Comm. Algebra, 46 (2018), no. 11, 4724-4738, https://doi.org/10.1080/00927872.2018.1455099

# Maximal Subrings and Covering Numbers of Finite Semisimple Rings

G. Peruginelli*
N. J. Werner†

September 25, 2018

**Abstract**

We classify the maximal subrings of the ring of $n \times n$ matrices over a finite field, and show that these subrings may be divided into three types. We also describe all of the maximal subrings of a finite semisimple ring, and categorize them into two classes. As an application of these results, we calculate the covering number of a finite semisimple ring.

Keywords: Maximal subring, matrix ring, semisimple ring, finite field, covering number

MSC Primary 16P10, Secondary 05E15

## 1 Introduction

When dealing with an algebraic structure, a standard goal is to understand its substructures. In this, special attention is often paid to those substructures that are maximal with respect to inclusion, such as maximal subgroups or maximal ideals. There are many papers in the literature studying maximal subalgebras of an algebra $\mathscr{A}$ over a field $F$ (see e.g. [9, 10, 11, 21, 22, 23] and the references therein), and for commutative rings the related notion of minimal ring extensions has become popular (for this, the papers [6, 7, 8] are a good starting point). However, less work has been done on classifying the maximal subrings of a general algebra $\mathscr{A}$. This problem is nontrivial, because there usually exist maximal subrings of $\mathscr{A}$ that are not $F$-subalgebras. An easy example of this is given by taking $\mathscr{A} = F$ and considering a minimal field extension $F/F_0$. In this case, $F_0$ is a maximal subring of $F$ but is not an $F$-algebra, and hence would fall outside any classification of maximal $F$-subalgebras.

The aim of the current paper is to classify all of the maximal subrings of an $n \times n$ matrix ring $M_n(\mathbb{F}_q)$ with entries from a finite field $\mathbb{F}_q$ with $q$ elements. We will also describe the maximal subrings of a finite semisimple ring (i.e. a direct product of the form $\prod_{i=1}^{t} M_{n_i}(\mathbb{F}_{q_i})$). Here and elsewhere, when we speak

*Department of Mathematics, University of Padova, Via Trieste, 63 35121 Padova, Italy. E-mail: gperugin@math.unipd.it

†Department of Mathematics, Computer and Information Science, SUNY College at Old Westbury, Old Westbury, NY 11568, United States. E-mail: wernern@oldwestbury.edu

of subrings, we mean a subset of a ring that is an Abelian group under addition and is closed under multiplication; we do not require subrings to contain a multiplicative identity. As it turns out, however, the maximal subrings of a unital ring $R$ often contain $1_R$ (see Lemma 2.1), so the omission of unity from the definition of a subring will not be a hindrance to our work.

The paper begins in Section 2 with some results on maximal subrings of a finite dimensional central simple algebra $\mathscr{A}$ over a field $F$. This allows us to build on the work of Racine [21, 22], who classified maximal $F$-subalgebras in various types of $F$-algebras, among them matrix algebras and central simple algebras. As we demonstrate in Proposition 2.4 and Theorem 3.3, as long as $\mathbb{F}_q \neq \mathbb{F}_p$ it is easy to produce maximal subrings of $M_n(\mathbb{F}_q)$ that are not $\mathbb{F}_q$-subalgebras. Thus, our work is more than just a corollary of Racine's theorems.

In Section 3, we begin to restrict our attention to $M_n(\mathbb{F}_q)$ and we prove that the maximal subrings of $M_n(\mathbb{F}_q)$ can be classified into three types (Theorem 3.3), which we call Types I, II, and III (Definition 3.1). We then provide precise counts for the number of maximal subrings of each type (Propositions 3.4, 3.7, 3.8). In Section 4, we work with finite semisimple rings and we prove (Theorem 4.5) that the maximal subrings of such a ring fall into two distinct classes, which we call Types $\Pi_1$ and $\Pi_2$ (Definition 4.3).

In the last section, we apply our results to determine the covering numbers of finite semisimple rings. A *cover* of a (unital, associative) ring $R$ is a collection of proper subrings $S_i \subseteq R$ such that $R = \bigcup_i S_i$. If such a union is possible, then we say that $R$ is *coverable* and the *covering number* of $R$, denoted by $\sigma(R)$, is the size of a minimal cover, i.e. the least number of subrings necessary to form a cover. A minimal cover (if it exists) can always be formed out of maximal subrings, so knowing the maximal subrings of $R$ is quite useful in determining $\sigma(R)$.

The analogous problem of covering numbers for groups has been well-studied and covering numbers are known for several types of groups, among them all solvable groups [26], various linear groups [1, 2, 3], assorted symmetric and alternating groups [4, 14, 19, 25], and some sporadic simple groups [12]. Less attention has been paid to covering numbers for rings. All rings with covering number three were determined in [18], [27] gives formulas for covering numbers of direct products of finite fields, and a formula for $\sigma(M_n(\mathbb{F}_q))$ was determined in [17] and [5] (see Theorem 5.2 of the present paper). The survey paper [13] gives an overview of theorems related to coverings for various algebraic structures, including groups and rings. Our contribution to this topic is to prove (Theorem 5.11) that if $R = \prod_{i=1}^{t} M_n(\mathbb{F}_q)$ and $n \geq 2$, then $\sigma(R) = \sigma(M_n(\mathbb{F}_q))$. When combined with some of the other theorems in Section 5, this result allows one to find the covering number for any finite semisimple ring.

## 2 Some Maximal Subrings of Central Simple Algebras

Throughout this section, $\mathscr{A}$ denotes a finite dimensional central simple algebra over a field $F$. We are interested in describing the maximal subrings of $\mathscr{A}$. To be consistent with the terminology used in [27], we use *subring* in the weakest sense: a subring $S$ of a unital ring $R$ is a subset of $R$ that is an Abelian group under addition and that is closed under multiplication. Thus, a priori we make no assumption that $S$ contains $1_R$, or that $S$ contains any multiplicative identity. In practice, however, we will be focusing on maximal subrings of $\mathscr{A}$, and our first results show that—except for the situation where $\mathscr{A} = \mathbb{F}_p$ for some prime $p$—any maximal subring of $\mathscr{A}$ contains $1_{\mathscr{A}}$.

**Lemma 2.1.** *Let $R$ be a ring with unity. Let $M$ be a maximal subring of $R$. Then, either*

*(1) $1_R \in M$, or*

*(2) $M$ is a maximal two-sided ideal of $R$ and $R/M \cong \mathbb{F}_p$ for some prime $p$.*

*Proof.* If $1_R \in M$ then we are done, so assume that $1_R \notin M$. Let $D$ be the subring of $R$ generated by $1_R$ and let $S = D + M$. Note that either $D \cong \mathbb{Z}$ if $R$ has characteristic 0, or $D \cong \mathbb{Z}/n\mathbb{Z}$ if $R$ has positive characteristic $n$.

Observe that $dm \in M$ for all $d \in D$ and all $m \in M$; it follows that a product of elements of $S$ remains in $S$. Since $S$ is also clearly closed under addition, we see that $S$ is a subring of $R$. But, $M \subsetneqq S$, and $M$ is a maximal subring of $R$, so in fact $S = R$. Finally, the fact that $dm \in M$ for all $d \in D$ and all $m \in M$ also implies that $M$ is a two-sided ideal of $R$. By the maximality of $M$, we conclude that $M$ is a maximal ideal of $R$.

It remains to show that $R/M \cong \mathbb{F}_p$ for some $p$. Since $M$ is a maximal two-sided ideal of $R$, the residue ring $R/M$ is a simple ring. Furthermore, since $R = D + M$, we have $R/M = (D + M)/M \cong D/D \cap M$. But, as noted above, $D$ is a residue ring of $\mathbb{Z}$, so the only possible simple residue rings of $D$ are the finite fields $\mathbb{F}_p$. Thus, $R/M \cong \mathbb{F}_p$ for some $p$. □

**Corollary 2.2.** *Let $R$ be a ring with unity. If $R$ has no residue ring isomorphic to a finite prime field $\mathbb{F}_p$, then every maximal subring of $R$ contains $1_R$. In particular, if $R$ is a simple ring and $R \neq \mathbb{F}_p$ for all primes $p$, then every maximal subring of $R$ contains $1_R$.*

We return now to the situation of a central simple algebra $\mathscr{A}$ with center $F$. In [21], Racine proved that maximal $F$-subalgebras of $\mathscr{A}$ fall into two types (Racine later gave an analogous classification of maximal subalgebras of central separable algebras over a commutative ring $R$ in [22]). Note that if $R$ is an $F$-subalgebra of $\mathscr{A}$ containing $1_{\mathscr{A}}$, $S$ is a subring of $\mathscr{A}$, and $R \subseteq S$, then $F \subseteq S$, so that $S$ is also an $F$-subalgebra. Thus, any maximal subalgebra of $\mathscr{A}$ is also a maximal subring of $\mathscr{A}$, although the converse does not hold, as we shall see below in Proposition 2.4.

