settings [GKNP00]. In particular, the following analogue of the classical Engel theorem on nilpotent Lie algebras is true.

Theorem 1.14 [GKNP00]. *Let L be a finite-dimensional Lie algebra defined over an infinite field k of characteristic different from 2, 3, 5. Define*

$$v_1 = [x, y], \quad v_{n+1} = [[v_n, x], [v_n, y]] \quad (n > 1). \tag{1.5}$$

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Then L is solvable if and only if for some n one of the identities $v_n(x,y) \equiv 0$ holds in L. (Here $[\ ,\ ]$ are Lie brackets.)

A much more challenging question is related to the infinite-dimensional case. Namely, the remarkable Kostrikin–Zelmanov theorem on locally nilpotent Lie algebras [Kos86, Zel90, Zel91] and Zelmanov's theorem [Zel88] lead to the following.

Problem 1.15. Suppose that L is a Lie algebra over a field k, the v_n are defined by formulas (1.5), and there is n such that the identity $v_n(x,y) \equiv 0$ holds in L. Is it true that L is locally solvable? If k is of characteristic 0, is it true that L is solvable?

Of course, it would be of significant interest to consider similar questions for arbitrary groups.

We call G an *Engel* group if there is an integer n such that the Engel identity $e_n(x,y) \equiv 1$ holds in G.

We call G an *unbounded Engel* group if for every $x, y \in G$ there is an integer $n = n(x,y)$ such that $e_n(x,y) = 1$.

We introduce the following.

Definition 1.16. We call G a *quasi-Engel* group if there is an integer n such that the identity $u_n(x,y) \equiv 1$ holds in G.

Definition 1.17. We call G an *unbounded quasi-Engel* group if for every $x, y \in G$ there is an integer $n = n(x,y)$ such that $u_n(x,y) = 1$.

Problem 1.18. Is every Engel group locally nilpotent?

Problem 1.19. Is every quasi-Engel group locally solvable?

A property is said to hold locally if it holds for all finitely generated subgroups.

Problem 1.18 has remained open for a long time, cf. [Plo58]. The answer in general is most likely negative, however, some positive results are known [BM98, Gru53, Plo54, Plo55, Wil91, WZ92], etc. In the solvable case the situation is even less clear. We dare to state the following.

Conjecture 1.20. Every residually finite, quasi-Engel group is locally solvable.

A group is said to be residually finite if the intersection of all its normal subgroups of finite index is trivial.

For pro-finite groups the situation looks more promising.

Theorem 1.21 [WZ92, Theorem 5]. *Every pro-finite, unbounded Engel group is locally nilpotent.*

Conjecture 1.22. Every pro-finite, unbounded quasi-Engel group is locally solvable.

It is quite natural to consider restricted versions of Problems 1.18 and 1.19 as is considered for the Burnside problem. Let E_n be the Engel variety defined by the identity $e_n \equiv 1$. Let $F = F_{k,n}$ be the free group with k generators in the variety E_n. One can prove that the intersection of all co-nilpotent normal subgroups H_α in F is also co-nilpotent. Hence, there exists a group $F^0_{n,k}$ in E_n such that every nilpotent group $G \in E_n$ with k generators is a homomorphic image of $F^0_{n,k}$. This implies that all locally nilpotent groups from E_n form a variety. In other words, the restricted Engel problem has a positive solution. The situation with the restricted quasi-Engel problem is unclear.

Problem 1.23. Let $F = F_{k,n}$ be the free group with k generators in the variety of all quasi-Engel groups with fixed n. Is it true that the intersection of all co-solvable normal subgroups in $F = F_{k,n}$ is also co-solvable?

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Our main theorem can be reformulated in pro-finite terms.

Theorem 1.24. *Let $F = F(x, y)$ denote the free group in two variables, and let $\widehat{F}$ be its pro-finite completion. Let $v_1, v_2, \ldots, v_m, \ldots$ be any convergent subsequence of (1.1) with limit f from $\widehat{F}$. Then the identity $f \equiv 1$ defines the pro-finite variety of pro-solvable groups.*

(See § A.2 for more details.)

It would be of great interest to consider the restricted quasi-Engel problem for pro-finite groups.

Remark 1.25. There is no sense in generalising Conjecture 1.22 too far: from the Golod–Shafarevich counterexamples one can deduce an example of an unbounded quasi-Engel group that is not locally nilpotent (and, hence, not locally solvable). We thank B. Plotkin for this observation.

Consider an interesting particular case of linear groups.

Corollary 1.26. *Suppose that $G \subset \mathrm{GL}(n, K)$ where K is a field. Then G is solvable if and only if it is quasi-Engel.*

Proof. The 'only if' part is obvious. The 'if' part is an immediate consequence of Theorem 1.1 and Platonov's theorem [Pla67] stating that every linear group over a field satisfying a non-trivial identity has a solvable subgroup of finite index. (Of course, if K is of characteristic zero, the assertion follows from the Tits alternative [Tit72].) □

Here is one more application of Theorem 1.2: it generates short presentations of finite simple groups. Let $\mathbf{B}$ be the group generated by x, y with the single relation $u_1(x, y) = u_2(x, y)$, that is $\mathbf{B} = \langle x, y \mid u_1 = u_2 \rangle$. The solvable quotients of $\mathbf{B}$ are all cyclic, but $\mathbf{B}$ has at least all minimal simple groups from Thompson's list as quotients. For example, we found that $\mathrm{PSL}(2, \mathbb{F}_5) = \langle x, y \mid u_1 = u_2, x^3 = y^2 = 1 \rangle$ and

$$\mathbf{Sz}(8) = \langle x, y \mid u_1 = u_2, x^7 = y^5 = (xy^2)^5 = (x^{-1}y^{-1}xy^2)^2 = 1 \rangle.$$

Notation. Owing to the extensive use of the Singular package, our notation sometimes differs from the standard notation: for example, in the output of computer sessions, powers such as a^{12} are denoted as `a12`. We refer the reader to [GP02a, GP02b, GPS01] for definitions of Singular commands and their usage, and to [Buc65, GP96, GP98, GP02a] for details on Gröbner bases.

All other notation is more or less standard.

Rings and fields. All rings are assumed commutative with 1; $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_q$ denote the ring of integers, the field of rational numbers, the field of q elements, respectively. The term $\overline{k}$ denotes a (fixed) algebraic closure of a field k.

Ideals and varieties. If I is an ideal in R and $i\colon R \to S$ is a ring homomorphism, IS stands for the image of I under i. The ideal generated by $f_1, \ldots f_k$ is denoted $\langle f_1, \ldots, f_k \rangle$.

For $f \in R$ we denote $I : f^\infty = \bigcup_{n=1}^{\infty} I : f^n$. If R is noetherian, the chain of ideals $I : f \subseteq I : f^2 \subseteq \ldots$ stabilises, and we have $I : f^\infty = I : f^n$ for some n.

The terms $\mathbb{A}^n$ and $\mathbb{P}^n$ denote affine and projective spaces. The term $\overline{C}$ denotes the projective closure of an affine set $C \subset \mathbb{A}^n$, and I_{h} stands for the homogenisation of an ideal I. $\mathbf{V}(J)$ denotes the affine variety defined by the ideal J. If $\mathbf{V}(J) \subset \mathbb{A}^n$, we denote $\mathbf{D}(J) = \mathbb{A}^n \setminus \mathbf{V}(J)$. We shorten $\mathbf{V}(\langle f_1, \ldots, f_k \rangle)$ to $\mathbf{V}(f_1, \ldots, f_k)$, and $\mathbf{D}(\langle f_1, \ldots, f_k \rangle)$ to $\mathbf{D}(f_1, \ldots, f_k)$. We denote by $V(k)$ the set of rational points of a k-variety V.

The term $\chi(V)$ denotes the Euler characteristic of a variety V.

If D is a projective curve (maybe singular), $p_{\mathrm{a}}(D)$ is the arithmetic genus of D, and $g(D)$ denotes the genus of the normalisation of D.

All other notation will be explained when needed.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

2. The details of the PSL(2) case

Our goal is to prove Theorem 1.5 and to compute the arithmetic genus of C. This will lead us to the following.

PROPOSITION 2.1. *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 $u_1(x, y) = u_2(x, y)$.*

Note that for $w = x^{-2}y^{-1}x$, the equation $u_1(x, y) = u_2(x, y)$ has a non-trivial solution if and only if it has a solution with $y \neq x^{-1}$.

The proof will use some explicit computations with the following matrices. Let R be a commutative ring with identity. Recall that we defined

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

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

Remark 2.2.

(1) We have

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

(2) for any $t, b, c \in R$ we have $y(b, c) \neq x(t)^{-1}$, even for the images of $x(t)$ and $y(b, c)$ in $\mathrm{PSL}(2, R)$.

The equation $u_1 = u_2$ is equivalent to $x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}$; we put $x = x(t)$, $y = y(b, c)$, and write

$$x^{-1}yx^{-1}y^{-1}x^2 - yx^{-2}y^{-1}xy^{-1} = \begin{pmatrix} n_1(t, b, c) & n_2(t, b, c) \\ n_3(t, b, c) & n_4(t, b, c) \end{pmatrix}.$$

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. Using SINGULAR[2] we can obtain four explicit generators for I.

Denote by C the $\mathbb{F}_q$-variety defined by the ideal $I\mathbb{F}_q[b, c, t]$. To prove Proposition 2.1, it is enough to prove the following.

PROPOSITION 2.3. *Let q be as in Proposition 2.1, then the set $C(\mathbb{F}_q)$ of rational points of C is not empty.*

The proof is based on the Hasse–Weil estimate (see Corollary 1.7).

Note that the Hilbert function of $\overline{C}$, $H(t) = dt - p_\mathrm{a} + 1$, 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 $\overline{C}$. The ideal I_h can be computed by homogenising the elements of a Gröbner basis of I with respect to a degree ordering (cf. [GP02a]).

In the following, let $q = p^k$ be an arbitrary, fixed prime power and $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$. To apply Corollary 1.7, we have to prove the following.

PROPOSITION 2.4. *The ideal $I\bar{\mathbb{F}}_q[b, c, t]$ is a prime ideal.*

To establish this and to provide the input for the application of Lemma 1.6 and Corollary 1.7 we first compute a Gröbner basis $J_1, \ldots, J_5$ of I in characteristic 0, i.e. over the rational numbers but

[2] A file with all SINGULAR computations can be found at http://www.mathematik.uni-kl.de/~pfister/SolubleGroups.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

with integer coefficients. This can be done in Singular or MAGMA. What we need is, however, a system of generators of I with integer coefficients that specialize to a Gröbner basis over $\mathbb{F}_q$ for any q (cf. [GP02b] for the relation between Gröbner bases and specialisation). Any Gröbner basis over the rationals represents, after clearing denominators, a Gröbner basis over $\mathbb{F}_q$ for sufficiently large q. Unfortunately, there are no *a priori* bounds nor does the computed Gröbner basis give estimates for q. In our situation, however, we are lucky. By using the `lift` command in Singular we can show that $J_1, \dots, J_5$ indeed generate I over the integers. Then we compute the s-polynomials of J_i and J_j for all i, j (with integer coefficients) and check, again by using `lift`, that they are integer linear combinations of $J_1, \dots, J_5$. Applying Buchberger's criterion [GP02a, Theorem 1.7.3] we deduce that $J_1, \dots, J_5$ represent a Gröbner basis of $I\overline{\mathbb{F}_q}[b, c, t]$ for any q. Some straightforward computations using Singular show the following.

Lemma 2.5. *Let*

$$f_1 = t^2b^4 - t^3(t-2)b^3 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b^2 + t^2(t^2 - 2t - 1)(t-2)b + (t^2 - 2t - 1)^2,$$
$$f_2 = t(t^2 - 2t - 1)c + t^2b^3 + (-t^4 + 2t^3)b^2 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b + (t^5 - 4t^4 + 3t^3 + 2t^2),$$
$$h = t(t^2 - 2t - 1).$$

Then the following holds for any prime power q:

(1) *$\{f_1, f_2\}$ is a Gröbner basis of $I\bar{\mathbb{F}}_q(t)[b, c]$ with respect to the lexicographical ordering $c > b$;*
(2) *$I : h = I$;*
(3) *$I\bar{\mathbb{F}}_q(t)[b, c] \cap L[t, b, c] = \langle f_1, f_2\rangle : h^2 = I$.*

We now give the proof of Proposition 2.4. We have $I\bar{\mathbb{F}}_q(t)[b, c] \cap \bar{\mathbb{F}}_q[b, c, t] = \langle f_1, f_2\rangle : h^2 = I\bar{\mathbb{F}}_q[b, c, t]$. Therefore, if $I\bar{\mathbb{F}}_q[b, c, t]$ were reducible, then $I\bar{\mathbb{F}}_q(t)[b, c]$ would also be reducible. We are going to prove that this is not the case.

