On Shalev's conjecture for type A_n and ${}^2A_n$

Alexey Galt, Amit Kulshrestha, Anupam Singh, Evgeny Vdovin

Kazan, 2019

Classical problem in number theory (it has its own MSC number, 11P06):

Classical problem in number theory (it has its own MSC number, 11P06):

Waring problem, 1770

Does for every integer $n > 1$ there exists $k = k(n)$ such that each natural N can be expressed as $x_1^n + x_2^n + \ldots + x_{k(n)}^n$ with integer nonnegative $x_1, x_2, \ldots, x_n$?

Classical problem in number theory (it has its own MSC number, 11P06):

Waring problem, 1770

Does for every integer $n > 1$ there exists $k = k(n)$ such that each natural N can be expressed as $x_1^n + x_2^n + \ldots + x_{k(n)}^n$ with integer nonnegative $x_1, x_2, \ldots, x_n$?

An affirmative answer was provided by (D. Hilbert, 1909).

Classical problem in number theory (it has its own MSC number, 11P06):

Waring problem, 1770

Does for every integer $n > 1$ there exists $k = k(n)$ such that each natural N can be expressed as $x_1^n + x_2^n + \ldots + x_{k(n)}^n$ with integer nonnegative $x_1, x_2, \ldots, x_n$?

An affirmative answer was provided by (D. Hilbert, 1909).
The similar problem in other algebraic systems are called Warring-type problems or simply Warring problems.

Definitions and notations

By F_d we denote a free group with free generators $x_1, \ldots, x_d$.
Any element $\omega = \omega(x_1, \ldots, x_d)$ of F_d is called a world.

Definitions and notations

By F_d we denote a free group with free generators $x_1, \ldots, x_d$.
Any element $\omega = \omega(x_1, \ldots, x_d)$ of F_d is called a world.
Any world can be written $\omega = x_{i_1}^{m_1} \ldots x_{i_k}^{m_k}$, $m_i \in \mathbb{Z}$

Definitions and notations

By F_d we denote a free group with free generators $x_1, \ldots, x_d$.
Any element $\omega = \omega(x_1, \ldots, x_d)$ of F_d is called a world.
Any world can be written $\omega = x_{i_1}^{m_1} \ldots x_{i_k}^{m_k}$, $m_i \in \mathbb{Z}$
For every group G and $g_1, \ldots, g_d \in G$, we define

$$\omega(g_1, \ldots, g_d) = g_{i_1}^{m_1} \ldots g_{i_k}^{m_k} \in G.$$

Definitions and notations

By F_d we denote a free group with free generators $x_1, \ldots, x_d$.
Any element $\omega = \omega(x_1, \ldots, x_d)$ of F_d is called a world.
Any world can be written $\omega = x_{i_1}^{m_1} \ldots x_{i_k}^{m_k}$, $m_i \in \mathbb{Z}$
For every group G and $g_1, \ldots, g_d \in G$, we define

$$\omega(g_1, \ldots, g_d) = g_{i_1}^{m_1} \ldots g_{i_k}^{m_k} \in G.$$

Thus the natural map $\omega : G^d \to G$ arises and we denote its image by $\omega(G)$.

The following two problems are of particular interest and are intensively studying

The following two problems are of particular interest and are intensively studying

Problem 1.

What is the size of $\omega(G)$?

The following two problems are of particular interest and are intensively studying

Problem 1.

What is the size of $\omega(G)$?

Problem 2.

What is the ω-length of G, i.e. what is the minimal k such that $\omega(G)^k = \langle \omega(G) \rangle$?

Notice that, for every $\omega = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$,

1. $1 \in \omega(G)$
   and
2. $\omega(G)$ is $\mathrm{Aut}(G)$-invariant.

Notice that, for every $\omega = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}$,

1. $1 \in \omega(G)$
   and
2. $\omega(G)$ is $\mathrm{Aut}(G)$-invariant.

Theorem (A. Lubotzky, 2014).

Let G be a finite simple group of Lie type, and let A be a subset of G such that $1 \in A$ and A is $\mathrm{Aut}(G)$-invatiant. Then there exists $\omega \in F_2$ with $\omega(G) = A$.