**Theorem 2.3.** *([21, Thm. 1]) Assume that $\mathscr{A} \cong M_n(\mathscr{D})$, where $\mathscr{D}$ is a division algebra with center $F$. Let $V$ be an $n$-dimensional right $\mathscr{D}$-vector space, so that $\mathscr{A} \cong \mathrm{End}_{\mathscr{D}}(V)$. Let $M$ be a maximal $F$-subalgebra of $\mathscr{A}$. Then, $M$ has one of the following two forms.*

*(I) $M$ is the stabilizer of a proper nonzero subspace of $V$. That is, $M = \mathscr{S}(W) = \{A \in \mathscr{A} \mid WA \subseteq W\}$, where $W$ is a proper nonzero subspace of $V$.*

*(II) $M$ is the centralizer of a minimal field extension of $F$ in $\mathscr{A}$. That is, $M = \mathscr{C}(K) = \{A \in \mathscr{A} \mid Au = uA \text{ for all } u \in K\}$, where $F \subseteq K \subseteq \mathscr{A}$ and $K/F$ is a minimal field extension.*

If we relax our requirements and allow $M$ to be a maximal subring of $\mathscr{A}$ rather than a maximal subalgebra, there are choices for $M$ that do not fit into Racine's classification. For instance, if $F/F_0$ is a minimal field extension, then $F_0$ is a maximal subring of $F$, but is not an $F$-algebra. Similar examples are possible with matrix rings and central simple algebras. In what follows, for any unital ring $R$ and for $1 \leq i, j \leq n$, we let $E_{ij} \in M_n(R)$ denote the standard matrix unit with 1 in the $(i, j)$-entry and 0 elsewhere. Also, we associate $R$ with the scalar matrices in $M_n(R)$, so that $1_R$ is the $n \times n$ identity matrix and we can write $R \subseteq M_n(R)$. Finally, for a nonzero subring $R$ of $\mathscr{A}$, the notation $F \cdot R$ denotes the extension of $R$ to an $F$-algebra, i.e. the subring of $\mathscr{A}$ generated by $F$ and $R$. Elements of $F \cdot R$ are finite sums $\sum_i u_i r_i$ where $u_i \in F$ and $r_i \in R$.

**Proposition 2.4.** *Assume that $F \neq \mathbb{F}_p$ and let $M$ be a maximal subring of $F$. Then, $M_n(M)$ is a maximal subring of $M_n(F)$ but is not an $F$-subalgebra of $M_n(F)$.*

*Proof.* Let $S$ be a subring of $M_n(F)$ properly containing $M_n(M)$ and let $A \in S \setminus M_n(M)$. Then, $A$ contains an entry $a$ such that $a \in F \setminus M$. Since $M$ is maximal in $F$, $a$ must be a generator of $F$ over $M$; that is, $F = M[a]$.

Now, $M_n(M)$ contains all of the matrix units $\{E_{ij}\}_{1 \leq i,j \leq n}$ of $M_n(F)$. Assume that $a$ occurs as the $(i, j)$-entry of $A$. Then, for each $1 \leq k \leq n$, we have $E_{ki} A E_{jk} = aE_{kk} \in S$. Hence, the scalar matrix $aI = \sum_k aE_{kk} \in S$. Thus, $S$ contains the matrix units and all of the scalar matrices in $M_n(F)$. Consequently, $S = M_n(F)$ and $M_n(M)$ is maximal. Finally, $F \not\subseteq M_n(M)$, so $M_n(M)$ is not an $F$-subalgebra. □

We suspect that a maximal subring of $M_n(F)$ that is not an $F$-algebra is (up to conjugacy by an invertible matrix in $GL(n, F)$) equal to $M_n(M)$ for some maximal subring $M$ of $F$. This is trivially true when $n = 1$, and we are able to prove it when $n \geq 2$ and $R$ is Artinian, and so in particular it is true when $F = \mathbb{F}_q$.

**Lemma 2.5.** *Let $R$ be a subring of $\mathscr{A}$.*

*(1) If $R$ is nonzero, maximal, and is not an $F$-algebra, then $F \cdot R = \mathscr{A}$.*

*(2) If $F \cdot R = \mathscr{A}$, then $Z(R) = R \cap F$.*

*(3) Let $I$ be a two-sided ideal of $R$. Then, $F \cdot I$ is a two-sided ideal of $F \cdot R$.*

*Proof.* (1) If $R$ is nonzero, maximal, and not an $F$-algebra, then $R \subsetneqq F \cdot R$, which means that $F \cdot R = \mathscr{A}$.

(2) Clearly, $R \cap F \subseteq Z(R)$. Conversely, let $c \in Z(R)$. Then $c$ commutes with both $R$ and $F$, and hence commutes with all elements of $F \cdot R = \mathscr{A}$. Thus, $c \in Z(\mathscr{A}) = F$.

(3) This is a straightforward calculation, noting that $F \cdot I = \{\sum_i u_i x_i \mid u_i \in F, x_i \in I\}$ and $F \cdot R = \{\sum_i u_i r_i \mid u_i \in F, r_i \in R\}$. □

Recall that a ring $R$ is called *decomposable* if there exist nonzero subrings $R_1$ and $R_2$ of $R$ such that $R = R_1 \oplus R_2$. The ring $R$ is *indecomposable* if no such subrings exist.

**Lemma 2.6.** *Let $R$ be a subring of $\mathscr{A}$ such that $F \cdot R = \mathscr{A}$. Then, $R$ is indecomposable.*

*Proof.* Since $F \neq \{0\}$ and $F \cdot R = \mathscr{A}$, we know that $R \neq \{0\}$. Assume first that $\mathscr{A}$ is a field. Since a decomposable ring always contains zero divisors, no subring of a field is decomposable. Hence, $R$ is indecomposable when $\mathscr{A}$ is a field.

For the remainder of the proof, assume that $\mathscr{A}$ is not a field. Let $R_1$ and $R_2$ be subrings of $R$ such that $R = R_1 \oplus R_2$ and $R_1 \neq \{0\}$. We will show that $R_2 = \{0\}$. Let $I_1 = R_1 \oplus \{0\}$ and $I_2 = \{0\} \oplus R_2$, which are both two-sided ideals of $R$. By Lemma 2.5 part (3), both $F \cdot I_1$ and $F \cdot I_2$ are two-sided ideals of $F \cdot R$. But, $F \cdot R = \mathscr{A}$ and $\mathscr{A}$ is simple, so each extended ideal is either $\{0\}$ or $\mathscr{A}$. Since $I_1 \neq \{0\}$, we have $F \cdot I_1 = F \cdot R_1 = \mathscr{A}$. If $F \cdot I_2 = \{0\}$, then $R_2 = I_2 = \{0\}$ and we are done. So, assume that $F \cdot I_2 = \mathscr{A}$.

Now, each element of $R_1$ commutes with each element of $R_2$, so in fact each element of $R_1$ commutes with each element of $F \cdot I_2 = \mathscr{A}$; hence, $R_1 \subseteq Z(\mathscr{A}) = F$. But, this means that $\mathscr{A} = F \cdot R_1 = F$ is a field, contrary to our assumption above. We conclude that $F \cdot I_2 \neq \mathscr{A}$ and that $R$ is indecomposable. □

With the additional assumption that $R$ is Artinian, we can use these two lemmas to prove that if $F \cdot R = \mathscr{A}$, then $R$ is isomorphic to a matrix ring with entries in a field. A key step in the process is to prove that $R$ must be semisimple. Recall that $R$ is semisimple if and only if the Jacobson radical of $R$ is $\{0\}$ and $R$ is Artinian; this is where the Artinian condition arises. Indeed, if $R$ is not Artinian, then it is possible that $F \cdot R = \mathscr{A}$ but $R$ is not semisimple. This occurs, for instance, if we take $\mathscr{A} = \mathbb{Q}$ and $R = \mathbb{Z}$ (or $R = \mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$).