In $\bar{\mathbb{F}}_q(t)[b, c]$ the polynomial f_2 is linear in c. As f_1 does not depend on c, we have $\bar{\mathbb{F}}_q(t)[b, c]/I \cong \bar{\mathbb{F}}_q(t)[b]/\langle f_1\rangle$ and, hence, it suffices to prove that the polynomial f_1 is irreducible.

Set $x = bt$, and let $p(x, t) = t^2 f_1(x/t, t)$, then

$$p(x, t) = x^4 - t^2(t-2)x^3 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)x^2 + t^3(t-2)(t^2 - 2t - 1)x + t^2(t^2 - 2t - 1)^2.$$

To prove that $f_1 \in \bar{\mathbb{F}}_q[t, b]$ is irreducible, it suffices to prove that $p \in \bar{\mathbb{F}}_q[x, t] = \bar{\mathbb{F}}_q[t][x]$ is irreducible. We show that p has no linear and no quadratic factor with respect to x.

First we prove that p has no linear factor, that is, that $p(x) = 0$ has no solution in $\bar{\mathbb{F}}_q[t]$.

Assume that $x(t) \in \bar{\mathbb{F}}_q[t]$ is a zero of $p(x) = 0$. Then $x(t) \mid t^2(t^2 - 2t - 1)^2$. If the characteristic of $\bar{\mathbb{F}}_q$ is not 2, it is not difficult to see that $x(t)$ cannot contain the square of an irreducible factor of $t^2(t^2 - 2t - 1)^2$. If the characteristic of $\bar{\mathbb{F}}_q$ is 2, it is not possible that $t^2 \mid x(t)$ or $(t+1)^3 \mid x(t)$. Moreover, it is easy to see that the leading coefficient of $x(t)$ is $(-1)^{\deg(x(t))-1}$.

By analysing possible zeroes of $p(x)$, separately for $\mathrm{char}(\bar{\mathbb{F}}_q) > 2$ and $\mathrm{char}(\bar{\mathbb{F}}_q) = 2$ we find that $p(x)$ has no linear factor with respect to x in $\bar{\mathbb{F}}_q[x, t]$.

Now assume that $p(x) = (x^2 + ax + b)(x^2 + gx + d)$, $a, b, g, d \in \bar{\mathbb{F}}_q[t]$. This implies:

(1) $bd = t^2(t^2 - 2t - 1)^2$;
(2) $ad + bg = t^3(t-2)(t^2 - 2t - 1)$;
(3) $d + ag + b = -t^5 + 3t^4 - 2t^3 + 2t + 1$;
(4) $a + g = -t^2(t-2)$.

If $t^2 \mid b$ then, because of equality (2), we obtain $t^2 \mid a$. Equality (4) implies $t^2 \mid g$ and equality (2) implies $t^3 \mid a$. Equality (3) implies that $d \equiv 1 + 2t \mod (t^2)$ and equality (4) implies

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

that $g \equiv 2t^2 \mod (t^3)$. If $\mathrm{char}(\bar{\mathbb{F}}_q) \neq 2$, we obtain $d = -(t^2-2t-1)$ and $b = -t^2(t^2-2t-1)$, because $(t^2-2t-1)^2 \equiv 1+4t \mod (t^2)$. If $\mathrm{char}(\bar{\mathbb{F}}_q) = 2$, then $t^3 \mid a$ and $t^3 \mid g$. Equality (2) implies that $(a/t^3)\cdot d + (g/t^3)b = (t+1)^2$. This implies $(t+1)^2 \mid b$ and $(t+1)^2 \mid d$. Therefore, we have in any characteristic $b = -t^2(t^2-2t-1)$ and $d = -(t^2-2t-1)$. Equality (3) implies that $ag = -t^3(t-2)^2$. This is a contradiction to the fact that $t^3 \mid a$ and $t^2 \mid g$.

We showed that $t^2 \nmid b$. Similarly, we obtain that $t^2 \nmid d$. This implies that $t \mid b$ and $t \mid d$. If $(t^2-2t-1)^2 \mid b$, then equality (2) implies that $t^2-2t-1 \mid a$. Let $d = d_1 t$ for a suitable $d_1 \in L$; then equality (3) implies that $t^2-2t-1 \mid -t^5+3t^4-2t^3+2t+1-d_1 t$, that is, $d_1 = -1$. Then $b = -t(t^2-2t-1)^2$. Now equality (3) implies that $ag = -t^4+4t^2+4t+1 = -(t^2-2t-1)(t+1)^2$.

However, $t^2-2t-1 \mid a$ and equality (4) implies that $\deg(a) = 3$ and $\deg(g) = 1$. This implies that $t+1 \mid a$ and $t+1 \mid g$, which is a contradiction to equality (4).

Similarly, we obtain that $(t^2-2t-1)^2 \nmid d$. This implies that $b = b_3 t(t^2-2t-1)$ and $d = (1/b_3)t(t^2-2t-1)$ for a suitable $b_3 \in L$. Equality (3) implies that $\deg(ag) = 5$. Owing to equality (4), we may assume that $\deg(a) = 3$ and $\deg(g) = 2$. Equality (4) implies that $a = -t^3+$ terms of lower degree. Equality (3) implies that $g = t^2+$ terms of lower degree. Equality (4) implies that $a = -t^3 + t^2+$ terms of lower degree. Equality (2) implies that $b_3 = -1$. Equality (3) implies that $ag = -t^5+3t^4-4t^2+1$. Let $a = t^3+t^2+a_1 t+a_0$ for suitable $a_1, a_0 \in L$; then, because of equality (4), $g = t^2-a_1 t-a_0$. Equality (3) implies that $a_0^2 = -1$. Now $-t^5+3t^4-4t^2+1 = a\cdot g$ implies that $a_0 = 0$, which is a contradiction. This proves that p is irreducible and Proposition 2.4 is proved.

We can now apply Corollary 1.7 to prove Proposition 2.3. We compute the Hilbert polynomial $H(t)$ of the projective curve corresponding to I_{h}, the homogenisation of I. We again use a computation in characteristic 0 (with SINGULAR) and a straightforward verification showing that the result stays correct over every $\bar{\mathbb{F}}_q$. We obtain $H(t) = 10t-11$. From this we get the degree $d = 10$ and the arithmetic genus $p_{\mathrm{a}} = 12$ of the projective closure. Using Corollary 1.7, we deduce that

$$N_q \geqslant q+1-24\sqrt{q}-10.$$

This implies that $C(\mathbb{F}_q)$ is not empty if $q > 593$. For small q, we directly find points by a computer search. Proposition 2.3 and, hence, Proposition 2.1 are proved.

Remark 2.6. Using the leading terms of J, we can even compute the Hilbert polynomial without computer. Hence (once the matrices are computed by the `lift` command and the Gröbner bases are given), we can in principle check everything by hand, as only simple (although tedious) polynomial computations are necessary. Therefore, the PSL(2) case can be verified without a computer.

Remark 2.7. Proposition 2.1 can also be proved by an analysis of the singularities of the curve C defined by the ideal I: the proof of the absolute irreducibility of the polynomial f_1 follows then by applying Bezout's theorem. Furthermore, the Hasse–Weil theorem can be applied here to the normalisation of the plane curve defined by f_1, while above it was applied to the curve defined by I and not to its projection defined by f_1. We used the Hasse–Weil theorem involving the arithmetic genus which avoids an analysis of the singularities. The arithmetic genus is 12 for the curve C and 15 for its projection to the plane defined by f_1. The analysis of singularities allows us to use the geometric genus, which is 8. Then the Hasse–Weil theorem applies already for $q > 277$. In principle, this does not make a big difference because we are using a computer for small fields $\mathbb{F}_q$, anyway. On the other hand, when analysing the singularities, we have the disadvantage of treating the field $\mathbb{F}_{864\,007}$. That such a large prime plays a special role in the analysis of singularities was rather unexpected for us.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

3. The details of the Suzuki case

3.1 The variety V and the Suzuki groups

We shall explain here in more detail the relationship of the variety V constructed in § 1.3 to the Suzuki groups. We use the following representation for $\mathrm{Sz}(q)$. Let $n = 2m+1$ and $q = 2^n$ and consider the automorphism $\theta\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $\theta(a) = a^{2^{m+1}}$. We have $\theta^2(a) = a^2$, that is, π is the square root of the Frobenius.

Let

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

$$M(c) = \begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{3.1}$$

Then $\mathrm{Sz}(q) = \langle U(a,b), M(c), T \mid a,b,c \in \mathbb{F}_q, c \neq 0\rangle \subset \mathrm{SL}(4,\mathbb{F}_q)$.

To show that $u_1(x,y) = u_2(x,y)$ has a solution with $y \neq x^{-1}$, we consider the matrices $X = TU(a,b)$ and $Y = TU(c,d)$ in $\mathrm{Sz}(q)$. It is easy to see that $Y = X^{-1}$ in $Sz(q)$ if and only if a,b,c,d are all 0.

To eliminate the dependence of X and Y on q, we replace $\theta(a),\dots,\theta(d)$ with $a_0,\dots,d_0$ which we regard as indeterminates, along with $a,\dots,d$. We thus arrive at the matrices $x,y \in \mathrm{GL}(4,R)$ defined in (1.4), where $R = \mathbb{F}_2[a,\dots,d,a_0,\dots,d_0]$ is the polynomial ring in eight variables.

Using the definition of the ideal $\mathfrak{a} \subset R$ and the variety V (see § 1.3), we can easily produce 16 generators of $\mathfrak{a}$ and prove that $\pi(\mathfrak{a}) = \mathfrak{a}$ and $\dim(V) = 2$ (a Singular computation). Also V is preserved by the operator α, and we have the following.

Proposition 3.1. *The matrices corresponding to a fixed point of α^n (n odd and $n \geqslant 3$) lie in $\mathrm{Sz}(2^n)$.*

Proof. Let $p = (a,\dots,d_0) \in V$ be a fixed point of α^{2m+1}. We have $a = a_0^{2^{m+1}}$, $a_0 = a^{2^{m+1}}$ (and, hence, $a = a^{2^n}$, $a_0 = \theta(a)$), and the same formulas hold for b,c,d,b_0,c_0,d_0. To finish the proof, it remains to combine this with formulas (1.4) and (3.1). □

To sum up, we obtained the following reduction.

