Covering numbers of rings with unity

Eric Swartz
(joint with Nicholas Werner)

William & Mary

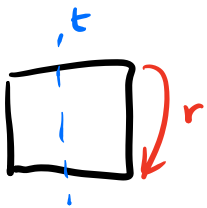
October 20, 2021

Covers and covering numbers of groups

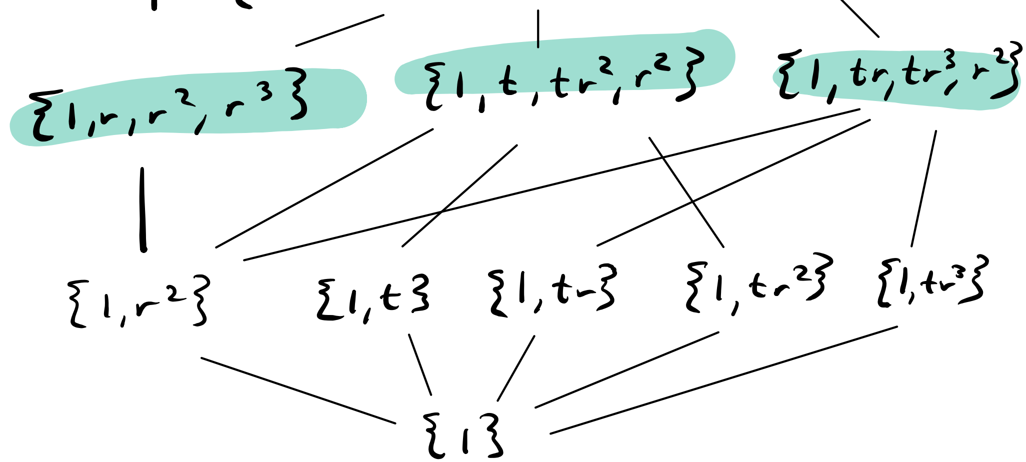
Definition

- A cover of a group G is a collection of proper subgroups of G whose set theoretic union is all of G.
- Assuming a cover exists for G, the covering number $\sigma(G)$ of G is the size of a minimum cover.

Ex



$$D_4 = \{1, r, r^2, r^3, t, tr, tr^2, tr^3\}$$



$$\sigma(D_4) = 3$$

Starting question

Question (1969 Putnam Competition, B2)

G is a finite group with identity 1. Show that we cannot find two proper subgroups A and $B (\neq \{1\}$ or $G)$ such that $A \cup B = G$. Can we find three proper subgroups A, B, C such that $A \cup B \cup C = G$?

Early history

$D_4/\langle r^2 \rangle \cong C_2 \times C_2$

Theorem (Scorza [Sco26])

A group G has $\sigma(G) = 3$ if and only if there is a surjective homomorphism from G onto the Klein 4-group, $C_2 \times C_2$.

This result was "rediscovered" many times in subsequent years!

For a nice proof of Scorza's result, see Bhargava [Bha09].

What about other integers?

For which integers n is there a group G with $\sigma(G) = n$?

How does one even begin to think about this question???

Theorem (B. H. Neumann [Neu54])

Suppose $\sigma(G) = n$. Then, G has a finite, noncyclic homomorphic image $\overline{G}$ with $\sigma(\overline{G}) = n$.

In other words, it suffices to consider finite groups.

Renewed interest: Cohn

Theorem (Cohn [Coh94])

For every integer of of the form $p^d + 1$, where p is a prime and d is a positive integer, there exists a group G with

$$\sigma(G) = p^d + 1.$$

~~2~~	3	4	5	6	7	8	9	10	11	12	13	14	15
					?				?		?		?

Cohn also makes the following conjectures:

(1) All *solvable groups* have covering number of the form $p^d + 1$.

(2) No group exists with covering number 7.

Tomkinson's work

Theorem (Tomkinson [Tom97])

(1) *All solvable groups have covering number of the form $p^d + 1$.*

(2) *No group exists with covering number 7.*

~~2~~	3	4	5	6	~~7~~	8	9	10	11	12	13	14	15

?

Tomkinson further conjectures there are no groups G with $\sigma(G) = 11, 13, 15$.

ACTUALLY: $\sigma(S_6) = 13$, $\sigma(\mathrm{PSL}(3,2)) = 15$

One direction of research

Tomkinson's result and the counterexamples suggest one line of research: what is $\sigma(G)$ for G a simple group (or an *almost simple group*)?

