Covering numbers of finite groups: a computational approach

Eric Swartz
(joint with **Luise-Charlotte Kappe**; Daniela Nikolova-Popova; Ryan Oppenheim; **Martino Garonzi**)

College of William and Mary

August 10, 2017

Definition

Definition

- G: group
- $\mathcal{A} = \{A_i \mid 1 \leqslant i \leqslant n\}$: collection of proper subgroups of G.
- If $G = \bigcup_{i=1}^{n} A_i$, then $\mathcal{A}$ is called a *cover* of G.
- A cover of size n is *minimal* if no cover of G has fewer than n members.

Definition

The size of a minimal covering of G (supposing one exists!) is called the *covering number*, denoted by $\sigma(G)$.

$\sigma(G)$ well-defined if G not cyclic

Motivation

Definition

$\omega(G)$: largest $m \in \mathbb{N}$ such that there exists $S \subseteq G$ such that:

- $|S| = m$,
- if $x, y \in S$, $x \neq y$, then $\langle x, y \rangle = G$.

Motivation

Definition

$\omega(G)$: largest $m \in \mathbb{N}$ such that there exists $S \subseteq G$ such that:

- $|S| = m$,
- if $x, y \in S$, $x \neq y$, then $\langle x, y \rangle = G$.

$\omega(G) \leqslant \sigma(G)$ (Pigeonhole), often tight

Previous results

Theorem (Tomkinson (1997))

Let G be a finite solvable group and let H/K be the smallest chief factor of G having more than one complement in G. Then $\sigma(G) = |H/K| + 1$.

Corollary

The covering number of any (noncyclic) solvable group has the form $p^d + 1$, where p is a prime and d is a positive integer.

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1, p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1, p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

This group has $p^d(p^d - 1)$ elements:

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1, p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

This group has $p^d(p^d - 1)$ elements:

- one normal elementary abelian subgroup of order p^d;

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1, p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

This group has $p^d(p^d - 1)$ elements:

- one normal elementary abelian subgroup of order p^d;
- remaining $p^d(p^d - 1) - p^d = p^d(p^d - 2)$ elements are in p^d distinct, conjugate subgroups isomorphic to C_{p^d-1} that intersect only in the identity.

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1,p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

This group has $p^d(p^d-1)$ elements:

- one normal elementary abelian subgroup of order p^d;
- remaining $p^d(p^d-1) - p^d = p^d(p^d-2)$ elements are in p^d distinct, conjugate subgroups isomorphic to C_{p^d-1} that intersect only in the identity.
- $\sigma(\mathrm{AGL}(1,p^d)) = p^d + 1$

"Natural" question

Which numbers actually **are** covering numbers?

Example

Consider the *affine group* $\mathrm{AGL}(1, p^d) \cong C_p^d \rtimes C_{p^d-1}$, where p is prime and d is a positive integer, $p^d \geqslant 3$.

This group has $p^d(p^d - 1)$ elements:

- one normal elementary abelian subgroup of order p^d;
- remaining $p^d(p^d - 1) - p^d = p^d(p^d - 2)$ elements are in p^d distinct, conjugate subgroups isomorphic to C_{p^d-1} that intersect only in the identity.
- $\sigma(\mathrm{AGL}(1, p^d)) = p^d + 1$

Hence **every** integer of the form $p^d + 1$ is a covering number.

Known results

Other numbers that are covering numbers depend on nonsolvable groups.

Known results

Other numbers that are covering numbers depend on nonsolvable groups.

Theorem

- *Tomkinson (1997): There is no finite group G such that $\sigma(G) = 7$.*
- *Detomi, Lucchini (2008): There is no finite group G such that $\sigma(G) = 11$.*

Known results

Other numbers that are covering numbers depend on nonsolvable groups.

Theorem

- *Tomkinson (1997): There is no finite group G such that $\sigma(G) = 7$.*
- *Detomi, Lucchini (2008): There is no finite group G such that $\sigma(G) = 11$.*

Theorem

- *Abdollahi, Ashraf, Shaker (2007):* $\sigma(S_6) = 13$
- *Bryce, Fedri, Serena (1999):* $\sigma(\mathrm{PSL}(3,2)) = 15$

Known results

Other numbers that are covering numbers depend on nonsolvable groups.

Theorem

- *Tomkinson (1997): There is no finite group G such that $\sigma(G) = 7$.*
- *Detomi, Lucchini (2008): There is no finite group G such that $\sigma(G) = 11$.*

Theorem

- *Abdollahi, Ashraf, Shaker (2007):* $\sigma(S_6) = 13$
- *Bryce, Fedri, Serena (1999):* $\sigma(\mathrm{PSL}(3,2)) = 15$

Theorem (Garonzi (2013))

The integers between 16 and 25 which are not covering numbers are $19, 21, 22, 25$.

