PROCEEDINGS OF THE LATVIAN ACADEMY OF SCIENCES. Section B, Vol. 57 (2003), No. 3/4 (626/627), pp. 97–101.

# A STRATEGY FOR HUMAN-COMPUTER STUDY OF EQUATIONS AND IDENTITIES IN FINITE GROUPS

Boris Kunyavskiĭ, Eugene Plotkin, and Roman Shklyar

Department of Mathematics and Statistics, Bar-Ilan University,
Ramat Gan 52900, ISRAEL; e-mail: kunyav@macs.biu.ac.il, plotkin@macs.biu.ac.il, rshklyar@macs.biu.ac.il

Communicated by Rūsiņš Mārtiņš Freivalds

In memory of Professor Indulis Strazdiņš

*Finite nilpotent groups can be characterised by Engel identities. We consider the problem of similar characterisation of finite solvable groups by two-variable identities and describe computer-aided approach to its solution.*

**Key words:** *finite group, matrix representation, algebraic variety*

**Mathematics Subject Classification (2000):** *20D10, 20F45, 20D05, 14G15*

## 1. INTRODUCTION

This paper, which is a part of a larger joint project with G.-M. Greuel and F. Grunewald, is motivated by a problem in the theory of finite groups. We describe here a general approach combining computer experiments and algebraic-geometric machinery. This approach was mainly elaborated at the initial stage of investigation when many important details remained mysterious. We want to emphasise that significant corrections and enrichments, made at further stages, emerged from our collaboration with Greuel and Grunewald, whose numerous ideas were crucial for the realisation of the proposed methodology. Although technical details are left aside here, we hope to convince the reader that the suggested strategy can prove fruitful to attack this problem as well as other group-theoretic problems.

Our goal is to characterise the class of finite solvable groups by two-variable identities, as the class of Abelian groups is characterised by the identity $xy = yx$, and the class of finite nilpotent groups is characterised by Engel identities. To be more precise, a finite group $G$ is nilpotent if and only if it satisfies one of the identities $[y, x, x, \dots, x] = 1$ (here $[y, x] = yxy^{-1}x^{-1}$, $[y, x, x] = [[y, x], x]$, etc.). Moreover, one can prove even the more general

Proposition 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 $[w(x, y), x, x, \dots, x] = 1$.*

This observation allows one to produce a lot of Engel-like sequences defining finite nilpotent groups by just varying the initial term (for example, one can take $w = x^{-2}y^{-1}x$, cf. 3.1 and 3.2 below). B. Plotkin suggested some Engel-like identities that could characterise finite solvable groups (see Plotkin *et al.*, 1999; Grunewald *et al.*, 2000). In a slightly modified form, B. Plotkin's conjecture can be formulated as follows. Let $w$ denote a word in $x$, $y$, $x^{-1}$, $y^{-1}$, and let ${}^{w}u_n(x, y)$ be an infinite sequence defined by the rule

$$\begin{aligned} {}^{w}u_1 &= w, \\ {}^{w}u_{n+1} &= [x\, {}^{w}u_n\, x^{-1}, y\, {}^{w}u_n\, y^{-1}], \dots \end{aligned} \tag{1}$$

Conjecture 1. *There exists $w$ such that a finite group $G$ is solvable if and only if for some $n$ the identity ${}^{w}u_n(x, y) \equiv 1$ holds in $G$.*

We believe that an even stronger statement is true.

Conjecture 2. *Let $w$ be any word satisfying the condition: if $w(x, y) \equiv 1$ in $G$ then $G$ is Abelian. Then a finite group $G$ is solvable if and only if for some $n$ the identity ${}^{w}u_n(x, y) \equiv 1$ holds in $G$.*

Should Conjecture 2 be true, the most natural choice for the initial word could be $w = [x, y]$.

At present, we have no approach to Conjecture 2. As to Conjecture 1, in Grunewald *et al.* (2000) one can find a proof of its Lie-algebraic analogue. Note that according to a theorem of J. Thompson (Thompson, 1968; Flavell, 1995), stating that if $G$ is a finite group in which every two elements generate a solvable subgroup then $G$ is solvable, one can expect that finite solvable groups can be characterised by two-variable identities. (However, this theorem does not provide any explicit two-variable identity for finite solvable groups.)

