# Covering Numbers of Rings

Nicholas J. Werner

SUNY College at Old Westbury

April 30, 2020

# Motivation: Covering Numbers of Groups

Let $G$ be a group.

- A cover of $G$ is a collection $\mathcal{H}$ of proper subgroups of $G$ whose union is all of $G$: $G = \bigcup_{H \in \mathcal{H}} H$
- $G$ is coverable if and only if $G$ is non-cyclic.
- The covering number of $G$ is the minimum number of subgroups necessary to cover $G$.
- $\sigma(G) =$ covering number of $G$.
- Questions to pursue:
  - Given $G$, what is $\sigma(G)$?
  - Given $n \in \mathbb{N}$, we can find a group $G$ such that $\sigma(G) = n$?
- Easy examples: $\sigma(C_2 \times C_2) = 3$
  In fact, for any group $G$, $\sigma(G) \geq 3$.
- Theorem: There is no group $G$ such that $\sigma(G) = 7$.
  There is no group $G$ such that $\sigma(G) = 11$.

# What about Covering Numbers for Rings?

Let $R$ be a ring.

- A cover of $R$ is a collection $\mathcal{C}$ of proper subrings of $R$ whose union is all of $R$: $R = \bigcup_{S \in \mathcal{C}} S$
- $R$ is coverable if and only if a cover exists.
- The covering number of $R$ is the minimum number of subrings necessary to cover $R$.
- $\sigma(R) =$ covering number of $R$.
- Questions to consider:
  - Should rings have unity? Should subrings have unity?
  - Which rings are coverable?
  - Given $R$, what is $\sigma(R)$?
  - Given $n \in \mathbb{N}$, we can find a ring $R$ such that $\sigma(R) = n$?

# Conventions about Unity

- All rings contain unity.
  Why we want this: nice structure theorems for finite rings.

- For $S \subseteq R$ to be a subring, we have three options.
  (S1) $S$ must contain $1_R$
  
  (S2) $S$ must contain some multiplicative identity ($1_S \neq 1_R$, possibly)
  
  (S3) $S$ need not contain any multiplicative identity

  Generally, (S1) and (S2) are too restrictive.

  We adopt (S3): a subring of a ring must be an Abelian group under addition, and must be closed under multiplication.

# Example: $\mathbb{Z}_2 \times \mathbb{Z}_2$

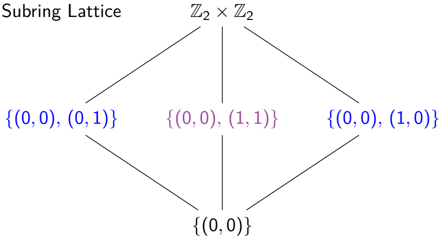
(S1) $S$ must contain $1_R$

(S2) $S$ must contain some multiplicative identity ($1_S \neq 1_R$, possibly)

(S3) $S$ need not contain any multiplicative identity

For each $n$, let $\mathbb{Z}_n$ be the ring of integers mod $n$.

**Example**. Let $R = \mathbb{Z}_2 \times \mathbb{Z}_2$




Under (S1), $R$ is not coverable.

Under (S2) or (S3), $R$ is coverable, and $\sigma(R) = 3$.

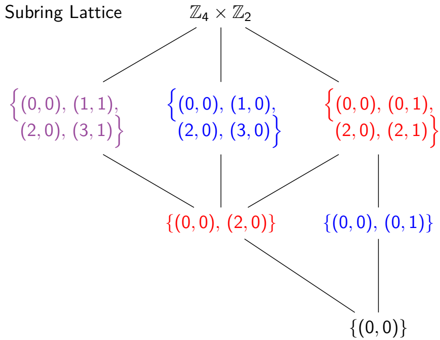
# Example: $\mathbb{Z}_4 \times \mathbb{Z}_2$

(S1) $S$ must contain $1_R$

(S2) $S$ must contain some multiplicative identity ($1_S \neq 1_R$, possibly)

(S3) $S$ need not contain any multiplicative identity

**Example**. Let $R = \mathbb{Z}_4 \times \mathbb{Z}_2$.




Under (S1) or (S2), $R$ is not coverable.

Under (S3), $R$ is coverable, and $\sigma(R) = 3$.

# Coverable Rings

A group $G$ is coverable if and only if $G$ is non-cyclic.

What is the analog of "cyclic" for rings?

## Notation

Let $R$ be a ring and $a \in R$.

The subring generated by $a$, denoted by $\langle\langle a \rangle\rangle$, is the smallest subring of $R$ containing $a$.