New results

Theorem (Garonzi, Kappe, S. (2017+))

The integers between 26 *and* 129 *which are not covering numbers are* 27, 34, 35, 37, 39, 41, 43, 45, 47, 49, 51, 52, 53, 55, 56, 58, 59, 61, 66, 69, 70, 75, 76, 77, 78, 79, 81, 83, 87, 88, 89, 91, 93, 94, 95, 96, 97, 99, 100, 101, 103, 105, 106, 107, 109, 111, 112, 113, 115, 116, 117, 118, 119, 120, 123, 124, 125*.*

New results

Theorem (Garonzi, Kappe, S. (2017+))

The integers between 26 *and* 129 *which are not covering numbers are* 27, 34, 35, 37, 39, 41, 43, 45, 47, 49, 51, 52, 53, 55, 56, 58, 59, 61, 66, 69, 70, 75, 76, 77, 78, 79, 81, 83, 87, 88, 89, 91, 93, 94, 95, 96, 97, 99, 100, 101, 103, 105, 106, 107, 109, 111, 112, 113, 115, 116, 117, 118, 119, 120, 123, 124, 125.

Theorem (GKS (2017+))

Let $q = p^d$ *be a prime power and* $n \geqslant 2$, $n \neq 3$ *be a positive integer. Then* $(q^n - 1)/(q - 1)$ *is a covering number.*

Ideas behind first result: Reduction

Definition

A group G is *σ-elementary* if $\sigma(G) < \sigma(G/N)$ for every nontrivial normal subgroup of G.

Ideas behind first result: Reduction

Definition

A group G is *σ-elementary* if $\sigma(G) < \sigma(G/N)$ for every nontrivial normal subgroup of G.

Theorem (GKS (2017+))

Let G be a nonabelian σ-elementary group with $\sigma(G) \leqslant 129$. Then G is primitive and monolithic with degree of primitivity at most 129, and the smallest degree of primitivity of G is at most $\sigma(G)$.

Primitive, monolithic groups

Definition

$G \leqslant \mathrm{Sym}(\Omega)$ is *primitive* on Ω if:

- G is transitive on Ω;
- G preserves no nontrivial partition of Ω.

Degree of primitivity of G: $|\Omega|$

Equivalent: G is *primitive* if it contains a core-free maximal subgroup

Primitive, monolithic groups

Definition

$G \leqslant \mathrm{Sym}(\Omega)$ is *primitive* on Ω if:

- G is transitive on Ω;
- G preserves no nontrivial partition of Ω.

Degree of primitivity of G: $|\Omega|$

Equivalent: G is *primitive* if it contains a core-free maximal subgroup

Definition

A group G is said to be *monolithic* if:

- G has a unique minimal normal subgroup N,
- N is contained in every nontrivial normal subgroup.

Reduction says we need "only" check primitive monolithic groups up to degree 129. (Counting repeats, over 700 nonsolvable groups.)

Reduction, cont.

We need to study the covering numbers of primitive groups of “small” degree.

Reduction, cont.

We need to study the covering numbers of primitive groups of "small" degree.

Exact values are desirable; sometimes lower bounds suffice.

Reduction, cont.

We need to study the covering numbers of primitive groups of "small" degree.

Exact values are desirable; sometimes lower bounds suffice.

Main tools:

- known formulas/asymptotic results
- linear programming
- "greedy" search for "hardest to cover" conjugacy classes

Known formulas/bounds: Symmetric groups

Group	Covering Number	Citation
S_5	16	Cohn (1994)
S_6	13	Abdollahi, Ashraf, Shaker (2007)
S_8	64	Kappe, Nikolova-Popova, S. (2016)
S_9	256	KNS (2016)
S_{10}	221	KNS (2016)
S_{12}	761	KNS (2016)
S_{14}	3096	Oppenheim, S. (2017+)
S_{18}	36773	S. (2016)
$S_{6k}, k \geqslant 4$	$\frac{1}{2}\binom{6k}{3k} + \sum_{i=0}^{2k-1} \binom{6k}{i}$	S. (2016)
$S_{2k+1}, k \neq 4$	2^{2k}	Maróti (2005)
S_{2k}	$> \frac{1}{2}\binom{2k}{k}$	Maróti (2005)

Known formulas/bounds: Alternating groups

Group	Covering Number	Citation
A_5	10	Cohn (1994)
A_6	16	Maróti (2005)
A_7	31	Kappe, Redden (2010)
A_8	71	Kappe, Redden (2010)
A_9	157	Epstein, Magliveras, Nikolova-Popova (2017)
A_{10}	256	Maróti (2005)
A_{11}	2751	Epstein, Magliveras, Nikolova-Popova (2017)
A_n	$\geqslant 2^{n-2}$	Maróti (2005)

Known formulas/bounds: Misc.