To prove Conjecture 1, we suggest to proceed as in Grunewald *et al.* (2000). Namely, one can easily derive Conjecture 1 from the following

CONJECTURE 3. *Let $G$ be one of the following groups:*

1. $\mathrm{PSL}(2,p)$ ($p = 5$ *or* $p = \pm 2 \pmod 5, p \neq 3$),
2. $\mathrm{PSL}(2,2^p)$,
3. $\mathrm{PSL}(2,3^p)$ ($p$ *odd* ),
4. $\mathrm{PSL}(3,3)$,
5. $\mathrm{Sz}(2^p)$ ($p$ *odd* ).

*Then there exists a word $w$ in $x$, $y$, $x^{-1}$, $y^{-1}$, independent of $G$, such that none of the identities ${}^w u_n(x,y) \equiv 1$ holds in $G$.*

PROPOSITION 2. *Conjecture 3 implies Conjecture 1.*

*Proof.* First note that the "only if" part of the statement of Conjecture 1 is obvious. Indeed, if $G$ is solvable of class $n$ then the identity ${}^w u_n \equiv 1$ holds in $G$ for any $w$, since the value ${}^w u_n(x,y)$ belongs to the corresponding term of the derived series. Thus, we only have to prove that the "if" part of the statement of Conjecture 1 follows from Conjecture 3. Let us assume that Conjecture 3 holds, take $w$ as in its statement, and suppose that there exists a non-solvable finite group in which the identity ${}^w u_n \equiv 1$ holds. Denote by $G$ a minimal counterexample, i.e. a finite non-solvable group with identity ${}^w u_n \equiv 1$, where all subgroups are solvable. However, the list of groups in Conjecture 3 is none other than the list of minimal finite non-solvable groups (that is, the groups whose every subgroup is solvable). Thus, for any $G$ from this list the identity ${}^w u_n \equiv 1$ does not hold in $G$, a contradiction. □

To prove Conjecture 3, it is enough to find a word $w$ and integers $i$ and $j$ such that the equation

$$ {}^w u_i(x,y) = {}^w u_j(x,y) \tag{2} $$

has a non-trivial solution in every $G$ from the above list (non-trivial means that ${}^w u_i(x,y) \neq 1$). In the next sections we explain how this can be done.

## 2. FIRST SCREENING

A possible attempt to find numerical evidence in support of the main conjecture could be as follows: pick a word $w$ (say, take $w = [x,y]$, as in the classical Engel sequence), and consider equation (2) for small $i,j$ in each group $G$ from the list of Conjecture 3. Let us focus on the case $G = \mathrm{PSL}(2,p)$, and consider $1 \leq i,j \leq 4$. Computer experiments (with the help of MAPLE) immediately show

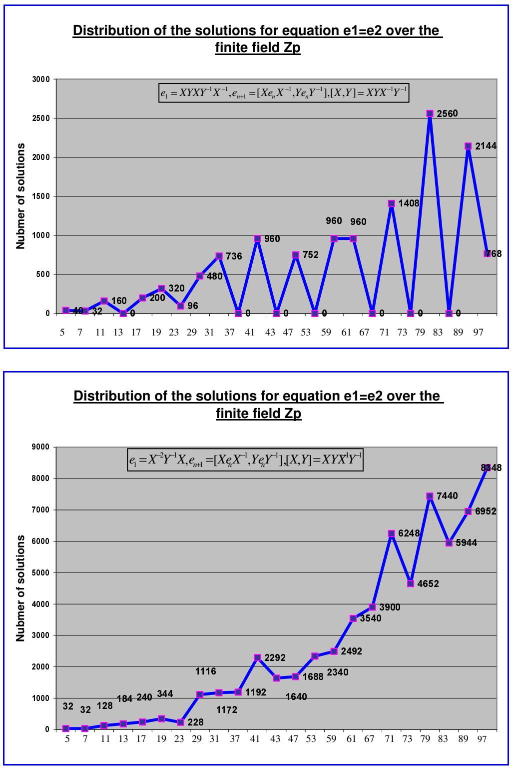


*Fig. 1.* Distribution of solutions to ${}^w u_1 = {}^w u_2$ for a "bad" word $w = xyxy^{-1}x^{-1}$ and a "good" word $w = x^{-2}y^{-1}x$

