involve
a journal of mathematics

Covering numbers of upper triangular matrix rings over finite fields

Merrick Cai and Nicholas J. Werner

msp

2019 vol. 12, no. 6

INVOLVE 12:6 (2019)
dx.doi.org/10.2140/involve.2019.12.1005

Covering numbers of upper triangular matrix rings over finite fields

Merrick Cai and Nicholas J. Werner

(Communicated by Scott T. Chapman)

A cover of a finite ring R is a collection of proper subrings $\{S_1, \dots, S_m\}$ of R such that $R = \bigcup_{i=1}^m S_i$. If such a collection exists, then R is called coverable, and the covering number of R is the cardinality of the smallest possible cover. We investigate covering numbers for rings of upper triangular matrices with entries from a finite field. Let $\mathbb{F}_q$ be the field with q elements and let $T_n(\mathbb{F}_q)$ be the ring of $n \times n$ upper triangular matrices with entries from $\mathbb{F}_q$. We prove that if $q \neq 4$, then $T_2(\mathbb{F}_q)$ has covering number $q+1$, that $T_2(\mathbb{F}_4)$ has covering number 4, and that when p is prime, $T_n(\mathbb{F}_p)$ has covering number $p+1$ for all $n \geq 2$.

1. Introduction

It is well known that no group is equal to the union of two proper subgroups. However, it is possible to achieve such a union if we allow the use of more than two proper subgroups. For example, the Klein 4-group is equal to the union of its three proper, nontrivial subgroups. More generally, any noncyclic group is equal to the union of its proper cyclic subgroups. Given a finite group G, we say that a collection of proper subgroups $\{H_1, \dots, H_m\}$ forms a *cover* of G if $G = \bigcup_{i=1}^m H_i$. If such a cover exists, then the *covering number* of G is the cardinality of the smallest possible cover.

Natural problems to study regarding covers and covering numbers include finding formulas for the covering number of groups or families of groups, and determining which groups have a specified covering number (e.g., "Which groups have covering number 3?"). Consideration of these types of questions dates back at least nine decades [Scorza 1926; Haber and Rosenfeld 1959; Bruckheimer et al. 1970]. The covering number problem for groups began to become more popular following papers by Cohn [1994] and Tomkinson [1997]. Over the past several years, researchers have begun to study the covering numbers for other algebraic structures [Kappe 2014], including rings [Crestani 2012; Lucchini and Maróti 2012; Werner 2015]. All rings with covering number 3 were characterized in [Lucchini and Maróti 2012],

MSC2010: primary 16P10; secondary 05E15.
Keywords: covering number, upper triangular matrix ring, maximal subring.

and a formula for the covering number of a matrix ring over a finite field was given in [Lucchini and Maróti 2010] (see also the related article [Crestani 2012]). Covering numbers for some other families of finite rings, including direct products of finite fields, were found in [Werner 2015]. The purpose of this paper is to examine the covering numbers for rings of upper triangular matrices with entries from a finite field.

In this paper, rings are assumed to be associative and have a unit element $1 \neq 0$. Subrings, however, need not contain a unit element. Given a ring R, we say that $S \subseteq R$ is a subring of R if S is a subgroup of R under addition and is closed under multiplication.

Definition 1.1. A *cover* of a ring R is a set $\mathcal{S}$ of proper subrings of R such that $R = \bigcup_{S \in \mathcal{S}} S$. If a cover of R exists, then R is said to be *coverable*. In this case, the *covering number* of R is the cardinality of the smallest possible cover. When R is coverable, $\sigma(R)$ denotes the covering number of R.

Not every ring, or even every finite ring, is coverable. For example, for any $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is not coverable because the unit element of $\mathbb{Z}/n\mathbb{Z}$ cannot lie in any proper subring. There is a similar obstruction with finite fields. For a prime power q, we let $\mathbb{F}_q$ be the finite field with q elements. Then, $\mathbb{F}_q$ is never coverable, because the generator of the unit group of $\mathbb{F}_q$ cannot lie in a proper subring.