Theorem 3.2. *Suppose that for every odd $n > 1$, the operator α^n has a non-zero $\mathbb{F}_q$-rational fixed point on the variety V. Then the equation $u_1 = u_2$ has a non-trivial solution in $\mathrm{Sz}(q)$ for every $q = 2^n$.*

3.2 The geometric structure of V

In this section we study the two-dimensional component V' of V defined in § 1.3. In order to make the formulas simpler, we slightly change notation: we denote $a_0 = v$, $b_0 = w$, $c_0 = x$, $d_0 = y$; we will replace $\mathfrak{a}$ by I, and $\mathfrak{a}'$ by J. Recall that J is defined to be the ideal quotient $J = I : a^3x^2$. To show that α^n has a rational fixed point on V, we want to apply the Lefschetz trace formula. This requires an absolutely irreducible variety to be acted on by α. As the variety V does not have this property we have introduced the subvariety $V' \subset V$. More formally we set $V' := \mathbf{V}(J) \subset \mathbf{V}(I) = V$. We show that V' is absolutely irreducible and apply the Lefschetz trace formula to the non-singular locus of V'.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

The ideal I has 16 generators whereas J needs only 10. As this still makes computations hard we temporarily work with generic a and c, that is, we do computations in $\mathbb{F}_2(a,c)[w,y,b,d,x,y]$, where $\mathbb{F}_2(a,c)$ denotes the field of fractions of $\mathbb{F}_2[a,c]$. Fortunately, SINGULAR allows the computation of Gröbner bases over such rings. We compute a Gröbner basis of the ideal $J3 := J\mathbb{F}_2(a,c)[w,y,b,d,x,v]$ with respect to the lexicographical ordering. As the polynomials of this Gröbner basis play an essential role in what is to follow we give them here. We define in SINGULAR notation:

```
J3[1]=(a8+a6c2+a4c4+a2c6)*v6+(a8+a7c3+a6c2+a5c3+a4c4+a3c7+a2c6
      +ac7)*v4+(a7c3+a6c2+a5c5+a5c3+a3c7+a3c5+a2c6+a2c4+ac9+c6)
      *v2+(ac9+ac5+c8+c4);
J3[2]=(a4c4+a3c7+a3c5+a3c3+a2c8+a2c4+ac7+c4)*x+(a8+a7c+a4c4
      +a3c5)*v5+(a8+a7c+a6c2+a5c3+a4c4+a4c2+a2c6+a2c4)*v3
      +(a4c4+a4c2+a3c7+a3c3+a2c8+a2c6)*v;
J3[3]=(c2+1)*d2+(xc3+xc)*d+(v3xa2+v3xc2+v2a4+v2a3c+v2ac3+v2c4
      +vxa4+vxa3c+vxa2c2+vxc4+x2a2c2+x2a2+x2ac3+x2c2+c4+c2);
J3[4]=(ac5+ac)*b+(v4a2c2+v4a2+v3xac+v2x2c4+v2x2c2+v2a5c+v2a4
      +v2a2c4+v2ac3+vx3ac+vx3+vxa5c+vxa4+vxa3c3+vxa2c4+vxa2c2
      +vxac5+vxac3+vxac+vxc2+vx+x2a3c3+x2a2c2+x2ac5+x2c4+a2c4
      +a2c2+ac3+ac+c4+c2)*d+(v2xa2c3+v2xc5+vx2a3+vx2ac2+va5c2
      +va4c+va3+va2c+vac6+vac4+vac2+vc5+xa5c2+xa4c+xa2c3+xa2c
      +xac6+xac2+xc3);
J3[5]=(c)*y+(va2c+va)*bd+(v2ac+v2c2+x4+c4+1)*b+(v4a3c+v4ac
      +v3xc2+v2x2ac3+v2x2ac+v2a4+v2a3c3+v2ac3+v2c2+vx3c2+vxa4
      +vxa3c3+vxa3c+vxa2c4+vxa2+vxac3+vxac+x2a3c+x2a2c4+x2a2
      +x2ac+x2+ac3+ac+c2+1)*d+(v3x2ac2+v3x2c3+v3a3c4+v3a3c2
      +v3a2c3+v3a2c+v3ac4+v3c3+v2xa3c2+v2xa3+v2xa2c5+v2xc5
      +v2xc+vx4a3+vx4a2c+vx4a+vx4c+vx2a7+vx2a5+vx2a3c2+vx2a2c3
      +vx2a+vx2c3+vx2c+va7c2+va7+va4c+va3c6+va3c4+va3c2+va2c5
      +va2c+vac6+vac4+vc3+vc+x5a+x5c+x3a6c+x3a5+x3a4c+x3a3
      +x3a2c+x3ac2+x3c+xa7c2+xa6c+xa5c2+xa4c3+xa3c6+xa3c4
      +xa3c2+xa3+xa2c5+xa2c3+xa2c+xac6+xac4+xa);
J3[6]=w+(vx+1)*y+(a)*b+(vxc+c)*d+(v3a2+v3ac+v2xa2+v2xc2+vx2a2
      +vx2ac+vx2c2+vx2+va2c2+va2+vac3+v+xa2c2+xa2+xac3+xc2);
```

and assert that $J3$ is generated by these polynomials. Computing the dimension of $J3$ gives 0, hence V' is a surface.

The least common multiple of the leading coefficients of the above Gröbner basis is

$$f(a,c) = (a^3 + a^2c^3 + a^2c + ac^4 + ac^2 + c)(ac+1)(a+c)(c+1)ac$$

Then, using SINGULAR,[3] we obtain

$$J3 \cap \mathbb{F}_2[a,c,w,y,b,d,x,v] = \langle J3[1],\ldots,J3[6]\rangle : f^\infty = \langle J3[1],\ldots,J3[6]\rangle : f^6 = J.$$

As $J : f = J$, no factor of f divides all elements of J. That is why the irreducibility of $J3$ as an ideal of $\mathbb{F}_2(a,c)[w,y,b,d,x,v]$ implies the irreducibility of J.

[3]The first equality is a general fact (cf. [GP02a]). To see that $\langle J3[1],\ldots,J3[6]\rangle : f^\infty = J$, it is sufficient to know that $J \supset \langle J3[1],\ldots,J3[6]\rangle$, $J = J : f$ and that $\langle J3[1],\ldots,J3[6]\rangle : f^\infty$ is a prime ideal, which we shall see later. This is, computationally, much easier to check than a direct computation.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Furthermore, we compute the vector space dimension over $\mathbb{F}_2(a,c)$ as

$$\dim_{\mathbb{F}_2(a,c)} \mathbb{F}_2(a,c)[w,y,b,d,x,v]/J3 = 12.$$

Next we compute directly by elimination (using Singular) that $J3 \cap \mathbb{F}_2(a,c)[b] = \langle h \rangle$ with a polynomial h which is of degree 12 with respect to b and we therefore have $\dim_{\mathbb{F}_2(a,c)} \mathbb{F}_2(a,c)[b]/(J3 \cap \mathbb{F}_2(a,c)[b]) = 12$. As $\dim_{\mathbb{F}_2(a,c)} \mathbb{F}_2(a,c)[w,y,b,d,x,v]/J3$ is also 12, we know that a lexicographical Gröbner basis with respect to $b < v < x < d < y < w$ of $J3$ must have leading polynomials as follows[4]: b^{12}, v, x, d, y, w.

It follows that the projection

$$[a,b,c,d,v,w,x,y] \to (a,b,c)$$

over the field $\mathbb{F}_2(a,c)$ is birational on $\mathbf{V}(J3)$. The image of $\mathbf{V}(J3)$ in $\mathbb{F}_2(a,c)[b]$ is defined by the polynomial h.

This implies that $J3\overline{\mathbb{F}}_2(a,c)[w,y,d,x,v,b]$ is a prime ideal if h is absolutely irreducible. In particular, we obtain that J is absolutely irreducible if h is absolutely irreducible.

To prove that h is absolutely irreducible, we proceed as follows.

First we show that the radical of the ideal of the coefficients of h in $\overline{\mathbb{F}}_2[a,c]$ with respect to b is $\langle a,c \rangle \cap \langle a+1, c+1 \rangle$. We do this using the factorising Gröbner basis algorithm. This implies that h cannot have a non-trivial factor in $\mathbb{F}_2[a,c]$. Then we consider $\tilde{h}(b,c) := h(1,b,c)$. We get

$$\begin{aligned}\tilde{h}(b,c) = {} & (c+1)^{14}b^{12} + (c+1)^{14}b^{10} + (c+1)^{11}(c^6+c^5+c^4+c+1)b^8 \\ & + (c+1)^{11}(c^6+c^4+c^2+c+1)b^6 + (c+1)^8(c^9+c^7+c^5+c^4+c^3+c^2+1)b^4 \\ & + (c+1)^{10}b^2 + (c+1)^{10}c^2.\end{aligned}$$

It is sufficient to show that $f(x,c) := \tilde{h}(x/(c+1),c)/(c+1)^2$ is absolutely irreducible. To simplify the situation, we make the transformation $c \mapsto c+1$. Let $a_4 = c^6+c^5+c^4+c^2+1$ and $a_2 = c^9+c^8+c^7+c^6+c^4+c^2+1$. By elementary considerations similar to those in § 2 we prove the following.

Lemma 3.3. *The polynomial*

$$f = x^{12} + c^2x^{10} + ca_4x^8 + c^3(c^6+c+1)x^6 + c^2a_2x^4 + c^6x^2 + c^8(c+1)^2$$

is irreducible in $\overline{\mathbb{F}}_2[x,c]$.

Altogether, we proved now that $V' = \mathbf{V}(J)$ is absolutely irreducible. Next we compute the singular locus of $\mathbf{V}(J)$, using Singular (with a special procedure).

Lemma 3.4. *The singular locus of* $\mathbf{V}(J)$ *is the union of six smooth curves.*

From the equations defining the six curves we find the following.

Corollary 3.5. *The singular locus of* V' *is contained in the set* $S = V' \cap \mathbf{V}(xc)$. *The variety* $U = V' \setminus S$ *is a smooth irreducible affine surface invariant under the morphism* α. *For any odd* n, α^n *has no fixed points in* S.

In what follows we only use that $U = V' \setminus S$ is non-singular and α-invariant, the precise equations giving the six curves is only relevant for the further statements of the corollary.

[4]We do not need to directly compute $J3 \cap \mathbb{F}_2(a,c)[b] = \langle h \rangle$, which is difficult. Once h is given, it suffices to know that h is irreducible of degree 12, $\dim_{\mathbb{F}_2(a,c)} \mathbb{F}_2(a,c)[w,y,b,d,x,v]/J3 = 12$ and $h \in J3$, which is much easier to check.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

3.3 Trace formula

Throughout this section $k = \bar{\mathbb{F}}_2$ denotes a (fixed) algebraic closure of $\mathbb{F}_2$. All varieties under consideration, even those defined over $\mathbb{F}_2$, are viewed as k-varieties.

Let V' be the variety defined in § 3.2. We have seen that this is an irreducible affine surface. Computations in § 3.2 show that the singular locus of V' is contained in the set $S = V' \cap \mathbf{V}(xc)$. By Corollary 3.5, the variety $U = V' \setminus S$ is a smooth irreducible affine surface invariant under the morphism α acting in $\mathbb{A}^8$ as

$$\alpha(a, b, c, d, v, w, x, y) = (v, w, x, y, a^2, b^2, c^2, d^2) \tag{3.2}$$

(see § 3.1).

Our goal is to prove that for n odd and large enough, the set U has an α^n-invariant point. In this section we prove the following estimate of Lang–Weil type.

THEOREM 3.6. *With the above notation, let* $\#\operatorname{Fix}(U, n)$ *be the number of fixed points of* α^n *(counted with their multiplicities). Then for any odd* $n > 1$ *the following inequality holds:*

$$|\#\operatorname{Fix}(U, n) - 2^n| \leqslant b^1(U)2^{3n/4} + b^2(U)2^{n/2}, \tag{3.3}$$

where $b^i(U) = \dim H^i_{\text{ét}}(U, \overline{\mathbb{Q}}_\ell)$ *are* ℓ*-adic Betti numbers* ($\ell \neq 2$).

The strategy of proof is as follows. The operator α and all its powers act on the étale ℓ-adic cohomology groups $H^i_{\mathrm{c}}(U, \overline{\mathbb{Q}}_\ell)$ of U (with compact support). We are going to apply Deligne's conjecture (proved by Zink for surfaces [Zin90], by Pink [Pin92] in arbitrary dimension (modulo resolution of singularities), and by Fujiwara [Fu97] in the general case) saying that the Lefschetz(–Weil–Grothendieck–Verdier) trace formula is valid for any operator on U composed with sufficiently large power of the Frobenius (in our case this means sufficiently large odd power of α). We shall show that in our case the trace formula is already valid after twisting with the first power of the Frobenius. This fact is a consequence of the above-mentioned results on Deligne's conjecture together with the following crucial observation: roughly speaking, if we consider the closure $\overline{U}$ of U in $\mathbb{P}^8$, α (as well as any of its odd powers) has no fixed points at the boundary (that is, on $\overline{U} \setminus U$). As soon as the trace formula is established, the proof can be finished by applying Deligne's estimates of the eigenvalues of the Frobenius.

Let us make all this more precise.

Denote by Γ (the transpose of) the graph of α acting on $\mathbb{A}^8$ by formulas (3.2), that is, $\Gamma = \{(\alpha(M), M) : M \in \mathbb{A}^8\}$, and let $\Gamma_U = \Gamma \cap (U \times U)$.

