Word maps and equations in simple algebras

Eugene Plotkin

Bar-Ilan University, Israel

October 15, 2010

Example

Let we have two words in the free group $F_2(x, y)$

$$v_1(x, y) = x^{-2}y^{-1}x,$$

and

$$v_2(x, y) = [xv_1(x, y)x^{-1}, yv_1(x, y)y^{-1}],$$

For some reason we have to show that the equation

$$v_1(x, y) = v_2(x, y)$$

has a non-trivial solution in every group $PSL_2(\mathbb{F}_q)$.

Let $R := \mathbb{Z}[t,\ a,\ b,\ c,\ d]$ be the polynomial ring over $\mathbb{Z}$ in five variables. Consider the following 2×2-matrices over R.

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

Let $\mathfrak{a}$ be the ideal of R generated by $\det(y) - 1$ and by the 4 polynomials arising from the matrix equation $v_1(x,y) = v_2(x,y)$, and let $\mathcal{V} \subset \mathbb{A}^5$ be the corresponding closed set of 5-dimensional affine space. Let further $\mathfrak{a}_0$ be the ideal of R generated by $\det(y) - 1$ and by the matrix entries arising from the equation $v_1(x,y) = 1$, and let $\mathcal{V}_0 \subset \mathbb{A}^5$ be the corresponding closed set.

Regard solutions of the equation $v_1(x,y) = v_2(x,y)$ as $\mathbb{F}_q$-points on the corresponding algebraic $\mathbb{F}_q$-variety $V = \mathcal{V} \setminus \mathcal{V}_0$. It remains to prove, the existence of a rational point on V. The set V has an absolutely irreducible curve $\mathcal{C}$ as an irreducible component.

We now use the Hasse-Weil bound as a main tool:

Theorem (Weil)

Lemma 1.6. Let $\mathcal{C}$ be an absolutely irreducible projective algebraic curve defined over a $\mathbb{F}_q$, and let N_q denote the number of its rational points. Then $|N_q - (q+1)| \leq 2p_a\sqrt{q}$, where p_a stands for the arithmetic genus of $\mathcal{C}$.

Using Weil's estimate we get that for $q > 593$ there exist enough $\mathbb{F}_q$-rational points on $\mathcal{C}$.

Similar methods have been used by Borisov-Sapir:

A. Borisov and M. Sapir, *Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms*, Invent. Math. **160** (2005), 341–356.
A. Borisov and M. Sapir, *Polynomial maps over p-adics and residual properties of mapping tori of group endomorphisms*, Intern. Math. Research Notices 2009; Vol. 2009.

Word Maps

Let Θ be a variety of algebras, $W(X)$, $X = \{x_1, \dots, x_n\}$ a free algebra in Θ. Take $H \in \Theta$. Fix a word

$$w = w(x_1, \dots, x_n) \in W(X)$$

Consider the map

$$w : H \times H \cdots H = H^n \to H$$

defined by this word. Namely

$$w : (a_1, \dots, a_n) \to w(a_1, \dots, a_n)$$

where $a_i \in H$. Such a map is called a word map defined by a word w.

Question

Let $w(x_1, \ldots, x_n)$ be an element of the free algebra $W(X)$ and an algebra H be given. Is the equation

$$w(x_1, \ldots, x_n) = h$$

solvable?

a) for all $h \in H$?,

b) for a “typical” $h \in H$?

Question

Denote by $w(H)$ the image of the map $w : H^n \longrightarrow H$ defined by the word w.

1. Is the map w surjective, i.e., is $w(H) = H$, i.e., is the equation $w(x_1, \dots, x_n) = h$ has a solution for any $h \in H$?
2. How "big" is the image $w(H) \subset H$?
3. Describe the image $w(H)$.

In general setting the questions of such type are reasonable for simple algebras.
Let Θ be a variety of groups, $F_d(X)$ be the free group over $X = \{x_1, \dots, x_d\}$ and $H = G$ be a simple group.

Many questions can be reduced to consideration of equations in simple groups. But how???

Let A and B be subsets in G. Then $AB = \{ab, a \in A, b \in B\}$.
Correspondingly $A^k = \{a_1 a_2 \cdots a_k\}$, where $a_i \in A$.

Examples of word maps:

1. $w = x$;
2. $w = x^k$,
3. $w = [x, y] = xyx^{-1}y^{-1}$, Commutator map,
4. $w = [x, y, \dots, y]$, Engel map,
5. $w = w(x_1, \dots, x_d)$, i.e., w is an arbitrary word.