By contrast, a noncommutative ring is always coverable (a short proof of this is given in Lemma 2.2). Most of this paper will focus on a particular class of noncommutative rings: those consisting of upper triangular matrices. For any ring R and any integer $n \geq 2$, we let $T_n(R)$ be the ring of $n \times n$ upper triangular matrices with entries from R. The main theorem of the paper is the calculation of the covering number for $T_2(\mathbb{F}_q)$.

Theorem 1.2. *Let q be a prime power. Then $\sigma(T_2(\mathbb{F}_q)) = q + 1$ when $q \neq 4$, and $\sigma(T_2(\mathbb{F}_4)) = 4$.*

When $n \geq 3$ and q itself is not prime, we are not able to determine the exact covering number for $T_n(\mathbb{F}_q)$. However, we are able to provide an upper bound for $\sigma(T_n(\mathbb{F}_q))$, and this bound equals the covering number when q is prime. In fact, we obtain a more general result about finite rings having a residue field of prime order.

Corollary 1.3. (1) *Let q be a prime power. If $n \geq 3$, then $\sigma(T_n(\mathbb{F}_q)) \leq q + 1$.*

(2) *Let R be a finite ring and let p be the smallest prime dividing the order of R. If R has $\mathbb{F}_p$ as a residue field, then $\sigma(T_n(R)) = p+1$ for all $n \geq 2$. In particular, $\sigma(T_n(\mathbb{F}_p)) = p + 1$ for all $n \geq 2$.*

We prove both Theorem 1.2 and Corollary 1.3 in Section 3 after stating some basic facts about coverings and covering numbers of rings in Section 2. The paper closes with some remarks on the difficulty of establishing equality in part (1) of Corollary 1.3.

2. Basic definitions and properties

For a group G, it is easy to see that G is coverable if and only if G is not cyclic. This is because if G is cyclic with generator g, then g cannot lie in any proper subgroup of G. On the other hand, if G is noncyclic, then a cover is formed by the collection of all cyclic subgroups of G. Furthermore, if $a \in G$ and $\langle a \rangle$ is a maximal subgroup of G, then $\langle a \rangle$ must be part of any cover of G, since a must lie in some subgroup in the cover, and by maximality that subgroup must equal $\langle a \rangle$. Similar statements are true for rings if we use subrings comparable to cyclic subgroups.

Definition 2.1. Let R be a ring. For any $r \in R$, we let $\langle\langle r \rangle\rangle$ be the subring of R generated by r. The subring $\langle\langle r \rangle\rangle$ is equal to the intersection of all subrings of R containing r, and $\langle\langle r \rangle\rangle$ consists of the elements of the form $c_n r^n + \cdots + c_1 r$, where $n \geq 1$ and $c_1, \ldots, c_n \in \mathbb{Z}$.

The relationships between a ring R and a subring $\langle\langle r \rangle\rangle$ are much the same as those between a group G and a cyclic subgroup $\langle a \rangle$.

Lemma 2.2. *Let R be a ring*:

(1) *R is coverable if and only if for all $r \in R$ we have $R \neq \langle\langle r \rangle\rangle$.*

(2) *For all $r \in R$, if $\langle\langle r \rangle\rangle$ is a maximal subring of R, then $\langle\langle r \rangle\rangle$ is part of any cover of R.*

(3) *If R is noncommutative, then R is coverable.*

(4) *Let I be a two-sided ideal of R. If R/I is coverable, then so is R, and $\sigma(R) \leq \sigma(R/I)$.*

Proof. Items (1) and (2) are proved just as for groups. For (3), notice that $\langle\langle r \rangle\rangle$ is a commutative ring for all $r \in R$. So, in a noncommutative ring R, $\langle\langle r \rangle\rangle$ must be a proper subring for all $r \in R$. Finally, for (4), let $\phi : R \to R/I$ be the quotient map. For any proper subring S of R/I, we have $\phi^{-1}(S)$ is a proper subring of R. So, any cover of R/I lifts to a cover of R. □

Part (4) of the lemma can be used to find upper bounds for $\sigma(R)$. Finding lower bounds is, in general, harder to do. However, a simple counting argument gives a basic lower bound.

