Solvability and order type for finite groups

Paweł Piwek

University of Oxford

Online, March 2025

Metaquestion

Which properties of a group G can we discern from knowing only the orders of its elements?

Definition

The *average order* of elements of a group G is defined as

$$\overline{\mathrm{ord}}(G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{ord}(g)$$

Definition

The *average order* of elements of a group G is defined as

$$\overline{\text{ord}}(G) = \frac{1}{|G|}\sum_{g\in G}\text{ord}(g)$$

Theorems A and C of Herzog et al. (2022)

If $\overline{\text{ord}}(G) < \overline{\text{ord}}(S_3) = \frac{13}{6}$ then $G \cong C_2 \times \ldots \times C_2$.

If $\overline{\text{ord}}(G) < \overline{\text{ord}}(A_5) = \frac{211}{60}$ then G is solvable.

Theorem[1]

Let $\psi'(G) := \overline{\text{ord}}(G)/\,\overline{\text{ord}}(C_{|G|})$.

[1]See Theorem 1.2 of Lazorec and Tărnăuceanu (2023) for the original references.

Theorem[1]

Let $\psi'(G) := \overline{\mathrm{ord}}(G)/\,\overline{\mathrm{ord}}(C_{|G|})$.

- If $\psi'(G) > \frac{7}{11} = \psi'(C_2 \times C_2)$, then G is cyclic.

[1] See Theorem 1.2 of Lazorec and Tărnăuceanu (2023) for the original references.

Theorem[1]

Let $\psi'(G) := \overline{\text{ord}}(G)/\,\overline{\text{ord}}(C_{|G|})$.

- If $\psi'(G) > \frac{7}{11} = \psi'(C_2 \times C_2)$, then G is cyclic.
- If $\psi'(G) > \frac{13}{21} = \psi'(S_3)$, then G is nilpotent.

[1] See Theorem 1.2 of Lazorec and Tărnăuceanu (2023) for the original references.

Theorem[1]

Let $\psi'(G) := \overline{\text{ord}}(G)/\overline{\text{ord}}(C_{|G|})$.

- If $\psi'(G) > \frac{7}{11} = \psi'(C_2 \times C_2)$, then G is cyclic.
- If $\psi'(G) > \frac{13}{21} = \psi'(S_3)$, then G is nilpotent.
- If $\psi'(G) > \frac{31}{77} = \psi'(A_4)$, then G is super-solvable.

[1] See Theorem 1.2 of Lazorec and Tărnăuceanu (2023) for the original references.

Theorem[1]

Let $\psi'(G) := \overline{\text{ord}}(G)/\,\overline{\text{ord}}(C_{|G|})$.

- If $\psi'(G) > \frac{7}{11} = \psi'(C_2 \times C_2)$, then G is cyclic.
- If $\psi'(G) > \frac{13}{21} = \psi'(S_3)$, then G is nilpotent.
- If $\psi'(G) > \frac{31}{77} = \psi'(A_4)$, then G is super-solvable.
- If $\psi'(G) > \frac{211}{1617} = \psi'(A_5)$, then G is solvable.

[1] See Theorem 1.2 of Lazorec and Tărnăuceanu (2023) for the original references.

Definitions

Let's denote by *spectrum* $\mathrm{spec}(G)$ of a group G the set of its element orders.

Definitions

Let's denote by *spectrum* spec(G) of a group G the set of its element orders.

Example

$$\mathrm{spec}(C_4) = \mathrm{spec}(D_4) = \mathrm{spec}(Q_8) = \{1, 2, 4\}.$$

Definitions

Let's denote by *spectrum* spec(G) of a group G the set of its element orders.

Example

$$\mathrm{spec}(C_4) = \mathrm{spec}(D_4) = \mathrm{spec}(Q_8) = \{1, 2, 4\}.$$

Theorem of Shi (1984)

Let G be a finite group such that

- there are at least 3 primes in spec(G);
- every element of spec(G) is either a power of 2 or a prime different from 5.

Then $G \cong \mathrm{PSL}(2, 7)$.

Definitions

Let's denote by *spectrum* spec(G) of a group G the set of its element orders.

Example

$$\mathrm{spec}(C_4) = \mathrm{spec}(D_4) = \mathrm{spec}(Q_8) = \{1, 2, 4\}.$$

Theorem of Shi (1984)

Let G be a finite group such that

- there are at least 3 primes in spec(G);
- every element of spec(G) is either a power of 2 or a prime different from 5.

Then $G \cong \mathrm{PSL}(2, 7)$. In particular

$$\mathrm{spec}(G) = \{1, 2, 3, 4, 7\} \implies G \cong \mathrm{PSL}(2, 7).$$

Theorems of Shi (1986); Brandl and Shi (1991)

$$\mathrm{spec}(G) = \{1, 2, 3, 5\} \implies G \cong A_5.$$

$$\mathrm{spec}(G) = \{1, 2, 3, 4, 5, 6, 7\} \implies G \cong A_7.$$

Such groups are called *recognisable*.[2]

[2] Most of the finite simple groups are in fact recognisable; see Shi (2012) for many more results.