What can be said about surjectivity of the map w in each of these examples.
1. Yes. 2. No. 3. Ore problem, Yes, 4. Unknown, conjecturely - Yes, 5. Waring-type problems

Ore conjecture

Let G be a "simple" group, let $g \in G$. The equality

$$[x, y] = g$$

has a solution in G?
Connected semisimple compact topological groups (Goto, 1949),
Connected complex semisimple Lie groups (S. Pasiencier, H.-C. Wang, 1962),
Algebraic groups defined over an algebraically closed field (Ree, 1964),
Some simple groups over reals (Dokovic, 1984) and more general fields (R. C. Thompson, 1961),

One has to note that the question on the existence of a simple group not every element of which is a commutator remained open for a long time. First examples of such groups appeared in geometric context, where the groups under consideration were infinitely generated; later on there were constructed finitely generated groups with the same property. So, the great challenge was the question about finite simple groups:

Theorem (Gow, 2000)

Let G be a finite simple group of Lie type. Let $C \subset G$ be a conjugacy class consisting of regular semisimple elements. Then for every semisimple element $1 \neq g \in G$ there exist $x \in C$ and $z \in G$ such that $g = [x, z]$.

Theorem (Ellers-Gordeev, 1998)

Let $G = G(\Phi, \mathbb{F}_q)$ *be a finite simple group of Lie type, and let* $|\mathbb{F}_q| > 8$. *Then every element of* G *is a commutator, i.e., Ore conjecture holds true.*

Theorem (Liebeck, O'Brien, Shalev, Tiep, 2010)

Let $G = G(\Phi, \mathbb{F}_q)$ *be a finite simple group of Lie type. Then every element of* G *is a commutator, i.e., Ore conjecture holds true.*

Some ideas.

In fact, Ellers-Gordeev proved for $|\mathbb{F}_q| > 8$, a more strong statement, known as J.Thompson Conjecture:

Conjecture (J.Thompson)

Every finite simple group contains a conjugacy class C such that $C^2 = G$.

J.Thompson conjecture implies Ore conjecture. Indeed, $C^2 = G$ implies $1 \in C^2$, thus $C^{-1} = C$. Hence, every element of G can be represented as an element of $C^2 = C^{-1}C$, i.e., as $g^{-1}hgh^{-1} = [g, h]$.

The main tool for Ellers-Gordeev proof is the following variant of the Gauss decomposition for Chevalley groups:

Theorem (EG)

Let G be a group of Lie-type, end H, U, V be a maximal split torus, and the subgroups of "upper" and "lower" unitriangular matrices, respectively. Let h be any fixed element of H. Then, for any $g \in G$ there exists an automorphism $\tau \in Aut(G)$ such that

$$g^{\tau} = vhu,$$

where $v \in V$, $u \in U$.

Then, it can be seen that given regular h_1, h_2 in H, for any $u_1 \in V$, $u_2 \in U$ there exist a representation

$$u_1 = v_1 h_1 v_1^{-1} h_1^{-1}, \qquad u_2 = h_2^{-1} v_2 h_2 v_2^{-1},$$

where $v_1 \in V$ and $v_2 \in U$. Then, for any $g \in G$ we have

$$g = u_1 h_1 h_2 u_2 = (v_1 h_1 v_1^{-1} h_1^{-1}) h_1 h_2 (h_2^{-1} v_2 h_2 v_2^{-1}) =$$

$$(v_1 h_1 v_1^{-1})(v_2 h_2 v_2^{-1}).$$

Another approach relies on character theory by Frobenius (1896). Let $Irr(G)$ denote the set of complex irreducible characters of the finite group G. Then an element $g \in G$ is a commutator if and only if

$$\sum_{\chi \in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0,$$

Then the use of Deligne-Lusztig character theory, information on conjugacy classes and hard computer calculations allow to work out the problem and to get the solution in the case, when there are not enough regular semisimple real elements.

Engel map

Let $w = [x, y, y, \dots, y]$ be the Engel word, where the commutator is taken n times.

Conjecture (A.Shalev)

Let G be a simple non-abelian group. Then the n-Engel map is surjective for any n.

Theorem (Bandman-Garion-Grunewald, 2010)

Let $G = PSL(2, \mathbb{F}_q)$.
1. The n-th Engel word map is surjective provided that $q > q_0(n)$.
2. If $n \leq 4$ then n-th Engel word map is surjective

The main ingredient of the proof is the dynamics of the so-called trace maps.

Theorem (Classical)

Let $F = F_2(x, y))$ be embedded into $SL(2, Z)$ and denote by tr the trace character. If w is an arbitrary element of F, then the character of w can be expressed as a polynomial $tr(w) = P(s, u, t)$ with integer coefficients in the three characters $s = tr(x)$, $u = tr(xy)$, and $t = tr(y)$.