**Theorem 2.7.** *Let $R$ be a subring of $\mathscr{A}$ such that $1_{\mathscr{A}} \in R$, $F \cdot R = \mathscr{A}$, and $R$ is Artinian. Then, $\mathscr{A} \cong M_n(F)$ for some $n$ and $R \cong M_n(F_0)$, where $F_0 = R \cap F$ is a subfield of $F$.*

*Proof.* Since $R$ is Artinian, the Jacobson radical $J$ of $R$ is a nilpotent ideal [15, Thm. 4.12]. Hence, there exists $m > 0$ such that $J^m = \{0\}$. Consider the extended ideal $F \cdot J$ of $\mathscr{A}$. Given $a = \sum_i u_i x_i \in F \cdot J$, we have $a^m = 0$, because each summand of $a^m$ involves a product of $m$ of the $x_i$, which is in $J^m$. Thus, $F \cdot J$ is nilpotent. Since $\mathscr{A}$ is simple, either $F \cdot J = \mathscr{A}$ or $F \cdot J = \{0\}$, and we must have $F \cdot J = \{0\}$ because $F \cdot J$ is nilpotent. Consequently, $J = \{0\}$ and we conclude that $R$ is semisimple [15, Thm. 4.14].

Now, by Lemma 2.6, $R$ is indecomposable. Since $R$ is also semisimple, we see that $R$ is actually a simple ring. Thus, by the Artin-Wedderburn Theorem [15, Thm. 3.10], $R \cong M_n(\mathscr{D})$ for some $n$ and some division ring $\mathscr{D}$. Since $F \cdot R = \mathscr{A}$, we see that $\mathscr{A} \cong M_n(F \cdot \mathscr{D})$, and since $F$ is the center of $\mathscr{A}$, we have $F \cdot \mathscr{D} = F$. This means that $\mathscr{D}$ is a subfield $F_0$ of $F$. So, $R \cong M_n(F_0)$. Finally, $F_0$ is the center of $R$ and equals $R \cap F$ by Lemma 2.5 part (2). □

**Theorem 2.8.** *Let $F$ be a field, let $S$ be a subring of $F$ containing $1_F$, and let $R$ be a subring of $M_n(F)$ such that $R \cong M_n(S)$. Then, $R$ is a $GL(n, F)$-conjugate of $M_n(S)$.*

*Proof.* Let $\{E_{ij}\}_{1 \leq i,j \leq n}$ be the standard matrix units of $M_n(F)$. Since $R \cong M_n(S)$, by [16, Thm. 17.5] the ring $R$ contains a full system of matrix units $\{r_{ij}\}_{1 \leq i,j \leq n}$. So, $r_{11} + r_{22} + \cdots + r_{nn} = I_n$, the $n \times n$ identity matrix, and $r_{ij} r_{k\ell} = \delta_{jk} r_{i\ell}$ for all $i, j, k$, and $\ell$, where $\delta_{jk}$ is the Kronecker delta.

Now, each $r_{ii}$ is an idempotent, and hence is a diagonalizable matrix (because the minimal polynomial of $r_{ii}$ is $x^2 - x$, which has no repeated roots). Moreover, since the $r_{ii}$ are mutually orthogonal, they all commute with one another. Hence, $r_{11}, r_{22}, \ldots r_{nn}$ are simultaneously diagonalizable. Thus, up to conjugation by elements of $GL(n, F)$, we may assume that $r_{ii} = E_{ii}$ for each $1 \leq i \leq n$.

Next, for all $1 \leq i, j \leq n$, let $f_{ij}$ denote the $(i, j)$-entry of $r_{ij}$. Then, for all $i$ and $j$,

$$r_{ij} = r_{ii} r_{ij} r_{jj} = E_{ii} r_{ij} E_{jj} = f_{ij} E_{ij} \tag{2.9}$$

and $f_{ij} \neq 0$ because $r_{ij} \neq 0$. Using (2.9), we get, for all $i$, $j$, and $k$,

$$f_{ik} E_{ik} = r_{ik} = r_{ij} r_{jk} = f_{ij} E_{ij} f_{jk} E_{jk} = f_{ij} f_{jk} E_{ij} E_{jk} = f_{ij} f_{jk} E_{ik}$$

from which we conclude that

$$f_{ik} = f_{ij} f_{jk}. \tag{2.10}$$

Let $U$ be the diagonal matrix $U = \sum_{k=1}^{n} f_{1k} E_{kk}$. Note that $U \in GL(n, F)$ with inverse $U^{-1} = \sum_{k=1}^{n} f_{1k}^{-1} E_{kk}$. Then, for $i$ and $j$,

$$\begin{aligned} U r_{ij} U^{-1} &= \Big( \sum_{k=1}^{n} f_{1k} E_{kk} \Big) r_{ij} \Big( \sum_{k=1}^{n} f_{1k}^{-1} E_{kk} \Big) \\ &= \Big( \sum_{k=1}^{n} f_{1k} E_{kk} \Big) f_{ij} E_{ij} \Big( \sum_{k=1}^{n} f_{1k}^{-1} E_{kk} \Big) \text{ by (2.9)} \\ &= f_{1i} E_{ii} (f_{ij} E_{ij}) f_{1j}^{-1} E_{jj} \\ &= f_{1i} f_{ij} f_{1j}^{-1} E_{ij} \\ &= f_{1j} f_{1j}^{-1} E_{ij} \text{ by (2.10)} \\ &= E_{ij}. \end{aligned}$$

Hence, via conjugation by elements of $GL(n, F)$, the matrix units of $R$ can be transformed into the standard matrix units of $M_n(F)$. Since the $E_{ij}$ are also the matrix units for $M_n(S)$, this means that $R$ is conjugate to $M_n(S)$, as desired. □

Combining Theorems 2.7 and 2.8 gives us a stronger version of the former theorem.

**Corollary 2.11.**

*(1) Let $R$ be a subring of $\mathscr{A}$ such that $1_{\mathscr{A}} \in R$, $F \cdot R = \mathscr{A}$, and $R$ is Artinian. Then, $\mathscr{A} \cong M_n(F)$ for some $n$ and $R$ is a $GL(n, F)$-conjugate of $M_n(F_0)$, where $F_0 = R \cap F$ is a subfield of $F$.*

*(2) Let $R$ be a nonzero maximal subring of $\mathscr{A}$ that is not an $F$-algebra. If $R$ is Artinian, then $R$ is a $GL(n, F)$-conjugate of $M_n(F_0)$, where $F_0 = R \cap F$ is a maximal subfield of $F$.*

*Proof.* (1) is clear from Theorems 2.7 and 2.8. For (2), assume that $R$ is nonzero and maximal, but is not an $F$-algebra. Since $R \neq \{0\}$, we cannot have $\mathscr{A} = \mathbb{F}_p$ (because $\{0\}$ is the only maximal subring of $\mathbb{F}_p$). So, $1_{\mathscr{A}} \in R$ by Corollary 2.2, and $F \cdot R = \mathscr{A}$ by Lemma 2.5. Next, by (1) $R$ is a conjugate of $M_n(F_0)$, where $F_0 = R \cap F$ is a subfield of $F$. It remains to show that $F_0$ is maximal in $F$. If $S$ is a subring of $F$ such that $F_0 \subsetneqq S \subseteq F$, then $R$ is properly contained in a conjugate of $M_n(S)$. By the maximality of $R$, we have $M_n(S) = M_n(F)$, and hence $S = F$. □

# 3 Maximal Subrings of $M_n(\mathbb{F}_q)$

We now specialize to the case of the ring $M_n(\mathbb{F}_q)$ of matrices with entries in the finite field $\mathbb{F}_q$, and with $n \geq 2$. These matrix rings—and later, direct products of them—will remain our focus for the remainder of the paper. Throughout, we assume that $q$ is a power of a prime $p$. We associate $\mathbb{F}_q$ with the $n \times n$ scalar matrices, so that $\mathbb{F}_q \subseteq M_n(\mathbb{F}_q)$. The group of invertible matrices in $M_n(\mathbb{F}_q)$ will be denoted by $GL(n, q)$.

Our goal in this section is to classify the maximal subrings of $M_n(\mathbb{F}_q)$, of which there are three types. We will give formulas for the exact number of maximal subrings of each type and discuss when two subrings of the same type are conjugate.