Consider the natural embedding $\mathbb{A}^8 \subset \mathbb{P}^8$, and denote by $\overline{\Gamma}$ (respectively $\overline{\Gamma}_U$) $\subset \mathbb{P}^8 \times \mathbb{P}^8$ the closure of Γ (respectively Γ_U) with respect to this embedding. Let $H_0 = (\mathbb{P}^8 \times \mathbb{P}^8) \setminus (\mathbb{A}^8 \times \mathbb{A}^8)$, $H_1 = (V' \times V') \setminus (U \times U)$, $H = H_0 \cup H_1$. Let Δ denote the diagonal of $\mathbb{A}^8 \times \mathbb{A}^8$, $\overline{\Delta}$ the diagonal of $\mathbb{P}^8 \times \mathbb{P}^8$, $\Delta_U = \Delta \cap \Gamma_U$, and $\overline{\Delta}_U = \overline{\Delta} \cap \overline{\Gamma}_U$. If n is a positive integer, denote the corresponding objects related to α^n by $\Gamma^{(n)}$, $\overline{\Gamma}^{(n)}$, $\Gamma^{(n)}_U$, $\overline{\Gamma}^{(n)}_U$, $\Delta^{(n)}_U$, $\overline{\Delta}^{(n)}_U$.

LEMMA 3.7. *If* n *is odd,* $\overline{\Delta}^{(n)}_U = \Delta^{(n)}_U$.

Proof. We have

$$\overline{\Delta}^{(n)}_U \setminus \Delta^{(n)}_U = \overline{\Gamma}^{(n)}_U \cap \overline{\Delta} \cap H.$$

We wish to prove that this set is empty. As

$$\overline{\Gamma}^{(n)}_U \cap \overline{\Delta} \cap H \subseteq \overline{\Gamma}^{(n)} \cap (\overline{U \times U}) \cap \overline{\Delta} \cap H,$$

it is enough to prove that

$$\overline{\Gamma}^{(n)} \cap \overline{\Delta} \cap H = \emptyset.$$

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

First note that

$$\overline{\Gamma}^{(n)} \cap \overline{\Delta} \cap H_1 = \Gamma^{(n)} \cap \Delta \cap H_1 = \emptyset$$

(the first equality is obvious as H_1 is contained in $\mathbb{A}^8 \times \mathbb{A}^8$, and the second equality immediately follows from Corollary 3.5). Hence, we only have to prove that $\overline{\Gamma}^{(n)} \cap \overline{\Delta} \cap H_0 = \emptyset$.

Let $(a, b, c, d, v, w, x, y), (a', b', \dots, y')$ be the coordinates in $\mathbb{A}^8 \times \mathbb{A}^8$, and let $(a : b : \cdots : t), (a' : b' : \cdots : t')$ be the homogeneous coordinates in $\mathbb{P}^8 \times \mathbb{P}^8$. Suppose that

$$M = ((a : b : \cdots : t), (a' : b' : \cdots : t')) \in \overline{\Gamma}^{(n)} \cap \overline{\Delta} \cap H_0.$$

If $n = 2m + 1$, denote $s = 2^m$. With this notation, as $M \in \overline{\Gamma}^{(n)}$, formulas (3.2) imply that

$$a' = v^s t^s, \quad b' = w^s t^s, \quad c' = x^s t^s, \quad d' = y^s t^s, \quad v' = a^{2s}, \quad w' = b^{2s}, \quad x' = c^{2s}, \quad y' = d^{2s}, \quad t' = t^{2s}.$$

On the other hand, as $M \in H_0$, we have $t = t' = 0$, and hence $a' = b' = c' = d' = 0$. Furthermore, as $M \in \overline{\Delta}$, we have $a' = \lambda a$, $b' = \lambda b$, $c' = \lambda c$, $d' = \lambda d$ for some $\lambda \in k$, and hence $a = b = c = d = 0$. This implies that $v' = w' = x' = y' = 0$, contradiction. □

The next goal is to show that the Lefschetz trace formula holds for all odd nth powers of α ($n > 1$). We shall do it using the above-mentioned results on Deligne's conjecture. First, we briefly recall the general approach ([SGA5, Zin90, Pin92, Fu97]); we mainly use the notation of [Pin92] and refer the reader to that paper for more details.

(i) *Global term.* We can (and shall) view our operator α as a particular case of the correspondence a:

$$U \xleftarrow{a_1} \Gamma_U \xrightarrow{a_2} U$$

(here a_1 and a_2 stand for the first and second projections, respectively). We regard an odd power α^{2m+1} as a 'twisted' correspondence $b = \mathrm{Fr}^m \circ a$ with $b_1 = \mathrm{Fr}^m \circ a_1$, $b_2 = a_2$.

Let Λ denote a finite field extension of $\mathbb{Q}_\ell$, L a constructible Λ-sheaf (in our situation it suffices to consider the constant sheaf $L = \overline{\mathbb{Q}}_\ell$). Then a cohomological correspondence u on L with support in b is a morphism $u\colon b_1^* L \to b_2^! L$, where * stands for the inverse image functor, and $^!$ for the extraordinary inverse image functor (cf. [Pin92, § 1] and references therein); in our situation $b_2 = \mathrm{id}$ and hence $b_2^! L = L$. As b_1 is a proper morphism, u induces an endomorphism $u_!\colon H_c^\bullet(U, L) \to H_c^\bullet(U, L)$ which possesses a well-defined trace $\mathrm{tr}(u_!) \in \Lambda$; this is the global term in the desired trace formula. In down-to-earth terms, in our situation we have

$$\mathrm{tr}(u_!) = \sum_{i=0}^{4} (-1)^i \,\mathrm{tr}(\alpha^n \mid H_c^i(U, \overline{\mathbb{Q}}_\ell)). \tag{3.4}$$

(ii) *Compactification.* Furthermore, as b_1 is proper, our correspondence b can be extended to a compactification $\bar{b}$

$$\begin{array}{ccccc} U & \xleftarrow{b_1} & \Gamma_U & \xrightarrow{b_2} & U \\ {\scriptstyle j}\downarrow & & \downarrow & & \downarrow \\ \bar{U} & \xleftarrow{\bar{b}_1} & \overline{\Gamma}_U & \xrightarrow{\bar{b}_2} & \bar{U} \end{array}$$

where the vertical arrows are open embeddings and the bottom line is proper. This gives rise to a cohomological correspondence $\bar{u}_!$ on the sheaf $j_! L$ with support in $\bar{b}$; here $_!$ stands for the direct image functor with compact support (extension by 0), cf. [Pin92, § 2.3].

The global term does not change after compactification:

$$\mathrm{tr}(\bar{u}_!) = \mathrm{tr}(u_!) \tag{3.5}$$

(see [Pin92, Lemma 2.3.1]).

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

For a compactified correspondence the Lefschetz–Verdier trace formula is known (cf. [Pin92, § 2.2.1]):

$$\operatorname{tr}(\bar{u}_!) = \sum_D LT_D(\bar{u}) \tag{3.6}$$

where D runs over all the connected components of $\operatorname{Fix}(\bar{b})$, and the local terms $LT_D(\bar{u})$ are defined as in [Pin92, § 2.1]. In our case $\operatorname{Fix}(\bar{b})$ consists of isolated points (as this is true for the Frobenius), and all these points are contained in U (because of Lemma 3.7 there are no fixed points at the boundary, neither on the singular locus, nor at infinity).

(iii) *Local terms.* Suppose that b_2 is quasifinite and y is a point not at infinity. Let $x = b_2(y)$, then

$$d(y) = [k(y)/k(x)]_i \cdot \operatorname{length} O_{\Gamma_U,y}/b_2^*(m_{U,x}O_{U,x}),$$

where $[k(y)/k(x)]_i$ denotes the inseparable degree of the residue field extension. Clearly, in our case $b_2 = \mathrm{id}$ implies that $d(y) = 1$.

By [Fu97, Theorem 5.2.1], for an isolated fixed point y at finite distance we have

$$LT_y(u) = \operatorname{tr}_y(u) \tag{3.7}$$

provided that $2^m > d(y)$. In our setting,

$$\operatorname{tr}_y(u) \text{ equals the multiplicity of } y \tag{3.8}$$

(cf. [Zin90, p. 338] and [Pin92, § 8.3.1]).

(iv) Summing up, items (i)–(iii) (or, more precisely, formulas (3.4), (3.5), (3.6), (3.7), (3.8), together with Lemma 3.7) imply the following.

PROPOSITION 3.8. *If $n > 1$ is an odd integer, then*

$$\#\operatorname{Fix}(U, n) = \sum_{i=0}^{4} (-1)^i \operatorname{tr}(\alpha^n \mid H_c^i(U, \overline{\mathbb{Q}}_\ell)). \tag{3.9}$$

We are now ready to prove Theorem 3.6. As U is non-singular, the ordinary and compact Betti numbers of U are related by Poincaré duality [Kat00, p. 6], and we have $b_c^i = b^{4-i}$. Since U is affine, $b^i(U) = 0$ for $i > 2$ (see [Kat00, p. 6]). As U is geometrically integral, $b^0(U) = 1$ and Fr acts on the one-dimensional vector space $H^0(U, \overline{\mathbb{Q}}_\ell)$ as multiplication by four [Kat00, p. 6]. Hence α acts on the same space as multiplication by two. (Indeed, if it were multiplication by (-2), for a sufficiently large power of α the right-hand side of (3.9) would be negative.) Hence, α^n acts as multiplication by 2^n. Thus $\operatorname{tr}(\alpha^n \mid H_c^4(U, \overline{\mathbb{Q}}_\ell)) = 2^n$.

On the other hand, according to Deligne [Del81, Theorem 1] for every eigenvalue α_{ij} of Fr acting on $H_c^i(U, \overline{\mathbb{Q}}_\ell)$ we have $|\alpha_{ij}| \leqslant 2^{i/2}$. This yields similar inequalities for the eigenvalues β_{ij} of α: $|\beta_{ij}| \leqslant 2^{i/4}$ and the eigenvalues $\beta_{ij,n}$ of α^n: $|\beta_{ij,n}| \leqslant 2^{ni/4}$. We thus obtain

$$|\operatorname{tr}(\alpha^n \mid H_c^3(U, \overline{\mathbb{Q}}_\ell))| \leqslant b^1(U)2^{3n/4}, \quad |\operatorname{tr}(\alpha^n \mid H_c^2(U, \overline{\mathbb{Q}}_\ell))| \leqslant b^2(U)2^{n/2}.$$

This proves the theorem. □

Remark 3.9. One can probably get another proof of Proposition 3.8 (and hence Theorem 3.6) using an approach of [DL76]. In that paper the Lefschetz trace formula is established for any endomorphism of finite order. A remark in [DL76, § 11] (see also [SGA4, Sommes trig., 8.2, p. 231]) says that the results of the paper can be extended to the case of an endomorphism α with the property $\alpha^2 = \mathrm{Fr}$.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

3.4 Estimates of Betti numbers

As in the previous section, we assume that the ground field is $k = \bar{\mathbb{F}}_2$.

Recall that the singular locus of the variety V' is contained in the set $S = V' \cap \mathbf{V}(xc)$ (see § 3.2). As before, we denote $U = V' \setminus S$; it is a smooth irreducible affine variety invariant under the morphism α. Our aim is to estimate $b^1(U)$ and $b^2(U)$.

First we deal with $b^1(U)$. We want to use the Lefschetz theorem on hyperplane sections. For technical reasons we want to use hyperplanes of special type, namely those defined by equations $\alpha a + \beta c + \gamma = 0$. These hyperplane sections are not general, and in order to apply the Lefschetz theorem, we have to provide a quasifinite map of the surface V' onto $\mathbb{A}^2$ with coordinates a, c.

The next step is to estimate the Euler characteristic of U. To do this, we represent U as the union of an open subset U' and a finite number of curves. We estimate the Euler characteristics of these curves and of U' separately, using the fact that U' is a double cover of a simpler variety. Having in hand bounds for $b^1(U)$ and $\chi(U)$, we estimate $b^2(U)$.

Proposition 3.10. *A regular map $\pi\colon \mathbb{A}^8 \to \mathbb{A}^2$ defined as $\pi(a,b,c,d,v,w,x,y) = (a,c)$ is quasi-finite on U.*

Proof. Consider the variety $\widetilde{W}$ defined in $\mathbb{A}^8$ by equations $J3[1-6]$.

