Finite groups and their arithmetic characteristics

Andrey Vasil′ev

Sobolev Institute of Mathematics and Novosibirsk State University

Kazan – 2021

Arithmetic Characteristics of a Finite Group

Let G be a finite group.

Arithmetic Characteristics of a Finite Group

Let G be a finite group. Arithmetic characteristics of G include

- $|G|$, the order of G
- $\pi(G)$, the set of prime divisors of $|G|$
- $N(G) = \{|x^G| = |G : C_G(x)| : x \in G\}$, the set of element indices of G
- $\omega(G)$, the spectrum of G that is the set of its element orders

Arithmetic Characteristics of a Finite Group

Let G be a finite group. Arithmetic characteristics of G include

- $|G|$, the order of G
- $\pi(G)$, the set of prime divisors of $|G|$
- $N(G) = \{|x^G| = |G : C_G(x)| : x \in G\}$, the set of element indices of G
- $\omega(G)$, the spectrum of G that is the set of its element orders
- $GK(G)$ is the prime (or Gruenberg – Kegel) graph of G : the graph with the vertex set equal to $\pi(G)$ and $p, q \in \pi(G)$ are adjacent iff $pq \in \omega(G)$ and $p \neq q$.

Finite Simple Groups

According to their classification, the finite simple groups are

1. the groups of prime order;
2. the alternating groups of degree at least 5;
3. the simple classical groups;
4. the simple exceptional groups of Lie type;
5. the 26 sporadic groups.

Finite Simple Groups

According to their classification, the finite simple groups are

1. the groups of prime order;
2. the alternating groups of degree at least 5;
3. the simple classical groups;
4. the simple exceptional groups of Lie type;
5. the 26 sporadic groups.

The center $Z(G)$ of a nonabelian simple group G is trivial, so G is isomorphic to the subgroup $\mathrm{Inn}(G)$ of the automorphism group $\mathrm{Aut}(G)$ consisting of the inner automorphisms of G.

Finite Simple Groups

According to their classification, the finite simple groups are

1. the groups of prime order;
2. the alternating groups of degree at least 5;
3. the simple classical groups;
4. the simple exceptional groups of Lie type;
5. the 26 sporadic groups.

The center $Z(G)$ of a nonabelian simple group G is trivial, so G is isomorphic to the subgroup $\mathrm{Inn}(G)$ of the automorphism group $\mathrm{Aut}(G)$ consisting of the inner automorphisms of G.

A finite group G is almost simple if $S \leq G \leq \mathrm{Aut}(S)$ for some nonabelian simple group S.

Two Conjectures of 1987

Conjecture (Shi Wujie, 1987)

If L is a finite simple group and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, then $G \simeq L$.

Conjecture (John Thompson, 1987)

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

Shi's Conjecture

W. Shi, J. Bi, H. Cao, M. Xu, 1987,...,2003:
Shi's conjecture is valid for all simple groups except symplectic and orthogonal groups (more precisely, except the simple groups $P\Omega^+_{2n}(q)$ with n even, $P\Omega_{2n+1}(q)$ and $Sp_{2n}(q)$).

Shi's Conjecture

W. Shi, J. Bi, H. Cao, M. Xu, 1987,...,2003:
Shi's conjecture is valid for all simple groups except symplectic and orthogonal groups (more precisely, except the simple groups $P\Omega^+_{2n}(q)$ with n even, $P\Omega_{2n+1}(q)$ and $Sp_{2n}(q)$).

M. Grechkoseeva, V. Mazurov and A. Vasil′ev, 2009:
Shi's conjecture is true for the remaining groups. It follows

Theorem A

If L is a finite simple group, and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, then $G \simeq L$.

Thompson's Conjecture

G. Chen, A. Vasil'ev, W. Shi, M. Xu, N. Ahanjideh, 1996,...,2019: Thomson's conjecture is valid for all simple groups except alternating groups and orthogonal groups of dimensions 8 and 16 (more precisely, except the simple groups $P\Omega_8^+(q)$ and $P\Omega_{16}^+(q)$).