**Definition 3.1.** Let $M$ be a maximal subring of $M_n(\mathbb{F}_q)$.

- We say that $M$ is *Type I-$k$* if $M$ is the stabilizer of a proper nonzero subspace of $\mathbb{F}_q^n$ of dimension $k$. That is, $M = \mathscr{S}(W) = \{A \in M_n(\mathbb{F}_q) \mid AW \subseteq W\}$, where $W$ is a proper nonzero $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with $\dim W = k$. If we do not wish to specify $k$, then we will say $M$ is simply of Type I.
- We say that $M$ is *Type II-$\ell$* if $M$ is the centralizer of a minimal degree $\ell$ field extension of $\mathbb{F}_q$ in $M_n(\mathbb{F}_q)$. That is, $M = \mathscr{C}_{M_n(\mathbb{F}_q)}(K) = \{A \in M_n(\mathbb{F}_q) \mid Au = uA, \text{ for all } u \in K\}$, where $K \subseteq M_n(\mathbb{F}_q)$, $K \cong \mathbb{F}_{q^\ell}$, and $\ell \in \mathbb{Z}$ is a prime dividing $n$. If we do not wish to specify $\ell$, then we will say $M$ is simply of Type II.
- We say that $M$ is *Type III-$r$* if $M$ is a $GL(n, q)$-conjugate of $M_n(\mathbb{F}_r)$, where $\mathbb{F}_r$ is a (nonzero) maximal subfield of $\mathbb{F}_q$. If there is no need to specify $r$, then we will say $M$ is of Type III.

**Notation 3.2.** Here and elsewhere, we use $\mathscr{S}(W)$ to denote the stabilizer of a subspace $W$ of $\mathbb{F}_q^n$, and we use $\mathscr{C}$ to denote centralizers of matrices or sets of matrices.

**Theorem 3.3.** *Let $M$ be a maximal subring of $M_n(\mathbb{F}_q)$.*

*(1) If $q = p$, then $M$ is Type I or Type II.*

*(2) If $q \neq p$, then $M$ is Type I, Type II, or Type III.*

*Proof.* If $M$ is an $\mathbb{F}_q$-subalgebra of $M_n(\mathbb{F}_q)$, then $M$ is either Type I or Type II by Racine's classification [21, 22] (summarized previously in Theorem 2.3), and if $q = p$ then these are the only possibilities. So, assume that $q \neq p$. Then, we know that there exist maximal subrings of $M_n(\mathbb{F}_q)$ that are not $\mathbb{F}_q$-algebras (Proposition 2.4). Assume $M$ is such a subring. Then, $\mathbb{F}_q \cdot M$ properly contains $M$, and since $M$ is maximal we must have $\mathbb{F}_q \cdot M = M_n(\mathbb{F}_q)$. Since $M$ is finite (hence Artinian), by Corollary 2.11 we know that $M$ is a $GL(n, q)$-conjugate of $M_n(\mathbb{F}_r)$, where $\mathbb{F}_r = M \cap \mathbb{F}_q$ is a maximal subfield of $\mathbb{F}_q$. □

We now investigate some of the properties of the three classes of maximal subrings of $M_n(\mathbb{F}_q)$, including counting how many of each type occur in the matrix ring.

It is clear that Type I maximal subrings are in one-to-one correspondence with the nonzero proper subspaces of $\mathbb{F}_q^n$. The number of such subspaces can be counted by using the *$q$-binomial coefficients* (also called *Gaussian binomial coefficients*) $\binom{n}{k}_q$, which for $0 \leq k \leq n$ are defined by

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-(k-1)} - 1)}{(q - 1)(q^2 - 1) \cdots (q^k - 1)}.$$

**Proposition 3.4.**

*(1) The number of Type I-$k$ maximal subrings of $M_n(\mathbb{F}_q)$ is $\binom{n}{k}_q$.*

*(2) Let $k \in \{1, \ldots, n\}$. Then any two Type I-$k$ maximal subrings are $GL(n, q)$-conjugate.*

*Proof.* (1) follows from the well known fact that $\binom{n}{k}_q$ equals the number of $k$-dimensional subspaces of $\mathbb{F}_q^n$. For (2), let $W_1$ and $W_2$ be $k$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$. Then, there exists $U \in GL(n,q)$ such that $UW_1 = W_2$, and it is easy to verify that $\mathscr{S}(W_2) = U\mathscr{S}(W_1)U^{-1}$. □

Next, we consider Type II maximal subrings. Note first that any such ring can be realized as the centralizer of a matrix $A \in M_n(\mathbb{F}_q)$ with irreducible minimal polynomial of degree $\ell$, where $\ell$ is a prime dividing $n$. For such $\ell$, if $K$ is a minimal field extension of $\mathbb{F}_q$ of degree $\ell$ contained in $M_n(\mathbb{F}_q)$, then let $A \in K$ be a matrix with irreducible minimal polynomial of degree $\ell$. Then, $K = \mathbb{F}_q[A]$, so that $\mathscr{C}_{M_n(\mathbb{F}_q)}(K) = \mathscr{C}_{M_n(\mathbb{F}_q)}(A)$.

As we show below in Lemma 3.6 part (1), any Type II maximal subring in $M_n(\mathbb{F}_q)$ is isomorphic to $M_{n/\ell}(\mathbb{F}_{q^\ell})$ for some prime divisor $\ell$ of $n$. The difficulty here is that while $M_n(\mathbb{F}_q)$ always contains subrings isomorphic to $M_{n/\ell}(\mathbb{F}_{q^\ell})$ (see [20, Thm. VIII.10]), there is no unique or canonical copy of $M_{n/\ell}(\mathbb{F}_{q^\ell})$ within $M_n(\mathbb{F}_q)$. To get around this obstacle, we describe one way to produce a Type II maximal subring by starting only with an irreducible polynomial of degree $\ell$ in $\mathbb{F}_q[x]$.

**Definition 3.5.** Let $\ell$ be a prime divisor of $n$ and let $\mu \in \mathbb{F}_q[x]$ be irreducible of degree $\ell$. We define the Type II maximal subring of $M_n(\mathbb{F}_q)$ associated to $\mu$, denoted by $T_\mu$, as follows. Let $C \in M_\ell(\mathbb{F}_q)$ be the companion matrix for $\mu$ and let

$$A_\mu = \begin{pmatrix} C & & & \\ & C & & \\ & & \ddots & \\ & & & C \end{pmatrix}$$

be the block diagonal matrix in $M_n(\mathbb{F}_q)$ where each diagonal block is equal to $C$. Then, $\mathbb{F}_q[A_\mu] \cong \mathbb{F}_{q^\ell}$ is a minimal field extension of $\mathbb{F}_q$ in $M_n(\mathbb{F}_q)$. We define $T_\mu = \mathscr{C}_{M_n(\mathbb{F}_q)}(\mathbb{F}_q[A_\mu]) = \mathscr{C}_{M_n(\mathbb{F}_q)}(A_\mu)$.

**Lemma 3.6.** *Let $\ell$ be a prime divisor of $n$ and let $\mu \in \mathbb{F}_q[x]$ be irreducible of degree $\ell$. Then,*

*(1) $T_\mu \cong M_{n/\ell}(\mathbb{F}_{q^\ell})$.*

*(2) Let $F$ be a subfield of $M_n(\mathbb{F}_q)$ such that $F \cong \mathbb{F}_{q^\ell}$. Then, $\mathscr{C}_{M_n(\mathbb{F}_q)}(F)$ is a $GL(n,q)$-conjugate of $T_\mu$.*

*(3) Let $M$ be a Type II-$\ell$ maximal subring of $M_n(\mathbb{F}_q)$. Then, $M = \mathscr{C}_{M_n(\mathbb{F}_q)}(A)$ for some $A \in M_n(\mathbb{F}_q)$ which is a $GL(n,q)$-conjugate of $A_\mu$.*

*Thus, any Type II-$\ell$ maximal subring of $M_n(\mathbb{F}_q)$ is isomorphic to $M_{n/\ell}(\mathbb{F}_{q^\ell})$ and is $GL(n,q)$-conjugate to $T_\mu$.*

*Proof.* (1) Since $T_\mu$ is the centralizer of $\mathbb{F}_q[A_\mu] \cong \mathbb{F}_{q^\ell}$, we get $T_\mu \cong M_{n/\ell}(\mathbb{F}_{q^\ell})$ by [20, Thm. VIII.10].

