BULL. AUSTRAL. MATH. SOC. 20E10, 20F45
VOL. 33 (1986), 245-251.

SIMPLE GROUPS OF SMALL ENGEL DEPTH

ROLF BRANDL AND DANIELA B. NIKOLOVA

It is proved that the simple group $PSL(2,q)$ satisfies a law $[x,_3y] = [x,_sy]$, $s > 3$, if and only if $q = 4, 5, 8$.

1. Introduction.

Every finite group G satisfies a law

$$[x,_ry] = [x,_sy] , \quad \text{for some} \quad s > r ,$$

where

$$[x,_0y] = x, \ [x,_ny] = [\ [x,_{n-1}y]\ ,y] , \quad \text{for} \quad n \geq 1.$$

If r is chosen minimal with respect to this property, then r is called the Engel depth of G ([1]). It was proved in [2], [1] and [5] that finite groups of Engel depth $r \leq 2$ are soluble. However, there are nonabelian simple groups of depth three. For example, the groups $PSL(2,4)$ and $PSL(2,8)$ have this property, as can be seen from the following table exhibiting the minimal parameters r, s for some groups

---

Received 19 June 1985. The second author wishes to express her gratitude to Professor H. Heineken for the excellent atmosphere offered to her in the University of Würzburg and to the DAAD-foundation for making this collaboration possible.

$G = PSL(2,q)$:

q	4	7	8	9	11	13
$\|G\|$	60	168	504	360	660	1092
r	3	4	3	4	6	7
s	63	172	129	124	1986	2191

The computations have been performed on a *TR 440* at the Rechenzentrum der Universitat Würzburg and on an *EC 1040* at the Computing Centre of the Bulgarian Academy of Sciences, Sofia. Note that there seems to be a relationship between $s-r$ and the order of the group.

We are interested in finite simple groups contained in the class V_r of all finite groups of Engel depth $\leq r$. In this context a theorem of H. Heineken and P. M. Neumann [3] deserves attention, stating that any nontrivial variety of groups contains only finitely many of the finite simple groups $PSL(2,q)$ or $Sz(q)$. The classes V_r are not varieties, but we feel that they should have some common properties with varieties. In particular, we conjecture that any V_r contains only finitely many nonabelian simple groups.

Here we prove the following

THEOREM. *Let* $G = PSL(2,q)$, *for* $q \geq 4$. *Then* $G \in V_3$ *if and only if* $q = 4, 5,$ *or* 8.

There is some evidence that the groups mentioned above are the only finite simple groups in V_3. For example, the smallest Suzuki group $Sz(8)$ has Engel depth at least 11.

2. Proof of the Theorem

For the proof of the Theorem we need to construct elements $x,y \in G$, such that $[x,_3y] \neq [x,_sy]$, for all $s > 3$. In computational experiments such elements abound, but for a general proof some care is needed. Our choice is motivated by the following

Example. Let $G = PSL(2,9)$. For all $x, y \in G$, such that $|y| \neq 4$, we have $[x,_3 y] = [x,_{63} y]$. Nevertheless, there exist $x \in G$ and $y = \begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{pmatrix} \in G^*$, for some $\varepsilon \in \mathbb{F}_9$, such that $[x,_3 y]$ is not a transvection, but $[x,_s y]$ is a transvection, for all $s > 3$.

The following result exhibits elements of Engel depth three:

LEMMA 1. *Let q be a prime power and let $\lambda, s, u, \varepsilon \in \mathbb{F}_q$ be such that*

$$\lambda s u(1 - \varepsilon^2) = 1 \quad \text{and} \quad \varepsilon \neq 0 . \qquad (C).$$

Let $z_1 = \begin{pmatrix} \lambda s & s \\ \varepsilon^2 \lambda u & u \end{pmatrix}$ *and* $y = \begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{pmatrix}$.

Then $[z_1,_2 y] = \begin{pmatrix} \varepsilon^{-2} & \lambda^{-1}(1-\varepsilon^4) \\ 0 & \varepsilon^2 \end{pmatrix}$.

If $\varepsilon^2 \neq \pm 1$, then $[z_1,_2 y] \neq [z_1,_s y]$, for all $s \geq 3$.

Proof. The statement follows from a straightforward calculation, as $[z_1,_s y]$ are all transvections, for $s \geq 3$.

The next result reduces the proof of the Theorem to solving a quadratic equation in the field of q elements.

LEMMA 2. *If the equation*

$$(1 - \varepsilon^2)u^2 + (\varepsilon^4 - 1)u + \varepsilon^2 = 0 \qquad (E)$$

has a solution $u, \varepsilon \in \mathbb{F}_q$, where $\varepsilon^2 \neq 0, \pm 1$, then there exists $z_0 \in PSL(2,q)$, such that $[z_0,_3 y] \neq [z_0,_s y]$, for all $s \geq 4$.