- Elements of $\langle\langle a \rangle\rangle$ are "polynomials in $a$":

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a$$

  where $n \geq 1$ and each $c_i \in \mathbb{Z}$.

- $R$ is coverable if and only if for all $a \in R$, $R \neq \langle\langle a \rangle\rangle$

# Examples

$\mathbb{Z}_n =$ ring of integers mod $n$

$\mathbb{F}_q =$ finite field with $q$ elements ($q$ a prime power)

Then:

- $\mathbb{Z}_n$ is **not** coverable, because $\mathbb{Z}_n = \langle\langle 1 \rangle\rangle$
- $\mathbb{F}_q$ is **not** coverable.
  **Proof**. The unit group of $\mathbb{F}_q$ is cyclic and isomorphic to $C_{q-1}$.
  Let $u$ be a generator of the unit group.
  Then, $\mathbb{F}_q = \langle\langle u \rangle\rangle$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$ are coverable
  Both have covering number 3.
  (If you get bored: Is $\mathbb{Z}_3 \times \mathbb{Z}_3$ coverable? Is $\mathbb{F}_4 \times \mathbb{F}_4$ coverable?)
- Note that $\langle\langle a \rangle\rangle$ is commutative.
  Consequently, any noncommutative ring is coverable.

# Easy Observations and Known Results

- If $R$ is coverable, then $\sigma(R) \geq 3$
- If $R/I$ is coverable, then $R$ is coverable, and $\sigma(R) \leq \sigma(R/I)$
- We can assume all subrings used in a minimal cover are maximal.
- A. Lucchini, A. Maróti (2012): classified all rings with covering number 3
- A. Lucchini, A. Maróti (2010), E. Crestani (2012): covering number for $M_n(\mathbb{F}_q)$ ($n \times n$ matrices over $\mathbb{F}_q$)
- N. W. (2015): covering number for direct products of finite fields
- G. Peruginelli, N. W. (2018): covering number for finite semisimple rings (direct products of matrix rings over finite fields)
- M. Cai, N. W. (2019): covering numbers for $2 \times 2$ upper triangular matrix rings over finite fields

# Reducing to the case of Finite Rings

## Proposition (B. H. Neumann, J. Lewin)

Let $R$ be a coverable 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 and $\sigma(R) = \sigma(R/I)$.

**Proof**.

- B. H. Neumann (1954): If $R = \bigcup_{i=1}^n S_i$, then each $S_i$ has finite index in $R$.
- J. Lewin (1967): The intersection $\bigcap_{i=1}^n S_i$ contains a two-sided ideal $I$ of finite index.
- So: a cover of $R$ can be pushed forward onto $R/I$. Thus, $\sigma(R/I) \leq \sigma(R)$.
- It is always true that $\sigma(R) \leq \sigma(R/I)$. Therefore, $\sigma(R) = \sigma(R/I)$.

Question: $\mathbb{R}$ is coverable, and $\sigma(\mathbb{R})$ is infinite.
Is $\sigma(\mathbb{R})$ countable?
What are the maximal subrings of $\mathbb{R}$?

# Reducing to Rings of Order $p^n$

## Chinese Remainder Theorem

Let $R$ be a finite ring with unity.

Then, $R$ is isomorphic to a direct product of rings of prime power order:

$$R \cong R_1 \times R_2 \times \cdots \times R_n$$

where $|R_i| = p_i^{e_i}$ for distinct primes $p_1, \ldots, p_n$.

Moreover, if $S$ is a subring of $R$, then

$$S \cong S_1 \times S_2 \times \cdots \times S_n$$

where each $S_i$ is a subring of $R_i$.

## Corollary

Let $R$ be as above.

If $R$ is coverable, then $\sigma(R) = \min_{1 \le i \le n} \sigma(R_i)$.

# Reducing to characteristic $p$

## Proposition (E. Swartz, N. W. (2019–))

Let $R$ be a finite coverable ring of characteristic $p^n$.
Then $\sigma(R) = \sigma(R/pR)$.

**Proof.**

- Let $M$ be a maximal subring of $R$. Show that $pR \subseteq M$.
  - If $pR \not\subseteq M$, then $R = M + pR$ by maximality.
  - Let $r \in R$. Then,
    $$\begin{aligned} r &= m_1 + pr_1 \\ &= m_1 + p(m_2 + pr_2) = m_1 + pm_2 + p^2 r_2 \\ &= m_1 + pm_2 + p^2(m_3 + pr_3) = m_1 + pm_2 + p^2 m_3 + p^3 r_3 \\ &= m_1 + pm_2 + p^2 m_3 + \cdots + p^{n-1} m_{n-1} \end{aligned}$$
    which is in $M$.
  - So, $M = R$. Contradiction!
- Since $pR$ is contained in every maximal subring, any minimal cover of $R$ can be pushed forward onto $R/pR$. So, $\sigma(R/pR) \leq \sigma(R)$.
- Certainly, $\sigma(R) \leq \sigma(R/pR)$. Thus, $\sigma(R/pR) = \sigma(R)$.