- **Bryce, Fedri, Serena [BFS99]:**
  $$\sigma(\mathrm{PSL}(2,q)) = \begin{cases} \frac{1}{2}q(q+1)+1, q > 9 \text{ odd}, \\ \frac{1}{2}q(q+1), q \geqslant 8 \text{ even}. \end{cases}$$
- **Maróti [Mar05]:** $\sigma(S_{2n+1}) = 2^{2n}$
- **S. [Swa16]:** $\sigma(S_{6n}) = \frac{1}{2}\binom{6n}{3n} + \sum_{i=0}^{2n-1}\binom{6n}{i}$
- **Holmes [Hol06]:** various sporadic simple groups
- **Britnell, Evseev, Guralnick, Holmes, Maróti [BEG$^+$08]:** $\mathrm{PSL}(n,q)$, $n \geqslant 13$

Work of Detomi & Lucchini

Theorem (Detomi, Lucchini [DL08])

There is no group G with covering number 11.

ALSO: provide a nice conceptual framework for determining whether or not an integer is a covering number

“Pulling back” a cover

Lemma

If $N \triangleleft G$ and G/N admits a finite cover, then $\sigma(G) \leqslant \sigma(G/N)$.

IDEA: $G/N = \overline{G}$ $\phi: G \longrightarrow \overline{G}$

(natural homomorphism)

$$\underline{G} \qquad \xleftarrow{\text{“Pull back”}} \qquad \underline{\text{cover for } \overline{G}}$$

$$H_1N, H_2N, \ldots, H_mN \qquad\qquad \overline{H_1}, \overline{H_2}, \ldots, \overline{H_m}$$

cover for G

σ-elementary groups

Definition

A group G is said to be σ-elementary if G has a finite cover and $\sigma(G) < \sigma(G/N)$ for all normal subgroups $N \lhd G$.

Conjecture (Detomi, Lucchini [DL08])

Nonabelian σ-elementary groups are monolithic and primitive.

unique minimal
normal subgroup

$G \leq \mathrm{Sym}(\Omega)$
G transitive on Ω
G does <u>not</u>
stabilize a nontrivial
partition of Ω

Further work

Theorem (Garonzi [Gar13])

The integers between 16 *and* 25 *that are* *not* *covering numbers of groups are* $19, 21, 22, 25$.

Further work, cont.

Theorem (Garonzi, Kappe, S. [GKS19])

The integers between 26 *and* 129 *that are* *not* *covering numbers of groups 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.

Conjecture (Garonzi, Kappe, S. [GKS19])

There are infinitely many integers that are not covering numbers of groups. Moreover,

$$\lim_{N\to\infty} \frac{\#\ \textit{of integers}\ \leqslant N\ \textit{that are covering numbers}}{N} = 0$$

Other algebraic structures???

- cover of an algebraic structure A: proper algebraic substructures whose set theoretic union is A
- covering number: size of a minimum cover

Theorem (Gagola III, Kappe [GK16])

Every integer $n > 2$ is a covering number of a loop.

Theorem (Donoven, Kappe [DK20])

- *The covering number of a finite semigroup that is not a group and not generated by a single element is always two.*
- *For each $n \geqslant 2$, there exists an inverse semigroup whose covering number (by inverse subsemigroups) is exactly n.*

What about rings???

Definition

A ring is a set R equipped with binary operations $+$ and $\cdot$ satisfying:

- $(R, +)$ is an abelian group,
- multiplication is associative,
- distributive laws hold.

Definition

A ring with unity is a ring that also has a unity (multiplicative identity).

NOTE: some authors refer to these as "rngs" and "rings," respectively

The covering number of a ring

Definition

For us, a subring $S \subseteq R$ is a group under addition and closed under multiplication; that is, **a subring need not contain a multiplicative identity**.

Definition

- A cover of a ring R is a collection of proper subrings of R whose set theoretic union is all of R.
- Assuming a cover exists for R, the covering number $\sigma(R)$ of R is the size of a minimum cover.

What's known?

Theorem (B. H. Neumann [Neu54], Lewin [Lew67])

If ring R has finite covering number, then there exists a finite homomorphic image of R with the same covering number.

In other words: to determine which integers are covering numbers of rings, it suffices to consider finite rings.

Fun fact:

Theorem (Greenfield [Gre20])

The covering number of $\mathbb{R}$ is countable.

What's known?

Theorem (Lucchini, Maróti [LM12])

If R is a ring (with or without unity) with $\sigma(R) = 3$, then R has a homomorphic image that is one of the five rings listed below.