Theorems of Shi (1986); Brandl and Shi (1991)

$$\mathrm{spec}(G) = \{1, 2, 3, 5\} \implies G \cong A_5.$$

$$\mathrm{spec}(G) = \{1, 2, 3, 4, 5, 6, 7\} \implies G \cong A_7.$$

Such groups are called *recognisable.*[2]

Problem 2.2 of Shi (2024)

Which types of sets of natural numbers can represent spec(G) for a finite group G?

[2] Most of the finite simple groups are in fact recognisable; see Shi (2012) for many more results.

Definition

The graph, whose vertices are prime numbers in $\mathrm{spec}(G)$, with vertices p, q connected when $pq \in \mathrm{spec}(G)$, is called the *prime graph* or the *Gruenberg–Kegel graph* of a group G.[3]

[3] See Gruenberg and Roggenkamp (1975) for the original paper and Cameron (2022) for a survey.

Definition

The graph, whose vertices are prime numbers in $\mathrm{spec}(G)$, with vertices p, q connected when $pq \in \mathrm{spec}(G)$, is called the *prime graph* or the *Gruenberg–Kegel graph* of a group G.[3]

Theorem A of Gruenberg and Roggenkamp (1975)

Let G be a group whose prime graph is disconnected. If $|G|$ is even let π_1 be the set of primes in the component of 2. Then G has one of the following structures.

- Frobenius, or 2-Frobenius,
- (π_1 group)-by-simple-by-(π_1 group).

[3] See Gruenberg and Roggenkamp (1975) for the original paper and Cameron (2022) for a survey.

Shi's Conjecture

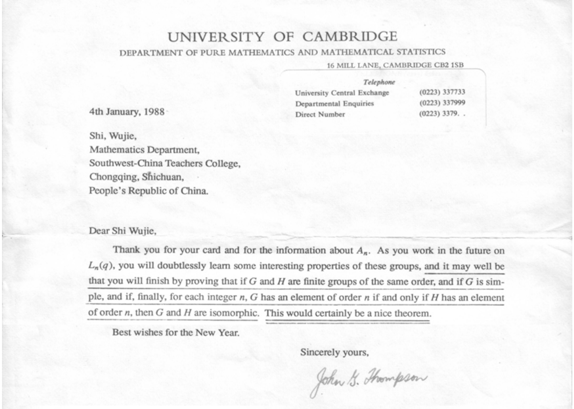
Let S be a simple group and G a group such that $|G| = |S|$. Then

$$\mathrm{spec}(G) = \mathrm{spec}(S) \implies G \cong S.$$

Shi's Conjecture

Let S be a simple group and G a group such that $|G| = |S|$. Then

$$\mathrm{spec}(G) = \mathrm{spec}(S) \implies G \cong S.$$



UNIVERSITY OF CAMBRIDGE

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS

16 MILL LANE, CAMBRIDGE CB2 1SB

Telephone

University Central Exchange	(0223) 337733
Departmental Enquiries	(0223) 337999
Direct Number	(0223) 3379. .

4th January, 1988

Shi, Wujie,
Mathematics Department,
Southwest-China Teachers College,
Chongqing, Shichuan,
People's Republic of China.

Dear Shi Wujie,

Thank you for your card and for the information about A_n. As you work in the future on $L_n(q)$, you will doubtlessly learn some interesting properties of these groups, and it may well be that you will finish by proving that if G and H are finite groups of the same order, and if G is simple, and if, finally, for each integer n, G has an element of order n if and only if H has an element of order n, then G and H are isomorphic. This would certainly be a nice theorem.

Best wishes for the New Year.

Sincerely yours,

John G. Thompson

Figure: Redacted letter from John G. Thompson to Wujie Shi.

Theorem

Let S be a simple group and G a group such that $|G| = |S|$. Then

$$\mathrm{spec}(G) = \mathrm{spec}(S) \implies G \cong S.$$

The proof was finished in Vasil'ev et al. (2009).

Theorem of Feit and Thompson (1963)

All finite groups of odd size are solvable.

Thompson's Problem

UNIVERSITY OF CAMBRIDGE

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS

16 MILL LANE, CAMBRIDGE CB2 1SB
TELEPHONE (0223) 65621

22nd April, 1987

Shi Wujie,
Department of Mathematics,
Southwest China Teachers
University,
Chongqing,
CHINA.

Dear Shi Wujie,

Thank you for your letter of March 12, which has arrived together with the abstract of the result you wish to present in Singapore.

I expect the conjecture you mention is correct, although I have no proof. But one idea which should be helpful, and which you have probably already realized, is that, if G is a finite simple group of Lie type defined over a field of characteristic p, then one can attempt to determine p uniquely from the knowledge of $\pi_e(G)$. This attempt will fail in a few cases, e.g.,

$G \cong L_2(4) \cong L_2(5)$ or $G \cong L_2(7) \cong L_3(2)$,

but it seems reasonable to think that if, in addition to being of Lie type and characteristic p, $|G| > 10^5$, then p can be recovered from $\pi_e(G)$.

A related problem to the one you have been considering is the following one:

For each finite group G and each integer $d \geq 1$, Let $G(d) = \{x \in G \mid x^d = 1\}$.