# Which Numbers occur as Covering Numbers of Rings?

Recall: there are no groups with covering number 7 or 11 (among others).
Are there similar restricted values for covering numbers of rings?

## Example

Let $q = p^n$ be a prime power.
Then, there exists a ring $R$ with $\sigma(R) = p^n + 1$.

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

- Maximal subrings of $R$ $\longleftrightarrow$ linear subspaces of $\mathbb{F}_q^2$

  $\left\{ \begin{bmatrix} a & xb & xc \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \ : \ a, x \in \mathbb{F}_q \right\} \longleftrightarrow \text{Span} \begin{pmatrix} b \\ c \end{pmatrix}$
- $\mathbb{F}_q^2$ has $q+1$ linear subspaces
- We need every maximal subring to cover $R$

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Using the fact that $p^n + 1$ occurs as a covering number

# Covering Numbers of Matrix Rings

### Theorem (Lucchini & Maróti (2010), Crestani (2012))

Let $n \geq 2$. Let $d$ be the smallest prime divisor of $n$.
Let $m$ be the number of subspaces $W \subseteq \mathbb{F}_q^n$ such that:

- $\dim(W) \leq \frac{n}{2}$, and
- $d$ does not divide $\dim(W)$.

Then,

$$\sigma(M_n(\mathbb{F}_q)) = m + \frac{1}{n} \prod_{\substack{i=1, \\ d \nmid i}}^{n-1} (q^n - q^i)$$

In particular,

$$\sigma(M_2(\mathbb{F}_q)) = q + 1 + \tfrac{1}{2}(q^2 - q)$$

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Using the fact that $p^n + 1$ occurs as a covering number

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Using the fact that $p^n + 1$ occurs as a covering number

Using covering numbers for $M_2(\mathbb{F}_q)$ : $\sigma = q + 1 + \frac{1}{2}(q^2 - q)$

# Examples: Direct Products of Finite Fields

| $R$ | Coverable? | $\sigma(R)$ |
| --- | --- | --- |
| $\mathbb{F}_q$ | **No** | — |
| $\mathbb{F}_2 \times \mathbb{F}_2$ | Yes | 3 |
| $\mathbb{F}_3 \times \mathbb{F}_3$ | **No**: $R = \langle\langle(1, -1)\rangle\rangle$ | — |
| $\mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3$ | Yes | 6 |
| $\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4$ | Yes | 4 |
| $\mathbb{F}_4 \times \mathbb{F}_4 \times \mathbb{F}_4$ | Yes | 4 |
| $\mathbb{F}_4 \times \mathbb{F}_4$ | Yes | 4 |
| $\mathbb{F}_2 \times \mathbb{F}_4$ | **No**: $R = \langle\langle(1, \alpha)\rangle\rangle$ where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ | — |

# Direct Products of the Same Field

**Theorem (N. W. (2015))**

Let $R = \prod_i (\prod_j F_i)$, where each $F_i$ is a distinct finite field. Then,

1. $R$ is coverable if and only if at least one $\prod_j F_i$ is coverable
2. if $R$ is coverable, then $\sigma(R) = \min_i \{\sigma(\prod_j F_i)\}$

**Theorem (N. W. (2015))**

For each prime power $q$, there exists a positive integer $\tau(q)$ such that

$$\prod_{i=1}^{t} \mathbb{F}_q \text{ is coverable if and only if } t \geq \tau(q).$$

Moreover, if $t \geq \tau(q)$, then $\sigma(\prod_{i=1}^{t} \mathbb{F}_q) = \sigma(\prod_{i=1}^{\tau(q)} \mathbb{F}_q)$.

# How to find $\tau(q)$?

$\tau(q)$: smallest value of $t$ such that $\prod_{i=1}^{t} \mathbb{F}_q$ is coverable.