Thompson's Conjecture

G. Chen, A. Vasil'ev, W. Shi, M. Xu, N. Ahanjideh, 1996,...,2019:
Thomson's conjecture is valid for all simple groups except alternating groups and orthogonal groups of dimensions 8 and 16 (more precisely, except the simple groups $P\Omega_8^+(q)$ and $P\Omega_{16}^+(q)$).

I. Gorshkov, 2020:
Thompson's conjecture is true for the remaining groups. It follows

Theorem B

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

Mazurov's Conjecture

- Groups G and H are isospectral if $\omega(G) = \omega(H)$
- G is recognizable (by spectrum) if $G \simeq H$ for every H isospectral to G
- G is almost recognizable if there are only finitely many (up to isomorphism) groups H isospectral to G.

Theorem (Shi, Mazurov, 1998)

If a finite group G includes a nontrivial normal abelian subgroup, then there exist infinitely many finite groups H with $\omega(H) = \omega(G)$.

Mazurov's Conjecture

- Groups G and H are isospectral if $\omega(G) = \omega(H)$
- G is recognizable (by spectrum) if $G \simeq H$ for every H isospectral to G
- G is almost recognizable if there are only finitely many (up to isomorphism) groups H isospectral to G.

Theorem (Shi, Mazurov, 1998)

If a finite group G includes a nontrivial normal abelian subgroup, then there exist infinitely many finite groups H with $\omega(H) = \omega(G)$.

Conjecture (Mazurov, 2007)

Generally, if L is a finite nonabelian simple group and G is a finite group with $\omega(G) = \omega(L)$, then $L \leqslant G \leqslant \mathrm{Aut}(L)$.

- A nonabelian simple group L is almost recognizable if $L \leqslant G \leqslant \mathrm{Aut}(L)$ for all groups G isospectral to L.

Mazurov's conjecture is valid in the following sense:

Theorem C (current version)

Let L be one of the following nonabelian simple groups:

- Sporadic groups other than J_2
- Alternating groups other than A_6 and A_{10}
- Exceptional groups of Lie type other than ${}^3D_4(2)$
- Classical groups of dimension at least 38.

If $\omega(G) = \omega(L)$, then $L \leq G \leq \operatorname{Aut} L$; all such groups G are known.

Mazurov's conjecture is valid in the following sense:

Theorem C (current version)

Let L be one of the following nonabelian simple groups:

- Sporadic groups other than J_2
- Alternating groups other than A_6 and A_{10}
- Exceptional groups of Lie type other than ${}^3D_4(2)$
- Classical groups of dimension at least 38.

If $\omega(G) = \omega(L)$, then $L \leq G \leq \operatorname{Aut} L$; all such groups G are known.

In short, "almost all simple groups are almost recognizable".

Mazurov's conjecture is valid in the following sense:

Theorem C (current version)

Let L be one of the following nonabelian simple groups:

- Sporadic groups other than J_2
- Alternating groups other than A_6 and A_{10}
- Exceptional groups of Lie type other than ${}^3D_4(2)$
- Classical groups of dimension at least 38.

If $\omega(G) = \omega(L)$, then $L \leq G \leq \operatorname{Aut} L$; all such groups G are known.

In short, "almost all simple groups are almost recognizable".

Open Problem 1

Obtain the complete answer for classical groups of dimension n, where $5 \leq n \leq 38$.

Mazurov's Conjecture: Sporadic and Alternating Groups

L is a nonabelian simple group, G is an arbitrary finite group, and $\omega(G) = \omega(L)$.

Mazurov's Conjecture: Sporadic and Alternating Groups

L is a nonabelian simple group, G is an arbitrary finite group, and $\omega(G) = \omega(L)$.

Theorem 1 (... Mazurov-Shi, 1998)

Let L be a sporadic simple group and $\omega(G) = \omega(L)$.

- If $L \neq J_2$, then $G \simeq L$.
- If $L = J_2$, then $\omega(L) = \omega(V \leftthreetimes A_8)$, where $V \simeq 2^6$.

Mazurov's Conjecture: Sporadic and Alternating Groups

L is a nonabelian simple group, G is an arbitrary finite group, and $\omega(G) = \omega(L)$.

Theorem 1 (... Mazurov-Shi, 1998)

Let L be a sporadic simple group and $\omega(G) = \omega(L)$.