(2) Since $F \cong \mathbb{F}_{q^\ell}$, there exists $A \in F$ such that the minimal polynomial of $A$ over $\mathbb{F}_q$ is equal to $\mu$, and the characteristic polynomial of $A$ (as a matrix in $M_n(\mathbb{F}_q)$) is equal to $\mu^{n/\ell}$. Then, the rational canonical form of $A$ is equal to the matrix $A_\mu$ from Definition 3.5, so there exists $U \in GL(n,q)$ such that $A = UA_\mu U^{-1}$. Hence, $\mathscr{C}(F) = \mathscr{C}(A) = U\mathscr{C}(A_\mu)U^{-1} = UT_\mu U^{-1}$. This also proves (3), because a Type II-$\ell$ maximal subring $M$ will equal $\mathscr{C}(F)$ for a field $F$ isomorphic to some $\mathbb{F}_{q^\ell}$. □

**Proposition 3.7.** *Let $\ell$ be a prime divisor of $n$. The number of Type II-$\ell$ maximal subrings of $M_n(\mathbb{F}_q)$ is equal to*

$$\frac{|GL(n,q)|}{|GL(n/\ell,q^\ell)| \cdot \ell} = \frac{1}{\ell} \prod_{\substack{k=1, \\ \ell \nmid k}}^{n-1} (q^n - q^k).$$

*Proof.* By [17, Lem. 7.2], the number of Type II-$\ell$ maximal subrings of $M_n(\mathbb{F}_q)$ is equal to $|GL(n,q)|/(|GL(n/\ell,q^\ell)| \cdot \ell)$. A routine calculation using the fact that $|GL(n,q)| = \prod_{k=0}^{n-1}(q^n - q^k)$ for all $n$ and $q$ shows that

$$\frac{|GL(n,q)|}{|GL(n/\ell,q^\ell)| \cdot \ell} = \frac{1}{\ell} \prod_{\substack{k=1, \\ \ell \nmid k}}^{n-1} (q^n - q^k).$$

□

Finally, we look at Type III maximal subrings.

**Proposition 3.8.** *Assume that $q \neq p$ and let $\mathbb{F}_r$ be a maximal subfield of $\mathbb{F}_q$.*

*(1) All Type III-r maximal subrings of $M_n(\mathbb{F}_q)$ are $GL(n,q)$-conjugate.*

*(2) The number of Type III-r maximal subrings of $M_n(\mathbb{F}_q)$ is equal to $\dfrac{|GL(n,q)|(r-1)}{|GL(n,r)|(q-1)}$.*

*Proof.* Part (1) is immediate from the definition of Type III maximal subrings. For (2), let $M = M_n(\mathbb{F}_r)$. By Theorem 2.8, any subring of $M_n(\mathbb{F}_q)$ that is isomorphic to $M$ is actually a $GL(n,q)$ conjugate of $M$. We will count the number of such conjugates. Let $\mathscr{N} = \{U \in GL(n,q) \mid UMU^{-1} = M\}$ be the normalizer of $M$ under the action of $GL(n,q)$. Note that $\mathscr{N}$ contains both $GL(n,r)$ and $\mathbb{F}_q^\times$ (which is the set of invertible scalar matrices).

Now, conjugation by $U \in \mathscr{N}$ acts as an $\mathbb{F}_r$-automorphism of $M$. By the Skolem-Noether Theorem [24, Thm. 24.40], the group $\mathrm{Aut}_{\mathbb{F}_r}(M)$ of $\mathbb{F}_r$-automorphisms of $M$ is isomorphic to $GL(n,r)/\mathbb{F}_r^\times$. Thus, there is a homomorphism $\phi : \mathscr{N} \to GL(n,r)/\mathbb{F}_r^\times$, and $\phi$ is surjective because $GL(n,r)$ is contained in $\mathscr{N}$. The kernel of $\phi$ is $\mathscr{C}_{GL(n,q)}(M) = \mathbb{F}_q^\times$. Since all the groups involved are finite, we get

$$|\mathscr{N}| = \frac{|GL(n,r)|}{|\mathbb{F}_r^\times|} \cdot |\mathbb{F}_q^\times| = \frac{|GL(n,r)|(q-1)}{r-1}$$

Hence, the number of conjugates of $M$ is $[GL(n,q) : \mathscr{N}] = \dfrac{|GL(n,q)|(r-1)}{|GL(n,r)|(q-1)}$. □

*Remark* 3.9. For any field $F$, let $PGL(n,F)$ denote the projective general linear group, which is $PGL(n,F) = GL(n,F)/F^\times$. With this notation, Proposition 3.8 says that number of $GL(n,q)$-conjugates of $M_n(\mathbb{F}_r)$ is equal to $[PGL(n,q) : PGL(n,r)]$.

# 4 Maximal Subrings of Products of Simple Rings

In this section, we classify the maximal subrings of a finite semisimple ring. By the Artin-Wedderburn Theorem, such a semisimple ring is isomorphic to a direct product of matrix rings over finite fields. The results of this section are an extension of Section 4 of [27], which dealt with the maximal subrings of a direct product of finite fields.

Any finite ring $R$ with unity is isomorphic to a direct product of rings of prime power order [20, Thm. I.1], and any subring $S \subseteq R$ respects this decomposition. In particular, if $R \cong \prod_{i=1}^t R_i$ with $|R_i| = p_i^{n_i}$ for distinct primes $p_i$ and positive integers $n_i$, and if $M$ is a maximal subring of $R$, then

$$M = R_1 \times \cdots \times R_{i-1} \times M_i \times R_{i+1} \times \cdots \times R_t$$

for some $1 \leq i \leq t$, where $M_i$ is a maximal subring of $R_i$. Hence, if we wish to classify the maximal subrings of a finite semisimple ring $R$, then we may assume that $R$ has prime power order. Consequently, throughout this section we could work with products of the form $R = \prod_{i=1}^t R_i$, where each $R_i$ is a finite simple ring of characteristic $p$. In fact, since our proofs rely only on the simplicity of each $R_i$, we can work in a broader context and assume that each $R_i$ is simple (but not necessarily finite) and has the same characteristic.

Given a product $R = \prod_{i=1}^t R_i$ with each $R_i$ simple and sharing the same characteristic, $F$ will denote the prime field of each $R_i$. Then, $F = \mathbb{Q}$ if the $R_i$ have characteristic 0, and $F = \mathbb{F}_p$ if their characteristic is $p$. For convenience, we will identify each simple ring with its canonical matrix ring. Thus, saying that $R_i$ is a simple ring means that $R_i = M_{n_i}(\mathscr{D}_i)$ for some division ring $\mathscr{D}_i$ with prime field $F$ and some positive integer $n_i$. Furthermore, having $R_i \cong R_j$ means that $R_i = R_j$.

We begin by examining the case $t = 2$, for which $R = R_1 \times R_2$. Proposition 4.2 shows that the maximal subrings of $R_1 \times R_2$ can be divided into two non-overlapping classes. These classes are then generalized to larger products of simple rings in Definition 4.3, and Theorem 4.5 shows that any maximal subring of such a product falls into one of the two classes.

When $t = 2$, it is clear that there exist maximal subrings of the form $M_1 \times R_2$ and $R_1 \times M_2$, where $M_i$ is maximal in $R_i$. However, other maximal subrings are possible. In the special case where $R_1 = R_2$, the ring $R = R_1 \times R_1$ admits a diagonal subring $M = \{(a, a) \mid a \in R_1\}$, which is actually maximal. We can generalize this subring by considering pairs $(a, \phi(a))$ where the entries are linked by an $F$-automorphism $\phi$ of $R_1$. The next lemma shows that a subring consisting of such elements is always maximal.

**Lemma 4.1.** *Let $R_1$ be a simple ring with prime field $F$ and let $R = R_1 \times R_1$. Let $\phi \in Aut_F(R_1)$ and let $M = \{(a, \phi(a)) \mid a \in R_1\}$. Then, $M$ is a maximal subring of $R$.*

*Proof.* Let $S$ be a subring of $R$ such that $M \subsetneq S$ and let $(x, y) \in S \setminus M$. Then, $(x, \phi(x)) \in M$, so $(0, \phi(x) - y) \in S$, and $\phi(x) - y \neq 0$ because $(x, y) \notin M$. Let $I$ be the two-sided ideal of $S$ generated by $(0, \phi(x) - y)$. Note that since $\phi$ is an automorphism, the set of components $\{b \in R_1 \mid (a, b) \in S \text{ for some } a\}$ is equal to $R_1$; this means that $I$ is actually an ideal of $\{0\} \times R_1$. Since $I$ is nonzero and $R_1$ is simple, we must have $I = \{0\} \times R_1 \subseteq S$. In a similar fashion, one may show that $R_1 \times \{0\} \subseteq S$, so $S = R_1 \times R_1$ and hence $M$ is maximal. □

We now prove that the maximal subrings discussed prior to Lemma 4.1 are the only ones possible in $R = R_1 \times R_2$.