Theorem (M. Larsen, A. Shalev, P. H. Tiep, 2011).

For every nonempty words $\omega_1, \omega_2 \in F_d$ there exists $N = N(\omega_1, \omega_2)$ such that for a finite nonabelian simple group G with $|G| \geqslant N$, the equality $\omega_1(G)\omega_2(G) = G$ holds.

Theorem (M. Larsen, A. Shalev, P. H. Tiep, 2011).

For every nonempty words $\omega_1, \omega_2 \in F_d$ there exists $N = N(\omega_1, \omega_2)$ such that for a finite nonabelian simple group G with $|G| \geqslant N$, the equality $\omega_1(G)\omega_2(G) = G$ holds.

Corollary (M. Larsen, A. Shalev, P. H. Tiep, 2011).

For every integer $k > 0$ there exists $N = N(k)$ such that in a finite simple group G with $|G| \geqslant N$ every element of G is a product of two k-th powers.

What words are surjective on simple groups?

What words are surjective on simple groups?

Conjecture (Ore, 1951).

Any element of a nonabelian simple group is a commutator.

What words are surjective on simple groups?

Conjecture (Ore, 1951).

Any element of a nonabelian simple group is a commutator.

The affirmative answer to the conjecture (Liebeck, O'Brien, Shalev, Tiep, 2010).

What words are surjective on simple groups?

Conjecture (Ore, 1951).

Any element of a nonabelian simple group is a commutator.

The affirmative answer to the conjecture (Liebeck, O'Brien, Shalev, Tiep, 2010).

Theorem (Guralnik, Liebeck, O'Brien, Shalev, Tiep, 2018).

(1) Let $N = p^a q^b$, where p, q are primes and a, b are nonnegative integers. Then the word $\omega(x, y) = x^N y^N$ is surjective for all finite nonabelian simple groups.

What words are surjective on simple groups?

Conjecture (Ore, 1951).

Any element of a nonabelian simple group is a commutator.

The affirmative answer to the conjecture (Liebeck, O'Brien, Shalev, Tiep, 2010).

Theorem (Guralnik, Liebeck, O'Brien, Shalev, Tiep, 2018).

(1) Let $N = p^a q^b$, where p, q are primes and a, b are nonnegative integers. Then the word $\omega(x, y) = x^N y^N$ is surjective for all finite nonabelian simple groups.
(2) Let N be an odd positive integer. Then the world $\omega(x, y, z) = x^N y^N z^N$ is surjective on all quasisimple finite groups.

Theorem (M. Larsen, A. Shalev, 2009).

Let G be a finite simple group of Lie type of rank n and $\omega \neq 1$ be a world. Then there exists $N = N(\omega)$ such that if G is not of type A_n or ${}^2A_n$, and $|G| \geqslant N$, then

$$|\omega(G)| \geqslant cn^{-1}|G|$$

for a constant $c = c(\omega) > 0$.

Theorem (M. Larsen, A. Shalev, 2009).

Let G be a finite simple group of Lie type of rank n and $\omega \neq 1$ be a world. Then there exists $N = N(\omega)$ such that if G is not of type A_n or ${}^2A_n$, and $|G| \geqslant N$, then

$$|\omega(G)| \geqslant cn^{-1}|G|$$

for a constant $c = c(\omega) > 0$.

Later in 2011 N. Nikolov and L. Pyber obtained a weaker bound for groups of type A_n and ${}^2A_n$ (of type $\frac{|G|}{k^2}$, where k is the minimal permutation representation degree of G, $k \geq 2^n - 1$, where n is the rank of G).

Conjecture

In a survey paper in 2013 A. Shalev provide the following

Conjecture 1. (A. Shalev).

For every $\omega \neq 1$ there exists $N = N(\omega)$ such that if G is an alternating group of degree n, or a finite simple group of Lie type of rank n with $|G| \geqslant N$, then

$$|\omega(G)| \geqslant cn^{-1}|G|,$$

where $c = c(\omega) > 0$ is a constant.