Group	Covering Number	Citation
(sporadic groups)	(bounds)	Holmes, Maróti (2010)
$\mathrm{Sz}(q)$	$\frac{1}{2}q^2(q^2+1)$	Lucido (2003)
$\mathrm{PSL}(2,q)$	$\frac{1}{2}q(q+1)$, q even	Bryce, Fedri, Serena (1999)
$\mathrm{PSL}(2,q)^*$	$\frac{1}{2}q(q+1)+1$, q odd	Bryce, Fedri, Serena (1999)
$\mathrm{PSL}(n,q)$	(long formula; $n \geqslant 12$)	Britnell et al (2008, 2011)

*: $q \neq 5, 7, 9$

In above known cases, $\sigma(\mathrm{PGL}(n,q)) = \sigma(\mathrm{PSL}(n,q))$.

Linear programming approach

- Group G, set $\{M_1, ..., M_k\}$ of maximal subgroups, list $\{g_1, ..., g_t\}$ of elements that need covered.

Linear programming approach

- Group G, set $\{M_1, ..., M_k\}$ of maximal subgroups, list $\{g_1, ..., g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)

Linear programming approach

- Group G, set $\{M_1, ..., M_k\}$ of maximal subgroups, list $\{g_1, ..., g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)
- If $g_i \in M_{j_1}, ..., M_{j_s}$, then we have equation $m_{j_1} + m_{j_2} + ... + m_{j_s} \geqslant 1$.

Linear programming approach

- Group G, set $\{M_1, \ldots, M_k\}$ of maximal subgroups, list $\{g_1, \ldots, g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)
- If $g_i \in M_{j_1}, \ldots, M_{j_s}$, then we have equation $m_{j_1} + m_{j_2} + \ldots + m_{j_s} \geqslant 1$.
- Minimize $\sum_{j=0}^{k} m_j$ subject to satisfying the above equations.

Linear programming approach

- Group G, set $\{M_1, ..., M_k\}$ of maximal subgroups, list $\{g_1, ..., g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)
- If $g_i \in M_{j_1}, ..., M_{j_s}$, then we have equation $m_{j_1} + m_{j_2} + ... + m_{j_s} \geqslant 1$.
- Minimize $\sum_{j=0}^{k} m_j$ subject to satisfying the above equations.
- Use GAP to create the set of equations, optimized using Gurobi.

Linear programming approach

- Group G, set $\{M_1, \ldots, M_k\}$ of maximal subgroups, list $\{g_1, \ldots, g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)
- If $g_i \in M_{j_1}, \ldots, M_{j_s}$, then we have equation $m_{j_1} + m_{j_2} + \ldots + m_{j_s} \geqslant 1$.
- Minimize $\sum_{j=0}^{k} m_j$ subject to satisfying the above equations.
- Use GAP to create the set of equations, optimized using Gurobi.

Example

Holmes, Maróti (2010): $380 \leqslant \sigma(J_2) \leqslant 1220$

Linear programming approach

- Group G, set $\{M_1, \ldots, M_k\}$ of maximal subgroups, list $\{g_1, \ldots, g_t\}$ of elements that need covered.
- $M_j \leftrightarrow$ variable m_j that is either 0 (not in cover) or 1 (in cover)
- If $g_i \in M_{j_1}, \ldots, M_{j_s}$, then we have equation $m_{j_1} + m_{j_2} + \ldots + m_{j_s} \geqslant 1$.
- Minimize $\sum_{j=0}^{k} m_j$ subject to satisfying the above equations.
- Use GAP to create the set of equations, optimized using Gurobi.

Example

Holmes, Maróti (2010): $380 \leqslant \sigma(J_2) \leqslant 1220$

GKS (2017+): $1063 \leqslant \sigma(J_2) \leqslant 1121$

The new formula

Theorem (GKS (2017+))

Let $q = p^d$ be a prime power and $n \geqslant 2$, $n \neq 3$ be a positive integer. Then $(q^n - 1)/(q - 1)$ is a covering number.