Definition. G_1 and G_2 are of the same order type iff $|G_1(d)| = |G_2(d)|$, $\forall d = 1, 2, \ldots$.

Here is an open problem. Suppose G_1, G_2 are finite groups of the same order type. Suppose also that G_1 is

- 2 -

solvable. Is it true that G_2 is also necessarily solvable? I do not know the answer.

In order to give some indication that the above problem is not too easy, let me mention that the Mathieu group M_{23} has two subgroups H, K, each of index 11.23, which are of the same order type, but that $H \cong M_{21}.2 \cong L_3(4).2$, while $K \cong 2^4.A_7$. This example shows that there are finite groups G_1, G_2 of the same order type which do not have the same set of composition factors.

I have talked with several mathematicians concerning groups of the same order type. The problem arose initially in the study of algebraic number fields, and is of considerable interest.

I expect to meet you in Singapore.

Sincerely yours,

John G. Thompson

Definition

For a group G we define its *order type* $o_G : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by

$$o_G(n) = |\{g \in G \mid \text{ord}(g) = n\}|$$

Definition

For a group G we define its *order type* $o_G : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by

$$o_G(n) = |\{g \in G \mid \operatorname{ord}(g) = n\}|$$

and its *exponent type* $e_G : \mathbb{N} \to \mathbb{N}$ by

$$e_G(n) = |\{g \in G \mid g^n = 1\}|.$$

Definition

For a group G we define its *order type* $o_G : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by

$$o_G(n) = |\{g \in G \mid \mathrm{ord}(g) = n\}|$$

and its *exponent type* $e_G : \mathbb{N} \to \mathbb{N}$ by

$$e_G(n) = |\{g \in G \mid g^n = 1\}|.$$

Thompson's Problem (1987)

Let G be a finite solvable group and H be any finite group such that $o_G = o_H$. Is H necessarily solvable?

Definition

For a group G we define its *order type* $o_G : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by

$$o_G(n) = |\{g \in G \mid \operatorname{ord}(g) = n\}|$$

and its *exponent type* $e_G : \mathbb{N} \to \mathbb{N}$ by

$$e_G(n) = |\{g \in G \mid g^n = 1\}|.$$

Thompson's Problem (1987)

Let G be a finite solvable group and H be any finite group such that $o_G = o_H$. Is H necessarily solvable?

Theorem of Piwek (2024)

No.

A positive result

Theorem 1.3 of Shen et al. (2023)

Let G_1 and G_2 be groups of the same order type whose prime graphs are disconnected. Then if G_1 is solvable, so is G_2.

Abelian

Proposition

If $x^2 = 1$ for every element $x \in G$, then $G \cong C_2 \times C_2 \times \ldots \times C_2$.

Abelian

Proposition

If $x^2 = 1$ for every element $x \in G$, then $G \cong C_2 \times C_2 \times \ldots \times C_2$.

Proof.

$$[x, y] = xy \cdot x^{-1} \cdot y^{-1} = xy \cdot x \cdot y = (xy)^2 = 1. \qquad \square$$

Abelian

Proposition

If $x^2 = 1$ for every element $x \in G$, then $G \cong C_2 \times C_2 \times \ldots \times C_2$.

Proof.

$$[x, y] = xy \cdot x^{-1} \cdot y^{-1} = xy \cdot x \cdot y = (xy)^2 = 1. \qquad \square$$

Example

The Heisenberg group $H = H_3(\mathbb{F}_3) \cong (C_3 \times C_3) \rtimes C_3$ of 3-by-3 unit upper-triangular matrices.

Abelian

Proposition

If $x^2 = 1$ for every element $x \in G$, then $G \cong C_2 \times C_2 \times \ldots \times C_2$.

Proof.

$$[x, y] = xy \cdot x^{-1} \cdot y^{-1} = xy \cdot x \cdot y = (xy)^2 = 1.$$ □

Example

The Heisenberg group $H = H_3(\mathbb{F}_3) \cong (C_3 \times C_3) \rtimes C_3$ of 3-by-3 unit upper-triangular matrices.

It is non-abelian, yet $A^3 = I$ for any $A \in H$, so $o_H = o_G$ for $G = C_3 \times C_3 \times C_3$.

Nilpotent

Definition

A group G is *nilpotent* if for some n the n-th iterated commutator $G_n = [G, [G, [\ldots, [G, G]] \ldots]]$ is trivial.

In other words, $G_n = 1$ where $G_0 = G$ and $G_{i+1} = [G, G_i]$.

Nilpotent

Theorem

A finite group G is nilpotent if and only if there exist groups $G_1, \ldots, G_k$ and primes $p_1, \ldots, p_k$ such that $G \cong G_1 \times G_2 \times \ldots G_k$ and $|G_i| = p_i^{\alpha_i}$.

Nilpotent

Theorem

A finite group G is nilpotent if and only if there exist groups $G_1, \dots, G_k$ and primes $p_1, \dots, p_k$ such that $G \cong G_1 \times G_2 \times \dots G_k$ and $|G_i| = p_i^{\alpha_i}$.