Arbitrary words

A map $f : X \to Y$ is dominant if the image of f is not contained in a closed subset of Y. Over closed fields it is equivalent to the fact that the image contains an open subset of Y.
The following teorem by Borel states that arbitrary word maps have "big" images:

Theorem (Borel, 1983, Larsen, 2004)

Let G be a connected semisimple algebraic K-group. Let $w \in F(x_1, \ldots, x_d)$. Then the word map $w : G^d \to G$ is dominant whenever $w \neq 1$, $m \geq 2$.

So, we know that the image of a word map is big, but the example of $w = x^k$ shows that it, sometimes, is not big enough to be onto.

Waring's problem after A.Shalev

Waring (1770) proposed a generalization of Lagrange's four-square theorem, stating that every rational integer is the sum of a fixed number $g(n)$ of n-th powers of positive integers, where n is any given positive integer and $g(n)$ depends only on n. Hilbert (1909) solved this problem positively.
Waring's problem for groups looks as follows. Let w be an arbitrary word from $F(x_1, \dots, x_d)$ and let G be a finite non-abelian simple group.

Is there a constant c (which may depend on w but not on G) such that

$$w(G)^c = G?$$

In other words can we represent any element $g \in G$ as

$$g = \underbrace{w(g_1)w(g_2)\cdots w(g_c)}_{c-\text{times}}$$

Theorem (Martinez-Zelmanov,Saxl-J.Wilson,1996,1997)

Let G be a large enough finite simple group. Let $w = x^k$. Then

$$g = \underbrace{w(g_1)w(g_2)\cdots w(g_c)}_{c=f(k)-\text{times}}.$$

The best possible and quite breathtaking result was obtained in the:

Theorem (Larsen-Shalev-Tiep,2010, announced)

Let w be an arbitrary word from $F(x_1, \dots, x_d)$. There exists a constant $N = N(w)$ such that for all non-abelian simple group of order greater than N

$$w(G)^2 = G.$$

Associative algebras

Word maps for associative algebras have't been considered in the same context as it was done for groups. However, one of long-standing problems in the theory of associative algebras is a typical word maps problem.

Let $w = w(x_1, x_2, \dots, x_n)$ be a word from the free associative algebra $W(X)$ over the field K , i.e., w a polynomial depending on n non-commuting variables with the coefficients from K. Let $M_n(K)$ be the matrix algebra.

Problem

What can be said about the image $w(M_n(K)) \subseteq M_n(K)$ of the word map defined by w?

Conjecture (Kaplansky-L'vov)

Let $w = w(x_1, x_2, \ldots, x_n)$ be a multilinear word from the free associative algebra $W(X)$ over the infinite field K. Then the image of w in $M_n(K)$ is represented by one of the following sets:

1. $\{0\}$,
2. *Scalar matrices,*
3. *Trace zero matrices,*
4. $M_n(K)$.

Theorem (Belov-Malev-Rowen,2010, announced)

Let K be a quadratically closed field. Then the Kaplansky-L'vov conjecture is true for $M_2(K)$.

Word maps in Lie algebras

Once again, for a given element $w(x_1, \dots, x_n)$ of the free Lie K-algebra $\mathfrak{L}_n$, and a given Lie algebra $\mathfrak{g}$ over K, one can ask :

Question

Is the equation

$$w(x_1, \dots, x_n) = A,$$

solvable for any $A \in \mathfrak{g}$.

Theorem (BGKP, 2010)

Let R be a reduced root system which does not contain irreducible components belonging to

$$\{\mathsf{A}_1, \mathsf{B}_r, \mathsf{C}_r, \mathsf{F}_4 \text{ if } \mathrm{char}(K) = 2,\ \mathsf{G}_2 \text{ if } \mathrm{char}(K) = 3\}\,. \tag{1}$$

Let $\mathfrak{g}$ be the corresponding semisimple split classical Lie K-algebra of rank r and dimension $r + 2m$. Suppose that K contains more than m elements. Then for every $n \geq 1$ the map $e_n \colon \mathfrak{g}^2 \to \mathfrak{g}$ taking (x, y) to $\underbrace{[[x, y], \dots, y]}_{n \text{ times}}$, is surjective.

Theorem (BGKP, 2010)

Let K be an algebraically closed field of characteristic $\neq 2$, and let $w = w(x_1, \ldots, x_n)$ be an element of the free Lie K-algebra $\mathfrak{L}_n$. Let $\mathfrak{g}$ be the semisimple split classical Lie K-algebra. Suppose that w is not an identity in $\mathfrak{s}l(2, K)$. Then the word map $w : \mathfrak{g}^n \to \mathfrak{g}$ is dominant.