Proof. Let z_1 and y be as in Lemma 1. According to it, it suffices to find $z_0 \in PSL(2,q)$, such that $[z_0, y] = z_1$. Let

---

* Henceforth, we shall identify $2x2$-matrices in $SL(2,q)$ with their images in $PSL(2,q)$.

https://doi.org/10.1017/S0004972700003117 Published online by Cambridge University Press

$z_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $[z_0, y] = z_1$ is equivalent to $y^{-1} z_0 y = z_0 z_1$, that is to

$$\begin{pmatrix} a & \varepsilon^2 b \\ \varepsilon^{-2} c & d \end{pmatrix} = \begin{pmatrix} \lambda s a + \varepsilon^2 \lambda u b & sa+ub \\ \lambda s c + \varepsilon^2 \lambda u d & sc+ud \end{pmatrix} .$$

This in turn, is equivalent to the following system of linear equations for a, b, c, d:

$$\left| \begin{array}{lcl} (\lambda s-1)a + \varepsilon^2 \lambda u b & = & 0 \\ sa + (u-\varepsilon^2)b & = & 0 \\ (\lambda s-\varepsilon^{-2})c + \varepsilon^2 \lambda u d & = & 0 \\ sc + (u-1)d & = & 0 . \end{array} \right. \qquad (S)$$

There exists a solution $(a,b) \neq (0,0)$ if and only if

$$D_1 = \begin{vmatrix} \lambda s-1 & \varepsilon^2 \lambda u \\ s & u-\varepsilon^2 \end{vmatrix} = 1 - u + \varepsilon^2 (1 - \lambda s) = 0.$$

Similarly, there exists a nontrivial solution (c,d) if and only if

$$D_2 = \begin{vmatrix} \lambda s-\varepsilon^{-2} & \varepsilon^2 \lambda u \\ s & u-1 \end{vmatrix} = \varepsilon^{-2}(1 - u + \varepsilon^2 (1 - \lambda s)) = 0.$$

Both conditions are equivalent to

$$1-u+\varepsilon^2(1-\lambda s) = 0 .$$

Using the condition (C) from Lemma 1, we get that (S) has a nontrivial solution if and only if

$$(1-\varepsilon^2)u^2 + (\varepsilon^4-1)u + \varepsilon^2 = 0$$

has a solution $u, \varepsilon \in \mathbb{F}_q$, where $\varepsilon^2 \neq 0, \pm 1$. Then the parameters λ and s can be determined from (C).

Moreover, it follows from (S) that the vectors (a, b) and $(\lambda s-1, \varepsilon^2 \lambda u)$ are perpendicular with respect to the usual scalar product, so are the vectors (c, d) and $(\lambda s-\varepsilon^{-2}, \varepsilon^2 \lambda u)$. Hence, if all non-trivial solutions (a, b) and (c,d) of (S) were linearly dependent,

https://doi.org/10.1017/S0004972700003117 Published online by Cambridge University Press

then $(\lambda s-1, \varepsilon^2\lambda u)$ and $(\lambda s-\varepsilon^{-2}, \varepsilon^2\lambda u)$ would be linearly dependent. But (C) implies that $\varepsilon^2\lambda u \neq 0$ and so $\lambda s-1 = \lambda s-\varepsilon^{-2}$, contradicting our assumption $\varepsilon^2 \neq 1$. So, there exists $z_0 \in GL(2,q)$ with $\det(z_0) \neq 0$ and $[z_0,y] = z_1$. Multiplying the first row of z_0 by the inverse of $\det(z_0)$, we get an element of $PSL(2,q)$ with the required properties.

We now solve (E) in $\mathbb{F}_q$. Let

$$F(x,y) = (1 - y^2)x^2 + (y^4 - 1)x + y^2$$

and let N be the number of pairs $(u,\varepsilon) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $F(u, \varepsilon) = 0$. A simple appeal to Eisenstein's Theorem shows that F is absolutely irreducible. From a well-known Theorem of A. Weil in Algebraic Geometry (see [6;p. 449]) it follows that $|N - q| \leq 12\sqrt{q} + 5$.

There are at most six "trivial" solutions u,ε of (E) where $\varepsilon^2 = 0,\pm 1$. Hence if $q \geq 169$, we get $N \geq 7$ and so (E) has at least one "nontrivial" solution.

We now deal with the remaining cases. First let q be odd. Then (E) has a solution $u \in \mathbb{F}_q$ if and only if its discriminant

$$D(\varepsilon) = (\varepsilon^4 - 2\varepsilon + 1)(\varepsilon^4 + 2\varepsilon + 1)$$

is a square in $\mathbb{F}_q$. Hence our problem is reduced in this case to proving that there exists $\varepsilon \in \mathbb{F}_q$, $\varepsilon^2 \neq 0,\pm 1$ such that $D(\varepsilon)$ is a square. If $q = p^f$ with $7 \leq p \leq 168$, then a direct calculation shows that such $\varepsilon \in \mathbb{F}_p$ exists.

We consider the cases $p = 2,3,5$ separately. Here the problem is more complicated as $PSL(2,p)$, $PSL(2,4)$ and $PSL(2,8)$ belong to V_3 and so, in these cases (E) does not have any solution with the required properties.