Proposition

A group G is nilpotent if and only if for each i

$$e_G(p_i^{\alpha_i}) = |\{g \in G \mid g^{p_i^{\alpha_i}} = 1\}| = p_i^{\alpha_i},$$

where $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Super-solvable

Definition

A group G is *super-solvable* if there is a series of normal subgroups $G_i \triangleleft G$ such that for some ordering of prime factors p_i of $|G|$

$$1 = G_0 < G_1 < \dots G_k = G$$

and $|G_i| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i}$, where $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Super-solvable

Definition

A group G is *super-solvable* if there is a series of normal subgroups $G_i \lhd G$ such that for some ordering of prime factors p_i of $|G|$

$$1 = G_0 < G_1 < \ldots G_k = G$$

and $|G_i| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}$, where $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Proposition

A group G is super-solvable if and only if, for some ordering of prime factors p_i of G, for each i

$$e_G(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}) = |\{g \in G \mid g^{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}} = 1\}| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i},$$

where $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

For details see Shen (2012).

Solvable

Definition

A group G is *solvable* if for some n the n-th term of derived series $G^{(n)} = [\ldots[[G, G], [G, G]]\ldots]$ is trivial.

In other words, $G^{(n)} = 1$ where $G_0 = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

Strategy

Main ideas

Strategy

Main ideas

- Orders of elements are ‘well-behaved’ under direct products.

Strategy

Main ideas

- Orders of elements are 'well-behaved' under direct products.
- $G_1 \times \ldots G_k$ is solvable if and only if each of G_i is solvable.

Order type and direct products

For $(g, h) \in G \times H$ we have: $\mathrm{ord}\big((g, h)\big) = \mathrm{lcm}\{\mathrm{ord}(g), \mathrm{ord}(h)\}$.

Order type and direct products

For $(g, h) \in G \times H$ we have: $\mathrm{ord}\big((g,h)\big) = \mathrm{lcm}\{\mathrm{ord}(g), \mathrm{ord}(h)\}$.
Thus

$$o_{G\times H}(m) = \sum_{k,l \text{ st. } \mathrm{lcm}\{k,l\}=m} o_G(k) \cdot o_H(l).$$

Order type and direct products

For $(g, h) \in G \times H$ we have: $\operatorname{ord}\big((g,h)\big) = \operatorname{lcm}\{\operatorname{ord}(g), \operatorname{ord}(h)\}$.
Thus

$$o_{G\times H}(m) = \sum_{k,l \text{ st. } \operatorname{lcm}\{k,l\}=m} o_G(k) \cdot o_H(l).$$

Exponent type and direct products

For $(g, h) \in G \times H$ we have: $(g, h)^n = (1, 1) \iff g^n = h^n = 1$.

Order type and direct products

For $(g, h) \in G \times H$ we have: $\operatorname{ord}\big((g, h)\big) = \operatorname{lcm}\{\operatorname{ord}(g), \operatorname{ord}(h)\}$.
Thus

$$o_{G\times H}(m) = \sum_{k,l \text{ st. } \operatorname{lcm}\{k,l\}=m} o_G(k) \cdot o_H(l).$$

Exponent type and direct products

For $(g, h) \in G \times H$ we have: $(g, h)^n = (1, 1) \iff g^n = h^n = 1$.
Thus

$$e_{G\times H}(n) = e_G(n) \cdot e_H(n).$$

Proposition

For any groups G and H

$$o_G = o_H \iff e_G = e_H.$$

Proposition

For any groups G and H

$$o_G = o_H \iff e_G = e_H.$$

Proof.

Each element $g \in G$ such that $g^n = 1$ has order dividing n, so

$$e_G(n) = \sum_{d|n} o_G(d).$$

Proposition

For any groups G and H

$$o_G = o_H \iff e_G = e_H.$$

Proof.

Each element $g \in G$ such that $g^n = 1$ has order dividing n, so

$$e_G(n) = \sum_{d|n} o_G(d).$$

Applying Möbius inversion to this equation we get

$$o_G(n) = \sum_{d|n} e_G(n/d) \cdot \mu(d). \qquad \square$$

Example

Example

o_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	1	0	0	0	0	0	0	0	0	0	0
S_3	1	3	2	0	0	0	0	0	0	0	0	0
D_6	1	7	2	0	0	2	0	0	0	0	0	0

Table: Order types of groups C_2, S_3 and D_6.

Example

o_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	1	0	0	0	0	0	0	0	0	0	0
S_3	1	3	2	0	0	0	0	0	0	0	0	0
D_6	1	7	2	0	0	2	0	0	0	0	0	0

Table: Order types of groups C_2, S_3 and D_6.

e_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	2	1	2	1	2	1	2	1	2
S_3	1	4	3	4	1	6	1	4	3	4	1	6
D_6	1	8	3	8	1	12	1	8	3	8	1	12

Table: Exponent types of groups C_2, S_3 and D_6.

Example

o_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	1	0	0	0	0	0	0	0	0	0	0
S_3	1	3	2	0	0	0	0	0	0	0	0	0
D_6	1	7	2	0	0	2	0	0	0	0	0	0

Table: Order types of groups C_2, S_3 and D_6.

e_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	2	1	2	1	2	1	2	1	2
S_3	1	4	3	4	1	6	1	4	3	4	1	6
D_6	1	8	3	8	1	12	1	8	3	8	1	12

Table: Exponent types of groups C_2, S_3 and D_6.