arising difficulties. Although the number of solutions to the above equations has a tendency to grow with growth of $p$, for each pair $i,j$ there is $p$ such that equation (2) has no non-trivial solutions in $\mathrm{PSL}(2,p)$. Here is a way out suggested by F. Grunewald (see also Proposition 1): we vary the initial word of the sequence. For simplicity, we limit ourselves by the equation

$$ {}^w u_1(x,y) = {}^w u_2(x,y). \tag{3} $$

The result may seem unexpected enough: there are certain words (less than 0.1% of the total number of words of given length) such that equation (3) has a non-trivial solution for all $p < 1000$; moreover, for such initial words the rate of growth of the number of solutions is significantly higher than for others. Here are the shortest words of this type: 1) $w = x^{-1}yxy^{-1}x$; 2) $w = x^{-2}y^{-1}x$; 3) $w = y^{-2}x^{-1}y$. The difference in the behaviour of the number of solutions for the cases when $w$ is "bad" or "good" can be seen very clearly from Figure 1.

This purely experimental numerical phenomenon allows us to reveal even deeper properties of the equations under consideration. These properties are of algebraic-geometric nature and are of key importance for further investigation.

## 3. ALGEBRAIC-GEOMETRIC VIEW

The general idea of our approach to proving Conjecture 3 can be described as follows. For a group $G$ in the list of Conjecture 3, we fix its standard linear representation (over the corresponding finite field $\mathbf{F}_q$). Then the equation ${}^{w}u_1(x,y) = {}^{w}u_2(x,y)$ can be viewed as a matrix equation. To be more precise, we regard the entries of the matrices corresponding to $x$ and $y$ in this representation as variables, and thus the above matrix equation becomes a system of polynomial equations defining an algebraic variety over $\mathbf{F}_q$. Our goal is to apply to this variety estimates of Lang–Weil type which guarantee the existence of a solution for a sufficiently large $q$ (see Lang and Weil (1954)). Small values of $q$ are checked case by case.

This strategy has been realised in a human-computer manner. We mean that the use of the problem-oriented software, in particular, the package SINGULAR (see Greuel *et al.* (2001) or Greuel and Pfister (2002), or try http://www.singular.uni-kl.de), was absolutely indispensable. In our case, SINGULAR enabled us to overcome heavy computational problems arising from the complexity of the geometric objects under consideration. Note that this is not the first example of successful application of algebraic-geometric methods to the theory of finite groups (see, for instance, a remarkable paper by Bombieri (1980) which served for us as an inspiring example). We believe that this kind of machinery may be applied to other interesting group-theoretical problems.

Here is how this strategy looks like in our setting.

**3.1. The $PSL(2)$ case.** As mentioned at the end of Section 2, our experimental data can only be explained by some algebraic-geometric phenomena. So, following the general strategy described above, we fix an initial word $w$ and represent equation (3) as an algebraic variety over $\mathbf{F}_q$. (Figure 2 presents a graph of such a variety.)

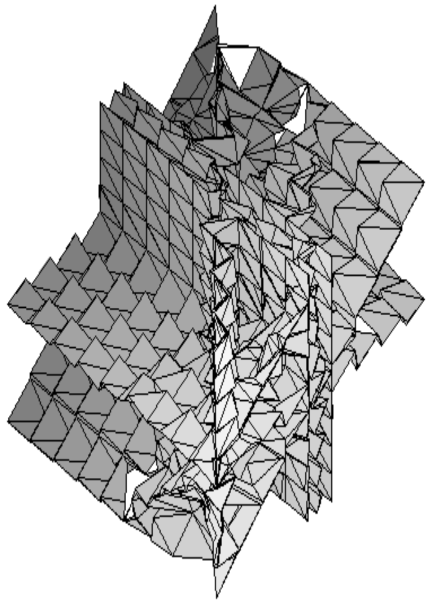

*Fig. 2.* Graph of the equation ${}^{w}u_1 = {}^{w}u_2$ in $\mathrm{PSL}(2,\mathbf{R})$, $w = x^{-2}y^{-1}x$

We start with the case $G = \mathrm{PSL}(2,p)$ and, for simplicity, limit ourselves by looking for solutions among the matrices $x, y \in G$ of the following form:

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

We then study the arising variety $C_w \subset \mathbf{A}^3$ (with affine coordinates $b, c, t$), defined by the matrix equation ${}^{w}u_1 = {}^{w}u_2$, with the help of the SINGULAR package. The first striking observation is the following *dimension jump*: there are four initial words $w$ among about 10000 shortest ones such that the dimension of $C_w$ is one (and not zero as one might expect and as it occurs for most words $w$). Here are these four words: $w_1 = x^{-1}yxy^{-1}x$, $w_2 = x^{-2}y^{-1}x$, $w_3 = y^{-2}x^{-1}y$, $w_4 = xy^{-2}x^{-1}yx^{-1}$. Note that if $w = w_i$ ($i = 1, \ldots, 4$), then any solution to ${}^{w}u_1 = {}^{w}u_2$ (except, possibly, for $t = 1$, $b = 1$, $c = -1$), is automatically non-trivial (cf. hypothesis 1 of Proposition 1).

For these "good" words, we proceed as follows. As explained above, the main idea is to apply the Lang–Weil bound for the number of rational points on a variety defined over a finite field. It turns out that in the $PSL(2)$ case for our purposes it is enough to use the classical Hasse–Weil bound (in a slightly modified form adapted for singular curves, cf. Fried and Jarden (1986), Th. 3.14, Aubry and Perret (1996)).

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

In fact, we need an affine version of the lower estimate of Lemma 1 (cf. Fried and Jarden (1986), Th. 4.9, Cor. 4.10)).

COROLLARY 1. *Let $C$ be an absolutely irreducible affine plane curve of degree $d$ defined over $\mathbf{F}_q$, $N_q = |C(\mathbf{F}_q)|$. Then $N_q \ge (d-1)(d-2)\sqrt{q} - d$. In particular, if $q > (d-1)^4$, there is a rational point on $C$.*

To apply Lemma 1 (or Corollary 1) we have to compute the arithmetic genus of the curve $C_w$ (or the degree of some plane projection of $C_w$) and to prove that the curve is absolutely irreducible. The first computation can be done by SINGULAR; as to the second one, this is a kind of human-computer argument. To be more precise, SINGULAR can only check irreducibility over the ground field, and some additional subtle considerations based upon the structure of the singular locus of $C_w$ are needed.

The cases of small characteristics $G = \mathrm{PSL}(2, 2^p)$ and $G = \mathrm{PSL}(2, 3^p)$ are treated in a similar way.

The case $G = \mathrm{PSL}(3, 3)$ is easily settled by full search. For example, for $w = w_2$ we find a solution to ${}^w u_1 = {}^w u_2$ given by the images in $G$ of the following matrices:

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

**3.2. The Suzuki case.** The last remaining case $G = \mathrm{Sz}(q)$ is the most complicated one, in particular, from the computational side. Large group orders require heavy computations (we used MAGMA for the group-theoretic part and SINGULAR for the algebraic-geometric one). Moreover, there are even deeper reasons making the Suzuki case especially difficult. Although both $\mathrm{PSL}(2, q)$ and $\mathrm{Sz}(q)$ are groups of Lie type of rank 1, and their algebraic structure is very similar, the geometric properties of equations under consideration are significantly different. Namely, in the $\mathrm{PSL}(2, p)$ case the algebraic variety given by equation (3) is in fact defined over the ring of integers $\mathbf{Z}$, and the corresponding variety over $\mathbf{F}_p$ is obtained by reducing modulo $p$; in particular, the degree is the same for all $p$, and we thus are able to apply the Lang–Weil estimates for a sufficiently large $p$. In the Suzuki case the situation is quite different. The group $\mathrm{Sz}(q)$ is defined with the help of a Frobenius-like automorphism, and hence the standard matrix representation for $\mathrm{Sz}(q)$ (see below) contains entries depending on $q$. Therefore, the degree of the resulting variety ${}^w u_1 = {}^w u_2$ depends on $q$ (and grows with growth of $q$) which prevents direct application of the Lang–Weil estimates.