- $\mathbb{F}_2 \times \mathbb{F}_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subseteq M_2(2)$
- $\left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\} \subseteq M_3(2)$
- $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\} \subseteq M_2(2)$
- $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\} \subseteq M_2(2)$
- $\mathbb{F}_2(+)\mathbb{F}_2^2 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{F}_2 \right\}$

Other recent progress

- **Lucchini, Maróti [LM10], Crestani [Cre12]:** full matrix rings $M_n(q)$
- **Werner [Wer15]:** products of fields
- **Peruginelli, Werner [PW18]:** products of full matrix rings
- **Cai, Werner [CW19]:** rings of upper triangular matrices
- **Cohen [Coh20]:** partial classification of rings R with unity and $\sigma(R) = 4$
- **S., Werner [SW21]:** commutative rings with unity,
  rings with unity with a product of fields as homomorphic image

Reductions

Lemma (S., Werner [SW21])

Let R be a ring with unity such that $\sigma(R)$ is finite. Then, there exists a two-sided ideal I of R such that:

- *R/I is finite;*
- *R/I has characteristic p;*
- *$\mathscr{J}(R/I)^2 = \{0\}$;*
- *and $\sigma(R/I) = \sigma(R)$.*

Jacobson radical
(intersection of all
max'l two-sided ideals)

The Wedderburn-Malcev Theorem

Theorem (Wedderburn-Malcev Theorem)

Let R be a finite ring with unity of characteristic p. Then, there exists an $\mathbb{F}_p$-subalgebra S of R such that $R = S \oplus \mathscr{J}(R)$, and $S \cong R/\mathscr{J}(R)$ as $\mathbb{F}_p$-algebras. Moreover, S is unique up to conjugation by elements of $1 + \mathscr{J}(R)$.

<u>semisimple</u>

$S \cong S_1 \oplus S_2 \oplus \cdots \oplus S_t$

each S_i is <u>simple</u>

$$\text{Each } S_i \cong \begin{cases} \mathbb{F}_{p^{d_i}} & (\text{field}) \\ M_{n_i}(p^{d_i}) & (\text{full matrix rings}) \end{cases}$$

Example: Products of fields (commutative, semisimple)

(Werner [Wer15])

R	$\sigma(R)$? coverable?
$\mathbb{F}_2$?	Not coverable!
$\mathbb{F}_2 \times \mathbb{F}_2$?	$\sigma(R) = 3$
$\mathbb{F}_3 \times \mathbb{F}_3$?	Not coverable! $R = \langle (1,-1) \rangle$
$\mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$?	$\sigma(R) = 6$
$\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4$?	$\sigma(R) = 4$
$\mathbb{F}_4 \times \mathbb{F}_4$?	$\sigma(R) = 4$ (!)

There exists $\tau(q) \in \mathbb{N}$ such that $\prod_{i=1}^{\tau(q)} \mathbb{F}_q$ is coverable (& $\tau(q)$ min'l)

Example: Full matrix rings (noncommutative, semisimple)

(Lucchini, Maróti [LM10], Crestani [Cre12])

$R = M_n(q)$ (n x n matrices, entries from $\mathbb{F}_q$)

a: smallest prime divisor of n

$$\sigma(R) = \frac{1}{a} \prod_{\substack{k=1;\\ a \nmid k}}^{n-1} (q^n - q^k) + \sum_{\substack{k=1;\\ a \nmid k}}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k}_q$$

<u>q-binomial coefficient</u>: $$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-(k-1)}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

Example: commutative, not semisimple

(S., Werner [SW21]) Let $q = p^d$

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} : a, b, c \in \mathbb{F}_q \right\}$$

J

$S \cong \mathbb{F}_q$

$$\cong \mathbb{F}_q \oplus \mathbb{F}_q^2$$

$$\sigma(R) = q + 1$$

Example: noncommutative, not semisimple

<u>DEF</u> $R = A(n, q_1, q_2)$ $\qquad q_1 = p^{d_1} \qquad q_2 = p^{d_2}$

$$q = q_1 \otimes q_2 := p^{\mathrm{LCM}(d_1, d_2)}$$

J

S

$$R = \left(\begin{array}{c|c} M_n(q_1) & \begin{matrix} q \\ q \\ \vdots \\ q \end{matrix} \\ \hline & \mathbb{F}_{q_2} \end{array}\right)$$

<u>EX</u>

$$R = \left(\begin{array}{c|c} M_4(2) & \begin{matrix} \mathbb{F}_2 \\ \mathbb{F}_2 \\ \mathbb{F}_2 \\ \mathbb{F}_2 \end{matrix} \\ \hline & \mathbb{F}_2 \end{array}\right)$$

$\sigma(R) = 31$

$< \sigma(M_4(2)) = 71$

Known so far

$\cancel{2}$	3	4	5	6	7	8	9	10	11	12	13	14	15

prime power $+ 1$

$\sigma(M_2(3)) = 7$

$\sigma(M_2(4)) = 11$

$\sigma(\prod_{i=1}^{5} \mathbb{F}_5) = 15$

Is there a ring with $\sigma(R) = 13$???