Revolved exponent type

Define

$$r_G(n) = \prod_{d|n} e_G(n/d)^{\mu(d)}.$$

Example

o_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	1	0	0	0	0	0	0	0	0	0	0
S_3	1	3	2	0	0	0	0	0	0	0	0	0
D_6	1	7	2	0	0	2	0	0	0	0	0	0

Table: Order types of groups C_2, S_3 and D_6.

e_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	2	1	2	1	2	1	2	1	2
S_3	1	4	3	4	1	6	1	4	3	4	1	6
D_6	1	8	3	8	1	12	1	8	3	8	1	12

Table: Exponent types of groups C_2, S_3 and D_6.

r_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	1	1	1	1	1	1	1	1	1
S_3	1	4	3	1	1	1/2	1	1	1	1	1	1
D_6	1	8	3	1	1	1/2	1	1	1	1	1	1

Table: Revolved exponent types of groups C_2, S_3 and D_6.

Example

e_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	2	1	2	1	2	1	2	1	2
S_3	1	4	3	4	1	6	1	4	3	4	1	6
D_6	1	8	3	8	1	12	1	8	3	8	1	12

Table: Exponent types of groups C_2, S_3 and D_6.

r_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	1	1	1	1	1	1	1	1	1
S_3	1	4	3	1	1	1/2	1	1	1	1	1	1
D_6	1	8	3	1	1	1/2	1	1	1	1	1	1

Table: Revolved exponent types of groups C_2, S_3 and D_6.

Factorised revolved exponent type

Define

$$v_G(n,p) = v_p\big(r_G(n)\big).$$

Example

e_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	2	1	2	1	2	1	2	1	2
S_3	1	4	3	4	1	6	1	4	3	4	1	6
D_6	1	8	3	8	1	12	1	8	3	8	1	12

Table: Exponent types of groups C_2, S_3 and D_6.

r_G	1	2	3	4	5	6	7	8	9	10	11	12
C_2	1	2	1	1	1	1	1	1	1	1	1	1
S_3	1	4	3	1	1	1/2	1	1	1	1	1	1
D_6	1	8	3	1	1	1/2	1	1	1	1	1	1

Table: Revolved exponent types of groups C_2, S_3 and D_6.

v_G	(2, 2)	(2, 3)	(2, 5)	...	(3, 2)	(3, 3)	...	(6, 2)	...
C_2	1	0	0	...	0	0	...	0	...
S_3	2	0	0	...	0	1	...	-1	...
D_6	3	0	0	...	0	1	...	-1	...

Table: Factorised revolved exponent types of groups C_2, S_3 and D_6.

Summary

Denoting by $\mathbb{P}$ the set of all primes, we proved as follows.

$$o_G : \mathbb{N} \to \mathbb{N} \cup \{0\}, \quad e_G : \mathbb{N} \to \mathbb{N}, \quad r_G : \mathbb{N} \to \mathbb{Q}, \quad v_G : \mathbb{N} \times \mathbb{P} \to \mathbb{Z}.$$

$$o_G = o_H \iff e_G = e_H \iff r_G = r_H \iff v_G = v_H.$$

$$e_{G \times H} = e_G \cdot e_H, \quad r_{G \times H} = r_G \cdot r_H, \quad v_{G \times H} = v_G + v_H.$$

More abstract statement

The assignment

$$\mathcal{V} : G \mapsto \left(v_G : \mathbb{N} \times \mathbb{P} \to \mathbb{Z}\right)$$

defines a homomorphism of monoids

$$\mathcal{V} : \left(\text{FiniteGroups}, \ \times\right) \to \left(\mathbb{Z}^{\mathbb{N} \times \mathbb{P}}, \ +\right).$$

More abstract statement

The assignment

$$\mathcal{V} : G \mapsto \left(v_G : \mathbb{N} \times \mathbb{P} \to \mathbb{Z}\right)$$

defines a homomorphism of monoids

$$\mathcal{V} : \left(\text{FiniteGroups}, \ \times\right) \to \left(\mathbb{Z}^{\mathbb{N}\times\mathbb{P}}, \ +\right).$$

Theorem of Remak (1911)

If finite groups $G_1, \ldots, G_n$ and $H_1, \ldots, H_m$ don't decompose non-trivially as direct products and $G_1 \times \ldots \times G_n \cong H_1 \times \ldots \times H_m$, then $n = m$ and for some permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ we have $G_i \cong H_{\sigma(i)}$ for $i = 1, \ldots, n$.

More abstract statement

The assignment

$$\mathcal{V} : \frac{G}{1} \mapsto \left(v_G : \mathbb{N} \times \mathbb{P} \to \mathbb{Z}\right)$$

extends to a homomorphism of free abelian groups

$$\mathcal{V} : \left(\frac{\text{FiniteGroups}}{\text{FiniteGroups}},\ \times\right) \to \left(\mathbb{Z}^{\mathbb{N}\times\mathbb{P}},\ +\right).$$

Theorem of Remak (1911)

If finite groups $G_1, \ldots, G_n$ and $H_1, \ldots, H_m$ don't decompose non-trivially as direct products and $G_1 \times \ldots \times G_n \cong H_1 \times \ldots \times H_m$, then $n = m$ and for some permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ we have $G_i \cong H_{\sigma(i)}$ for $i = 1, \ldots, n$.