Lemma 2.3. *Let R be a finite coverable ring of order m. Let p be the smallest prime dividing m. Then, $p + 1 \leq \sigma(R)$.*

Proof. Every proper subring of R has order at most m/p. Let $S_1, \ldots, S_p$ be proper subrings of R. Since $0 \in S_i$ for each i, the total number of elements in the union of all p subrings is at most $1 + p(m/p - 1) < m$. Thus, R cannot be covered by fewer than $p + 1$ proper subrings. □

3. Main results

In this section, we prove Theorem 1.2 and Corollary 1.3. Our strategy is to show that (when $q \neq 2$ or 4) we may form a cover of $T_2(\mathbb{F}_q)$ by using $q+1$ maximal subrings, each of which is generated by a single matrix. By Lemma 2.2, each of these subrings is part of any cover of $T_2(\mathbb{F}_q)$, so we must have $\sigma(T_2(\mathbb{F}_q)) = q+1$.

Throughout this section, q is a power of the prime p, and $g \in \mathbb{F}_q$ denotes an element of multiplicative order $q-1$ (so, in particular, $\mathbb{F}_q = \mathbb{F}_p(g)$). We let I denote the 2×2 identity matrix, and let M be the matrix $M = \left(\begin{smallmatrix} g & 1 \\ 0 & g \end{smallmatrix}\right) \in T_2(\mathbb{F}_q)$. The matrix M is useful because — as we will prove — it generates a maximal subring of $T_2(\mathbb{F}_q)$.

Lemma 3.1. *Let S be a subring of $T_2(\mathbb{F}_q)$ that contains all of the scalar matrices. Then, $|S|$ is either q, q^2, or q^3. Consequently, if $|S| = q^2$, then S is maximal.*

Proof. Since S contains all of the scalar matrices, it is closed under $\mathbb{F}_q$-scalar multiplication, and hence is an $\mathbb{F}_q$-vector space. This means that $|S| = q^d$, where $d = \dim_{\mathbb{F}_q}(S)$. Since $\dim_{\mathbb{F}_q}(T_2(\mathbb{F}_q)) = 3$, we see that any subring of $T_2(\mathbb{F}_q)$ of order q^2 that contains all of the scalar matrices must be maximal. □

Proposition 3.2. *The subring $\langle\langle M \rangle\rangle$ is maximal, and $\langle\langle M \rangle\rangle = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q \right\}$.*

Proof. Let $S = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q \right\}$. Then, S is a subring of order q^2 and contains all of the scalar matrices, so S is maximal by Lemma 3.1. We will prove that $S \subseteq \langle\langle M \rangle\rangle$.

Note that $M^q = \left(\begin{smallmatrix} g^q & 0 \\ 0 & g^q \end{smallmatrix}\right) = \left(\begin{smallmatrix} g & 0 \\ 0 & g \end{smallmatrix}\right)$. Since $\langle\langle g \rangle\rangle = \mathbb{F}_q$, $\langle\langle M \rangle\rangle$ contains all of the scalar matrices as well as the matrix $M - M^q = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. This implies that $S \subseteq \langle\langle M \rangle\rangle$, and by maximality $S = \langle\langle M \rangle\rangle$. □

By Lemma 2.2, $\langle\langle M \rangle\rangle$ will be part of any cover of $T_2(\mathbb{F}_q)$. When q is odd, we can form other maximal subrings by using matrices of the form $\left(\begin{smallmatrix} g & b \\ 0 & -g \end{smallmatrix}\right)$, where $b \in \mathbb{F}_q$. This will not work if q is even, because $\left(\begin{smallmatrix} g & b \\ 0 & -g \end{smallmatrix}\right) \in \langle\langle M \rangle\rangle$ in this case. So, in characteristic 2, we must use different matrices.

