МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2001
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2001
Proceedings of Thirtieth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 8–11, 2001

MATRIX EQUATIONS IN LINEAR GROUPS*

Daniela Nikolova, Eugene Plotkin

It is a well known fact that a finite group is nilpotent iff it satisfies an Engel law of some length. The subject of our recent research has been to establish a similar characterization for finite soluble groups. It is sufficient to check the problem on two-generated subgroups. For this purpose a sequence of two-variable commutator formulae are investigated (Conjecture of B.I.Plotkin). The solubility is checked by examining a counter-example of least possible order, i.e. to show that in minimal simple groups there are no such identities. Thus, we solve equations in matrix groups, especially for the generic case $G = PSL(2, p)$.
There is a strong evidence that Plotkin's conjecture is true. We give some results by computer calculations using GAP and formulate some conjectures.
The solution of such equations is connected with some well-known problems in finite matrix groups, as for example the Ore conjecture.
Similar result was obtained for finitely dimensional Lie algebras by E.B.Plotkin and B.Kunyavski (personal communication).
Keywords: soluble groups, matrix groups, commutators, identities, equations.
AMS Mathematics Subject Classifications (1991): 17B01, 17B30, 20F16, 20G15.

1. Introduction. If G is a group, $x, y \in G$, let $[x, y] = x^{-1}y^{-1}xy$.
An *Engel word* in the variables x, y is a left-normed commutator
$e_n(x, y) = [x,_n y] = \underbrace{[x, y, \ldots, y]}_{n \text{ entries}}$.

It is a well known fact that a finite group G is nilpotent iff it satisfies an Engel law $e_n \equiv 1$ for some $n \in \mathbb{N}$.

The subject of our recent research has been to establish a similar characterization for finite soluble groups. We would like to find a sequence of formulae $u_1, u_2, \ldots, u_n, \ldots$ such that a finite group G is soluble iff $u_n \equiv 1$ for some $n \in \mathbb{N}$.

Moreover, it is sufficient to check the problem of solvability on 2-generated subgroups, i.e. we can look for 2-variable identities which determine the property of solubility, because of the following Theorem of Thompson:

Theorem 1.1 [14], [2]**.** *Let G be a finite group in which every two elements generate a soluble subgroup. Then G is soluble.*

*This research was supported by the Joint Research Project on Computer Algebra between the Bulgarian Academy of Sciences and the Ben-Gurion University of the Negev, Israel.

2. Previous results. This problem coincides with some similar results proved in the 80-s in [1, 5, 6, 7]. We were interested in the laws of the type:

$$e_m(x,y) = e_n(x,y), m < n, \tag{1}$$

which hold in a group G. When m was chosen minimal with respect to this property, we were able to characterize finite groups in terms of m. It is easy to see that every finite group satisfies such a law. It was proved that for such a group $m = 1$ yelds abeliancy, $m = 2$ yields solubility, while there exist finite simple groups with a law $m = 3$, such as $A_5, PSL(2,8))$, etc.

The solubility was proved by examining a counter-example G_0 of least possible order, i.e. G_0 belongs to the list of minimal finite non-soluble groups (that is, nonsoluble groups in which every proper subgroup is soluble) [14]: PSL$(2,p)$ ($p = 5$ or $p \equiv \pm 2 \pmod 5, p \neq 3$), PSL$(2,2^p)$, PSL$(2,3^p)$ (p odd), Sz(2^p) (p odd), PSL$(3,3)$.

3. The conjecture (B. I. Plotkin). Let

$$\begin{array}{lllllllll} u_1 & = & [x,y], & & & & & & \\ u_1' & = & [u_1,x], & u_1'' & = & [u_1,y], & u_2 & = & [u_1',u_1''], \quad \ldots \\ u_n' & = & [u_n,x], & u_n'' & = & [u_n,y], & u_{n+1} & = & [u_n',u_n''], \quad \ldots \end{array} \tag{2}$$

Conjecture 3.1 (B. Plotkin)**.** *A finite group G is soluble if and only if for some n the identity $u_n \equiv 1$ holds in G.*

In order to prove this, it is sufficient to show that in minimal simple groups there are no such identities, i.e., the equation

$$\exists k \in \mathbb{N}, \exists n \in \mathbb{N} : u_k = u_n \tag{3}$$

has a non-trivial solution.

Thus, we solve equations of type (3) in matrix groups, especially for the generic case $G = PSL(2,p)$.