- If $L \neq J_2$, then $G \simeq L$.
- If $L = J_2$, then $\omega(L) = \omega(V \leftthreetimes A_8)$, where $V \simeq 2^6$.

Theorem 2 (... Gorshkov, 2012)

Let L be an alternating group A_n, $n \geqslant 5$, and $\omega(G) = \omega(L)$.

- If $n \notin \{6, 10\}$, then $G \simeq L$.
- If $n = 6$, then $\omega(L) = \omega(V \leftthreetimes A_5)$, where $V \simeq 2^4$.
- If $n = 10$, then $\omega(L) = \omega(V \leftthreetimes H)$, where V is abelian and H contains a section isomorphic to A_5.

Mazurov's Conjecture: Groups of Lie Type

Theorem 3 (...Staroletov-Vasil'ev, 2013)

Let L be a simple exceptional group of Lie type, and $\omega(G) = \omega(L)$.

- If $L \neq {}^3D_4(2)$, then $L \leqslant G \leqslant \mathrm{Aut}(L)$.
- If $L = {}^3D_4(2)$, then $\omega(L) = \omega(V \leftthreetimes L)$, where $V \simeq 2^{24}$.

Mazurov's Conjecture: Groups of Lie Type

Theorem 3 (...Staroletov-Vasil'ev, 2013)

Let L be a simple exceptional group of Lie type, and $\omega(G) = \omega(L)$.

- If $L \neq {}^3D_4(2)$, then $L \leqslant G \leqslant \mathrm{Aut}(L)$.
- If $L = {}^3D_4(2)$, then $\omega(L) = \omega(V \leftthreetimes L)$, where $V \simeq 2^{24}$.

Theorem 4 (... Grechkoseeva-Vasil'ev, 2015)

If L is a classical group of sufficiently large dimension, and $\omega(G) = \omega(L)$, then $L \leqslant G \leqslant \mathrm{Aut}(L)$.

General Structure of a Group Isospectral to Simple

Let L be a finite nonabelian simple group.
G is a finite group with $\omega(G) = \omega(L)$.

General Structure of a Group Isospectral to Simple

Let L be a finite nonabelian simple group.
G is a finite group with $\omega(G) = \omega(L)$.

Williams (+ Gruenberg-Kegel's theorem), 1981, Kondrat′ev, 1989, Vasil′ev, Vasil′ev-Vdovin, 2005, Gorshkov, 2012:

Proposition

If L differs from $PSL_3(3)$, $PSU_3(3)$, $PSp_4(3)$, then G has exactly one nonabelian composition factor. Thus,