Lemma 3.3. *Let $q = 2^k$, where $k \geq 3$. Let $G = \{a \in \mathbb{F}_q \mid \mathbb{F}_2(a) = \mathbb{F}_q\}$ be the set of elements of $\mathbb{F}_q$ that generate $\mathbb{F}_q$ over $\mathbb{F}_2$. Then, there exists $\alpha \in \mathbb{F}_q$ such that $\alpha^2 + \alpha \in G$.*

Proof. Let $H = \{b^2 + b \mid b \in \mathbb{F}_q\}$. We show that $|G| > q/2$ and $|H| = q/2$, which means that $G \cap H$ is nonempty.

For G, note that $c \in \mathbb{F}_q \setminus G$ if and only if c lies in some maximal subfield of $\mathbb{F}_q$. For $q = 2^k$, the proper subfields of $\mathbb{F}_q$ are precisely $\mathbb{F}_{2^d}$ for $d \mid k$ and $d < k$. In particular, $|\mathbb{F}_{2^d}| \leq 2^{k/2}$. When $k = 3$, the only subfield of $\mathbb{F}_8$ is $\mathbb{F}_2$ so $|G| = 6$ and the result holds. For $k = 4$, the only maximal subfield of $\mathbb{F}_{16}$ is $\mathbb{F}_4$, so $|G| = 12$ and the result holds again. Now assume $k \geq 5$. Then consider $\omega(k)$, the number of distinct prime factors of k. There are thus $\omega(k)$ maximal subfields. We easily find that $\omega(k) < k/2$ for $k \geq 5$. Letting $d_1, d_2, \ldots, d_{\omega(k)}$ be the maximal divisors of k (i.e., k/d_i is a prime), we get

$$\left|\bigcup_{i=1}^{\omega(k)} \mathbb{F}_{2^{d_i}}\right| < \sum_{i=1}^{\omega(k)} 2^{d_i} \leq \frac{k}{2} \cdot 2^{k/2} < 2^{k-1} = \frac{q}{2}.$$

Thus, $|G| > q/2$.

Now, for H, observe that for all $x, y \in \mathbb{F}_q$, we have $x^2 + x = y^2 + y$ if and only if $x + y = x^2 + y^2 = (x + y)^2$, which holds if and only if $x + y = 0$ or $x + y = 1$. Hence, $x^2 + x = y^2 + y$ if and only if $x = y$ or $x = y + 1$. As a result, we get $q/2$ distinct values of $x^2 + x$ as x runs through $\mathbb{F}_q$. So, $|H| = q/2$ and $G \cap H \neq \varnothing$. $\square$

Remark 3.4. Lemma 3.3 fails when $q = 4$. In this case, $\mathbb{F}_4 = \{0, 1, a, a+1\}$, where $a^2 + a + 1 = 0$. So, $\alpha^2 + \alpha$ equals 0 or 1 for all $\alpha \in \mathbb{F}_4$, and neither 0 nor 1 generates $\mathbb{F}_4$ over $\mathbb{F}_2$.

Definition 3.5. When q is odd, for each $b \in \mathbb{F}_q$ let $X_b = \left(\begin{smallmatrix} g & b \\ 0 & -g \end{smallmatrix}\right)$. When q is even and $q \geq 8$, let $\alpha \in \mathbb{F}_q$ be such that $\alpha^2 + \alpha$ generates $\mathbb{F}_q$ over $\mathbb{F}_2$, and for each $b \in \mathbb{F}_q$ let $Y_b = \left(\begin{smallmatrix} \alpha & b \\ 0 & \alpha+1 \end{smallmatrix}\right)$.

The subrings $\langle\langle X_b \rangle\rangle$ and $\langle\langle Y_b \rangle\rangle$ are the subrings we require to complete the covers of $T_2(\mathbb{F}_q)$. Proving that this is the case involves several lemmas and propositions.