Our strategy is essentially the same: we start with screening for "good" initial words $w$ such that the equation ${}^w u_1 = {}^w u_2$ has a solution in $\mathrm{Sz}(q)$ for $q = 8, 32, 128, \ldots$, and the number of solutions grows with growth of $q$ (this last condition should be emphasised because it gives hope for using algebraic-geometric machinery). To be more precise, we use the standard embedding of $\mathrm{Sz}(q)$ into $\mathrm{GL}(4, q)$ (see Huppert and Blackburn (1982), Ch. XI, §3) and look for solutions among the matrices of the following form:

$$x = \begin{pmatrix} a^{2+\theta} + ab + b^{\theta} & b & a & 1 \\ a^{1+\theta} + b & a^{\theta} & 1 & 0 \\ a & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad ,$$

$$y = \begin{pmatrix} c^{2+\theta} + cd + d^{\theta} & d & c & 1 \\ c^{1+\theta} + d & c^{\theta} & 1 & 0 \\ c & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad .$$

Here $a, b, c, d \in \mathbf{F}_q$, and $\theta$ stands for the automorphism of $\mathbf{F}_q$ with $\theta^2 = 2$. F. Grunewald noticed the following amazing fact: "good" initial words $w$ are those for which the variety, corresponding to the equation ${}^w u_1(x, y) = {}^w u_2(x, y)$ with $x, y$ chosen as above, is, in a certain sense, $\theta$-invariant. It turns out that for such good words one can apply estimates of the Lang–Weil type to guarantee the existence of a solution for a sufficiently large $q$ (small values of $q$ are checked directly). Thus, our final step here is another screening for initial words satisfying this invariance condition. Luckily enough, among these words we find the word $w_2 = x^{-2}y^{-1}x$, which is also good for the PSL(2) case and for the $\mathrm{PSL}(3, 3)$ case. This establishes Conjecture 3.

## 4. CONCLUDING REMARKS

We want to emphasise that the role of computer technology in our decision strategy was absolutely indispensable. In fact, it was used in the same manner as in experimental sciences: not just for checking some properties or conjectures but rather for providing experimental material for formulating main results and suggesting methods for their proofs.

At the next stage of our research, we plan even more intensive use of computer tools for the study of graphs on finite groups arising from the obtained solvability identities (see Grunewald *et al.*, 2000). This can be viewed as a generalisation of the commuting graph of a finite group applied by Segev and Seitz for the proof of the Margulis–Platonov conjecture on arithmetic groups (see Segev (1999), Segev and Seitz (2002)).

*ACKNOWLEDGEMENTS*

*This research was partially supported by the Israel Science Foundation founded by the Israel Academy of Sciences — Centres of Excellence Programme "Group-theoretic methods in the study of algebraic varieties," within the INTAS project "Algebraic K-theory, groups and algebraic homotopy theory," by the EU RTN programme "Algebraic K-theory, linear algebraic groups and related structures," and by the Minerva Foundation (Germany) through the Emmy Noether Research Institute of Mathematics. The first two authors were partially supported by the Ministry of Absorption (Israel).*

REFERENCES

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

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

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

Fried, M., Jarden, M. (1986) *Field Arithmetic*. Springer-Verlag, Berlin. 458 pp.

Greuel, G.-M., Pfister, G. (2002) *A SINGULAR Introduction to Commutative Algebra*. Springer-Verlag, Berlin. 588 pp.

Greuel, G.-M., Pfister, G., Schönemann, H. (2001) SINGULAR — A computer algebra system for polynomial com- putations. In: *Symbolic Computation and Automated Reasoning: the Calculemus-2000 Symposium*. Kerber, M., Kohlhase, M. (eds.). A K Peters, Ltd., Natick, Mass., pp. 227–233.

Grunewald, F., Kunyavskiĭ, B., Nikolova, D., Plotkin, E. (2000) Two-variable identities in groups and Lie algebras. *Zap. Nauch. Semin. POMI*, **272**, 161–176.

Huppert, B., Blackburn, N. (1982) *Finite Groups*, III. Springer-Verlag, Berlin–Heidelberg–New York. 454 pp.

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

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

Segev, Y. (1999) On finite homomorphic images of the multiplicative group of a division algebra. *Ann. Math.*, **149**, 219–251.

Segev, Y., Seitz, G. (2002) Anisotropic groups of type $A_n$ and the commuting graph of finite simple groups. *Pacific J. Math.*, **202**, 125–225.

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

Received 23 April 2002

## GALĪGU GRUPU VIENĀDOJUMU UN IDENTITĀŠU PĒTĪŠANAS STRATĒĢIJA CILVĒKAM KOPĀ AR DATORU

Galīgas nilpotentas grupas var raksturot ar Engela identitātēm. Apskatīta līdzīgas raksturošanas problēma galīgām atrisināmām grupām ar divu mainīgo identitātēm un aprakstīta uz datora izmantošanu orientēta pieeja tās risināšanai.