How big can a minimal generating set be?

Scott Harper

University of St Andrews

New Perspectives in Pure Mathematics

University of Bristol

29 March 2023

LEVERHULME TRUST

University of St Andrews

Generating sets

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Examples

1 $G = C_p^n$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Examples

1. $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Examples

1. $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$
2. $G = S_n$
   $(n \geqslant 3)$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Examples

1. $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$
2. $G = S_n$ $(n \geqslant 3)$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1. $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$
2. $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$
   $(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$ so $d(G) = 2$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\;n) \rangle$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$ so $d(G) = 2$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$ so $m(G) \geqslant n-1$

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$ so $d(G) = 2$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$ so $m(G) \geqslant n - 1$

Theorem (Whiston | 2000)

If $n \geqslant 3$, then $m(S_n) = n - 1$.

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$ so $d(G) = 2$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$ so $m(G) \geqslant n - 1$

Theorem (Whiston | 2000)

If $n \geqslant 3$, then $m(S_n) = n - 1$ and $m(A_n) = n - 2$.

Generating sets

Let G be a finite group.

A generating set of G is a **minimal** if no proper subset generates G.

Write: $\boldsymbol{d(G)}$ for the minimum size of a (minimal) generating set of G

$\boldsymbol{m(G)}$ for the maximum size of a minimal generating set of G

Examples

1 $G = C_p^n$ a minimal generating set is a basis of $\mathbb{F}_p^n$ so $d(G) = m(G) = n$

2 $G = S_n$ $G = \langle (1\,2), (1\,2\ \ldots\ n) \rangle$ so $d(G) = 2$

$(n \geqslant 3)$ $G = \langle (1\,2), (2\,3), (3\,4), \ldots, (n\text{-}1\ n) \rangle$ so $m(G) \geqslant n - 1$

Theorem (Whiston | 2000)

If $n \geqslant 3$, then $m(S_n) = n - 1$ and $m(A_n) = n - 2$.

Theorem (Tarski | 1975)

For all $d(G) \leqslant k \leqslant m(G)$, the group G has a minimal generating set of size k.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Whiston & Saxl | 2002)

If p is prime, then $2 + \omega(f) \leqslant m(\mathrm{PSL}_2(p^f)) \leqslant \max\{2 + \omega(f), 6\}$.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Whiston & Saxl | 2002)

If p is prime, then $2 + \omega(f) \leqslant m(\mathrm{PSL}_2(p^f)) \leqslant \max\{2 + \omega(f), 6\}$.

Write $\omega(n)$ for the number of distinct prime divisors of n.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Whiston & Saxl | 2002)

If p is prime, then $2 + \omega(f) \leqslant m(\mathrm{PSL}_2(p^f)) \leqslant \max\{2 + \omega(f), 6\}$.

Theorem (H | 2023)

If G is a finite simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, where p is prime, then $2r + \omega(f) \leqslant m(G) \leqslant a(2r + \omega(f))^b$.

Write $\omega(n)$ for the number of distinct prime divisors of n.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Whiston & Saxl | 2002)

If p is prime, then $2 + \omega(f) \leqslant m(\mathrm{PSL}_2(p^f)) \leqslant \max\{2 + \omega(f), 6\}$.

Theorem (H | 2023)

If G is a finite simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, where p is prime, then $2r + \omega(f) \leqslant m(G) \leqslant a(2r + \omega(f))^b$. [e.g. $a = 10^5$ & $b = 10$]

Write $\omega(n)$ for the number of distinct prime divisors of n.

Theorem (Steinberg | 1962 + CFSG)

If G is a finite simple group, then $d(G) \leqslant 2$.

Theorem (Whiston & Saxl | 2002)

If p is prime, then $2 + \omega(f) \leqslant m(\mathrm{PSL}_2(p^f)) \leqslant \max\{2 + \omega(f), 6\}$.

Theorem (H | 2023)

If G is a finite simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, where p is prime, then $2r + \omega(f) \leqslant m(G) \leqslant a(2r + \omega(f))^b$. [e.g. $a = 10^5$ & $b = 10$]

e.g. If $n \geqslant 2$,

$$\mathrm{PSL}_n(p) = \left\langle \begin{pmatrix} 1 & 1 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 1 & 1 \end{pmatrix} \right\rangle.$$

Write $\omega(n)$ for the number of distinct prime divisors of n.

Remark

There are very similar results for all almost simple groups.

Remark

There are very similar results for all almost simple groups.

A group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

Remark

There are very similar results for all almost simple groups.

A group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

e.g. $G_0 = A_n$ and $G = S_n$,

Remark

There are very similar results for all almost simple groups.