We have $\widetilde{W} \supset V'$ and $\widetilde{W} \setminus V' \subset \mathbf{V}(f) \subseteq \mathbb{A}^8$, where

$$f(a,c) = c(ac+1)a(a+c)(c+1)(a^3 + a^2c^3 + a^2c + ac^4 + ac^2 + c)$$

(see § 3.2). This means that the coordinates of any point of V' (and, in particular, of U), satisfy the equations $J[1-10]$. If $f(a,c) \neq 0$, the equation $J3[1]$ provides at most six different possible values for v. The equation $J3[2]$ implies that for each of these six values only one value of x is possible. The equation $J3[3]$ gives at most two values for d, and all of the proceeding equations provide one value for b, y and w. Hence, for any point $(a,c) \in \mathbb{A}^2$ with $f(a,c) \neq 0$, the preimage $\pi^{-1}(a,c)$ is finite in V' and hence in U.

Now let $A = \mathbf{V}(f) \subset \mathbb{A}^2$. Then $\pi^{-1}(A) \cap U = \bigcup A_i$, $i = 1, \ldots, 6$, which may be described as follows.

(1) $A_1 = U \cap \mathbf{V}(c+1)$.

According to calculations, $A_1 = A_1^1 \cup A_1^2$, where $A_1^1 = U \cap \mathbf{V}(c+1) \cap \mathbf{D}(a(a+1)(a^2+a+1))$ and $A_1^2 = U \cap \mathbf{V}(c-1, a(a+1)(a^2+a+1))$.

The equations defining A_1^1 show that for a fixed value of a, if $a(a+1)(a^2+a+1) \neq 0$, there are at most four points in $U \cap \pi^{-1}(a,1)$. The equations defining A_1^2 show that $\pi^{-1}(1,1) = \emptyset$; $\pi^{-1}(0,1) = \emptyset$; $\pi^{-1}(a_0,1)$, where a_0 is a root of a^2+a+1, consists of two points.

(2) $A_2 = U \cap \mathbf{V}(c) = \emptyset$.

(3) $A_3 = U \cap \mathbf{V}(a) = \emptyset$.

(4) $A_4 = U \cap \mathbf{V}(a+c) = \emptyset$.

(5) $A_5 = U \cap \mathbf{V}(ac+1) = A_5^1 \cup A_5^2$.

Here $A_5^1 = U \cap \mathbf{V}(ac+1) \cap \mathbf{D}((a^2+a+1)(a+1)a)$ and $A_5^2 = U \cap \mathbf{V}((ac+1), (a+1)(a^2+a+1)a)$. The equations for A_5^1 show that for any point $a \neq 0, 1$, or a_0 (a root of a^2+a+1), the set $\pi^{-1}(a, 1/a)$ contains at most four points. The set A_5^2 consists of four points only.

(6) $A_6 = U \cap \mathbf{V}(h_1)$, where $h_1(a,c) = a^3 + a^2c^3 + a^2c + ac^4 + ac^2 + c$.
$A_6 = A_6^1 \cup A_6^2 \cup A_6^3$, where
$A_6^1 = U \cap \mathbf{V}(h_1) \cap \mathbf{D}(v^2 + ac^3 + c^2 + a^2, a(a+1)(a^2+a+1))$;
$A_6^2 = U \cap \mathbf{V}(h_1, v^2 + ac^3 + c^2 + a^2) \cap \mathbf{D}(a(a+1)(a^2+a+1))$;
$A_6^3 = U \cap \mathbf{V}(h_1, v^2 + ac^3 + c^2 + a^2, a(a+1)(a^2+a+1))$.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

The equations for A_6^1 show that each point (a, c) satisfying $f(a, c) = 0$, $v^2 + ac^3 + c^2 + a^2 \neq 0$ and $a(a + 1)(a^2 + a + 1) \neq 0$ has at most four preimages in U_1. In case of the set A_6^2 the preimage of each point also contains at most four points. The set A_6^3 consists of 54 points.

Thus, any point in $\mathbb{A}^2$ has a finite (maybe, empty) preimage. Hence, π is quasi-finite. □

Further on we shall consider the following sets: $V' \subset \mathbb{A}^8$, defined by the ideal J; $\widetilde{W} \subset \mathbb{A}^8$, defined by the ideal J3; $U = V' \setminus \mathbf{V}(xc) \subset \mathbb{A}^8$; $U' = V' \setminus \mathbf{V}(f) \subset \mathbb{A}^8$; $W \subset \mathbb{A}^4$ with coordinates (a, c, v, x), defined by the ideal $\langle \text{J3}(1), \text{J3}(2) \rangle$; $L = W \cap \mathbf{V}(f) \subset \mathbb{A}^4$; $Z = W \setminus L \subset \mathbb{A}^4$; $Y = \mathbf{V}(J3[1]) \cap \mathbf{D}(f) \subset A^3$ with coordinates (a, c, v).

These affine sets are included in the following diagram.

$$\begin{array}{ccccccc} \widetilde{W} & \supset & V' & \supset & U & \supset & U' \\ \downarrow{\scriptstyle \pi_1} & & & & & & \downarrow{\scriptstyle \pi_1} \\ W & & & \supset & & & Z \\ & & & & & & \downarrow{\scriptstyle \pi_2} \\ & & & & & & Y \end{array}$$

The inclusion $U \supset U'$ follows from computations: we have $V' \cap \mathbf{V}(x) \subset \mathbf{V}(f) \cap V'$. The map $\pi_1 \colon U' \to Z$ is a double unramified cover. This follows from the structure of equations $J3[1], \ldots, J3[6]$: all the branch points are contained in the set $\mathbf{V}(f)$. The map π_2 is an isomorphism as x appears linearly in the equation $J3[2]$ and its coefficient does not vanish in U'.

PROPOSITION 3.11. *We have* $b^1(U) \leqslant 675$.

Proof. This estimate follows from the Weak Lefschetz Theorem proved by Katz [Kat93, Corollary 3.4.1]. Indeed, we have:

- an algebraically closed field of characteristic $2 \leqslant \ell$;
- U, a separated k-scheme of finite type which is a local complete intersection, purely of dimension $2 > 0$
- $U \to \mathbb{A}^2$, a quasi-finite morphism (see Proposition 3.10).

Then, for a constant $\mathbb{Q}_\ell$-sheaf $\mathcal{F}$ on U, there exists a dense open set $\mathcal{U} \subset \mathbb{A}^3$ such that for any $(\alpha, \beta, \gamma) \in \mathcal{U}$ the restriction map

$$H^1(U, \mathcal{F}) \to H^1(U \cap \{\alpha a + \beta c + \gamma = 0\}, i^*\mathcal{F})$$

is injective (i denotes the embedding of the hyperplane section into U).

Denote:

$$\begin{aligned} S_1 &= U \cap \mathbf{V}(\alpha a + \beta c + \gamma); \\ \widetilde{S} &= S_1 \cap U' = U' \cap \mathbf{V}(\alpha a + \beta c + \gamma) \subset S_1; \\ S &= Y \cap \mathbf{V}(\alpha a + \beta c + \gamma) \subset Y. \end{aligned}$$

As U' is a double unramified cover of Y, $\widetilde{S}$ is a double unramified cover of S. The curve S is defined in $\mathbb{A}^3$ with coordinates (a, c, v) by $\mathbf{V}(J3[1], \alpha a + \beta c + \gamma) \cap \mathbf{D}(f)$.

Let $\overline{S}$ be the projectivisation of S in $\mathbb{P}^3$. For a general triple (α, β, γ) it is an irreducible complete intersection of degree $d = 14$. By [GL02, Corollary 7.4], we have

$$b^1(\overline{S}) \leqslant (d - 1)(d - 2) \leqslant 156.$$

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Let B be the union of the plane at infinity with the closure of the set $\mathbf{V}((\alpha a+\beta c+\gamma)f(a,c))$. As $\deg f = 11$, we have $\deg B = 13$. Thus, $\overline{S}\cap B$ contains at most $14\times 13 = 182$ points. Hence, $b^1(S)\leqslant 156+182 = 338$. As $\widetilde{S}$ is a double unramified cover of S, $b^1(\widetilde{S}) = 2b^1(S)-1\leqslant 675$. As $\widetilde{S}\subset S_1$, $b^1(S_1)\leqslant b^1(\widetilde{S})\leqslant 675$. □

Proposition 3.12. *The Euler characteristic of L satisfies $\chi(L)\leqslant 71\,430 < 2^{17}$.*

Proof. The set $L = W\cap \mathbf{V}(f)$ consists of several components. According to computations, the list of components is as follows:

$$\begin{aligned}
&F_1 = \mathbf{V}(a,c); && \dim F_1 = 2, \quad \chi(F_1) = 1\\
&F_2 = \mathbf{V}(v,c); && \dim F_2 = 2, \quad \chi(F_2) = 1\\
&F_3 = \mathbf{V}(v-1,c); && \dim F_3 = 2, \quad \chi(F_3) = 1\\
&F_4 = \mathbf{V}(a-1,c-1); && \dim F_4 = 2, \quad \chi(F_4) = 1\\
&E = \mathbf{V}(ac-1,v); && \dim E = 2, \quad \chi(E) = 0\\
&G = \mathbf{V}(ac-1, av^2+c^2+av+cv+v^2+v), && \dim G = 2, \quad \chi(G) = -3\\
&C_1 = \mathbf{V}(x,a,c^2+cv+1), && \dim C_1 = 1, \quad \chi(C_1) = 0\\
&C_2 = \mathbf{V}(c-1,v,x), && \dim C_2 = 1, \quad \chi(C_2) = 1\\
&C_3 = \mathbf{V}(I_3), && \dim C_3 = 1,\\
&H_1 = \mathbf{V}(I_1), && \dim H_1 = 2,\\
&H_2 = \mathbf{V}(I_2), && \dim H_2 = 2,
\end{aligned}$$

where

$$\begin{aligned}
I_3 = \langle & c-1, a^2v^2x+a^2v+v^2x+av+ax+v+x, a^4x^2+a^2vx^3+a^3v^2+a^3x^2+a^4+a^2vx+vx^3\\
&+avx+ax^2+a^2+vx+1, av^2x^4+v^5x+v^4x^2+v^2x^4+av^4+avx^3+v^4+a^2vx+a^2x^2\\
&+vx^3+x^4+avx+vx+x^2\rangle,
\end{aligned}$$

$$I_1 = \langle c^3+c^2v+c^2+av+cv+v^2, acv+ac+c^2+av+v^2+a+c+v, a^2v+a^2+ac+cv+v^2+c\rangle,$$

and

$$\begin{aligned}
I_2 = \langle & ac^2v+c^3v+c^3+c^2v+av^2+cv^2+cv+a, c^4+acv+c^2v+ac+cv+v+1, a^3v^2+a^2v^3+acv^3\\
&+c^3v+a^2v^2+acv^2+cv^2\rangle.
\end{aligned}$$

Let us explain how the Euler characteristics were computed. We have $\chi(F_i) = 1, i = 1,\dots,4$ because the F_i are just affine spaces. The component E is isomorphic to $(\mathbb{A}^1\setminus\{0\})$ with coordinates a and x respectively, so $\chi(E) = 1\cdot(1-1) = 0$. The component G is the direct product of $\mathbb{A}^1$ with coordinate x and a curve T which is a ramified covering of $\mathbb{A}^1$ with coordinate a. For a fixed point (a,c,v) in T we have $c = 1/a$, and v is defined by the quadratic equation

$$v^2(a^3+a)+v(a^3+a^2+a)+1 = 0.$$

It follows that if $a\neq 0, a\neq 1, a^2+a+1\neq 0$, there are precisely two points in T with this value of a. There are no points with $a = 0$ and precisely one point for each value $a = 1$ or $a^2+a+1 = 0$. As the Euler characteristics of $\mathbb{A}^1$ without four points is -3, we have $\chi(G) = 2(-3)+3 = -3$.

The curve C_1 is isomorphic to $\mathbb{A}^1\setminus\{0\}$ with coordinate c: $v = (1+c^2)/c$, $\chi(\mathbb{A}^1\setminus\{0\}) = 0$.

The curve C_2 is $\mathbb{A}^1$, $\chi(\mathbb{A}^1) = 1$.