Conjecture

In a survey paper in 2013 A. Shalev provide the following

Conjecture 1. (A. Shalev).

For every $\omega \neq 1$ there exists $N = N(\omega)$ such that if G is an alternating group of degree n, or a finite simple group of Lie type of rank n with $|G| \geqslant N$, then

$$|\omega(G)| \geqslant cn^{-1}|G|,$$

where $c = c(\omega) > 0$ is a constant.

We say that ω is a power world, if $\omega = \upsilon^m$ for $m > 1$ and a world υ.

Conjecture

In a survey paper in 2013 A. Shalev provide the following

Conjecture 1. (A. Shalev).

For every $\omega \neq 1$ there exists $N = N(\omega)$ such that if G is an alternating group of degree n, or a finite simple group of Lie type of rank n with $|G| \geqslant N$, then

$$|\omega(G)| \geqslant cn^{-1}|G|,$$

where $c = c(\omega) > 0$ is a constant.

We say that ω is a power world, if $\omega = \upsilon^m$ for $m > 1$ and a world υ.

Conjecture 2. (A. Shalev).

Let ω be a non-power world and G be a finite simple group. Then there exist $N = N(\omega), c = c(\omega) > 0$ such that for a nonabelian simple group G with $|G| \geqslant N$ the inequality $|\omega(G)| \geqslant c|G|$ holds.

We consider the first conjecture for finite groups of type A_n and ${}^2A_n$, and a power world $\omega = x^M$.

We consider the first conjecture for finite groups of type A_n and ${}^2A_n$, and a power world $\omega = x^M$.
Notice that if

$$\omega = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}, \quad m_1 + \dots + m_k \neq 0,$$

then $|\omega(G)| \geqslant |\bar{\omega}(G)|$, where $\bar{\omega} = x^{m_1+\dots+m_k}$.

We consider the first conjecture for finite groups of type A_n and ${}^2A_n$, and a power world $\omega = x^M$.
Notice that if

$$\omega = x_{i_1}^{m_1} \dots x_{i_k}^{m_k}, \quad m_1 + \dots + m_k \neq 0,$$

then $|\omega(G)| \geqslant |\bar{\omega}(G)|$, where $\bar{\omega} = x^{m_1+\dots+m_k}$.
Moreover if, for some free variable, the sum of its powers in the world ω equals $k \neq 0$, then $|\omega(G)| \geqslant |\bar{\omega}(G)|$, where $\bar{\omega} = x^k$. So an affirmative solution to Conjecture 1 for a world x^M implies an affirmative answer for any $\omega \in F_d \setminus F_d'$.

First we we show that the constant c in the conjecture does depend on ω.

First we we show that the constant c in the conjecture does depend on ω.

Theorem 1.

Let n be a positive integer and p be a prime. Choose odd l so that $(l, n) = 1$ (in particular l could be equal to 1). Assume that T is a maximal torus of $G = \mathrm{PSL}_n^{\varepsilon}(p^l)$. Consider $\omega(x) = x^M$, where $M = p^n - (\varepsilon 1)^n$. Then

$$|\omega(G)| \leqslant \frac{4n|G|}{p-1}.$$

Theorem 2.

If $G \simeq \mathrm{SL}_n^{\varepsilon}(q)$, then for every $\omega = x^M$ there exists $N = N(\omega)$ such that

$$|\omega(G)| \geqslant \frac{1}{2nM}|G|$$

for $|G| \geqslant N$.

Theorem 2.

If $G \simeq \mathrm{SL}_n^{\varepsilon}(q)$, then for every $\omega = x^M$ there exists $N = N(\omega)$ such that

$$|\omega(G)| \geqslant \frac{1}{2nM}|G|$$

for $|G| \geqslant N$.

Moreover, an asymptotically better bound is obtained

Theorem 2.

If $G \simeq \mathrm{SL}_n^{\varepsilon}(q)$, then for every $\omega = x^M$ there exists $N = N(\omega)$ such that

$$|\omega(G)| \geqslant \frac{1}{2nM}|G|$$

for $|G| \geqslant N$.

Moreover, an asymptotically better bound is obtained

Theorem 3.