Lemma 3.6. *When q is odd, g^2 generates $\mathbb{F}_q$ over $\mathbb{F}_p$.*

Proof. Note that $|\langle g^2 \rangle| = (q-1)/2$ as a multiplicative group. Combined with the element 0, we have $|\mathbb{F}_p(g^2)| \geq (q+1)/2$. Since $\mathbb{F}_p(g^2)$ is a subfield of $\mathbb{F}_q$, its order divides q. Hence, $\mathbb{F}_p(g^2)$ must be all of $\mathbb{F}_q$. $\square$

Lemma 3.7. *When q is odd, X_b, X_c, and I are linearly independent over $\mathbb{F}_q$ for all distinct $b, c \in \mathbb{F}_q$. When q is even and $q \geq 8$, Y_b, Y_c, and I are linearly independent over $\mathbb{F}_q$ for all distinct $b, c \in \mathbb{F}_q$.*

Proof. Assume that q is odd. Let $x_1, x_2, x_3 \in \mathbb{F}_q$ be such that $x_1 \cdot X_b + x_2 \cdot X_c + x_3 \cdot I = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. This corresponds to the matrix equation

$$\begin{pmatrix} g & g & 1 \\ b & c & 0 \\ -g & -g & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

The 3×3 matrix for this system has determinant $2g(c - b)$, which is nonzero because $\mathbb{F}_q$ has odd characteristic and $b \neq c$. Hence, $x_1 = x_2 = x_3 = 0$ and X_b, X_c, and I are linearly independent. The proof for characteristic 2 is the same, except that the determinant of the relevant matrix is $b + c$, which is still nonzero. So, Y_b, Y_c, and I are also linearly independent. $\square$

Proposition 3.8. *When q is odd, $\langle\langle X_b \rangle\rangle$ is maximal for each $b \in \mathbb{F}_q$ and has order q^2. When q is even and $q \geq 8$, $\langle\langle Y_b \rangle\rangle$ is maximal for each $b \in \mathbb{F}_q$ and has order q^2.*

Proof. Assume that q is odd. Observe that $X_b^2 = \left(\begin{smallmatrix} g^2 & 0 \\ 0 & g^2 \end{smallmatrix}\right)$. By Lemma 3.6, $\langle\langle X_b \rangle\rangle$ contains all of the scalar matrices in $T_2(\mathbb{F}_q)$. Since X_b itself is not scalar, Lemma 3.1 shows that $|\langle\langle X_b \rangle\rangle|$ is either q^2 or q^3. But, $\langle\langle X_b \rangle\rangle \neq T_2(\mathbb{F}_q)$ because $\langle\langle X_b \rangle\rangle$ is commutative, so $|\langle\langle X_b \rangle\rangle| = q^2$ and $\langle\langle X_b \rangle\rangle$ is maximal by Lemma 3.1. The proof for $\langle\langle Y_b \rangle\rangle$ is identical after noting that $Y_b^2 + Y_b = \left(\begin{smallmatrix} \alpha^2+\alpha & 0 \\ 0 & \alpha^2+\alpha \end{smallmatrix}\right)$. □

Proposition 3.9. *Let $F = \{a \cdot I \mid a \in \mathbb{F}_q\}$ be the subring of scalar matrices in $T_2(\mathbb{F}_q)$:*

(1) *If q is odd, then $\langle\langle X_b \rangle\rangle \cap \langle\langle M \rangle\rangle = F$ for all $b \in \mathbb{F}_q$, and $\langle\langle X_b \rangle\rangle \cap \langle\langle X_c \rangle\rangle = F$ for all distinct $b, c \in \mathbb{F}_q$.*

(2) *If q is even and $q \geq 8$, then $\langle\langle Y_b \rangle\rangle \cap \langle\langle M \rangle\rangle = F$ for all $b \in \mathbb{F}_q$, and $\langle\langle Y_b \rangle\rangle \cap \langle\langle Y_c \rangle\rangle = F$ for all distinct $b, c \in \mathbb{F}_q$.*