In order to estimate the Euler characteristics of C_3, H_1, H_2, we use the following theorem of Adolphson and Sperber.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

PROPOSITION 3.13 (see [AS88, Theorem 5.27] and [Kat01]). *If an affine variety V is defined in $\mathbb{A}^N$ by r polynomial equations all of degree $\leqslant d$, then*

$$|\chi(V)| \leqslant 2^r D_{N,r} \underbrace{(1, 1+d, \dots, 1+d)}_{r+1}, \tag{3.10}$$

where $D_{N,r}(x_0, \dots, x_r) = \sum_{|W|=N} X^W$ is the homogeneous form of degree N in $x_0, \dots, x_r$ all of whose coefficients equal 1.

According to formula (3.10),

$$|\chi(C_3)| \leqslant 2^3 D_{3,3}(1,8,8,8) \leqslant 44\,232 < 2^{16}$$
$$|\chi(H_1)| \leqslant 2^3 D_{3,3}(1,4,4,4) \leqslant 5992 < 2^{13}$$
$$|\chi(H_2)| \leqslant 2^3 D_{3,3}(1,6,6,6) \leqslant 19\,160 < 2^{15}.$$

The pairwise intersection of these components is a union of 16 lines and 10 points. The triple intersections contain three lines and three points. No four of these components intersect. Thus, $|\chi(L)| \leqslant 5 + 3 + 44\,232 + 5992 + 21\,224 + 26 + 6 = 71\,488 < 2^{17}$. □

PROPOSITION 3.14. *We have $b^2(U) \leqslant 2^{22}$.*

Proof. We consider the following two cases.

(I) $\chi(U) \leqslant 0$. Then $1 - b^1(U) + b^2(U) \leqslant 0$ and $b^2(U) \leqslant b^1(U) < 675$.

(II) $\chi(U) > 0$. We first find $|\chi(U')|$. As U' is a double cover of Z, we have $|\chi(U')| = 2|\chi(Z)|$. As $Z = W \setminus L$, we have $\chi(Z) = \chi(W) - \chi(L)$. By formula (3.10), we get $|\chi(W)| \leqslant 2^2 D_{4,2}(1, 15, 15) \leqslant 1\,069\,324$. In view of Proposition 3.12, we have $|\chi(L)| \leqslant 71\,488$. Hence, $|\chi(Z)| \leqslant |\chi(W)| + |\chi(L)| \leqslant 1\,140\,812$, and therefore $|\chi(U')| \leqslant 2\,281\,624 < 2^{22}$. On the other hand, $\chi(U) = \chi(U') + \chi(U \setminus U')$. In order to find $\chi(U)$, we have to evaluate $\chi(U \setminus U')$. Let $N = U \bigcap \mathbf{V}(f)$. As N is the intersection of the smooth affine surface U with the hypersurface $\mathbf{V}(f)$, all of its irreducible components N_i are curves (that is, $\dim N_i = 1$). This follows from [Sha94, Theorem 5, p.74], and is confirmed by calculations. As by Proposition 3.10, the projection $\pi\colon U \to \mathbb{A}^2$ is quasi-finite, none of N_i is mapped into a point. Hence, $\pi(N_i) \subset \mathbb{A}^2$ is a curve. This curve does not meet the lines $\mathbf{V}(c)$ and $\mathbf{V}(a)$ because $\mathbf{V}(a) \cap U = \emptyset$. This means that the ring $O(\pi(N_i))$ contains the non-vanishing function ac. If $ac =$ constant on $\pi(N_i)$, then $\pi(N_i)$ has two punctures at infinity. If $ac \neq$ constant, then the normalisation of $\pi(N_i)$ has at least two punctures, as does any curve having a non-constant and non-vanishing regular function. Thus, $\chi(\pi(N_i)) \leqslant 0$.

Let k denote the degree of the map $N_i \to \pi(N_i)$. By Hurwitz's formula, $\chi(N_i) = k\chi(\pi(N_i)) - s$, where $s \geqslant 0$ is the branching number. It follows that

$$\chi(N_i) \leqslant k\chi(\pi(N_i)) \leqslant 0.$$

It follows that

$$\chi\Big(\bigcup N_i\Big) = \sum \chi(N_i) - T,$$

where $T = \sum_{x \in \bigcup N_i} (k(x) - 1) \geqslant 0$, and $k(x)$ stands for the multiplicity of a point $x \in \bigcup N_i$. Hence,

$$\chi\Big(\bigcup N_i\Big) = \chi(N) \leqslant 0;$$
$$\chi(U) = \chi(U') + \chi(N) \leqslant \chi(U') \leqslant 2\,281\,624,$$

and, therefore,

$$b^2(U) = \chi(U) + b^1(U) \leqslant 2\,282\,299 < 2^{22}.$$ □

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Corollary 3.15. *Let $n > 48$, $q = 2^n$. Then V_n has an $\mathbb{F}_q$-point.*

Proof. On plugging the estimates of Propositions 3.11 and 3.14 into formula (3.3), we see that $\#\operatorname{Fix}(U, n) > 0$ as soon as $n > 48$. This proves the corollary. □

3.5 Small fields

The purpose of this section is to give some information concerning the fixed points and also numbers of fixed points of the operator α^n on the variety V' given by the equations $J[1], \dots, J[10]$. Let k denote the algebraic closure of $\mathbb{F}_2$ and N_n the number of fixed points of α^n on $V'(k)$. As explained before, if n is even ($n = 2k$) then N_n is just the number of points of V' in the field $\mathbb{F}_{2^k}$.

The zeta-function $Z(\alpha, T)$ of the operator α is defined as in Remark 1.12. It is known to be a rational function. By a computer calculation using MAGMA we have shown the following.

Proposition 3.16. *The power series $Z(\alpha, T)$ agrees with*

$$(1-2T)(1-T)(1-T^2)^5(1+T^2)^2(2T^4+2T^2+1)(4T^8+2T^4+1)(2T^2+2T+1)(8T^6+4T^5+T+1)$$

up to terms of degree 32.

Note that the absolute values of the zeros of this polynomial are equal to 1, $1/2$, $1/\sqrt{2}$, or $1/\sqrt[4]{2}$, as general theory predicts. The above formula implies the statement in Remark 1.12 above.

The data encoded in the approximate formula for $Z(\alpha, T)$ are not enough to close the gap between Corollary 3.15 and Theorem 1.2. However, we have used our method of computation to exhibit, for each $3 \leqslant p \leqslant 47$, a fixed point of α^p acting on $V'(k)$. With these data at hand we have finished the proof of Theorem 1.1.

Acknowledgements

We are grateful to N. Gordeev, D. Grayson, L. Illusie, A. Lubotzky, A. Mann, S. Margolis, R. Pink, J. Piontkowski, L. Rowen, D. Segal, Y. Segev, J-P. Serre, M. Stoll, Y. Varshavsky, and N. Vavilov for useful comments and advice. We thank D. Nikolova and R. Shklyar for help in computer experiments and H. Schönemann for extending the functionality of the Singular kernel. Our special thanks go to B. Plotkin for numerous enlightening, encouraging, and inspiring discussions.

Appendix

A.1 A variant of Zorn's theorem

In this appendix we prove the following.

Proposition A.1. *Let G be a finite group, and let $w = w(x, y)$ be a word in two variables such that:*

(1) *if $w(x, y) \equiv 1$ in G then $G = \{1\}$;*
(2) *the words x and $w(x, y)$ generate the free group $F_2 = \langle x, y\rangle$. Then G is nilpotent if and only if it satisfies one of the identities $[w(x, y), x, x, \dots, x] = 1$.*

Proof. Necessity. Let G be a nilpotent group of class n. As the element $e_n(x, y) = [w(x, y), x, \dots, x]$ lies in the nth term of the invariant series, $e_n(x, y)$ is an identity.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Sufficiency. We want to prove that any G satisfying the identity $e_n(x,y) \equiv 1$ for some n is nilpotent. Assume the contrary.

Suppose that $n = 1$. Then according to assumption (1) of the proposition, the group G is trivial. Let $n > 1$. Let Γ denote a minimal counterexample, that is, a non-nilpotent group of the smallest order satisfying the identity $e_n(x,y) \equiv 1$. Obviously, all subgroups of Γ are nilpotent. Then Γ is a Schmidt group, that is, a non-nilpotent group all of whose proper subgroups are nilpotent (see [Sch24, Red56] for the description of these groups). In particular, the commutator subgroup Γ' is the unique maximal Sylow subgroup in Γ. As Γ' is nilpotent, it contains a non-trivial centre $Z(\Gamma')$. Take a non-trivial $a \in Z(\Gamma')$. For any element $x \notin \Gamma'$ there exists $y \in G$ such that $w(x,y) = a$ (condition (2)). Consider the sequence $[a,x,x,\dots,x] = [w(x,y),x,x,\dots,x] = e_n(x,y)$. There exists n such that $[w(x,y),x,x,\dots,x] \equiv 1$. Let n denote the smallest number satisfying this equality, and let $b = [w(x,y),x,x,\dots,x] = e_{n-1}(x,y)$. Clearly, $b \in Z(\Gamma')$. Moreover, $[b,x] = e_n(x,y) = 1$ and hence b is a non-trivial element from $Z(\Gamma)$. Take $\bar{\Gamma} = \Gamma/Z(\Gamma)$. Then the order of $\bar{\Gamma}$ is less than the order of Γ, hence $\bar{\Gamma}$ is nilpotent. Therefore Γ is nilpotent. As $e_n(x,y)$ is an identity in Γ, we get a contradiction.

The proposition is proved. □

A.2 Pro-finite setting

A.2.1 *Pseudo-varieties of finite groups.* A *variety* of groups is a class C of groups defined by some set of identities T (that is, $G \in C$ if and only if for every $u \in T$ the identity u holds in G). Birkhoff's theorem says that C is a variety if and only if C is closed under taking subgroups, homomorphic images, and direct products. To work with classes of finite groups (which cannot be closed under taking infinite direct products), one needs a more general notion.

DEFINITION A.2. A *pseudo-variety* of groups is a class of groups closed under taking subgroups, homomorphic images, and *finite* direct products.

By Birkhoff's theorem every variety of groups is a pseudo-variety. We are interested in pseudo-varieties of all finite groups, all finite solvable groups, and all finite nilpotent groups.

Let $F = F(X^0)$ be a free group with countable set of generators X^0. Consider a sequence of words $u = u_1, u_2, \dots, u_n, \dots$ in F. The sequence u determines a class of groups V_u by the following rule: a group G belongs to V_u if and only if almost all elements u are identities in G. The class V_u is a pseudo-variety. It turns out that this construction is universal.

THEOREM A.3 [ES76]. *For every pseudo-variety of finite groups V there exists a sequence of elements $u\colon \mathbb{N} \to F$, $u = u_1, u_2, \dots, u_n, \dots$ such that $V = V_u$.*

We shall consider a special class of sequences.

DEFINITION A.4. Let X be a finite set. We say that a sequence of elements (not necessarily distinct) $u = u_1, u_2, \dots, u_n, \dots$ of the free group $F(X)$ is *correct* if given any group G, as soon as an identity $u_n \equiv 1$ holds in G, for all $m > n$ the identities $u_m \equiv 1$ also hold in G.

As above, a correct sequence u defines a pseudo-variety of groups V by the rule: $G \in V$ if and only if some identity $u_n \equiv 1$, $u_n \in u$, holds in G.

Remark A.5. If u is a correct sequence defining a pseudo-variety V and v is a subsequence of u, then v is also correct and defines the same pseudo-variety V.

Let $F = F(x,y)$ and

$$e_1 = [x,y], \quad e_{n+1} = [e_n, y\,], \dots \tag{A.1}$$

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

This sequence is correct and defines the pseudo-variety of all finite Engel groups. According to Zorn's theorem [Zor36], this pseudo-variety coincides with the pseudo-variety of all finite nilpotent groups.

Our main sequence of quasi-Engel words

$$u_1 = w = x^{-2}y^{-1}x, \quad u_{n+1} = [xu_nx^{-1}, yu_ny^{-1}], \dots \tag{A.2}$$

is also correct, and according to Theorem 1.1 it defines the pseudo-variety of all finite solvable groups.

A.2.2 *Residually finite groups.*

Definition A.6. We say that a group G is *residually finite* if the intersection of all its normal subgroups of finite index H_α, $\alpha \in I$, is trivial.

Define a partial order on the set I by: $\alpha < \beta$ if and only if $H_\beta \subset H_\alpha$. The intersection of two normal subgroups of finite index is also of finite index, and therefore for every $\alpha, \beta \in I$ there is $\gamma \in I$ such that $\alpha < \gamma$, $\beta < \gamma$. Thus, the set I is directed.