$$1 \leqslant K < H \leqslant G,$$

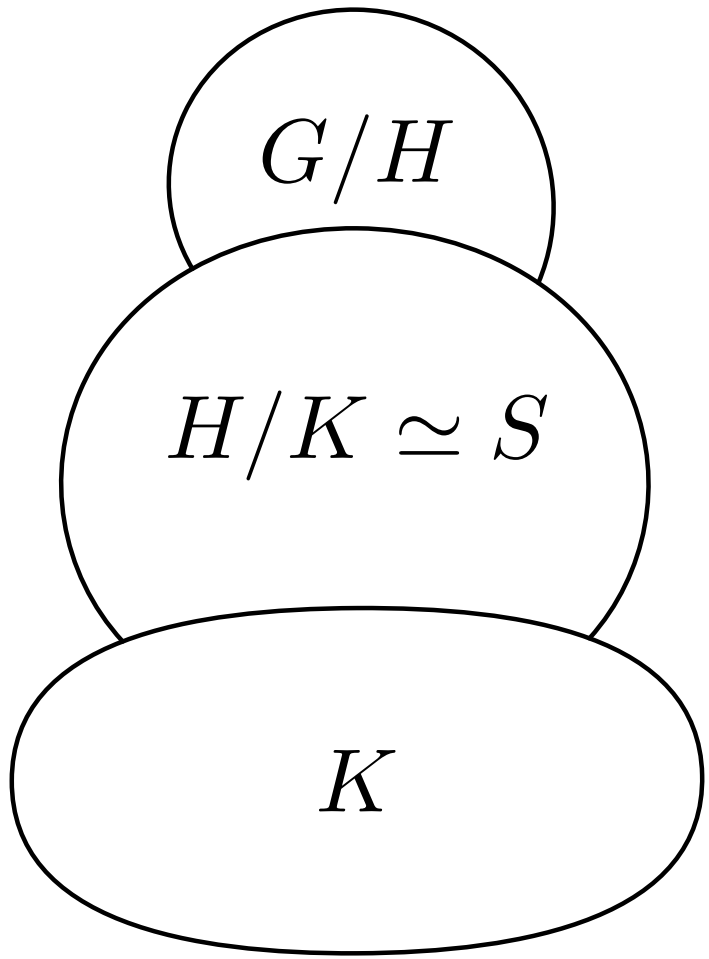
where K is the solvable radical of G,

$H/K \simeq S$, where S is a nonabelian simple group,

and $G/H \leq \mathrm{Out}(S)$ is a solvable group.

L is a nonabelian simple group, G is a group with $\omega(G) = \omega(L)$

$$1 \leqslant K < H \leqslant G$$



Theorem (N. Yang, M. Grechkoseeva, A. Vasil′ev, 2020)

If G is an nonsolvable finite group isospectral to some finite simple group L, then

$$1 \leqslant K < H \leqslant G,$$

where H/K is a nonabelian simple group, and K being the solvable radical of G is nilpotent provided $L \neq A_{10}$.

Remark. The claim is not true for A_{10} (Mazurov, 1998)

Theorem (N. Yang, M. Grechkoseeva, A. Vasil'ev, 2020)

If G is an nonsolvable finite group isospectral to some finite simple group L, then

$$1 \leqslant K < H \leqslant G,$$

where H/K is a nonabelian simple group, and K being the solvable radical of G is nilpotent provided $L \neq A_{10}$.

Remark. The claim is not true for A_{10} (Mazurov, 1998)

The quotient $G/H \leq \mathrm{Out}(S)$, so it is a solvable group by the validity of the Schreier conjecture.

Open Problem 2

Is it true that G/H is cyclic?

Remark. This is true for all known almost recognizable simple groups (see Theorem C).

Recognition of non-simple groups

By the Mazurov-Shi theorem, groups with nontrivial solvable radical are nonrecognizable.

Do there exist recognizable or almost recognizable finite groups which are not simple?

Recognition of non-simple groups

By the Mazurov-Shi theorem, groups with nontrivial solvable radical are nonrecognizable.

Do there exist recognizable or almost recognizable finite groups which are not simple?

Theorem (Mazurov, 1997)

Let $L = Sz(2^7) = {}^2B_2(2^7)$. The following groups are recognizable:

- $L \times L$;
- $L \wr F$, the permutation wreath product of L and the Frobenius group $F = 23 : 11$ of degree 23.

Recognition of non-simple groups

By the Mazurov-Shi theorem, groups with nontrivial solvable radical are nonrecognizable.

Do there exist recognizable or almost recognizable finite groups which are not simple?

Theorem (Mazurov, 1997)

Let $L = Sz(2^7) = {}^2B_2(2^7)$. The following groups are recognizable:

- $L \times L$;
- $L \wr F$, the permutation wreath product of L and the Frobenius group $F = 23 : 11$ of degree 23.

Theorem (Gorshkov, Maslova, 2020)

The group $J_4 \times J_4$, where J_4 is the sporadic Janko group, is recognizable.

Despite the examples from the previous slide, it is easy to see that

- $\omega(A_5 \times A_5) = \omega(F_1 \times F_2)$, where F_1 and F_2 are Frobenius groups with the kernels isomorphic to Z_5^2 and complements of order 2 and 3, respectively.
- $\omega(A_5 \times A_5 \times A_5) = \omega(Z_2^6 \times Z_3^3 \times Z_5^3)$ and these two groups are of the same order!

Despite the examples from the previous slide, it is easy to see that

- $\omega(A_5 \times A_5) = \omega(F_1 \times F_2)$, where F_1 and F_2 are Frobenius groups with the kernels isomorphic to Z_5^2 and complements of order 2 and 3, respectively.
- $\omega(A_5 \times A_5 \times A_5) = \omega(Z_2^6 \times Z_3^3 \times Z_5^3)$ and these two groups are of the same order!