Proof. We will prove part (1); the proof of part (2) is the same. Assume that q is odd. Certainly, $\langle\langle X_b \rangle\rangle \cap \langle\langle M \rangle\rangle$ contains F. Suppose that there exists $A \in \langle\langle X_b \rangle\rangle \cap \langle\langle M \rangle\rangle$ that is not scalar. Now, $\{X_b, I\}$ forms an $\mathbb{F}_q$-basis for $\langle\langle X_b \rangle\rangle$, so $A = a_1 \cdot X_b + a_2 \cdot I$ for some $a_1, a_2 \in \mathbb{F}_q$ with $a_1 \neq 0$. But then, $X_b = a_1^{-1}(A - a_2 \cdot I) \in \langle\langle M \rangle\rangle$, which is impossible by Proposition 3.2. Hence, $\langle\langle X_b \rangle\rangle \cap \langle\langle M \rangle\rangle = F$.

Similarly, we know that $\langle\langle X_b \rangle\rangle \cap \langle\langle X_c \rangle\rangle \supseteq F$ for distinct $b, c \in \mathbb{F}_q$. As above, if there exists a nonscalar matrix $A \in \langle\langle X_b \rangle\rangle \cap \langle\langle X_c \rangle\rangle$, then $X_b \in \langle\langle X_c \rangle\rangle$. But then, X_b, X_c, and I are all in $\langle\langle X_c \rangle\rangle$. By Lemma 3.7, these three matrices are linearly independent over $\mathbb{F}_q$, so $|\langle\langle X_c \rangle\rangle| = q^3$, which contradicts Proposition 3.8. Thus, $\langle\langle X_b \rangle\rangle \cap \langle\langle X_c \rangle\rangle = F$. □

The results above are sufficient to compute $\sigma(T_2(\mathbb{F}_q))$ when q is odd, or q is even and $q \geq 8$. The cases $q = 2$ and $q = 4$ must be dealt with separately. When $q = 4$, we must rule out the possibility that $\sigma(T_2(\mathbb{F}_4))$ equals 3.

Lemma 3.10. $\sigma(T_2(\mathbb{F}_4)) \neq 3$.

Proof. A classification of all rings (with or without unity) with covering number 3 is given in [Lucchini and Maróti 2012, Theorem 1.2]. When applied to a ring R with unity, this classification says that $\sigma(R) = 3$ if and only if R has a residue ring isomorphic to either $\mathbb{F}_2 \times \mathbb{F}_2$ or the ring

$$\left\{ \begin{pmatrix} a & 0 & 0 \\ b & a & 0 \\ c & 0 & a \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{F}_2 \right\}, \tag{3.11}$$

which has order 8. Now, $T_2(\mathbb{F}_4)$ has order 64, and any ideal of $T_2(\mathbb{F}_4)$ is an $\mathbb{F}_4$-vector space, and hence has order equal to a power of 4. So, $T_2(\mathbb{F}_4)$ contains no ideal of order 8, and hence has no residue ring isomorphic to the ring in (3.11). The only ideals of $T_2(\mathbb{F}_4)$ of order 16 are the maximal ideals

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_4 \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \,\middle|\, b, c \in \mathbb{F}_4 \right\}.$$

For each of these, the associated residue ring is isomorphic to $\mathbb{F}_4$. Hence, $T_2(\mathbb{F}_4)$ does not satisfy the conditions of [Lucchini and Maróti 2012, Theorem 1.2], and so $\sigma(T_2(\mathbb{F}_4)) \neq 3$. □

We can now prove Theorem 1.2 and Corollary 1.3, which are restated for convenience.

Theorem 1.2. *Let q be a prime power. Then $\sigma(T_2(\mathbb{F}_q)) = q+1$ when $q \neq 4$, and $\sigma(T_2(\mathbb{F}_4)) = 4$.*

Proof. One may check that a cover of $T_2(\mathbb{F}_2)$ is formed by the three subrings

$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\},$$
$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix}\right\},$$
$$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix}\right\}.$$

Since no ring can be covered by only two subrings, we get $\sigma(T_2(\mathbb{F}_2)) = 3$.