Denote $G_\alpha = G/H_\alpha$. If $\alpha < \beta$ then there is a natural homomorphism $\varphi_\alpha^\beta : G_\beta \to G_\alpha$. If gH_β is an element of G_β then its image in G_α is gH_α. Let $\bar{G}$ be the direct product of all G_α. Then there is an embedding $G \to \bar{G}$ which associates to each $g \in G$ the element $\bar{g} = (gH_\alpha)_{\alpha \in I}$. Hence, G can be approximated by finite groups G_α, that is, if f, g are distinct elements of G, then there is α such that $\bar{f}_\alpha$ and $\bar{g}_\alpha$ are distinct elements of G_α.

A group G is regarded as a topological group, with the topology defined by the system of neighbourhoods of 1 consisting of all normal subgroups of finite index H_α. The system of neighbourhoods of an element $g \in G$ is given by the cosets gH_α. The group $\bar{G}$ is also a topological group. To define the topology, consider the projections $\pi_\alpha \colon \bar{G} \to G_\alpha$. Let $\ker \pi_\alpha = U_\alpha$. Then $\bar{G}/U_\alpha$ is isomorphic to $G_\alpha = G/H_\alpha$. For every $g \in G$ the element $\bar{g}$ lies in U_α if and only if $g \in H_\alpha$. The system of neighbourhoods of 1 in $\bar{G}$ consists of all finite intersections of normal subgroups U_α. This defines the Tikhonov topology on $\bar{G}$. As all groups G_α are finite, the group $\bar{G}$ is compact.

Let $g_1, \dots, g_n, \dots$ be a sequence of elements of G. As usual, we say that this sequence tends to 1 if for every neighbourhood H_α there exists a natural number $N = N(\alpha)$ such that for all $n > N$ the element g_n lies in H_α.

Definition A.7. Let $F = F(X)$ be a free group. We say that a sequence $u = u_1, \dots, u_n, \dots$ of elements of F *identically converges to 1* in a group G if for any homomorphism $\mu \colon F \to G$ the sequence $\mu(u) = \mu(u_1), \dots, \mu(u_n), \dots$ tends to 1 in G. In this case we write $u \equiv 1$ in G.

Proposition A.8. *Let X be a finite set. If a sequence $u_1, \dots, u_n, \dots$ identically converges to 1 in G then for every neighbourhood H_α there exists $N = N(\alpha)$ such that all $u_n, n > N$, are identities of the group G/H_α.*

Proof. Take a homomorphism $\mu \colon F \to G$, and let $\mu^0 \colon G \to G/H_\alpha$ be the natural projection. Then $\nu = \mu^0\mu$ is a homomorphism $F \to G/H_\alpha$, and every homomorphism $\nu \colon F \to G/H_\alpha$ can be represented in this way. As both G/H_α and X are finite, the set of different ν is also finite. Denote them by $\{\nu_1, \dots, \nu_k\}$.

Define an equivalence relation on the set of all homomorphisms $\mu \colon F \to G$ by $\mu_1 \equiv \mu_2$ if $\mu^0\mu_1 = \mu^0\mu_2$. For an arbitrary $u \in F$ we have $\mu(u) \in H_\alpha$ if and only if $\mu^0\mu(u) = 1$. Thus, if $\mu_1 \equiv \mu_2$, then for every $u \in F$ we have $\mu_1(u) \in H_\alpha$ if and only if $\mu_2(u) \in H_\alpha$. Indeed, let $\mu_1(u) \in H_\alpha$. Then $\mu^0\mu_1(u) = 1 = \mu^0\mu_2(u) = 1$, and $\mu_2(u) \in H_\alpha$.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

For every ν_i, $i = 1, \dots, k$ take μ_i such that $\mu^0 \mu_i = \nu_i$. Consider the equivalence classes $[\mu_1], \dots, [\mu_k]$. Each $\mu\colon F \to G$ belongs to one of these classes. As the sequence $u_1, \dots, u_n, \dots$ identically converges to 1 in G, for every $\mu\colon F \to G$ there exists $N = N(\alpha, \mu)$ such that $\mu(u_n) \in H_\alpha$ for $n > N$. Let N_0 be the maximum of $N(\alpha, \mu_i)$, $i = 1, \dots, k$. If $n > N_0$, then $\mu_i(u_n) \in H_\alpha$ for every μ_i. As every μ is equivalent to some μ_i, we have $\mu(u_n) \in H_\alpha$ for every μ. This means that $\nu(u_n) = 1$ for every $\nu : F \to G/H_\alpha$. Thus the element u_n defines an identity of the group G/H_α. □

A.2.3 *Pro-finite groups.* We now focus on pro-finite groups, with a goal to establish a relationship with pseudo-varieties and give another reformulation of our main result. Generalities on pro-finite groups can be found in [RZ00, Alm94], etc. We recall here some basic notions.

Let V be a pseudo-variety of finite groups. Given a group G, consider all its normal subgroups of finite index H_α such that $G/H_\alpha = G_\alpha \in V$. If the intersection of all these H_α is trivial, we say that G is a *residually V-group*. This is a topological group with V-topology (the subgroups H_α as above are taken as the neighbourhoods of 1).

Let $\bar{G}$ be the direct product of all G_α. Denote by $\widehat{G}$ a subgroup in $\bar{G}$ defined as follows: an element $f \in \bar{G}$ belongs to $\widehat{G}$ if and only if for every α and β such that $H_\beta \subset H_\alpha$ the equality $\varphi_\alpha^\beta(f_\beta) = f_\alpha$ holds. Denote $f_\alpha = g_\alpha H_\alpha$. Then

$$\varphi_\alpha^\beta(g_\beta H_\beta) = g_\alpha H_\alpha = g_\beta H_\alpha.$$

Recall that φ_α^β are natural homomorphisms.

The group $\widehat{G}$ turns out to be the completion of G in its V-topology [ES52].

Such a group $\widehat{G}$ is called a *pro-V-group*. If V is the pseudo-variety of all finite groups, $\widehat{G}$ is called *a pro-finite group*. Thus, in the class of all pro-finite groups one can distinguish subclasses related to particular pseudo-varieties V.

A free group $F = F(X)$ is residually finite. Take all normal subgroups of finite index in F. They define the pro-finite topology in F. Denote by $\widehat{F}$ the completion of F in this topology. This group is a free pro-finite group (see, for example, [RZ00]).

Indeed, if $\widehat{G}$ is the pro-finite completion of an arbitrary residually finite group G, then every map $\mu\colon X \to \widehat{G}$ induces a homomorphism $\mu\colon F \to \widehat{G}$ which turns out to be a continuous homomorphism of topological groups and therefore induces a continuous homomorphism $\hat{\mu}\colon \widehat{F} \to \widehat{G}$.

Another approach to free pro-finite groups is based on the idea of implicit operations (cf. [Alm94, Alm02, AV01, MSW01, Wei02], etc.). This approach has a lot of advantages but we do not use it as it needs additional notions which are not necessary for our aims.

Definition A.9. Let $f \in \widehat{F}$. The expression $f \equiv 1$ is called a *pro-finite identity* of a pro-finite group $\widehat{G}$ if for every continuous homomorphism $\widehat{\mu}\colon \widehat{F} \to \widehat{G}$ we have $\widehat{\mu}(f) = 1$.

Definition A.10. (See also [AV01, Alm94]). A variety of pro-finite groups (for brevity, a *pro-variety*) is a class of pro-finite groups defined by some set of pro-finite identities.

An analogue of Birkhoff's theorem for pro-finite groups says that a class of pro-finite groups is a pro-variety if and only if it is closed under taking closed subgroups, images under continuous homomorphisms, and direct products. This implies that for an arbitrary pseudo-variety V of finite groups, the class of all pro-V-groups is a pro-variety. The converse statement is also true. For any pro-variety C there exists a pseudo-variety of finite groups V such that the class of all pro-V-groups coincides with C. In the case where V is a correct pseudo-variety of finite groups (that is, is defined by a correct sequence), one can construct identities defining the pro-variety of pro-V-groups in an explicit form.

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

Let X be a finite set. Let $u = u_1, \dots, u_n, \dots$ be a sequence of elements of a free group $F = F(X)$. As $\widehat{F}$ is a compact group, there exists a convergent subsequence $v = v_1, \dots, v_m, \dots$ of u.

Proposition A.11. *Let $v = v_1, v_2, \dots, v_n, \dots$ be a convergent sequence of elements of F with $\lim \bar{v}_n = f$. Let $\widehat{G}$ be a pro-finite group. Then the identity $f \equiv 1$ holds in $\widehat{G}$ if and only if $v \equiv 1$ in G (that is, v identically converges to 1 in G, see Definition A.7).*

Proof. First of all the sequence $\bar{g}_1, \dots, \bar{g}_n, \dots$ converges to 1 in $\widehat{G}$ if and only if $g_1, \dots, g_n, \dots$ converges to 1 in G.

Let the identity $f \equiv 1$ be fulfilled in $\widehat{G}$. Then

$$\widehat{\mu}(f) = \lim \widehat{\mu}(\bar{v}_n) = \lim \overline{\mu(v_n)} = 1.$$

Thus, $\lim \mu(v_n) = 1$ in G. This means that $v \equiv 1$ in G. Conversely, let $v \equiv 1$ in G. Then for every $\mu\colon F \to G$ the sequence $\mu(v)$ converges to 1 in G. The sequence $\overline{\mu(v)}$ converges to 1 in $\widehat{G}$. Using

$$\lim \widehat{\mu}(\bar{v}_n) = \lim \overline{\mu(v_n)} = 1 = \widehat{\mu}(f),$$

we conclude that $\widehat{\mu}(f) = 1$ for arbitrary μ. This means that the identity $f \equiv 1$ holds in $\widehat{G}$. □

Let V be a pseudo–variety of finite groups defined by a correct sequence $u = u_1, u_2, \dots, u_n, \dots$, and let $v = v_1, v_2, \dots, v_n, \dots$ be a convergent subsequence of u. Denote the limit of v by f. As u is a correct sequence, v determines the same class V as u.

Theorem A.12. *With the above notation, the class of all pro-V-groups is the pro-variety defined by the pro-finite identity $f \equiv 1$.*

Proof. Let the pro-finite identity $f \equiv 1$ hold in a pro-finite group $\widehat{G}$. Then by Proposition A.11, $v \equiv 1$ in G. Proposition A.8 implies that for every neighbourhood H in G and all sufficiently large n the identity $v_n \equiv 1$ holds in G/H. This means that G/H lies in V and $\widehat{G}$ is a pro-V-group.

Conversely, let G/H lie in V. By the definition of V, this means that v identically converges to 1 in G. Therefore, the identity $f \equiv 1$ holds in $\widehat{G}$. □

Remark A.13. Although all convergent subsequences of a correct sequence define the same pseudo-variety, their limits may be different. For example, consider a correct sequence of the form $u = v_1, av_1a^{-1}, v_2, av_2a^{-1}, \dots, v_n, av_na^{-1}, \dots$, where $a \in F$ and $v = v_1, v_2, \dots, v_n, \dots$ is a correct convergent sequence. If the limit of the subsequence v is f, we get a new convergent subsequence $v' = av_1a^{-1}, av_2a^{-1}, \dots, av_na^{-1}, \dots$ with limit afa^{-1}. However, the elements f and afa^{-1} define the same variety.

Corollary A.14. *Let $F = F(x, y)$, and let u_n be defined by*

$$u_1 = w, \quad u_{n+1} = [u_n, y], \dots \tag{A.3}$$

where $w = [x, y]$ or w is any word satisfying the conditions the hypotheses of Proposition A.1.

Let $v_1, v_2, \dots, v_m, \dots$ be any convergent subsequence of (A.3) with limit f from $\widehat{F}$. Then the identity $f \equiv 1$ defines the pro-finite variety of pro-nilpotent groups.

Proof. The corollary immediately follows from Proposition A.1, Zorn's theorem, and Theorem A.12. □

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

THEOREM A.15. *Let $F = F(x, y)$, let*

$$u_1 = w = x^{-2}yx^{-1}, \quad u_{n+1} = [xu_nx^{-1}, yu_ny^{-1}], \dots \tag{A.4}$$

be our main sequence, and let $v_1, v_2, \dots, v_m, \dots$ be any convergent subsequence of (A.4) with limit f from $\widehat{F}$. Then the identity $f \equiv 1$ defines the pro-finite variety of pro-solvable groups.