Main Result

$$\tau(q) = \begin{cases} 1, & \text{if } d = 1 \\ [\text{\# of irred poly of deg } d \text{ in } \mathbb{F}_p[x]] + 1, & d > 1 \end{cases}$$

$$\nu(q) = \begin{cases} 1, & \text{if } d = 1 \\ \omega(d) = \text{\# distinct prime divisors of } d, & d > 1 \end{cases}$$

Theorem (S., Werner (2021+))

Let R be a σ-elementary ring with unity. Then, one of the following holds.

(1) *If R is commutative and semisimple, then for some prime power $q = p^d$, $R \cong \prod_{i=1}^{\tau(q)} \mathbb{F}_q$ and*

$$\sigma(R) = \tau(q)\nu(q) + d\binom{\tau(q)}{2}.$$

(This case was originally determined by Werner [Wer15].)

Main Result, cont.

Theorem (S., Werner (2021+))

Let R be a σ-elementary ring with unity. Then, one of the following holds.

(2) *If R is commutative but not semisimple, then for some prime power q, $R \cong \mathbb{F}_q(+)\mathbb{F}_q^2$ and*

$$\sigma(R) = q + 1.$$

(This case was originally done by S., Werner [SW21].)

Main Result, cont.

Theorem (S., Werner (2021+))

Let R be a σ-elementary ring with unity. Then, one of the following holds.

(3) *If R is noncommutative and semisimple, then for some prime power q and integer $n \geqslant 2$, $R \cong M_n(q)$ and*

$$\sigma(R) = \frac{1}{a} \prod_{k=1; a \nmid k}^{n-1} (q^n - q^k) + \sum_{k=1; a \nmid k}^{\lfloor n/2 \rfloor} \binom{n}{k}_q,$$

where a is the smallest prime divisor of n.

(This case was finished by Peruginelli, Werner [PW18], building on work of Crestani [Cre12] and Lucchini, Maróti [LM10].)

Main Result, cont.

Theorem (S., Werner (2021+))

Let R be a σ-elementary ring with unity. Then, one of the following holds.

(4) *If R is noncommutative and not semisimple, then $R \cong A(n, q_1, q_2)$ and one of the two cases below holds. Let $q = q_1 \otimes q_2 = q_1^d$, and let a be the smallest prime divisor of n.*

- i. *$n = 1$ and $(q_1, q_2) \neq (2, 2)$ or $(4, 4)$. In this case, $\sigma(R) = q + 1$.*
- ii. *$n \geqslant 3$, $d < n - (n/a)$, and $(n, q_1) \neq (3, 2)$. In this case,*

$$\sigma(R) = q^n + \binom{n}{d}_{q_1} + \omega(d).$$

$q_1 \otimes q_2 = p^{d_1} \otimes p^{d_2} = p^{\mathrm{LCM}(d_1, d_2)}$

$\omega(d)$ = # distinct prime divisors of d

$$A(n, q_1, q_2) = \left(\begin{array}{c|c} M_n(q_1) & \begin{smallmatrix} q \\ q \\ \vdots \\ q \end{smallmatrix} \\ \hline & \mathbb{F}_{q_2} \end{array}\right)$$

Immediate consequences

Corollary (S., Werner (2021+))

There is no ring R with unity with $\sigma(R) = 13$.

Immediate consequences, cont.

Corollary (S., Werner (2021+))

Let $\mathscr{E}(N) := \{m : m \leqslant N, \sigma(R) = m$ *for some ring with unity* $R\}$.
Then, for all $N \geqslant 5$,

$$\frac{N}{\log N} < |\mathscr{E}(N)| < \frac{128N}{\log N},$$

where $\log N$ *denotes the binary (base* 2*) logarithm of* N.
In particular, we have

$$|\mathscr{E}(N)| = \Theta(N/\log(N))$$

and

$$\lim_{N\to\infty} \frac{|\mathscr{E}(N)|}{N} = 0.$$

How do we analyze $A(n, q_1, q_2)$?