More abstract statement

The assignment

$$\mathcal{V} : \frac{G}{1} \mapsto \left(v_G : \mathbb{N} \times \mathbb{P} \to \mathbb{Z}\right)$$

extends to a homomorphism of free abelian groups

$$\mathcal{V} : \left(\frac{\text{FiniteGroups}}{\text{FiniteGroups}},\ \times\right) \to \left(\mathbb{Z}^{\mathbb{N}\times\mathbb{P}},\ +\right).$$

Furthermore

$$\frac{G}{H} \in \ker \mathcal{V} \iff v_G = v_H \iff o_G = o_H .$$

Thompson's Problem reformulated

Do there exist groups S and N such that S is solvable, N is non-solvable and $\frac{N}{S} \in \ker \mathcal{V}$?

Thompson's Problem reformulated

Do there exist groups S and N such that S is solvable, N is non-solvable and $\frac{N}{S} \in \ker \mathcal{V}$?

Equivalently, does there exist a non-solvable group N such that

$$\mathcal{V}(\frac{N}{1}) \in \left\{ \mathcal{V}(\frac{S_1}{S_2}) \middle| S_1 \text{ and } S_2 \text{ are solvable} \right\}?$$

Thompson's Problem reformulated

Do there exist groups S and N such that S is solvable, N is non-solvable and $\frac{N}{S} \in \ker \mathcal{V}$?

Equivalently, does there exist a non-solvable group N such that

$$\mathcal{V}\left(\frac{N}{1}\right) \in \left\{ \mathcal{V}\left(\frac{S_1}{S_2}\right) \middle| S_1 \text{ and } S_2 \text{ are solvable} \right\}?$$

STRATEGY

Thompson's Problem reformulated

Do there exist groups S and N such that S is solvable, N is non-solvable and $\frac{N}{S} \in \ker \mathcal{V}$?

Equivalently, does there exist a non-solvable group N such that

$$\mathcal{V}(\frac{N}{1}) \in \left\{ \mathcal{V}(\frac{S_1}{S_2}) \middle| S_1 \text{ and } S_2 \text{ are solvable} \right\}?$$

STRATEGY

1. Compute many $\mathcal{V}(S)$ and $\mathcal{V}(N)$. Arrange $\mathcal{V}(S_i)$ into matrix V.

Thompson's Problem reformulated

Do there exist groups S and N such that S is solvable, N is non-solvable and $\frac{N}{S} \in \ker \mathcal{V}$?

Equivalently, does there exist a non-solvable group N such that

$$\mathcal{V}\left(\frac{N}{1}\right) \in \left\{ \mathcal{V}\left(\frac{S_1}{S_2}\right) \middle| S_1 \text{ and } S_2 \text{ are solvable} \right\}?$$

STRATEGY

1. Compute many $\mathcal{V}(S)$ and $\mathcal{V}(N)$. Arrange $\mathcal{V}(S_i)$ into matrix V.
2. For each j solve the matrix equation

$$V\ x = y_j$$

where $y_j = \mathcal{V}(N_j)$ and x has rational entries.

Groups and properties

Steps 1

Use MAGMA to access the SmallGroups database,[4] loop through all groups G of size at most 2000 excluding those of size divisible by 128 and compute the following.

- Is G solvable?
- Is G a direct product?
- Its order type o_G.

[4]See the database Besche et al. and the paper detailing the construction Besche et al. (2002).

Parsing and rephrasing

Steps 2-4

Parse the results into a `.csv` file for ease of use with `Python`. For non-decomposable groups G compute the factorised revolved exponent types $\mathcal{V}(G)$, thereby getting the matrix V and the candidates for vectors y_j.

Parsing and rephrasing

Steps 2-4

Parse the results into a `.csv` file for ease of use with `Python`.
For non-decomposable groups G compute the factorised revolved exponent types $\mathcal{V}(G)$, thereby getting the matrix V and the candidates for vectors y_j.

V is of size 9945×100972.

Numerical and exact solutions

Step 5

Attempt to solve $Vx = y_j$ numerically using Sparse Least Squares method of `SciPy` library.

Numerical and exact solutions

Step 5

Attempt to solve $Vx = y_j$ numerically using Sparse Least Squares method of `SciPy` library.

This fails for most groups (e.g. A_5), but works for about 15 of them (e.g. $\mathrm{GL}(3, 2)$).

Numerical and exact solutions

Step 5

Attempt to solve $Vx = y_j$ numerically using Sparse Least Squares method of `SciPy` library.

This fails for most groups (e.g. A_5), but works for about 15 of them (e.g. $\mathrm{GL}(3,2)$).

Step 6

Attempt to solve $V\ x = \mathcal{V}(N)$ exactly for $N = \mathrm{GL}(3,2)$ using symbolic computation library `SymPy`.