Proof. The theorem immediately follows from Theorems 1.1 and A.12. □

We can now state the pro-finite analogue of the Thompson–Flavell theorem.

COROLLARY A.16. *A pro-finite group G is pro-solvable if and only if every closed two-generator subgroup of G is pro-solvable.*

Proof. Let every two-generator subgroup of $\widehat{G}$ be pro-solvable. Take an element $f \in \widehat{F}(x, y)$ which is the limit of a convergent subsequence of our sequence u. Let μ be an arbitrary continuous homomorphism $\widehat{F}(x, y) \to \widehat{G}$. Then $\mu(f) = 1$, as $\mu(f)$ lies in a two-generator subgroup of $\widehat{G}$. This is true for arbitrary μ and, therefore, $f \equiv 1$. According to Theorem A.15, $\widehat{G}$ is pro-solvable. □

Corollary A.14 and Theorem A.15 should be compared with results of Almeida [Alm02]. He used the language of implicit operations and the notion of $n!$-type convergent subsequence to get nice proofs of theorems of similar type. He also noticed that if our main theorem about solvable groups is true for the sequence u_n^w with initial term $w = [x, y]$, then the $n!$ version of the corresponding statement is also true.

REFERENCES

AS88 A. Adolphson and S. Sperber, *On the degree of the L-function associated with an exponential sum*, Compositio Math. **68** (1988), 125–159.

Alm94 J. Almeida, *Finite Semigroups and Universal Algebra* (World Scientific, Singapore, 1994).

Alm02 J. Almeida, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002), 387–411.

AV01 J. Almeida and M. Volkov, *Profinite methods in finite semigroup theory*, Preprint (2001), CMUP 2001-02.

AP96 Y. Aubry and M. Perret, *A Weil theorem for singular curves*, in *Arithmetic, Geometry and Coding Theory*, eds R. Pellikaan, M. Perret and S. G. Vlăduţ (de Gruyter, Berlin, 1996), 1–7.

Bae57 R. Baer, *Engelsche Elemente Noetherscher Gruppen*, Math. Ann. **133** (1957), 256–270.

BGGKPP03 T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskiĭ, G. Pfister and E. Plotkin, *Two-variable identities for finite solvable groups*, C. R. Acad. Sci. Paris, Ser. I **337** (2003), 581–586.

BP91 M. Boffa and F. Point, *Identités de Thue–Morse dans les groupes*, C. R. Acad. Sci. Paris, Sér. I **312** (1991), 667–670.

Bom80 E. Bombieri, *Thompson's problem $\sigma^2 = 3$*, Invent. Math. **58** (1980), 77–100.

Bra81 R. Brandl, *Zur Theorie der untergruppenabgeschlossenen Formationen: endliche Varietäten*, J. Algebra **73** (1981), 1–22.

BN86 R. Brandl and D. Nikolova, *Simple groups of small Engel depth*, Bull. Austral. Math. Soc. **33** (1986), 245–251.

BW88 R. Brandl and J. S. Wilson, *Characterization of finite soluble groups by laws in a small number of variables*, J. Algebra **116** (1988), 334–341.

BWW05 J. N. Bray, J. S. Wilson and R. A. Wilson, *A characterization of finite soluble groups by laws in two variables*, Bull. London Math. Soc. **37** (2005), 179–186.

Buc65 B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, University of Innsbruck, Austria (1965).

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press

BM98 R. G. Burns and Yu. Medvedev, *A note on Engel groups and local nilpotence*, J. Aust. Math. Soc., Ser. A **64** (1998), 92–100.

Del81 P. Deligne, *La conjecture de Weil II*, Publ. Math. Inst. Hautes Études Sci. **52** (1981), 313–428.

DL76 P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. (2) **103** (1976), 103–161.

SGA4 P. Deligne *et al.*, *Cohomologie étale*, in *Séminaire de Géometrie Algébrique du Bois-Marie* (SGA $4\frac{1}{2}$), Lecture Notes in Mathematics, vol. 569 (Springer, Berlin, 1977).

ES76 S. Eilenberg and S. Schützenberger, *On pseudovarieties*, Adv. Math. **19** (1976), 413–418.

ES52 S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology* (Princeton University Press, Princeton, NJ, 1952).

Fl95 P. Flavell, *Finite groups in which every two elements generate a soluble group*, Invent. Math. **121** (1995), 279–285.

FJ86 M. Fried and M. Jarden, *Field Arithmetic* (Springer, Berlin, 1986).

Fu97 K. Fujiwara, *Rigid geometry, Lefschetz–Verdier trace formula and Deligne's conjecture*, Invent. Math. **127** (1997), 480–533.

GL02 S. R. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Moscow Math. J. **2** (2002), 589–631.

GP96 G.-M. Greuel and G. Pfister, *Advances and improvements in the theory of standard bases and syzygies*, Arch. Math. (Basel) **66** (1996), 163–176.

GP98 G.-M. Greuel and G. Pfister, *Gröbner bases and algebraic geometry*, in *Gröbner Bases and Applications*, eds B. Buchberger and F. Winkler, London Mathematical Society Lecture Note Series, vol. 251 (Cambridge University Press, Cambridge, 1998), 109–143.

GP02a G.-M. Greuel and G. Pfister, *A* Singular *Introduction to Commutative Algebra* (Springer, Berlin, 2002).

GP02b G.-M. Greuel and G. Pfister, *Computer algebra and finite groups*, in *Proceedings of the First International Congress on Mathematical Software* (Beijing 2002), eds A. Cohen, X.-S. Gao and N. Takayama (World Scientific, Singapore, 2002).

GPS01 G.-M. Greuel, G. Pfister and H. Schönemann, Singular 2.0. *A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserslautern (2001), http://www.singular.uni-kl.de.

SGA5 A. Grothendieck *et al.*, *Cohomologie ℓ-adique et fonctions L* in *Séminaire de Géometrie Algébrique du Bois-Marie 1965–66* (SGA 5), ed. L. Illusie, Lecture Notes in Mathematics, vol. 589 (Springer, Berlin, 1977).

Gru53 K. Gruenberg, *Two theorems on Engel groups*, Proc. Camb. Phil. Soc. **49** (1953), 377–380.

GKNP00 F. Grunewald, B. Kunyavskiĭ, D. Nikolova and E. Plotkin, *Two-variable identities in groups and Lie algebras*, Zap. Nauch. Semin. POMI **272** (2000), 161–176; J. Math. Sci. (New York) **116** (2003), 2972–2981.

Gup66 N. D. Gupta, *Some group laws equivalent to the commutative law*, Arch. Math. (Basel) **17** (1966), 97–102.

GH67 N. D. Gupta and H. Heineken, *Groups with a two-variable commutator identity*, Math. Z. **95** (1967), 276–287.

Hup79 B. Huppert, *Endliche Gruppen, I* (Springer, Berlin, 1979).

HB82 B. Huppert and N. Blackburn, *Finite Groups, III* (Springer, Berlin, 1982).

Kat93 N. M. Katz, *Affine cohomological transforms, perversity, and monodromy*, J. Amer. Math. Soc. **6** (1993), 149–222.

Kat00 N. M. Katz, *L-functions and monodromy: four lectures on Weil II*, Preprint (2000), http://www.math.princeton.edu/∼nmk/arizona34.pdf.

Kat01 N. M. Katz, *Sums of Betti numbers in arbitrary characteristics*, Finite Fields Appl. **7** (2001), 29–44.

Kos86 A. N. Kostrikin, *Around Burnside* (Nauka, Moscow, 1986), English transl. (Springer, Berlin, 1990).

LW54 S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

LY94 D. Leep and C. Yeomans, *The number of points on a singular curve over a finite field*, Arch. Math. (Basel) **63** (1994), 420–426.

Lub01 A. Lubotzky, *Pro-finite presentations*, J. Algebra **242** (2001), 672–690.

MSW01 S. Margolis, M. Sapir and P. Weil, *Closed subgroups in pro-V topologies and the extension problem for inverse automata*, Internat. J. Algebra Comput. **11** (2001), 405–445.

Neu67 H. Neumann, *Varieties of Groups* (Springer, New York, 1967).

Nik83 D. Nikolova, *Groups with a two-variable commutator identity*, C. R. Acad. Bulgare Sci. **36** (1983), 721–724.

Nik85 D. Nikolova, *Solubility of finite groups with a two-variable commutator identity*, Serdica **11** (1985), 59–63.

Pin92 R. Pink, *On the calculation of local terms of the Lefschetz–Verdier trace formula and its application to a conjecture of Deligne*, Ann. of Math. (2) **135** (1992), 483–525.

Pla67 V. P. Platonov, *Linear groups with identical relations*, Dokl. Akad. Nauk BSSR **11** (1967), 581–582 (in Russian).

Plo54 B. I. Plotkin, *On nilgroups*, Dokl. Akad. Nauk SSSR **94** (1954), 999–1001 (in Russian).

Plo55 B. I. Plotkin, *Radical groups*, Mat. Sb. N.S. **37(79)** (1955), 507–526. (English transl. Amer. Math. Soc. Transl. (2) **17** (1961), 9–28.)

Plo58 B. I. Plotkin, *Generalized soluble and generalized nilpotent groups*, Uspekhi Mat. Nauk **13** (1958), 89–172. (English transl. Amer. Math. Soc. Transl. (2) **17** (1961), 29–115.)

PPT99 B. Plotkin, E. Plotkin and A. Tsurkov, *Geometrical equivalence of groups*, Comm. Algebra **27** (1999), 4015–4025.

Red56 L. Rédei, *Die endlichen einstufig nichtnilpotenten Gruppen*, Publ. Math. Debrecen **4** (1956), 303–324.

RZ00 L. Ribes and P. Zalesskii, *Profinite Groups* (Springer, Berlin, 2000).

Sch24 O. J. Schmidt, *Groups all of whose subgroups are special*, Mat. Sbornik **31** (1924), 366–372 (in Russian).

Sha94 I. R. Shafarevich, *Basic Algebraic Geometry*, second edition (Springer, Berlin, 1994).

Tho68 J. Thompson, *Non-solvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968), 383–437.

Tit72 J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

Wei02 P. Weil, *Profinite methods in semigroups*, Internat. J. Algebra Comput. **12** (2002), 137–178.

Wil91 J. S. Wilson, *Two-generator conditions for residually finite groups*, Bull. London Math. Soc. **23** (1991), 239–248.

WZ92 J. S. Wilson and E. Zelmanov, *Identities for Lie algebras of pro-p groups*, J. Pure Appl. Algebra **81** (1992), 103–109.

Zel88 E. I. Zelmanov, *Engel Lie algebras*, Sibirsk. Mat. Zh. **29** (1988), 112–117, 238. (English transl. Siberian Math. J. **29** (1988), 777–781.)

Zel90 E. I. Zelmanov, *Solution of the restricted Burnside problem for groups of odd exponent*, Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), 42–59. (English transl. Math. USSR Izv. **36** (1991), 41–60.)

Zel91 E. I. Zelmanov, *Solution of the restricted Burnside problem for* 2*-groups*, Mat. Sb. **182** (1991), 568–592. (English transl. Math. USSR Sb. **72** (1992), 543–565.)

Zin90 T. Zink, *The Lefschetz trace formula for an open algebraic surface*, in *Proceedings of the Conference on Automorphic Forms, Shimura Varieties and L-Functions* (Ann Arbor, 1988), eds L. Clozel and J. S. Milne, Perspectives in Mathematics, vol. 11 (Academic Press, Boston, MA, 1990), 337–376.

Zor36 M. Zorn, *Nilpotency of finite groups*, Bull. Amer. Math. Soc. **42** (1936), 485–486.

Tatiana Bandman bandman@macs.biu.ac.il
Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel

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

Fritz Grunewald grunewald@math.uni-duesseldorf.de
Mathematisches Institut der Universität Heinrich Heine Düsseldorf, Universitätsstrße 1, 40225 Düsseldorf, Germany

Boris Kunyavskiĭ kunyav@macs.biu.ac.il
Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel

Gerhard Pfister pfister@mathematik.uni-kl.de
Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany

Eugene Plotkin plotkin@macs.biu.ac.il
Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel

https://doi.org/10.1112/S0010437X0500179X Published online by Cambridge University Press