**Example**. Let $R = \mathbb{F}_q \times \mathbb{F}_q$.

Suppose there exist $\alpha, \beta \in \mathbb{F}_q$ such that

- $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ and $\mathbb{F}_q = \mathbb{F}_p(\beta)$
- $\alpha$ and $\beta$ have different minimal polynomials over $\mathbb{F}_p$
  - $f(x) =$ minimial polynomial for $\alpha$
  - $g(x) =$ minimial polynomial for $\beta$
  - $f(x) \neq g(x)$

Let $S = \langle\langle(\alpha, \beta)\rangle\rangle$. Then, $S = R$, because:

- $f((\alpha, \beta)) = (f(\alpha), f(\beta)) = (0, f(\beta)) \in S$
- $(0, f(\beta))^{q-1} = (0, 1) \in S$
- $(0, 1)(\alpha, \beta) = (0, \beta) \in S$
- $\{0\} \times \mathbb{F}_q \subseteq S$
- Likewise, $\mathbb{F}_q \times \{0\} \subseteq S$

Conclusion: $t$ needs to be big enough to prevent this

# A Formula for $\tau(q)$

$\tau(q)$: smallest value of $t$ such that $\prod_{i=1}^{t} \mathbb{F}_q$ is coverable.

**Theorem**

Let $q = p^n$.

Let $\psi(p, n)$ be the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree $n$.

Then

$$\tau(q) = \begin{cases} p & n = 1 \\ \psi(p, n) + 1 & n > 1 \end{cases}$$

A formula for $\psi(p, n)$ is known:

$$\psi(p, n) = \frac{1}{n} \sum_{d \mid n} \mu(d) p^{n/d}$$

where the sum is taken over all positive divisors $d$ of $n$, and $\mu$ is the Möbius $\mu$-function.

# A Formula for the Covering Number

**Theorem**

Let $q = p^n$.

Let $\omega(n) = \begin{cases} 1 & n = 1 \\ \# \text{ prime divisors of } n & n > 1 \end{cases}$

Then,

$$\sigma\left(\prod_{i=1}^{\tau(q)} \mathbb{F}_q\right) = \tau(q)\omega(n) + n\binom{\tau(q)}{2}$$

When $n = 1$, we have $\tau(p) = p$ and $\sigma(\prod_{i=1}^{p} \mathbb{F}_p) = p + \binom{p}{2} = p + \frac{1}{2}(p^2 - p)$

Here are the covering numbers of $R = \prod_{i=1}^{\tau(q)} \mathbb{F}_q$ for some other values of $q$:

| $q$ | 4 | 8 | 9 | 16 | 25 | 27 | 32 | 49 | 64 | 81 | 125 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\tau(q)$ | 2 | 3 | 4 | 4 | 11 | 9 | 7 | 22 | 10 | 19 | 41 |
| $\sigma(R)$ | 4 | 12 | 16 | 28 | 121 | 117 | 112 | 484 | 290 | 703 | 2501 |

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Using the fact that $p^n + 1$ occurs as a covering number

Using covering numbers for $M_2(\mathbb{F}_q)$: $\sigma = q + 1 + \frac{1}{2}(q^2 - q)$

# Which Numbers occur as Covering Numbers of Rings?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Using the fact that $p^n + 1$ occurs as a covering number

Using covering numbers for $M_2(\mathbb{F}_q)$ : $\sigma = q + 1 + \frac{1}{2}(q^2 - q)$

Using covering numbers for $\prod_{i=1}^{p} \mathbb{F}_p$ : $\sigma = p + \frac{1}{2}(p^2 - p)$

# Conjectures

## Conjecture

There does not exist a ring with unity that has covering number 13.

## (Much stronger) Conjecture (maybe too strong?)

For rings with unity, the only possible (finite) covering numbers are

- $p^n + 1$
- those coming from $M_n(\mathbb{F}_q)$
- those coming from $\prod_{i=1}^{\tau(q)} \mathbb{F}_q$

Thank you!

# References


- M. Cai, N. Werner. *Covering numbers of upper triangular matrix rings over finite fields*. Involve 12 (2019), no. 6, 1005–1013.
- E. Crestani. *Sets of elements that pairwise generate a matrix ring*. Comm. Algebra 40 (2012), no. 4, 1570–1575.
- L.-C. Kappe. *Finite coverings: a journey through groups, loops, rings, and semigroups*, in Group Theory, Combinatorics, and Computing. Contemporary Mathematics, Vol. 611. Amer. Math. Soc., Providence, RI, 2014. 79–88.
- A. Lucchini, A. Maróti. *Rings as the union of proper subrings*. Preprint (2010). http://arxiv.org/abs/1001.3984v1
- A. Lucchini, A. Maróti. *Rings as the union of proper subrings*. Algebr. Represent. Theory 15 (2012) 1035–1047.
- G. Peruginelli, N. Werner. *Maximal subrings and covering numbers of finite semisimple rings*. Comm. Algebra 46 (2018), no. 11, 4724–4738.
- N. Werner. *Covering numbers of finite rings*. Amer. Math. Monthly 122 (2015), no. 6, 552–566.