The infinite series of recognizable non-simple groups is given by

Theorem (Gorshkov, 2021)

The groups $PSL_{2^m}(2) \times PSL_{2^m}(2) \times PSL_{2^m}(2)$ are recognizable for $m \geq 6$.

Despite the examples from the previous slide, it is easy to see that

- $\omega(A_5 \times A_5) = \omega(F_1 \times F_2)$, where F_1 and F_2 are Frobenius groups with the kernels isomorphic to Z_5^2 and complements of order 2 and 3, respectively.
- $\omega(A_5 \times A_5 \times A_5) = \omega(Z_2^6 \times Z_3^3 \times Z_5^3)$ and these two groups are of the same order!

The infinite series of recognizable non-simple groups is given by

Theorem (Gorshkov, 2021)

The groups $PSL_{2^m}(2) \times PSL_{2^m}(2) \times PSL_{2^m}(2)$ are recognizable for $m \geq 6$.

Open Problem 3

Does there exist a recognizable group which is a direct product of

1. non-isomorphic simple groups,
2. m copies of a simple group for arbitrarily large m?

Spectra of Finite Simple Groups

- Spectra of sporadic and alternating groups are well known
- Spectra of simple classical groups (... Buturlakin, 2009)
- Spectra of simple exceptional groups (... Buturlakin, 2018).

Spectra of Finite Simple Groups

- Spectra of sporadic and alternating groups are well known
- Spectra of simple classical groups (... Buturlakin, 2009)
- Spectra of simple exceptional groups (... Buturlakin, 2018).

Set $\mu(G)$ for the set of maximal w.r.t divisibility elements of the spectrum $\omega(G)$ of a group G. Clearly, $\omega(G)$ can be recovered from $\mu(G)$ and even from any set $\nu(G)$ satisfying

$$\mu(G) \subseteq \nu(G) \subseteq \omega(G).$$

Spectra of Finite Simple Groups

- Spectra of sporadic and alternating groups are well known
- Spectra of simple classical groups (... Buturlakin, 2009)
- Spectra of simple exceptional groups (... Buturlakin, 2018).

Set $\mu(G)$ for the set of maximal w.r.t divisibility elements of the spectrum $\omega(G)$ of a group G. Clearly, $\omega(G)$ can be recovered from $\mu(G)$ and even from any set $\nu(G)$ satisfying

$$\mu(G) \subseteq \nu(G) \subseteq \omega(G).$$

The spectrum of G is known if some $\nu(G)$ is described.

Theorem D

If G is a finite simple group, then $\omega(G)$ is known.

Spectra of Finite Simple Groups

- Spectra of sporadic and alternating groups are well known
- Spectra of simple classical groups (... Buturlakin, 2009)
- Spectra of simple exceptional groups (... Buturlakin, 2018).

Set $\mu(G)$ for the set of maximal w.r.t divisibility elements of the spectrum $\omega(G)$ of a group G. Clearly, $\omega(G)$ can be recovered from $\mu(G)$ and even from any set $\nu(G)$ satisfying

$$\mu(G) \subseteq \nu(G) \subseteq \omega(G).$$

The spectrum of G is known if some $\nu(G)$ is described.

Theorem D

If G is a finite simple group, then $\omega(G)$ is known.

Open Problem 4

Describe the spectra of the finite almost simple groups.

Constructive Recognition of Simple Groups

$\mathcal{M}$ is a finite set of positive integers
$\omega(\mathcal{M})$ is the set of all divisors of elements of $\mathcal{M}$
$\mu(\mathcal{M}) \subseteq \mathcal{M}$ consists of the elements maximal w.r.t divisibility.

Constructive Recognition of Simple Groups

$\mathcal{M}$ is a finite set of positive integers
$\omega(\mathcal{M})$ is the set of all divisors of elements of $\mathcal{M}$
$\mu(\mathcal{M}) \subseteq \mathcal{M}$ consists of the elements maximal w.r.t divisibility.

If G is a finite group, then $\mu(G) = \mu(\omega(G))$.