A similar result was obtained for finitely dimensional Lie algebras by E. Plotkin and B. Kunyavski (personal communication).

The solution of such equations is connected to some well-known problems in finite matrix groups, as for example the *Ore conjecture*.

4. Matrix equations in linear groups. In various situations it is instructive to represent a matrix as a product of matrices of a special nature. Given a class of matrices, one studies products of elements from the class, and asks about the minimal number of factors in a factorization. In Linear Algebra, one writes an invertible matrix as a product of elementary matrices. One can ask how many elementary matrices (or commutators) are needed to represent any product of elementary matrices (respectively, commutators).

In 1990 L. N. Vaserstein and E. Wheland [15] studied invertible matrices over rings and decomposed them into products of triangular matrices, companion matrices, and commutators. In particular, they proved that if $n \geq 3$, and A is a commutative ring, then every matrix in $SL(n,A)$ is a product of two commutators.

Definition 4.1. *Let G be a group. The least integer $c(G) \geq 0$ such that every product of commutators is the product of s commutators is called the commutator length of G.*

If no such an s exists, then $c(G) = \infty$.

Note that $c(G) = 0 \Leftrightarrow G$ is commutative. The question whether $c(G) \leq 1$, i.e. every element of the commutator subgroup $[G, G]$ is a single commutator, is of particular interest. This question was first studied by Shoda in 1936 [9].

In 1951 Ore conjectured [8] that $c(G) \leq 1$ for every finite simple group, and he showed for the series of the alternating groups that $c(A_n) = 1$ if $n \geq 5$. Later this was proved for:

- all finite linear groups with the exception of one or two classes
- nearly all sporadic groups,
- many classes of infinite simple groups, etc.

In 1977 I. M. Isaacs [4] noted that no simple group G is known with $c(G) > 1$. In particular, Thompson showed (1961-1962) [10, 11, 12, 13] that $c(GL(n, F)) \leq 1$, $c(SL(n, F)) \leq 2, c(PSL(n, F)) \leq 1, \forall n \geq 1$, where F is a field. He also gave examples of finite perfect groups G with $c(G) = 2$, when $G = SL(n, R)$, and R is a ring.

5. Experimental results. There is a strong evidence that Plotkin's Conjecture 3.1 is true. We give further some results of solving equations of type (3) by computer calculations (*GAP*):

1. Using *GAP* we proved that equations of type (3) can be solved for: $PSL(3, 3)$ and $PSL(2, p)$ for all primes $p < 100$.

   For the latter case we only run through transvections.

2. We further ask which is the minimal k, and respectively the minimal n for it such that $u_k = u_n$ has a non-trivial solution in $PSL(2, p)$. The next conjecture is that *Such non-trivial solutions can appear "quite early"*. The results are given in the following table for a prime $p < 50$. For $p \geq 13$ y runs through the representatives of the conjugacy classes, x is arbitrary.

3. Let (x, y) be a solution.
   $$\forall c_y \in C_G(y), (x^{c_y}, y^{c_y}) = (x^{c_y}, y)$$
   will also be a solution. The above experiments showed that this is the way to obtain half of the solutions. Moreover, the number of the solutions is either $p-1$, or $p+1$ for a given equation $u_k = u_n$.

6. Some other problems and results.

1. We could further ask for the probability a given pair of elements (x, y) in a group G to represent a solution, i.e. to calculate *the volume* of the variety of solutions:

   Let T_G be the set of solutions for $G = PSL(2, p)$.
   $$\frac{|T_G|}{|G|^2} \; p \stackrel{\longrightarrow}{\to} \infty$$

   This question refers to Asymptotic Theory of Finite Groups.