Idea behind proof

- $G = \mathrm{AGL}(n,q) \cong V \rtimes \mathrm{GL}(n,q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$

Idea behind proof

- $G = \mathrm{AGL}(n, q) \cong V \rtimes \mathrm{GL}(n, q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$
- Already shown for $n = 1$, so assume $n \geqslant 3$

Idea behind proof

- $G = \mathrm{AGL}(n, q) \cong V \rtimes \mathrm{GL}(n, q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$
- Already shown for $n = 1$, so assume $n \geqslant 3$
- Detomi, Lucchini (2008): $\sigma(G) \leqslant (q^{n+1} - 1)/(q - 1)$

Idea behind proof

- $G = \mathrm{AGL}(n, q) \cong V \rtimes \mathrm{GL}(n, q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$
- Already shown for $n = 1$, so assume $n \geqslant 3$
- Detomi, Lucchini (2008): $\sigma(G) \leqslant (q^{n+1} - 1)/(q - 1)$
- We will show that we need at least this many groups; consider first the q^n "point stabilizers" isomorphic to $\mathrm{GL}(n, q)$

Idea behind proof

- $G = \mathrm{AGL}(n, q) \cong V \rtimes \mathrm{GL}(n, q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$
- Already shown for $n = 1$, so assume $n \geqslant 3$
- Detomi, Lucchini (2008): $\sigma(G) \leqslant (q^{n+1} - 1)/(q - 1)$
- We will show that we need at least this many groups; consider first the q^n "point stabilizers" isomorphic to $\mathrm{GL}(n, q)$
- Necessity of $\mathrm{GL}(n, q)$ subgroups when $n > 2$:

$$\sigma(\mathrm{GL}(n, q)) \geqslant \frac{|\mathrm{GL}(n, q)|}{m} \sim q^{n^2(1-\frac{1}{b})} \geqslant q^{\frac{n^2}{2}} >> \frac{q^{n+1} - 1}{q - 1},$$

where $m \sim |\mathrm{GL}(n/b, q^b)| \sim \left(q^b\right)^{(n/b)^2} = q^{n^2/b}$

Idea behind proof

- $G = \mathrm{AGL}(n,q) \cong V \rtimes \mathrm{GL}(n,q)$, where V is n-dimensional vector space over $\mathrm{GF}(q)$
- Already shown for $n = 1$, so assume $n \geqslant 3$
- Detomi, Lucchini (2008): $\sigma(G) \leqslant (q^{n+1} - 1)/(q-1)$
- We will show that we need at least this many groups; consider first the q^n "point stabilizers" isomorphic to $\mathrm{GL}(n,q)$
- Necessity of $\mathrm{GL}(n,q)$ subgroups when $n > 2$:

$$\sigma(\mathrm{GL}(n,q)) \geqslant \frac{|\mathrm{GL}(n,q)|}{m} \sim q^{n^2(1-\frac{1}{b})} \geqslant q^{\frac{n^2}{2}} >> \frac{q^{n+1}-1}{q-1},$$

where $m \sim |\mathrm{GL}(n/b, q^b)| \sim \left(q^b\right)^{(n/b)^2} = q^{n^2/b}$

- If these groups are not in a minimal cover, then a smaller cover of $\mathrm{GL}(n,q)$ is induced, a contradiction

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v
- No fixed elements of V, so not in any $\mathrm{GL}(n, q)$

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v
- No fixed elements of V, so not in any $\mathrm{GL}(n, q)$
- Given two such elements g_1 and g_2 (from vectors v_1 and v_2), g_1^p and g_2^p are Singer cycles

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v
- No fixed elements of V, so not in any $\mathrm{GL}(n, q)$
- Given two such elements g_1 and g_2 (from vectors v_1 and v_2), g_1^p and g_2^p are Singer cycles
- If g_1^p, g_2^p don't stabilize same hyperplane, then $\langle g_1, g_2 \rangle = \mathrm{AGL}(n, q)$

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v
- No fixed elements of V, so not in any $\mathrm{GL}(n, q)$
- Given two such elements g_1 and g_2 (from vectors v_1 and v_2), g_1^p and g_2^p are Singer cycles
- If g_1^p, g_2^p don't stabilize same hyperplane, then $\langle g_1, g_2 \rangle = \mathrm{AGL}(n, q)$
- $(q^n - 1)/(q - 1)$ different hyperplanes, so need at least this many additional subgroups

Idea, cont.

- Take $v \in V$, U a complementary hyperplane to $\langle v \rangle$, and consider element corresponding to:
  - a Singer cycle of U that centralizes v
  - followed by a translation by v
- No fixed elements of V, so not in any $\mathrm{GL}(n, q)$
- Given two such elements g_1 and g_2 (from vectors v_1 and v_2), g_1^p and g_2^p are Singer cycles
- If g_1^p, g_2^p don't stabilize same hyperplane, then $\langle g_1, g_2 \rangle = \mathrm{AGL}(n, q)$
- $(q^n - 1)/(q - 1)$ different hyperplanes, so need at least this many additional subgroups
- $\sigma(AGL(n, q)) = (q^{n+1} - 1)/(q - 1)$ when $n \neq 2$

Thanks!

Thanks!