For $q = 4$, note that $\mathcal{I} = \left\{\left(\begin{smallmatrix}0&b\\0&0\end{smallmatrix}\right) \;\middle|\; b \in \mathbb{F}_4\right\}$ is an ideal of $T_2(\mathbb{F}_4)$ and $T_2(\mathbb{F}_4)/\mathcal{I} \cong \mathbb{F}_4 \times \mathbb{F}_4$. By [Werner 2015, Theorem 5.3], $\mathbb{F}_4 \times \mathbb{F}_4$ is coverable and $\sigma(\mathbb{F}_4 \times \mathbb{F}_4) = 4$, so $\sigma(T_2(\mathbb{F}_4)) \leq 4$ by Lemma 2.2. But, $\sigma(T_2(\mathbb{F}_4)) \neq 3$ by Lemma 3.10, so we conclude that $\sigma(T_2(\mathbb{F}_4)) = 4$.

Now, assume that either q is odd, or that q is even and $q \geq 8$. By Propositions 3.2 and 3.8, $T_2(\mathbb{F}_q)$ contains $q+1$ maximal subrings, each generated by a single matrix, and each of order q^2. These subrings are all distinct by Proposition 3.9, so each one must be part of any cover of $T_2(\mathbb{F}_q)$ by Lemma 2.2. Hence, $\sigma(T_2(\mathbb{F}_q)) \geq q+1$. On the other hand, by Proposition 3.9 any pairwise intersection of these subrings is equal to the set of scalar matrices, so the union of all these subrings has cardinality

$$(q+1)(q^2-q)+q = q^3 = |T_2(\mathbb{F}_q)|.$$

Thus, this collection of $q+1$ subrings forms a cover, and hence $\sigma(T_2(\mathbb{F}_q)) = q+1$. □

Corollary 1.3. (1) *Let q be a prime power. If $n \geq 3$, then $\sigma(T_n(\mathbb{F}_q)) \leq q+1$.*

(2) *Let R be a finite ring and let p be the smallest prime dividing the order of R. If R has $\mathbb{F}_p$ as a residue field, then $\sigma(T_n(R)) = p+1$ for all $n \geq 2$. In particular, $\sigma(T_n(\mathbb{F}_p)) = p+1$ for all $n \geq 2$.*

Proof. For (1), let $\mathcal{I}$ be the set of matrices in $T_n(\mathbb{F}_q)$ whose (1, 1), (1, 2), and (2, 2) entries are all 0, and there are no restrictions on the other entries. Then, $\mathcal{I}$ is an ideal of $T_n(\mathbb{F}_q)$ and $T_n(\mathbb{F}_q)/\mathcal{I} \cong T_2(\mathbb{F}_q)$. So, $\sigma(T_n(\mathbb{F}_q)) \leq \sigma(T_2(\mathbb{F}_q)) \leq q+1$ by Lemma 2.2 and Theorem 1.2.

For (2), note that when $n \geq 2$, $T_n(R)$ is coverable because it is noncommutative. So, $\sigma(T_n(R)) \geq p+1$ by Lemma 2.3. Let J be an ideal of R such that $R/J \cong \mathbb{F}_p$. Let $\mathcal{J}$ be the set of matrices in $T_n(R)$ whose (1, 1), (1, 2), and (2, 2) entries come from J and there are no restriction on the other entries. Then, $\mathcal{J}$ is an ideal of $T_n(R)$ and $T_n(R)/\mathcal{J} \cong T_2(\mathbb{F}_p)$. By Lemma 2.2, $\sigma(T_n(R)) \leq \sigma(T_2(\mathbb{F}_p))$, and so $\sigma(T_n(R)) = p+1$ by Theorem 1.2. □

We suspect that equality holds in part (1) of Corollary 1.3 (except when $q = 4$), and a few words are in order about our inability to prove this. The main obstruction to generalizing Theorem 1.2 for $n \geq 3$ is that the maximal subrings we desire to use are not generated by a single matrix. For instance, in the 3×3 case,

$$\left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & e \end{pmatrix} \,\middle|\, a, b, c, d, e \in \mathbb{F}_q \right\}$$

(which generalizes $\langle\langle M \rangle\rangle$) is a maximal subring of $T_3(\mathbb{F}_q)$, but it is not commutative, and hence is not generated by a single matrix. Consequently, we cannot conclude that such a subring must be part of every cover of $T_3(\mathbb{F}_q)$.