Let $q = 3^f$ or $q = 5^f$. As $\mathbb{F}_{p^f}$ contains $\mathbb{F}_{p^d}$ for every divisor d of f, we may assume that f is a prime. So it remains to consider the cases when $f = 2,3$.

https://doi.org/10.1017/S0004972700003117 Published online by Cambridge University Press

We have

$$D(x) = (x^2 - 1)(x^3 + x^2 + x - 1)(x^3 - x^2 + x + 1) ,$$

where the cubic factors are irreducible over $\mathbb{F}_3$ and $\mathbb{F}_5$. Hence, if $f = 3$, there exists $\varepsilon \in \mathbb{F}_q$, $\varepsilon^2 \neq 0, \pm 1$, such that $D(\varepsilon) = 0$.

Now, let $\varepsilon_1 \in \mathbb{F}_9$ be a root of the polynomial $X^2 + X - 1$. Then $D(\varepsilon_1) = -\varepsilon_1^2$. As -1 is a square in $\mathbb{F}_9$, $D(\varepsilon_1)$ is a square. Moreover, $\varepsilon_1^2 = -\varepsilon_1 + 1$ implies $\varepsilon_1^2 \neq 0, \pm 1$. Similarly, if $\varepsilon_2 \in \mathbb{F}_{25}$ is a root of $X^2 - X + 1$, then $D(\varepsilon_2) = 4$ and $\varepsilon_2^2 \neq 0, \pm 1$.

The following result completes the proof of the Theorem.

LEMMA 3. *Let $q = 2^f$, where $f \geq 4$. Then (E) has a solution $u, \varepsilon \in \mathbb{F}_q$, such that $\varepsilon \neq 0, 1$.*

Proof. In characteristic 2 equation (E) reads as follows:

$$(1+\varepsilon)^2 u^2 + (1+\varepsilon)^4 u + \varepsilon^2 = 0 .$$

Let $\varepsilon \neq 1$. Setting $u = y(1+\varepsilon)^2$ the solubility of (E) is equivalent to the solubility of

$$y^2 + y + \mu(\varepsilon) = 0 , \quad \text{where} \quad \mu(\varepsilon) = \varepsilon^2/(1+\varepsilon)^6 .$$

Now, by Hilbert's Theorem 90[4, p. 215] this is equivalent to showing that there exists ε with $Tr(\mu(\varepsilon)) = 0$. Let $\varepsilon = \varepsilon_1^{-1} + 1$. Then $\mu(\varepsilon) = \varepsilon_1^4 + \varepsilon_1^6$ and so

$$Tr(\mu(\varepsilon)) = Tr(\varepsilon_1^4)+Tr(\varepsilon_1^6) = Tr(\varepsilon_1)+Tr(\varepsilon_1^3) ,$$

since $Tr(\alpha) = Tr(\alpha^2)$, $\alpha \in \mathbb{F}_q$. Hence if (E) cannot be solved, then

$$Tr(\alpha)+Tr(\alpha^3) = 1 , \quad \text{for all} \quad \alpha \neq 0, 1$$

and so

$$g(x) = (x^2+x)(Tr(x)+Tr(x^3) + 1)$$

would be zero on $\mathbb{F}_q$. Hence, $g(x)$ would be divisible by $x^q + x$. We now show that this is not the case if $f \geq 4$. We have

$$g(x) = (x^2+x)(1+x+x^3+\ldots+x^{2^i}+x^{3.2^i}+\ldots+x^{2^{f-1}}+x^{3.2^{f-1}}) .$$

As the degree of $g(x)$ is less than $2q-1 = 2^{f+1}-1$, for $f \geq 3$, it is sufficient to consider the coefficients of x^q and x. If we can show that these are different, then it is clear that $g(x)$ **is** not divisible by $x^q + x$. Now, every exponent occuring in $g(x)$ equals 1 or is of the form

$$2^i+1,\ 2^i+2,\ 3.2^i+1,\ 3.2^i+2, \quad \text{for some } 0 \leq i \leq f-1.$$

If $i \geq 2$, then all of these numbers are congruent to 1 or 2 $(\mathrm{mod}\ 4)$, and if $i = 0, 1$, then these numbers are equal to $2, 3, 4, 5, 7, 8$. As $q \geq 16$, the coefficient of x^q is zero. As the coefficient of x equals 1, the conclusion follows.

References

[1] R. Brandl, "On groups with small Engel depth", *Bull. Austral. Math. Soc.* 28 (1983), 101-110.

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

[3] H. Heineken and P.M. Neumann, "Identical relations and decision procedures for groups", *J. Austral. Math. Soc.* 7 (1967), 39-47.

[4] S. Lang, *Algebra*, (Addison-Wesley, Reading, Massachusetts 1971).

[5] D. B. Nikolova, "Groups with a two-variable commutator identity", *R. Bulgare Sci.* 36 (1983), 721-724.

[6] W. M. Schmidt, "A lower bound for the number of solutions of equations over finite fields", *J. Number Theory* 6 (1974) 448-480.

Mathematisches Institut
der Universität,
Am Hubland 12,
D-8700 Würzburg
BRD

Mathematical Institute
Bulgarian Academy of Sciences
str."Acad.G.Bonchev", bl.8,
1113 Sofia
Bulgaria.