Numerical and exact solutions

Step 5

Attempt to solve $Vx = y_j$ numerically using Sparse Least Squares method of `SciPy` library.

This fails for most groups (e.g. A_5), but works for about 15 of them (e.g. $\mathrm{GL}(3,2)$).

Step 6

Attempt to solve $V\ x = \mathcal{V}(N)$ exactly for $N = \mathrm{GL}(3,2)$ using symbolic computation library `SymPy`.

Step 7

Check, check, check again. Cross-reference. Compute it in a different way...

Theorem A of Piwek (2024)

Theorem A of Piwek (2024)

Let G_i and H_i be the collections of finite groups described in tables (a) and (b), and let m_i and n_i be the associated natural numbers from the tables. Let G and H be the direct products

$$G = \prod G_i^{m_i}, \quad H = \prod H_i^{n_i}.$$

Then $o_G = o_H$, G is solvable, and H is not solvable.

i	G_i	Id	m_i
1	C_4	(4, 1)	9
2	D_3	(6, 1)	6
3	C_7	(7, 1)	1
4	D_4	(8, 3)	9
5	D_7	(14, 1)	18
6	$\mathrm{SL}(2,3)$	(24, 3)	21
7	$C_{24} \rtimes C_2$	(48, 6)	3
8	$C_7 \rtimes D_4$	(56, 7)	3
9	$C_7 \rtimes C_{12}$	(84, 1)	6
10	Dic_{21}	(84, 5)	6
11	$C_7 \rtimes A_4$	(84, 11)	21
12	$C_7 \rtimes D_7$	(98, 4)	2
13	$C_4 \rtimes F_7$	(168, 9)	21
14	$C_{21} \rtimes D_4$	(168, 15)	9
15	$C_7 \rtimes D_{12}$	(168, 17)	6
16	$F_8 \rtimes C_3$	(168, 43)	3
17	$D_8 \rtimes D_7$	(224, 106)	3
18	$C_7 \rtimes D_{24}$	(336, 31)	3

(a) Groups G_i and numbers m_i.

i	H_i	Id	n_i
1	C_2	(2, 1)	21
2	C_3	(3, 1)	3
3	Dic_3	(12, 1)	6
4	A_4	(12, 3)	21
5	SD_{16}	(16, 8)	3
6	$C_7 \rtimes C_3$	(21, 1)	4
7	D_{12}	(24, 6)	6
8	$C_3 \rtimes D_4$	(24, 8)	6
9	Dic_7	(28, 1)	15
10	F_7	(42, 1)	18
11	D_{21}	(42, 5)	6
12	D_{24}	(48, 7)	3
13	D_{28}	(56, 5)	27
14	$\mathrm{Dic}_7 \rtimes C_6$	(168, 11)	3
15	$C_{14}.A_4$	(168, 23)	21
16	$\mathrm{GL}(3,2)$	(168, 42)	3
17	$C_7 \rtimes F_7$	(294, 10)	2
18	$D_{12}.D_7$	(336, 36)	3

(b) Groups H_i and numbers n_i.

Table: The groups G_i and H_i and their multiplicities m_i and n_i. The column labelled 'Id' contains the `SmallGroups` isomorphism type identifier (see Besche et al.).

Smaller examples

Smaller examples

The examples of Piwek (2024) are of size

$$2^{365} \cdot 3^{105} \cdot 7^{104} \approx 7.3 \cdot 10^{247}.$$

Smaller examples

The examples of Piwek (2024) are of size

$$2^{365} \cdot 3^{105} \cdot 7^{104} \approx 7.3 \cdot 10^{247}.$$

Müller (2024) constructed much smaller examples of size

$$2^{13} \cdot 3^4 \cdot 7^3 = 227598336.$$

Theorem 1 of Müller (2024)

Let G_i and H_i be finite groups in the tables with $G = G_1 \times G_2 \times G_3$ and $H = H_1 \times H_2 \times H_3 \times H_4$. Then $o_G = o_H$ and G is solvable, while H isn't solvable.

i	G_i	Id
1	$(C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3)$	(168, 43)
2	$C_7 \rtimes (C_3 \times (C_3 \rtimes Q_{16}))$	(1008, 289)
3	$C_7 \rtimes (((C_4 \times D_8) \rtimes C_2) \rtimes C_3)$	(1344, 6967)

(a) Groups G_i

i	H_i	Id
1	$C_7 \rtimes C_3$	(21, 1)
2	$Q_8 \times C_{12}$	(96, 166)
3	$C_7 \rtimes (C_4 \times A_4)$	(336, 136)
4	$\mathrm{PGL}(2, 7)$	(336, 208)

(b) Groups H_i

Theorem 1 of Müller (2024)

Let G_i and H_i be finite groups in the tables with $G = G_1 \times G_2 \times G_3$ and $H = H_1 \times H_2 \times H_3 \times H_4$. Then $o_G = o_H$ and G is solvable, while H isn't solvable.

i	G_i	Id
1	$(C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3)$	(168, 43)
2	$C_7 \rtimes (C_3 \times (C_3 \rtimes Q_{16}))$	(1008, 289)
3	$C_7 \rtimes (((C_4 \times D_8) \rtimes C_2) \rtimes C_3)$	(1344, 6967)

(a) Groups G_i

i	H_i	Id
1	$C_7 \rtimes C_3$	(21, 1)
2	$Q_8 \times C_{12}$	(96, 166)
3	$C_7 \rtimes (C_4 \times A_4)$	(336, 136)
4	$\mathrm{PGL}(2,7)$	(336, 208)

(b) Groups H_i

Mystery / Question

All of the examples we know of have $\mathrm{PSL}(2,7) \cong \mathrm{GL}(3,2)$ as a composition factor... Is that necessary?