Constructive Recognition of Simple Groups

$\mathcal{M}$ is a finite set of positive integers
$\omega(\mathcal{M})$ is the set of all divisors of elements of $\mathcal{M}$
$\mu(\mathcal{M}) \subseteq \mathcal{M}$ consists of the elements maximal w.r.t divisibility.

If G is a finite group, then $\mu(G) = \mu(\omega(G))$.

General problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite group G such that

$$\omega(G) = \mathcal{M},$$

and if it exists, describe all finite groups with this property.

Constructive Recognition of Simple Groups

$\mathcal{M}$ is a finite set of positive integers
$\omega(\mathcal{M})$ is the set of all divisors of elements of $\mathcal{M}$
$\mu(\mathcal{M}) \subseteq \mathcal{M}$ consists of the elements maximal w.r.t divisibility.

If G is a finite group, then $\mu(G) = \mu(\omega(G))$.

General problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite group G such that

$$\omega(G) = \omega(\mathcal{M}),$$

and if it exists, describe all finite groups with this property.

Constructive Recognition of Simple Groups

$\mathcal{M}$ is a finite set of positive integers
$\omega(\mathcal{M})$ is the set of all divisors of elements of $\mathcal{M}$
$\mu(\mathcal{M}) \subseteq \mathcal{M}$ consists of the elements maximal w.r.t divisibility.

If G is a finite group, then $\mu(G) = \mu(\omega(G))$.

Problem for simple groups

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that

$$\omega(G) = \omega(\mathcal{M}),$$

and if it exists, describe all finite groups with this property.

Problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that

$$\omega(G) = \omega(\mathcal{M}).$$

Problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that

$$\omega(G) = \omega(\mathcal{M}).$$

If the problem is solved and we obtained a simple group, then Theorem C (in most cases) yields the complete (and finite) list of groups enjoying this property.

Problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that

$$\omega(G) = \omega(\mathcal{M}).$$

If the problem is solved and we obtained a simple group, then Theorem C (in most cases) yields the complete (and finite) list of groups enjoying this property.

Since we have the description of spectra of finite simple groups (Theorem D), we can solve the problem (at least theoretically).

Thus, the really intriguing question is if we can do this effectively?

Problem

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that

$$\omega(G) = \omega(\mathcal{M}).$$

If the problem is solved and we obtained a simple group, then Theorem C (in most cases) yields the complete (and finite) list of groups enjoying this property.

Since we have the description of spectra of finite simple groups (Theorem D), we can solve the problem (at least theoretically).

Thus, the really intriguing question is if we can do this effectively?

More precisely, can we do this in time polynomial in the length m of a set $\mathcal{M}$, that is the sum of $\log x$ where x runs over $\mathcal{M}$.

Theorem (Buturlakin – Vasil′ev, 2019)

There is an algorithm that, given a set $\mathcal{M}$ of positive integers, outputs either an empty set, in which case there is no finite simple group H with $\omega(H) = \omega(\mathcal{M})$, or a unique simple group G satisfying the properties: (1) $\omega(\mathcal{M}) \subseteq \omega(G)$; (2) $\omega(H) \neq \omega(\mathcal{M})$ for every finite simple group H whose spectrum differs from $\omega(G)$. The running time of the algorithm is polynomial in the length of the input.

Theorem (Buturlakin – Vasil′ev, 2019)

There is an algorithm that, given a set $\mathcal{M}$ of positive integers, outputs either an empty set, in which case there is no finite simple group H with $\omega(H) = \omega(\mathcal{M})$, or a unique simple group G satisfying the properties: (1) $\omega(\mathcal{M}) \subseteq \omega(G)$; (2) $\omega(H) \neq \omega(\mathcal{M})$ for every finite simple group H whose spectrum differs from $\omega(G)$. The running time of the algorithm is polynomial in the length of the input.

Thus, to complete the task, one need to verify that

$$\omega(G) \subseteq \omega(\mathcal{M})$$

for the unique possible simple group G (if it exists).