A group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

e.g. $G_0 = A_n$ and $G = S_n$, $G_0 = \mathrm{PSL}_n(q)$ and $G = \mathrm{PGL}_n(q)$,

Remark

There are very similar results for all almost simple groups.

A group G is **almost simple** if $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

e.g. $G_0 = A_n$ and $G = S_n$, $\quad G_0 = \mathrm{PSL}_n(q)$ and $G = \mathrm{PGL}_n(q)$, $\quad G_0 = G =$ 

Bases for permutation groups

Bases for permutation groups

Let G act faithfully on a finite set X.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G,X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G,X)}$ for the maximum size of a minimal base for G on X

Examples

1 Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \dots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\dots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Examples

1 Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n. Therefore $b(G, X) = B(G, X) = n$.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Examples

1 Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n. Therefore $b(G, X) = B(G, X) = n$.

2 Let $G = \mathrm{PGL}_n(F)$ act on $X = \{\{\langle v_1\rangle, \ldots, \langle v_n\rangle\} \mid \{v_1, \ldots, v_n\} \text{ a basis of } F^n\}$.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G,X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G,X)}$ for the maximum size of a minimal base for G on X

Examples

1. Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n. Therefore $b(G,X) = B(G,X) = n$.
2. Let $G = \mathrm{PGL}_n(F)$ act on $X = \{\{\langle v_1\rangle, \ldots, \langle v_n\rangle\} \mid \{v_1, \ldots, v_n\} \text{ a basis of } F^n\}$. Then $b(G,X) = 2$ & $B(G,X) \geqslant n-1$.

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Examples

1 Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n.
Therefore $b(G, X) = B(G, X) = n$.

2 Let $G = \mathrm{PGL}_n(F)$ act on $X = \{\{\langle v_1\rangle, \ldots, \langle v_n\rangle\} \mid \{v_1, \ldots, v_n\}$ a basis of $F^n\}$.
Then $b(G, X) = 2$ & $B(G, X) \geqslant n - 1$.
[**e.g.** $\{e_1, e_2, e_3, e_4\}$, $\{e_1, (e_1 + e_2), (e_1 + e_2 + e_3), (e_1 + e_2 + e_3 + e_4)\}$

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Examples

1. Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n. Therefore $b(G, X) = B(G, X) = n$.
2. Let $G = \mathrm{PGL}_n(F)$ act on $X = \{\{\langle v_1\rangle, \ldots, \langle v_n\rangle\} \mid \{v_1, \ldots, v_n\}$ a basis of $F^n\}$. Then $b(G, X) = 2$ & $B(G, X) \geqslant n - 1$.
   [**e.g.** $\{e_1, e_2, e_3, e_4\}$, $\{e_1, (e_1 + e_2), (e_1 + e_2 + e_3), (e_1 + e_2 + e_3 + e_4)\}$
   $\{(e_1 + e_2), e_2, e_3, e_4\}$, $\{e_1, (e_2 + e_3), e_3, e_4\}$, $\{e_1, e_2, (e_3 + e_4), e_4\}$]

Bases for permutation groups

Let G act faithfully on a finite set X.

A subset $\{x_1, \ldots, x_n\} \subseteq X$ is a **base** if the pointwise stabiliser $G_{(x_1,\ldots,x_n)}$ is 1.

Write: $\boldsymbol{b(G, X)}$ for the minimum size of a (minimal) base for G on X

$\boldsymbol{B(G, X)}$ for the maximum size of a minimal base for G on X

Examples

1 Let $G = \mathrm{GL}_n(F)$ act on $X = F^n$. Then a minimal base is just a basis of F^n.
Therefore $b(G, X) = B(G, X) = n$.

2 Let $G = \mathrm{PGL}_n(F)$ act on $X = \{\{\langle v_1 \rangle, \ldots, \langle v_n \rangle\} \mid \{v_1, \ldots, v_n\}$ a basis of $F^n\}$.
Then $b(G, X) = 2$ & $B(G, X) \geqslant n - 1$.
[**e.g.** $\{e_1, e_2, e_3, e_4\}$, $\{e_1, (e_1 + e_2), (e_1 + e_2 + e_3), (e_1 + e_2 + e_3 + e_4)\}$
$\{(e_1 + e_2), e_2, e_3, e_4\}$, $\{e_1, (e_2 + e_3), e_3, e_4\}$, $\{e_1, e_2, (e_3 + e_4), e_4\}$]

Question Is there a minimal base of size k for all $b(G, X) \leqslant k \leqslant B(G, X)$?

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G, X) \leqslant 7$ with equality if and only if $G = \mathrm{M}_{24}$ and $|X| = 24$.