How do we analyze $A(n, q_1, q_2)$?

How do we analyze $A(n, q_1, q_2)$?

How do we analyze $A(n, q_1, q_2)$?

Thank you!

References I

J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, and A. Maróti, *Sets of elements that pairwise generate a linear group*, J. Combin. Theory Ser. A **115** (2008), no. 3, 442–465. MR 2402604

R. A. Bryce, V. Fedri, and L. Serena, *Subgroup coverings of some linear groups*, Bull. Austral. Math. Soc. **60** (1999), no. 2, 227–238. MR 1711930

Mira Bhargava, *Groups as unions of proper subgroups*, Amer. Math. Monthly **116** (2009), no. 5, 413–422. MR 2510838

J. H. E. Cohn, *On n-sum groups*, Math. Scand. **75** (1994), no. 1, 44–58. MR 1308936

Jonathan Cohen, *On rings as unions of four subrings*, `https://arxiv.org/abs/2008.03803`, 2020.

References II

- Eleonora Crestani, *Sets of elements that pairwise generate a matrix ring*, Comm. Algebra **40** (2012), no. 4, 1570–1575. MR 2913003
- Merrick Cai and Nicholas J. Werner, *Covering numbers of upper triangular matrix rings over finite fields*, Involve **12** (2019), no. 6, 1005–1013. MR 3990794
- Casey Donoven and Luise-Charlotte Kappe, *Finite coverings of semigroups and related structures*, `https://arxiv.org/pdf/2002.04072.pdf`, 2020.
- Eloisa Detomi and Andrea Lucchini, *On the structure of primitive n-sum groups*, Cubo **10** (2008), no. 3, 195–210. MR 2467921
- Martino Garonzi, *Finite groups that are the union of at most 25 proper subgroups*, J. Algebra Appl. **12** (2013), no. 4, 1350002, 11. MR 3037278

References III

- Stephen M. Gagola, III and Luise-Charlotte Kappe, *On the covering number of loops*, Expo. Math. **34** (2016), no. 4, 436–447. MR 3578007
- Martino Garonzi, Luise-Charlotte Kappe, and Eric Swartz, *On integers that are covering numbers of groups*, *Experimental Mathematics*, `https://doi.org/10.1080/10586458.2019.1636425`, 2019, pp. 1–19.
- Be'eri Greenfield, *Personal communication to N. Werner*, 2020.
- P. E. Holmes, *Subgroup coverings of some sporadic groups*, J. Combin. Theory Ser. A **113** (2006), no. 6, 1204–1213. MR 2244142
- Jacques Lewin, *Subrings of finite index in finitely generated rings*, J. Algebra **5** (1967), 84–88. MR 200297

References IV

- Andrea Lucchini and Attila Maróti, *Rings as the unions of proper subrings*, http://arxiv.org/abs/1001.3984v1, 2010.
- ———, *Rings as the unions of proper subrings*, Algebr. Represent. Theory **15** (2012), no. 6, 1035–1047. MR 2994015
- Attila Maróti, *Covering the symmetric groups with proper subgroups*, J. Combin. Theory Ser. A **110** (2005), no. 1, 97–111. MR 2128968
- B. H. Neumann, *Groups covered by permutable subsets*, J. London Math. Soc. **29** (1954), 236–248. MR 62122
- G. Peruginelli and N. J. Werner, *Maximal subrings and covering numbers of finite semisimple rings*, Comm. Algebra **46** (2018), no. 11, 4724–4738. MR 3864260
- Gaetano Scorza, *I gruppi che possone pensarsi come somma di tre lori sottogruppi*, Boll. Un. Mat. Ital. **5** (1926), 216–218.

References V

- Eric Swartz and Nicholas J. Werner, *Covering numbers of commutative rings*, J. Pure Appl. Algebra **225** (2021), no. 8, 106622, 17. MR 4177971
- Eric Swartz, *On the covering number of symmetric groups having degree divisible by six*, Discrete Math. **339** (2016), no. 11, 2593–2604. MR 3518409
- M. J. Tomkinson, *Groups as the union of proper subgroups*, Math. Scand. **81** (1997), no. 2, 191–198. MR 1613772
- Nicholas J. Werner, *Covering numbers of finite rings*, Amer. Math. Monthly **122** (2015), no. 6, 552–566. MR 3361734