Generating the Spectra of Simple Groups

Theorem (Buturlakin, 2008)

Let $G = PSL_n(q)$, where $n \geqslant 2$ and q is a power of a prime p. Put $d = (n, q-1)$. Let $\nu(G)$ consists of the following numbers:

(1) $\frac{q^n-1}{d(q-1)}$;

(2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2),q-1)}$ for $n_1, n_2 > 0$ such that $n_1 + n_2 = n$;

(3) $[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ for $s \geqslant 3$ and $n_1, n_2, \ldots, n_s > 0$ such that $n_1 + n_2 + \ldots + n_s = n$;

(4) $p^k \frac{q^{n_1}-1}{d}$ for $k, n_1 > 0$ such that $p^{k-1} + 1 + n_1 = n$;

(5) $p^k[q^{n_1}-1, q^{n_2}-1, \ldots, q^{n_s}-1]$ for $s \geqslant 2$ and $k, n_1, n_2 \ldots, n_s > 0$ such that $p^{k-1} + 1 + n_1 + n_2 + \ldots + n_s = n$;

(6) p^k, if $p^{k-1} + 1 = n$ for $k > 0$.

Then $\mu(G) \subseteq \nu(G) \subseteq \omega(G)$.

The analysis of the efficiency of the most straightforward algorithms provided by the known description of spectra of groups of Lie type implies that $\mu(G)$ can be found

- in time polynomial in the length m of $\mu(G)$ if G is an alternating group or exceptional group of Lie type;
- in time $m^{O(\sqrt{\log \log m})}$ if G is a classical group.

The analysis of the efficiency of the most straightforward algorithms provided by the known description of spectra of groups of Lie type implies that $\mu(G)$ can be found

- in time polynomial in the length m of $\mu(G)$ if G is an alternating group or exceptional group of Lie type;
- in time $m^{O(\sqrt{\log\log m})}$ if G is a classical group.

Theorem E

There is an algorithm that given a set $\mathcal{M}$ of positive integers outputs a finite simple group G with $\omega(G) = \omega(\mathcal{M})$, or says that there is no such a group. The running time of the algorithm is $m^{O(\sqrt{\log\log m})}$, where m is the length of $\mathcal{M}$.

The analysis of the efficiency of the most straightforward algorithms provided by the known description of spectra of groups of Lie type implies that $\mu(G)$ can be found

- in time polynomial in the length m of $\mu(G)$ if G is an alternating group or exceptional group of Lie type;
- in time $m^{O(\sqrt{\log\log m})}$ if G is a classical group.

Theorem E

There is an algorithm that given a set $\mathcal{M}$ of positive integers outputs a finite simple group G with $\omega(G) = \omega(\mathcal{M})$, or says that there is no such a group. The running time of the algorithm is $m^{O(\sqrt{\log\log m})}$, where m is the length of $\mathcal{M}$.

Open Problem 5

Does there exist a polynomial-time algorithm?

$N(G) = \{|x^G| : x \in G\}$, the set of element indices of G.

Theorem B

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

$N(G) = \{|x^G| : x \in G\}$, the set of element indices of G.

Theorem B

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

Open Problem 6

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that $N(G) = \mathcal{M}$.

$N(G) = \{|x^G| : x \in G\}$, the set of element indices of G.

Theorem B

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

Open Problem 6

Given a finite set $\mathcal{M}$ of positive integers, determine whether there exists a finite simple group G such that $N(G) = \mathcal{M}$.

Open Problem 7

Describe the sets $N(G)$ for all finite (almost) simple groups G.

Theorem A (Shi's Conjecture)

If L is a finite simple group and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$, then $G \simeq L$.

Theorem B (Thompson's Conjecture)

If L is a finite simple group and G is a finite group with $N(G) = N(L)$ and $Z(G) = 1$, then $G \simeq L$.

Theorem C (Mazurov's Conjecture)

If L is a finite simple group and G is a finite group with $\omega(G) = \omega(L)$, then (in most cases) $L \leq G \leq \mathrm{Aut}(L)$.

Theorem D

If G is a finite simple group, then $\omega(G)$ is known.

Theorem E

There is a quasi-polynomial algorithm that given $\mathcal{M} \subseteq \mathbb{N}$ decides if there is a finite simple group G with $\omega(G) = \omega(\mathcal{M})$.