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G, X) \leqslant 7$ with equality if and only if $G = \mathrm{M}_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G, X) \leqslant ar^b + \omega(f)$ [H | 2023]

[e.g. $a = 177$ & $b = 8$]

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G, X) \leqslant 7$ with equality if and only if $G = M_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G, X) \leqslant ar^b + \omega(f)$ [H | 2023]

[e.g. $a = 177$ & $b = 8$]

Write: $\omega(n)$ for the number of distinct prime divisors of n

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G, X) \leqslant 7$ with equality if and only if $G = \mathrm{M}_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G, X) \leqslant ar^b + \omega(f)$ [H | 2023]

[e.g. $a = 177$ & $b = 8$]

Write: $\omega(n)$ for the number of distinct prime divisors of n

Connection A stronger version of **(a)** is a crucial ingredient for proving the upper bound on $m(G)$ for almost simple groups Lie type G.

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G,X) \leqslant 7$ with equality if and only if $G = \mathrm{M}_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G,X) \leqslant ar^b + \omega(f)$ [H | 2023]

[e.g. $a = 177$ & $b = 8$]

Write: $\boldsymbol{\omega(n)}$ for the number of distinct prime divisors of n

Connection A stronger version of **(a)** is a crucial ingredient for proving the upper bound on $m(G)$ for almost simple groups Lie type G.

Write $\boldsymbol{I(G,X)}$ for the maximum size of an **irredundant base** $\{x_1, \dots, x_n\} \subseteq X$, i.e. $G > G_{(x_1)} > G_{(x_1,x_2)} > \cdots > G_{(x_1,\dots,x_n)} = 1$. Note that $B(G,X) \leqslant I(G,X)$.

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G,X) \leqslant 7$ with equality if and only if $G = \mathrm{M}_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G,X) \leqslant ar^b + \omega(f)$ [H | 2023]

(b) $I(G,X) \leqslant ar^b + \Omega(f)$ [Gill & Liebeck | 2022] [e.g. $a = 177$ & $b = 8$]

Write: $\boldsymbol{\omega(n)}$ for the number of distinct prime divisors of n

Connection A stronger version of **(a)** is a crucial ingredient for proving the upper bound on $m(G)$ for almost simple groups Lie type G.

Write $\boldsymbol{I(G,X)}$ for the maximum size of an **irredundant base** $\{x_1, \ldots, x_n\} \subseteq X$, i.e. $G > G_{(x_1)} > G_{(x_1,x_2)} > \cdots > G_{(x_1,\ldots,x_n)} = 1$. Note that $B(G,X) \leqslant I(G,X)$.

Theorem (Burness et al. | 2011)

If G is a finite almost simple group with a faithful primitive nonstandard action on X, then $b(G,X) \leqslant 7$ with equality if and only if $G = M_{24}$ and $|X| = 24$.

Theorem

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$ with a faithful primitive action on X, then

(a) $B(G,X) \leqslant ar^b + \omega(f)$ [H | 2023]

(b) $I(G,X) \leqslant ar^b + \Omega(f)$ [Gill & Liebeck | 2022] [e.g. $a = 177$ & $b = 8$]

Write: $\omega(n)$ for the number of distinct prime divisors of n

$\Omega(n)$ for the number of prime divisors of n with multiplicity

Connection A stronger version of **(a)** is a crucial ingredient for proving the upper bound on $m(G)$ for almost simple groups Lie type G.

Write $I(G,X)$ for the maximum size of an **irredundant base** $\{x_1, \ldots, x_n\} \subseteq X$, i.e. $G > G_{(x_1)} > G_{(x_1,x_2)} > \cdots > G_{(x_1,\ldots,x_n)} = 1$. Note that $B(G,X) \leqslant I(G,X)$.

The connection

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\text{max}}{<} G$.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\text{max}}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\text{max}}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\max}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

We're done if there is a small number of conjugacy classes of G.

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\max}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

We're done if there is a small number of conjugacy classes of G.

By applying [Aschbacher | 1986] and [Liebeck & Seitz | 1990] there is just a small number of known classes,

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\max}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

We're done if there is a small number of conjugacy classes of G.

By applying [Aschbacher | 1986] and [Liebeck & Seitz | 1990] there is just a small number of known classes, plus other almost simple groups that are:

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\max}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

We're done if there is a small number of conjugacy classes of G.

By applying [Aschbacher | 1986] and [Liebeck & Seitz | 1990] there is just a small number of known classes, plus other almost simple groups that are:

1 of small order – we're also done

The connection

Let G be an almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$.

Let S be a minimal generating set for G.