Metaquestion

Metaquestion

Let G be a group and $T_G : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by

$$T_G(k, l, m) = |\{(x, y, z) \in G \times G \times G \mid x^k = y^l = z^m = xyz = 1\}|.$$

Which properties of G does this invariant discern?

Metaquestion

Let G be a group and $T_G : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by

$$T_G(k,l,m) = |\{(x,y,z) \in G \times G \times G \mid x^k = y^l = z^m = xyz = 1\}|.$$

Which properties of G does this invariant discern?

Digression?

$T_G(k,l,m)$ equals the number of distinct homomorphisms to G from a triangle group

$$\Delta(k,l,m) = \{x,y,z \mid x^k = y^l = z^m = xyz = 1\}.$$

Metaquestion

Let G be a group and $T_G : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by

$$T_G(k, l, m) = |\{(x, y, z) \in G \times G \times G \mid x^k = y^l = z^m = xyz = 1\}|.$$

Which properties of G does this invariant discern?

Digression?

$T_G(k, l, m)$ equals the number of distinct homomorphisms to G from a triangle group

$$\Delta(k, l, m) = \{x, y, z \mid x^k = y^l = z^m = xyz = 1\}.$$

As a consequence of a difficult theorem of Bridson et al. (2016) for any triples (k_1, l_1, m_1) and (k_2, l_2, m_2) which aren't permutations of each other there exists a finite group G which is a quotient of exactly one of $\Delta(k_1, l_1, m_1)$ and $\Delta(k_2, l_2, m_2)$.

Hans Ulrich Besche, Bettina Eick, and Eamonn O'Brien. Small Groups Library. https://magma.maths.usyd.edu.au/magma/handbook/text/779. Accessed: 2024-03-14.

Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(05):623–644, 2002.

Rolf Brandl and Wujie Shi. Finite groups whose element orders are consecutive integers. *Journal of Algebra*, 143(2):388–400, 1991.

Martin R Bridson, Marston DE Conder, and Alan W Reid. Determining fuchsian groups by their finite quotients. *Israel Journal of Mathematics*, 214(1):1–41, 2016.

Peter J. Cameron. Graphs defined on groups. *International Journal of Group Theory*, 11(2):53–107, 2022. ISSN 2251-7650. URL https://ijgt.ui.ac.ir/article%5F25608.html.

Walter Feit and John G Thompson. Chapter i, from solvability of groups of odd order, pacific j. math, vol. 13, no. 3 (1963). *Pacific J. Math.*, 13(4):775–787, 1963.

KW Gruenberg and KW Roggenkamp. Decomposition of the augmentation ideal and of the relation modules of a finite group. *Proceedings of the London Mathematical Society*, 3(2):149–166, 1975.

Marcel Herzog, Patrizia Longobardi, and Mercede Maj. Another criterion for solvability of finite groups. *J. Algebra*, 597:1–23, 2022.

Mihai-Silviu Lazorec and Marius Tărnăuceanu. On the average order of a finite group. *J. Pure Appl. Algebra*, 227(4):107276, 2023.

Peter Müller. A note about solvable and non-solvable finite groups of the same order type. *arXiv preprint arXiv:2408.07732*, 2024.

Paweł Piwek. Solvable and non-solvable finite groups of the same order type. *arXiv:2403.02197*, 2024.

R. Remak. Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren. *Journal für die reine und angewandte Mathematik*, 139:293–308, 1911.

Rulin Shen. On Groups with Given Same-Order Types. *Comm. Algebra*, 40(6): 2140–2150, 2012.

Rulin Shen, Wujie Shi, and Feng Tang. On Thompson problem. *arXiv:2308.07183*, 2023.

Wujie Shi. A characteristic property of PSL2(7). *Journal of the Australian Mathematical Society*, 36(3):354–356, 1984.

Wujie Shi. A characteristic property of A5. *Journal of Southwest China Normal University (Natural Science Edition)*, 11:11–14, 1986.

Wujie Shi. On the order and the element orders of finite groups: results and problems. In *Ischia Group Theory 2010*, pages 313–333. World Scientific, 2012.

Wujie Shi. Quantitative characterization of finite simple groups: a complement. *International Journal of Group Theory*, pages –, 2024. ISSN 2251-7650. doi: 10.22108/ijgt.2024.140804.1893. URL https://ijgt.ui.ac.ir/article%5F28685.html.

Andrey Viktorovich Vasil'ev, Mariya Aleksandrovna Grechkoseeva, and Victor Danilovich Mazurov. Characterization of the finite simple groups by spectrum and order. *Algebra and Logic*, 48(6):385–409, 2009.