**Proposition 4.2.** *Let $R = R_1 \times R_2$, where $R_1$ and $R_2$ are simple rings with prime field $F$. Let $M$ be a maximal subring of $R$. Then, $M$ has one of the following forms:*

1. *(a) $M = M_1 \times R_2$ for some maximal subring $M_1$ of $R_1$,*
   *(b) $M = R_1 \times M_2$ for some maximal subring $M_2$ of $R_2$,*
2. *$R_1 = R_2$ and $M = \{(a, \phi(a)) \mid a \in R_1\}$ for some $\phi \in Aut_F(R_1)$.*

*Proof.* If $M$ has the form $M = M_1 \times R_2$ or $M = R_1 \times M_2$, then we are done. So, assume that $M$ is not of this form. In particular, this means that $M$ cannot be a maximal ideal of $R$. By Lemma 2.1, $(1, 1) \in M$.

From here, we break the proof into a number of claims.

*Claim 1*: Let $\pi_1 : R \to R_1$ and $\pi_2 : R \to R_2$ be the projection maps. Then, $\pi_1(M) = R_1$ and $\pi_2(M) = R_2$.
*Proof of claim.* If $\pi_1(M) \neq R_1$, then $\pi_1(M) \subseteq M_1$ for some maximal subring $M_1$ of $R_1$. But then, $M \subseteq M_1 \times R_2$ and so $M = M_1 \times R_2$ by the maximality of $M$, which is contrary to our assumption. Thus, $\pi_1(M) = R_1$. Similarly, $\pi_2(M) = R_2$.

*Claim 2*: For all $(a, b) \in M$, $a = 0$ if and only if $b = 0$.
*Proof of claim.* Suppose there exists $(0, b) \in M$ with $b \neq 0$ and let $I$ be the two-sided ideal of $M$ generated by $(0, b)$. By Claim 1, $\pi_2(M) = R_2$, so (as in the proof of Lemma 4.1) $I$ is actually an ideal of $\{0\} \times R_2$. Since $R_2$ is simple we must have $I = \{0\} \times R_2 \subseteq M$. The only way this can be true with $M$ maximal is if $M$ has the form $M_1 \times R_2$, and we are assuming this is not the case. Thus, if $(a, b) \in M$ with $a = 0$, then $b = 0$. The proof of the converse is similar.

*Claim 3*: For all $(a, b), (c, d) \in M$, $a = c$ if and only if $b = d$.
*Proof of claim.* We always have $(a - c, b - d) \in M$, so by Claim 2 if $a = c$ then $(0, b - d) \in M$ and hence $b = d$, and analogously for the converse.

*Claim 4*: For each $a \in R_1$, there is a unique $\phi(a) \in R_2$ such that $(a, \phi(a)) \in M$. Moreover, the mapping $\phi : R_1 \to R_2$ is an $F$-isomorphism.

*Proof of claim.* The uniqueness of $\phi(a)$ follows from Claim 3, and this uniqueness guarantees that the mapping $\phi$ is well-defined. Claim 3 also shows that $\phi$ is injective, and surjectivity follows from Claim 1 because $\pi_2(M) = R_2$. Thus, $\phi$ is a bijection. Next, $\phi$ respects operations because $M$ is a ring. Indeed, if $(a, b), (c, d) \in M$, then $(a + c, b + d), (ac, bd) \in M$, and so $\phi(a + c) = b + d = \phi(a) + \phi(c)$ and $\phi(ac) = bd = \phi(a)\phi(c)$. Finally, the function $\phi$ commutes with the action of $F$ because $(1, 1) \in M$, and so $\phi(1) = 1$.

The existence of the isomorphism $\phi$ from Claim 4 shows that $R_1 \cong R_2$ (and hence $R_1 = R_2$ by our convention) and that $M = \{(a, \phi(a)) \mid a \in R_1\}$, so the proof is now complete. □

**Definition 4.3.** Let $R = \prod_{i=1}^{t} R_i$ be a direct product of simple rings with prime field $F$. Let $M$ be a maximal subring of $R$. We say that $M$ is of *Type* $\Pi_1$ if there exists an index $i$ and a maximal subring $M_i$ of $R_i$ such that

$$M = R_1 \times \cdots \times R_{i-1} \times M_i \times R_{i+1} \times \cdots \times R_t.$$

We say that $M$ is of *Type* $\Pi_2$ if there exist indices $i < j$ and $\phi \in \mathrm{Aut}_F(R_i)$ such that $R_i = R_j$ and

$$M = \{(a_1, \ldots, a_n) \in R \mid a_j = \phi(a_i)\};$$

here, there are no restrictions on the entries $a_k$ for $k \neq i, j$.

We employ this $\Pi$-notation in Definition 4.3 so as not to conflict with Definition 3.1, and as an implicit reminder that these definitions apply to direct products of rings. Subrings of Type $\Pi_1$ are clearly maximal. Proving that subrings of Type $\Pi_2$ are maximal proceeds as in Lemma 4.1. Indeed, if $M$ is of Type $\Pi_2$ and $M \subsetneq S \subseteq R$, then let $\pi_{ij} : R \to R_i \times R_j$ be the projection map. Then, $\pi_{ij}(M)$ is maximal in $R_i \times R_j$ and $\pi_{ij}(M) \subsetneq \pi_{ij}(S)$, so $\pi_{ij}(S) = R_i \times R_j$. It follows that $S = R$ and $M$ is maximal.

In Theorem 4.5, we will prove that every maximal subring of $R$ is of Type $\Pi_1$ or Type $\Pi_2$. The proof of the theorem uses the following lemma.

**Lemma 4.4.** *Let $R = \prod_{i=1}^{t} R_i$ be a direct product of simple rings with prime field $F$, and assume that $t \geq 3$. For each $1 \leq i \leq t$, let $\widehat{\pi}_i : R \to \prod_{j \neq i} R_j$ be the projection map. If $S$ is a subring of $R$ such that $\widehat{\pi}_i(S) = \prod_{j \neq i} R_j$ for each $i$, then $S = R$.*

*Proof.* Assume that $S$ is a subring of $R$ such that $\widehat{\pi}_i(S) = \prod_{j \neq i} R_j$ for each $i$. For each $1 \leq i < j \leq t$, let $Z_{ij} = \{(a_1, \ldots, a_t) \in R \mid a_i = a_j = 0\}$ be the ideal of $R$ with $\{0\}$ in the $i^{\text{th}}$ and $j^{th}$ components and $R_k$ elsewhere.

First, we show that $Z_{12} \subseteq S$. Since $\widehat{\pi}_1(S) = \prod_{j \neq 1} R_j$, there exists $a \in R_1$ such that $(a, 0, 1, 1, \ldots, 1) \in S$. Since $\widehat{\pi}_2(S) = \prod_{j \neq 2} R_j$ and each $R_j$ is simple, the two-sided ideal of $S$ generated by $(a, 0, 1, 1, \ldots, 1)$ in $S$ is equal to either $\{0\} \times \{0\} \times R_3 \times \cdots \times R_t$ (if $a = 0$) or $R_1 \times \{0\} \times R_3 \times \cdots \times R_t$ (if $a \neq 0$). In either case, we conclude that $Z_{12} \subseteq S$.

Now, the technique used in the previous paragraph can be applied to $Z_{ij}$ for any $1 \leq i < j \leq t$, so each $Z_{ij}$ is contained in $S$. Since $t \geq 3$, this means that $Z_{12}, Z_{13}, Z_{23} \subseteq S$; but, $Z_{12} + Z_{13} + Z_{23} = R$, so $S = R$. □

**Theorem 4.5.** *Let $R = \prod_{i=1}^{t} R_i$ be a direct product of simple rings with prime field $F$. Then, any maximal subring of $R$ is of Type $\Pi_1$ or Type $\Pi_2$.*

*Proof.* The proof is by induction on $t$. The theorem is trivial when $t = 1$, and the case $t = 2$ was completed in Proposition 4.2. So, assume that $t \geq 3$ and that the result holds for any direct product of less than $t$ simple rings.

Define the projection maps $\widehat{\pi}_i$ as in Lemma 4.4. Since $t \geq 3$ and $M \neq R$, by Lemma 4.4 there is some $1 \leq i \leq t$ such that $\widehat{\pi}_i(M) \neq \prod_{j \neq i} R_j$. Without loss of generality, assume that $\widehat{\pi}_1(M) \neq \prod_{j=2}^{t} R_j$. Then, $\widehat{\pi}_1(M)$ is contained in a maximal subring $M'$ of $\prod_{j=2}^{t} R_j$. By induction, $M'$ is of Type $\Pi_1$ or Type $\Pi_2$. Hence, $M \subseteq R_1 \times M'$, and by the maximality of $M$ we must have $M = R_1 \times M'$. Since $M'$ is of Type $\Pi_1$ or Type $\Pi_2$, so is $M$. □

# 5 The Covering Number of a Finite Semisimple Ring

In this final section, we show how to calculate the covering number of a finite semisimple ring. Recall from the introduction that for a unital ring $R$, a cover is a collection of proper subrings $S_i \subsetneq R$ such that $R = \bigcup_i S_i$, and the covering number $\sigma(R)$ is the size of a minimal cover (if one exists). Not every finite ring admits a cover. For example, a finite field $F$ is not coverable, because the generator of the unit group cannot lie in any proper subring of $F$. If $R$ is not coverable, then we take $\sigma(R) = \infty$.