Claim $|S|$ is small i.e. $|S| \leqslant a(r + \omega(f))^b$.

For $x \in S$, fix $\langle S \setminus x \rangle \leqslant M_x \underset{\max}{<} G$.

Lemma $\bigcap_{x \in S} M_x < \bigcap_{x \in S \setminus y} M_x$ for all $y \in S$.

A version of **(a)** implies that a small number of the M_x are conjugate.

We're done if there is a small number of conjugacy classes of G.

By applying [Aschbacher | 1986] and [Liebeck & Seitz | 1990] there is just a small number of known classes, plus other almost simple groups that are:

1. of small order – we're also done
2. of Lie type of smaller rank – we apply induction.

Application: a local-to-global theorem

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n $\qquad d(G) = m(G) = n$

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	

[$G = G_{p_1} \times \cdots \times G_{p_k}$ where G_p is a Sylow p-subgroup]

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	$d(G) = \max_{p \text{ prime}} d(G_p)$ & $m(G) = \sum_{p \text{ prime}} d(G_p)$
	[$G = G_{p_1} \times \cdots \times G_{p_k}$ where G_p is a Sylow p-subgroup]

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	$d(G) = \max_{p \text{ prime}} d(G_p)$ & $m(G) = \sum_{p \text{ prime}} d(G_p)$
	[$G = G_{p_1} \times \cdots \times G_{p_k}$ where G_p is a Sylow p-subgroup]

Theorem (Guralnick // Lucchini | 1989)

If G is finite, then $d(G) \leqslant \max_{p \text{ prime}} d(G_p) + 1$.

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	$d(G) = \max_{p \text{ prime}} d(G_p)$ & $m(G) = \sum_{p \text{ prime}} d(G_p)$
	[$G = G_{p_1} \times \cdots \times G_{p_k}$ where G_p is a Sylow p-subgroup]

Theorem (Guralnick // Lucchini | 1989)

If G is finite, then $d(G) \leqslant \max_{p \text{ prime}} d(G_p) + 1$.

However, the bound $m(G) \leqslant \sum_{p \text{ prime}} d(G_p) + 1$ is true for soluble groups G but is false in general [Lucchini, Moscatiello, Spiga | 2021].

Application: a local-to-global theorem

Question Are $d(G)$ and $m(G)$ controlled by the Sylow subgroups of G?

G is C_p^n	$d(G) = m(G) = n$
G is a p-group	$d(G) = m(G)$
G is nilpotent	$d(G) = \max_{p \text{ prime}} d(G_p)$ & $m(G) = \sum_{p \text{ prime}} d(G_p)$
	[$G = G_{p_1} \times \cdots \times G_{p_k}$ where G_p is a Sylow p-subgroup]

Theorem (Guralnick // Lucchini | 1989)

If G is finite, then $d(G) \leqslant \max_{p \text{ prime}} d(G_p) + 1$.

However, the bound $m(G) \leqslant \sum_{p \text{ prime}} d(G_p) + 1$ is true for soluble groups G but is false in general [Lucchini, Moscatiello, Spiga | 2021].

Theorem (H | 2023)

If G is finite, then $m(G) \leqslant a(\sum_{p \text{ prime}} d(G_p))^b$. [e.g. $a = 10^{10}$ & $b = 10$]

How big can a minimal generating set be?

How big can a minimal generating set be?

Theorem (H | 2023)

If G is finite, then $m(G) \leqslant a(\sum_{p \text{ prime}} d(G_p))^b$. [e.g. $a = 10^{10}$ & $b = 10$]

How big can a minimal generating set be?

Theorem (H | 2023)

If G is finite, then $m(G) \leqslant a(\sum_{p \text{ prime}} d(G_p))^b$. [e.g. $a = 10^{10}$ & $b = 10$]

$\uparrow$

Theorem (H | 2023)

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, for prime p, then $m(G) \leqslant a(r + \omega(f))^b$. [e.g. $a = 10^5$ & $b = 10$]

How big can a minimal generating set be?

Theorem (H | 2023)

If G is finite, then $m(G) \leqslant a(\sum_{p \text{ prime}} d(G_p))^b$. [e.g. $a = 10^{10}$ & $b = 10$]

$\uparrow$

Theorem (H | 2023)

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, for prime p, then $m(G) \leqslant a(r + \omega(f))^b$. [e.g. $a = 10^5$ & $b = 10$]

$\uparrow$

Theorem (H | 2023)

If G is a finite almost simple group of Lie type of rank r over $\mathbb{F}_{p^f}$, for prime p, acting primitively on X, then $B(G, X) \leqslant ar^b + \omega(f)$. [e.g. $a = 177$ & $b = 8$]