Let $\omega = x^M$ be a power word and $G = \mathrm{PSL}_n^{\varepsilon}(q)$. Then there exist positive constant N depending only on M such that if $|G| \geqslant N$, then

$$|\omega(G)| \geqslant \frac{\ln(n)}{2n \cdot M^2}|G|.$$

We believe that the bound in Theorem 2 could be strengthen to

We believe that the bound in Theorem 2 could be strengthen to

$$|\omega(G)| \geqslant c\frac{\ln^k(n)}{n}|G|,$$

where k is any positive integer.

We believe that the bound in Theorem 2 could be strengthen to

$$|\omega(G)| \geqslant c\frac{\ln^k(n)}{n}|G|,$$

where k is any positive integer.
However, we see no way to avoid the multiplier n^{-1} in the Conjecture.

We believe that the bound in Theorem 2 could be strengthen to

$$|\omega(G)| \geqslant c\frac{\ln^k(n)}{n}|G|,$$

where k is any positive integer.
However, we see no way to avoid the multiplier n^{-1} in the Conjecture.

Teorem 4.

Let $\omega = x^M$ be a power word, where $M = q - 1$. Then for any N, c there exists $G = \mathrm{PSL}_n(q)$ such that $|G| \geqslant N$ and

$$|\omega(G)| < c|G|.$$

The idea of the proof is the following. A group G can be obtained as $O^{p'}(\overline{G}_\sigma)$, where $\overline{G}$ is a simple algebraic group and σ is a Steinberg map.

The idea of the proof is the following. A group G can be obtained as $O^{p'}(\overline{G}_\sigma)$, where $\overline{G}$ is a simple algebraic group and σ is a Steinberg map. . We say that T is a maximal torus of G, if there exists a maximal σ-stable torus $\overline{T}$ of $\overline{G}$ such that $\overline{T} \cap G = T$.

The idea of the proof is the following. A group G can be obtained as $O^{p'}(\overline{G}_\sigma)$, where $\overline{G}$ is a simple algebraic group and σ is a Steinberg map. .
We say that T is a maximal torus of G, if there exists a maximal σ-stable torus $\overline{T}$ of $\overline{G}$ such that $\overline{T} \cap G = T$.
An element $s \in T$ is called regular, if $C_{\overline{G}}(s)^0 = \overline{T}$, or, equivalently, if it is contained in a unique maximal torus of G.

The idea of the proof is the following. A group G can be obtained as $O^{p'}(\overline{G}_\sigma)$, where $\overline{G}$ is a simple algebraic group and σ is a Steinberg map. .
We say that T is a maximal torus of G, if there exists a maximal σ-stable torus $\overline{T}$ of $\overline{G}$ such that $\overline{T} \cap G = T$.
An element $s \in T$ is called regular, if $C_{\overline{G}}(s)^0 = \overline{T}$, or, equivalently, if it is contained in a unique maximal torus of G.
Known result (Guralnik, Lübeck, 2001) says that

$$|G_{rs}| \geqslant |G| \left(1 - \frac{3}{q-1} - \frac{2}{(q-1)^2}\right),$$

where G_{rs} is the set of regular semisimple elements of G.

The idea of the proof is the following. A group G can be obtained as $O^{p'}(\overline{G}_\sigma)$, where $\overline{G}$ is a simple algebraic group and σ is a Steinberg map. .
We say that T is a maximal torus of G, if there exists a maximal σ-stable torus $\overline{T}$ of $\overline{G}$ such that $\overline{T} \cap G = T$.
An element $s \in T$ is called regular, if $C_{\overline{G}}(s)^0 = \overline{T}$, or, equivalently, if it is contained in a unique maximal torus of G.
Known result (Guralnik, Lübeck, 2001) says that

$$|G_{rs}| \geqslant |G| \left(1 - \frac{3}{q-1} - \frac{2}{(q-1)^2}\right),$$

where G_{rs} is the set of regular semisimple elements of G.
Now we can find $|\omega(T)|$, since T is abelian, and this allows as to derive both upper and lower bounds on $|\omega(G)|$.

THANK YOU FOR ATTENTION!