It should be possible to compute $\sigma(T_n(\mathbb{F}_q))$ given the complete classification of maximal subrings of $T_n(\mathbb{F}_q)$. Unfortunately, such a classification is not known. Even in the case of 2×2 matrices, identifying all maximal subrings appears to be nontrivial. In this paper, we made use of the maximal subrings $\langle\langle M \rangle\rangle$, $\langle\langle X_b \rangle\rangle$, and $\langle\langle Y_b \rangle\rangle$, but other maximal subrings of $T_2(\mathbb{F}_q)$ exist. For instance, let R be a maximal subring of $\mathbb{F}_q$. Then, the subrings

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a \in R \text{ and } b, c \in \mathbb{F}_q \right\} \quad \text{and} \quad \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_q \text{ and } c \in R \right\}$$

are both maximal in $T_2(\mathbb{F}_q)$. Similar examples exist in $T_n(\mathbb{F}_q)$ when $n \geq 3$. Given these considerations, we propose the classification of maximal subrings of $T_n(\mathbb{F}_q)$ and the associated calculation of covering numbers as problems for further research.

References

[Bruckheimer et al. 1970] M. Bruckheimer, A. C. Bryan, and A. Muir, "Groups which are the union of three subgroups", *Amer. Math. Monthly* **77** (1970), 52–57. MR Zbl

[Cohn 1994] J. H. E. Cohn, "On n-sum groups", *Math. Scand.* **75**:1 (1994), 44–58. MR Zbl

[Crestani 2012] E. Crestani, "Sets of elements that pairwise generate a matrix ring", *Comm. Algebra* **40**:4 (2012), 1570–1575. MR Zbl

[Haber and Rosenfeld 1959] S. Haber and A. Rosenfeld, "Groups as unions of proper subgroups", *Amer. Math. Monthly* **66** (1959), 491–494. MR Zbl

[Kappe 2014] L.-C. Kappe, "Finite coverings: a journey through groups, loops, rings and semigroups", pp. 79–88 in *Group theory, combinatorics, and computing* (Boca Raton, FL, 2012), edited by R. F. Morse et al., Contemp. Math. **611**, Amer. Math. Soc., Providence, RI, 2014. MR Zbl

[Lucchini and Maróti 2010] A. Lucchini and A. Maróti, "Rings as the unions of proper subrings", preprint, 2010. arXiv

[Lucchini and Maróti 2012] A. Lucchini and A. Maróti, "Rings as the unions of proper subrings", *Algebr. Represent. Theory* **15**:6 (2012), 1035–1047. MR Zbl

[Scorza 1926] G. Scorza, "I gruppi che possono pensarsi come somma di tre loro sottogruppi", *Boll. Un. Mat. Ital.* **5** (1926), 216–218. Zbl

[Tomkinson 1997] M. J. Tomkinson, "Groups as the union of proper subgroups", *Math. Scand.* **81**:2 (1997), 191–198. MR Zbl

[Werner 2015] N. J. Werner, "Covering numbers of finite rings", *Amer. Math. Monthly* **122**:6 (2015), 552–566. MR Zbl

Received: 2018-09-16 Revised: 2018-11-18 Accepted: 2019-03-05

merrickcai@gmail.com *Kings Park High School, Kings Park, NY, United States*

wernern@oldwestbury.edu *Department of Mathematics, Computer and Information Science, SUNY College at Old Westbury, Old Westbury, NY, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2019 is US $195/year for the electronic version, and $260/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2019 vol. 12 no. 6

1944-4176(2019)12:6;1-#