The following theorem from [27] describes exactly when a finite semisimple ring is coverable.

**Theorem 5.1.** *[27, Cor. 3.8] For each prime $p$ and positive integer $n$, let $Irr(p, n)$ denote the set of monic irreducible polynomials of degree $n$ in $\mathbb{F}_p[x]$. For a prime power $q = p^n$, let*

$$\tau(q) = \begin{cases} p & \text{if } n = 1, \\ |Irr(p, n)| + 1 & \text{if } n > 1. \end{cases}$$

*Let $R = \prod_{i=1}^{t} M_{n_i}(\mathbb{F}_{q_i})$ be a finite semisimple ring, where for each $i$, $n_i$ is a positive integer and $q_i$ is a prime power. Then, $R$ is coverable if and only if one of the following conditions holds:*

1. *some $n_i > 1$.*
2. *all $n_i = 1$ and some $\mathbb{F}_{q_i}$ occurs in the product at least $\tau(q_i)$ times.*

Section 5 of [27] gives a formula for $\sigma(R)$ when $R$ is a coverable product of finite fields. The covering number of a matrix ring $M_n(\mathbb{F}_q)$ with $n \geq 2$ has been established by the work of Lucchini, Maròti, and Crestani.

**Theorem 5.2.** *(Lucchini, Maròti, Crestani) Let $n \geq 2$ and let $\ell$ be the smallest prime divisor of $n$. Then,*

$$\sigma(M_n(\mathbb{F}_q)) = \frac{1}{\ell} \prod_{\substack{k=1, \\ \ell \nmid k}}^{n-1} (q^n - q^k) + \sum_{\substack{k=1, \\ \ell \nmid k}}^{\lfloor n/2 \rfloor} \binom{n}{k}_q .$$

*Proof.* In the terminology of Section 3, the theorem is saying that a minimal cover for $M_n(\mathbb{F}_q)$ is found by taking the union of all the Type II-$\ell$ maximal subrings and all the Type I-$k$ subrings for $k = 1, \ldots, \lfloor n/2 \rfloor$ such that $\ell \nmid k$. For convenience, let $X$ denote the expression on the right-hand side of the above equation. A proof that $\sigma(M_n(\mathbb{F}_q)) \leq X$ is given in [17, Prop. 7.3]. The inequality $\sigma(M_n(\mathbb{F}_q)) \geq X$ is shown in [17, Sec. 7], and also follows from the main result in [5]. □

Interestingly, the work done in [17, Sec. 7] and [5] relied on a classification of the maximal subrings of $M_n(\mathbb{F}_q)$ that did not include Type III maximal subrings (see [17, Lem. 7.1], which is equivalent to Racine's classifications [21, 22] of maximal $\mathbb{F}_q$-subalgebras of $M_n(\mathbb{F}_q)$). However, the techniques employed in [17] and [5] were robust enough that Type III maximal subrings where automatically excluded from the minimal covers that were formed, and so $\sigma(M_n(\mathbb{F}_q))$ can be determined by using only Type I and Type II maximal subrings.

To calculate the covering number of a general finite semisimple ring, we will need a few elementary results from [27]. We state them here for easy reference.

**Lemma 5.3.**

(1) *[27, Lem. 2.1] Let $R$ be a finite unital ring with a minimal cover $R = \bigcup_{i=1}^{\sigma(R)} M_i$, where each $M_i$ is a maximal subring of $R$. If $M$ is a maximal subring of $R$ containing a multiplicative identity and such that $M \neq M_i$ for each $i$, then $\sigma(M) \leq \sigma(R)$.*

(2) *[27, Thm. 2.2] Let $R = \prod_{i=1}^{t} R_i$, where each $R_i$ is a finite unital ring. Assume that each maximal subring $M$ of $R$ has the form*

$$M = R_1 \times \cdots \times R_{i-1} \times M_i \times R_{i+1} \times \cdots \times R_t,$$

*for some $1 \leq i \leq t$, where $M_i$ is a maximal subring of $R_i$. Then, $\sigma(R) = \min_{1\leq i\leq t}\{\sigma(R_i)\}$.*

(3) *[27, Cor. 2.4] Let $R = \prod_{i=1}^{t} R_i$, where each $R_i$ is a finite unital ring and $|R_i| = p_i^{n_i}$ for some distinct primes $p_i$ and some positive integers $n_i$. Then, $\sigma(R) = \min_{1\leq i\leq t}\{\sigma(R_i)\}$.*

When $R = \prod_{i=1}^{t} R_i$ is a product of finite simple rings $R_i$, we can always reindex the product so that identical simple rings are grouped together. When this kind of decomposition is used, determining $\sigma(R)$ reduces to the case where $R$ is a product of copies of a single simple ring.

**Proposition 5.4.** *Let $R_1, \dots, R_t$ be distinct finite simple rings. Let $R = \prod_{i=1}^{t} \Big(\prod_{j=1}^{t_i} A_{ij}\Big)$, where $A_{ij} = R_i$ for every $j \in \{1, \dots, t_i\}$. Then, $\sigma(R) = \min_{1\leq i\leq t}\Big\{\sigma\Big(\prod_{j=1}^{t_i} A_{ij}\Big)\Big\}$.*

*Proof.* By Lemma 5.3 part (3), we may assume that $R_i$ has the same characteristic for each $1 \leq i \leq t$. Then, by Theorem 4.5, each maximal subring of $R$ is of Type $\Pi_1$ or Type $\Pi_2$. For each $1 \leq i \leq t$, let $P_i = \prod_{j=1}^{t_i} A_{ij}$. Then, $R = \prod_{i=1}^{t} P_i$ and each maximal subring $M$ of $R$ has the form

$$M = P_1 \times \cdots \times P_{i-1} \times M_i \times P_{i+1} \times \cdots \times P_t$$

where $M_i$ is a maximal subring of $P_i$. By Lemma 5.3 part (2), we get $\sigma(R) = \min_{1\leq i\leq t}\{\sigma(P_i)\}$. □

As mentioned earlier, the value of $\sigma(\prod_{i=1}^{t} \mathbb{F}_q)$ is determined in [27, Sec. 5]. It remains to consider the case where $R = \prod_{i=1}^{t} M_n(\mathbb{F}_q)$ for some $n \geq 2$. After an ugly proof of an inequality, we will show (Theorem 5.11) that $\sigma(R) = \sigma(M_n(\mathbb{F}_q))$.

**Lemma 5.5.** *Let $n \geq 2$. Then, $\sigma(M_n(\mathbb{F}_q)) < |Aut_{\mathbb{F}_p}(M_n(\mathbb{F}_q))|$.*

*Proof.* Let $\ell$ be the smallest prime divisor of $n$. By Theorem 5.2,

$$\sigma(M_n(\mathbb{F}_q)) = \frac{1}{\ell}\prod_{\substack{k=1,\\ \ell\nmid k}}^{n-1}(q^n - q^k) + \sum_{\substack{k=1,\\ \ell\nmid k}}^{\lfloor n/2\rfloor}\binom{n}{k}_q.$$

By the Skolem-Noether Theorem [24, Thm. 24.40], the group of $\mathbb{F}_q$-automorphisms of $M_n(\mathbb{F}_q)$ has order $|GL(n,q)|/(q-1)$. Every $\mathbb{F}_q$-automorphism is also an $\mathbb{F}_p$-automorphism, so we get the following lower bound for $|\mathrm{Aut}_{\mathbb{F}_p}(M_n(\mathbb{F}_q))|$:

$$\begin{aligned}|\mathrm{Aut}_{\mathbb{F}_p}(M_n(\mathbb{F}_q))| &\geq \frac{|GL(n,q)|}{q-1}\\ &= \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}\\ &= (1+q+\cdots+q^{n-1})(q^n-q)\cdots(q^n-q^{n-1}). \qquad (5.6)\end{aligned}$$