G	$u_1{=}u_2$	$u_1{=}u_3$	$u_2{=}u_3$	comments	$\lvert C_G(x)\rvert$	$\lvert C_G(y)\rvert$	No.solutions
PSL(2,5)	no	no	no	$\forall x, \forall y$			
PSL(2,7)	$\lvert x\rvert{=}4{=}\frac{p+1}{2}$ $\lvert y\rvert{=}3{=}\frac{p-1}{2}$ $\lvert u\rvert{=}4{=}\frac{p+1}{2}$			$\forall x, \forall y$			
PSL(2,11)	no	$\lvert x\rvert{=}6{=}\frac{p+1}{2}$ $\lvert y\rvert{=}5{=}\frac{p-1}{2}$ $\lvert u\rvert{=}5{=}\frac{p-1}{2}$	no	$\forall x, \forall y$			
PSL(2,13)	no	no	$\lvert x\rvert{=}7{=}\frac{p+1}{2}$ $\lvert y\rvert{=}3{=}\frac{p-1}{4}$ $\lvert u\rvert{=}13{=}p$ $\lvert xy\rvert{=}13{=}p$		7	6	$12{=}$ $p{-}1$
PSL(2,17)	no	$\lvert x\rvert{=}4$ 9 17 $\lvert y\rvert{=}9$ 9 8 $\lvert u\rvert{=}4$ 4 2 $\lvert xy\rvert{=}3$ 2 17	$\lvert x\rvert{=}2$ 17 4 $\lvert y\rvert{=}9$ 2 8 $\lvert u\rvert{=}2$ 2 9 $\lvert xy\rvert{=}9$ 17 3				200
PSL(2,19)	no	no	$\lvert x\rvert{=}10{=}\frac{p+1}{2}$ $\lvert y\rvert{=}5{=}\frac{p+1}{4}$ $\lvert u\rvert{=}9{=}\frac{p-1}{2}$ $\lvert xy\rvert{=}19{=}p$			10	$20{=}$ $p{+}1$
PSL(2,23)	no	no	$\lvert x\rvert{=}11{=}\frac{p-1}{2}$ $\lvert y\rvert{=}11{=}\frac{p-1}{2}$ $\lvert u\rvert{=}2$ $\lvert xy\rvert{=}12{=}\frac{p+1}{2}$			11	$22{=}$ $p{-}1$
PSL(2,29)	no	no	no	$u_1{=}u_4$ $\lvert x\rvert{=}15{=}\frac{p+1}{2}$ $\lvert y\rvert{=}5$ $\lvert u\rvert{=}3$ $\lvert xy\rvert{=}14{=}\frac{p-1}{2}$	15	15	$30{=}$ $p{+}1$
PSL(2,31)	no	$\lvert x\rvert{=}16{=}\frac{p+1}{2}$ $\lvert y\rvert{=}5$ $\lvert u\rvert{=}5$ $\lvert xy\rvert{=}3$	$\lvert x\rvert{=}2$ 2 16 15 $\lvert y\rvert{=}15$ 16 2 2 $\lvert u\rvert{=}2$ 2 2 2 $\lvert xy\rvert{=}15$ 16 16 15				250
PSL(2,37)	$\lvert x\rvert{=}19{=}(p{+}1)/2$ $\lvert y\rvert{=}6$ $\lvert u\rvert{=}19$ $\lvert xy\rvert{=}9$				19	18	$36{=}$ $p{-}1$
PSL(2,41)	no	no	$\lvert x\rvert{=}20{=}\frac{p-1}{2}$ $\lvert y\rvert{=}21{=}\frac{p+1}{2}$ $\lvert u\rvert{=}5$ $\lvert xy\rvert{=}7$		20	21	$42{=}$ $p{+}1$
PSL(2,43)	$\lvert x\rvert{=}11{=}\frac{p+1}{4}$ $\lvert y\rvert{=}21{=}\frac{p-1}{2}$ $\lvert u\rvert{=}21{=}\frac{p-1}{2}$ $\lvert xy\rvert{=}21{=}\frac{p-1}{2}$						$42{=}$ $p{-}1$
PSL(2,47)	no	$\lvert x\rvert{=}6$ 2 $\lvert y\rvert{=}23$ 23 $\lvert u\rvert{=}24$ 2 $\lvert xy\rvert{=}24$ 23	$\lvert x\rvert{=}23{=}\frac{p-1}{2}$ $\lvert y\rvert{=}2$ $\lvert u\rvert{=}2$ $\lvert xy\rvert{=}23$				330

2. Compute the minimal k, l for which an identity $u_m(x, y) = u_n(x, y)$ holds for particular classes of finite groups. This problem is similar to some previous results of one of the authors: In [5], Engel invariants have been computed in some groups, classes of groups and varieties of groups such as some groups of small order; the class of dihedral groups D_p where p is an odd prime; the soluble locally finite varieties of groups $A_k A_l$ for k and l powers of one and the same prime number p, and for k and l coprime integers; the infinite series of simple groups (the alternating groups A_n for $n > 5$ and the special projective groups $\mathrm{PSL}(2, q)$ for some of the first groups in the series).

3. There are several results concerning characterization of soluble groups in terms of two-variable identities [6, 7, 1]. Namely, it was proved in [6, 7] that if a finite group G satisfies for some n the identity $e_2 \equiv e_n$, where $\{e_i\}$ is the sequence of Engel words, then G is soluble. However, it is easy to find a soluble group satisfying no identity of the form $e_2 \equiv e_m$. For example, take G a finite nilpotent group of class 3 such that the identity $e_2 \equiv 1$ does not hold in G. Since $e_3 \equiv 1$, the group G cannot satisfy any identity of the form $e_2 \equiv e_m$. However, G is soluble.

   In [1] it was proved that the identity $e_3 \equiv e_n$ can hold in certain finite simple groups such as $\mathrm{PSL}(2, 4)$, $\mathrm{PSL}(2, 8)$, etc. Let us also mention a pioneer result of N. Gupta [3]: any finite group satisfying the identity $e_1 \equiv e_n$ is abelian.

   We can ask for similar characterizations for our new identities.

Acknowledgements. This work was done while D. Nikolova was visiting Bar-Ilan University and Ben-Gurion University of the Negev, Israel, and the National University of Ireland, Galway. The hospitality and support of these institutions are gratefully appreciated. Our special thanks go to B. Plotkin whose ideas and encouragement were indispensable, and to A. Feldman for his help in computer experiments.

REFERENCES

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

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

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

[4] I. M. Isaacs. Commutators and the Commutator Subgroup. *Amer. Math. Monthly*, **84**, 1977, 720–722.

[5] D. Nikolova. Groups with a 2-variable commutator identity. Ph. D. thesis, Sofia Univ., 1983.

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

[7] D. Nikolova. Solubility of finite groups with a two-variable commutator identity. *Serdica Bulg. Math. Publ.*, **11** (1985), 59–63.

[8] O. Ore. Some Remarks on Commutators. *Proc. Amer. Math. Soc.*, **2** (1951), 307–314.

[9] K. Shoda. Einige Satze ueber Matrizen. *Japan J. Math.*, **13** (1936), 361–365.

[10] R. C. Thompson, Commutators in the Special and General Linear Groups. *Trans. Amer. Math. Soc.*, **101(1)** (1961), 16–33.
[11] R. C. Thompson. On Matrix Commutators. *Portugal. Math.*, **21** (1962), 143–153.
[12] R. C. Thompson. Commutators of Matrices with Coefficients from the Field of Two Elements. *Duke Math. J.*, **29** (1962), 367–373.
[13] R. C. Thompson. Commutators of Matrices with Prescribed Determinant. *Canad. J. Math.*, **20** (1968), 203–221.
[14] J. Thompson. Non-solvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, **74** (1968), 383–437.
[15] L. N. Vaserstein, E. Wheland. Commutators and Companion Matrices over Rings of Stable Rank 1. *Linear Algebra and its Applications*, **142** (1990), 263–277.

Daniela Nikolova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., bl. 8
1113 Sofia, Bulgaria
e-mail: daniela@moi.math.bas.bg

Eugene Plotkin
Department of Mathematics and Computer Science
Bar-Ilan University
52900 Ramat Gan
Israel
e-mail: plotkin@macs.biu.ac.il

МАТРИЧНИ УРАВНЕНИЯ В ЛИНЕЙНИ ГРУПИ

Даниела Николова, Евгений Плоткин

Добре е известно, че една крайна група е нилпотентна тогава и само тогава, когато удовлетворява Енгеловото тъждество от някаква степен. Обект на нашите изследвания напоследък бе да намерим подобна характеризация за крайните разширими групи. Достатъчно е да ограничим проблема върху дву-породените групи. За целта, се построява серия от дву-породени комутаторни формули (хипотеза на Б. И. Плоткин). Разширяемостта се проверява чрез изследване на минимален контра-пример, т.е. доказва се, че в минималните прости групи такива тъждества не се изпълняват. Така се стига до решаване на уравнения в матрични групи, като например, групите от серията $PSL(2,p)$.
Привеждат се резултати от компютърни изчисления използвайки системата GAP, които потвърждават верността на хипотезата на Плоткин. Формулират се и нови хипотези.
Решаването на тези уравнения е свързано с някои добре известни проблеми в областта на крайните матрични групи, като например хипотезата на Оре.