An upper bound for the first part of the formula for $\sigma(M_n(\mathbb{F}_q))$ is

$$\begin{aligned}\frac{1}{\ell}\prod_{\substack{k=1,\\ \ell\nmid k}}^{n-1}(q^n-q^k) &\leq \frac{1}{2}\prod_{k=1}^{n-1}(q^n-q^k)\\ &= \frac{1}{2}(q^n-q)\cdots(q^n-q^{n-1}). \qquad (5.7)\end{aligned}$$

For readability, let $f = \lfloor n/2 \rfloor$. Then, an upper bound for the second part of the formula is

$$\begin{aligned}\sum_{\substack{k=1,\\ \ell \nmid k}}^{f} \binom{n}{k}_q &\leq \sum_{k=1}^{f} \binom{n}{k}_q \\ &= \sum_{k=1}^{f} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-(k-1)}-1)}{(q-1)(q^2-1)\cdots(q^k-1)} \\ &= \frac{q^n-1}{q-1}\Big(1+\sum_{k=2}^{f} \frac{(q^{n-1}-1)\cdots(q^{n-(k-1)}-1)}{(q^2-1)\cdots(q^k-1)}\Big). \qquad (5.8)\end{aligned}$$

Clearly, the expression in (5.6) is greater than the expression in (5.7). After comparing these two, we see that it suffices to show that the expression in (5.8) is strictly less than

$$(\frac{1}{2} + q + \cdots + q^{n-1})(q^n - q)\cdots(q^n - q^{n-1}). \qquad (5.9)$$

Note that

$$\begin{aligned}(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) &= q(q^{n-1}-1)q^2(q^{n-2}-1)\cdots q^{n-1}(q-1) \\ &= q^{(n-1)n/2}(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1)\end{aligned}$$

so that (5.9) is equal to

$$\begin{aligned}&(\frac{1}{2}+q+\cdots+q^{n-1})q^{(n-1)n/2}(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1) \\ &\quad = (\frac{q}{2}+q^2+\cdots+q^n)q^{(n^2-n-2)/2}(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1).\end{aligned}$$

Now, certainly

$$\frac{q^n-1}{q-1} = 1 + q + \cdots + q^{n-1} < \frac{q}{2} + q^2 + \cdots + q^n,$$

so it will be enough to prove the following inequality:

$$\begin{aligned}1+&\sum_{k=2}^{f} \frac{(q^{n-1}-1)\cdots(q^{n-(k-1)}-1)}{(q^2-1)\cdots(q^k-1)} \\ &\leq q^{(n^2-n-2)/2}(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1).\end{aligned} \qquad (5.10)$$

The product $(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1)$ is at least as large as the numerator of each fraction in the left-hand side of (5.10). So, inequality (5.10) will hold once we verify that $q^{(n^2-n-2)/2}$ is greater than or equal to $f$, the number of summands in the left-hand side of (5.10).

If $n = 2$, then $f = \lfloor n/2 \rfloor = 1$ and $q^{(n^2-n-2)/2} = 1$, so (5.10) holds. So, assume that $n \geq 3$. Then, $n \leq n^2 - n - 2$, so

$$f \leq \frac{n}{2} < q^{n/2} \leq q^{(n^2-n-2)/2}.$$

Thus, (5.10) holds in this case as well, and the proof is complete. □

**Theorem 5.11.** *Let $n \geq 2$ and let $R = \prod_{i=1}^{t} M_n(\mathbb{F}_q)$, where $t \geq 1$. Then, $\sigma(R) = \sigma(M_n(\mathbb{F}_q))$.*

*Proof.* We will use induction on $t$. There is nothing to prove if $t = 1$, so assume that $t \geq 2$ and that the result holds for $\prod_{i=1}^{t-1} M_n(\mathbb{F}_q)$. Since $t \geq 2$, $R$ has $M_n(\mathbb{F}_q)$ as a residue ring. Since a cover can be lifted from a residue ring up to $R$, we see that $\sigma(R) \leq \sigma(M_n(\mathbb{F}_q))$.

Now, each Type $\Pi_2$ maximal subring of $R$ corresponds to a choice of two indices $i < j$ and an $\mathbb{F}_p$-automorphism $\phi$ of $M_n(\mathbb{F}_q)$. It follows that the number of Type $\Pi_2$ maximal subrings of $R$ is $\binom{t}{2}|\mathrm{Aut}_{\mathbb{F}_p}(M_n(\mathbb{F}_q))|$, which by Lemma 5.5 is strictly greater than $\sigma(M_n(\mathbb{F}_q))$. Thus, it is possible to form a minimal cover of $R$ that does not include some Type $\Pi_2$ maximal subring $M$. By Lemma 5.3 part (1), $\sigma(R) \geq \sigma(M)$. But, $M \cong \prod_{i=1}^{t-1} M_n(\mathbb{F}_q)$, because $M$ consists of $t-2$ factors equal to $M_n(\mathbb{F}_q)$, and the remaining two factors are linked by an automorphism, and hence comprise a single ring isomorphic to $M_n(\mathbb{F}_q)$. By induction, $\sigma(M) = \sigma(M_n(\mathbb{F}_q))$, so we are done. □

# References

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

[2] Britnell, J. R., Evseev, A., Guralnick, R. M., Holmes, P. E., Maròti, A. Corrigendum to "Sets of elements that pairwise generate a linear group". *J. Combin. Theory Ser. A* 118 (2011), no. 3, 1152–1153.

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

[4] Cohn, J. H. E. On $n$-sum groups. *Math. Scand.* 75 (1994) 44–58.

[5] Crestani, E. Sets of elements that pairwise generate a matrix ring. *Comm. Algebra* 40 (2012), no. 4, 1570–1575.

[6] Dobbs, D. Every commutative ring has a minimal ring extension. *Comm. Algebra* 34 (2006), no. 10, 3875–3881.

[7] Dobbs, D., Shapiro, J. A classification of the minimal ring extensions of an integral domain. *J. Algebra* 305 (2006), no. 1, 185–193.

[8] Dobbs, D., Shapiro, J. A classification of the minimal ring extensions of certain commutative rings. *J. Algebra* 308 (2007), no. 2, 800–821.

[9] Elduque, A. On maximal subalgebras of central simple Mal'cev algebras. *J. Algebra* 103 (1986), no. 1, 216–227.

[10] Elduque, A., Laliena, J., Sacristán, S. Maximal subalgebras of associative superalgebras. *J. Algebra 275* (2004), no. 1, 40–58.

[11] Elduque, A., Laliena, J., Sacristán, S. Maximal subalgebras of Jordan superalgebras. *J. Pure Appl. Algebra* 212 (2008), no. 11, 2461–2478.

[12] Holmes, P. E. Subgroup coverings of some sporadic groups. *J. Comb. Theory, Ser. A* 113 (2006) 1204–1213.

[13] Kappe, L.-C. 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.

[14] Kappe, L.-C., Redden, J. On the covering number of small alternating groups, in *Computational Group Theory and the Theory of Groups II*, Contemporary Mathematics, Vol. 511, Amer. Math. Soc., Providence, RI, 2010. 109–125.

[15] Lam, T. Y. A First Course in Noncommutative Rings, 2nd edition. Graduate Texts in Mathematics 131. Springer, 2001.

[16] Lam, T. Y. Lectures on Modules and Rings. Graduate Texts in Mathematics 189. Springer, 1999.

[17] Lucchini, A., Maròti, A. Rings as the union of proper subrings (2010). Available at: http://arxiv.org/abs/1001.3984v1

[18] Lucchini, A., Maròti, A. Rings as the union of proper subrings. *Algebr. Represent. Theory* 15 (2012) 1035–1047.

[19] Maròti, A. Covering the symmetric groups with proper subgroups. *J. Comb. Theory, Ser. A* 110 (2005) 97–111.

[20] McDonald, B. R. Finite Rings with Identity. Pure Appl. Math., Vol. 28. Marcel Dekker, New York, 1974.

[21] Racine, M. L. On maximal subalgebras. *J. Algebra* 30 (1974) 155–180.

[22] Racine, M. L. Maximal subalgebras of central separable algebras. *Proc. Amer. Math. Soc.* 68 (1978), no. 1, 11–15.

[23] Racine, M. L. Maximal subalgebras of exceptional Jordan algebras. *J. Algebra* 46 (1977), no. 1, 12–21.

[24] Rowen, L. H. Graduate Algebra: Noncommutative View. Graduate Studies in Mathematics, 91. Amer. Math. Soc., Providence, 2008.

[25] Swartz, E. On the covering number of symmetric groups having degree divisible by six. *Discrete Math.* 339 (2016), no. 11, 2593–2604.

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

[27] Werner, N. J. Covering numbers of finite rings. *Amer. Math. Monthly* 122 (2015), no. 6, 552–566.