Strong primeness in matrix rings

Henry R. Thackeray, John E. van den Berg [*]

*Department of Mathematics and Applied Mathematics, University of Pretoria, Private Bag X20,
Hatfield, Pretoria, 0028, South Africa*

*[*]Corresponding author.
E-mail addresses: thackeray@iburst.co.za (H.R. Thackeray), john.vandenberg@up.ac.za (J.E. van den* ***Berg)***

ABSTRACT

The bound of uniform strong primeness of the ring $\mathbb{M}_n(R)$ of n by n matrices over the unitary ring R is denoted $m_n(R)$. The concepts of uniform, right and left strong primeness for matrix rings are reinterpreted in terms of bilinear equations and multiplication of vectors. These interpretations are used to prove new results. Bounds of strong primeness of unitary rings R are linked to the bounds for $\mathbb{M}_n(R)$. The bound $m_2(D)$ is investigated for division rings D. Results by van den Berg (1998) and Beidar and Wisbauer (2004) linking uniform strong primeness to the existence of certain, possibly nonassociative, division algebras are generalised from fields to division rings. The result $m_n(D) \leq 2n - 1$ of van den Berg (1998) for division rings is extended to $m_{nn'}(R) \leq (2n - 1)m_{n'}(R)$ for general unitary rings. In the case of formally real fields F, it is improved to $m_n(F) \leq 2n - 2$ for integers $n > 1$ and $m_n(F) \leq 2n - 4$ for even $n > 2$. This improvement, used in conjunction with a generalisation of an algebraic–topological proof of Hopf's theorem on real division algebras, yields $m_{2^k+1}(\mathbb{R}) = m_{2^k+2}(\mathbb{R}) = 2^{k+1}$. Bounds on $m_n(\mathbb{R})$ for other n are also obtained.

Keywords:
Strongly prime Uniformly strongly prime Matrix ring

1. Introduction

There are several notions of strong primeness in the literature. The oldest of these has its origin in two independent works: the MSc thesis of Lawrence [1] and the PhD thesis of Viola-Prioli [2]. The former is an investigation of primitivity in group rings; one of its striking results shows that a condition, somewhat stronger than primeness (but not as strong as being a domain), is required of a ring R in order that the group ring $R[G]$ over a suitable free product G of groups be right primitive. This condition, later christened "right strongly prime", was seen as interesting in its own right and there followed the development of a theory for strongly prime rings in [3,4] (see also [2]).

A ring R is said to be *right strongly prime* if for each nonzero $a \in R$, there exists a nonempty finite subset S (dependent on a) of R such that the set aS has trivial right annihilator. In this situation the subset S is called a *right insulator* for a. More specifically, the ring R is said to be *right strongly prime of bound n* if there exists a positive integer n with the property that every nonzero element in R possesses a right insulator of size n and no smaller such n exists. *Left strongly prime* rings and *left insulators* are defined in the obvious dual fashion.

Handelman and Lawrence also introduce in [4] a stronger, and left–right symmetric, variant of strong primeness that is the notion of primary interest in this paper: they call a ring R *uniformly strongly prime* if R contains a finite subset S that is a right insulator for *every* nonzero $a \in R$ (such a set is called a *uniform insulator* for R); that is, $aSb = 0$ only if $a = 0$ or $b = 0$. The ring R is called *uniformly strongly prime of bound n* if n is the smallest positive integer for which R possesses a uniform insulator of size n.

It is shown in [4] that if D is any division ring, then $\mathbb{M}_n(D)$ is right (and left) strongly prime of bound n, and uniformly strongly prime of bound at most n^2 since the set of matrix units is easily shown to constitute a uniform insulator. Van den Berg [5] sharpened this result, showing that the bound of uniform strong primeness of $\mathbb{M}_n(D)$ always lies from n to $2n - 1$ inclusive. Curiously, its exact value is not determined solely by n, but also depends on subtle algebraic features of the ground division ring D. Indeed, it has been shown that the bound of uniform strong primeness of $\mathbb{M}_n(F)$ is $2n - 1$ if F is an algebraically closed field [5, Proposition 8], and n if and only if there exists a (possibly nonassociative) division algebra over F of dimension n ([6, Theorem 1.2], [7, Theorem 11]); this means, for example, that the bound of $\mathbb{M}_n(\mathbb{Q})$, with $\mathbb{Q}$ the field of rationals, is always n, for there exists, for every n, an irreducible polynomial of degree n over $\mathbb{Q}$ and thus an n-dimensional field extension of $\mathbb{Q}$. The bound of uniform strong primeness of $\mathbb{M}_n(F)$ can, however, lie strictly between n and $2n - 1$ as examples in this paper and earlier papers show; the ring of 3 by 3 matrices over the reals, for example, is uniformly strongly prime of bound 4.

This paper continues the work of Beidar, Wisbauer and the second author [5–7] on bounds of uniform strong primeness in matrix rings.

It is important to note that the sole focus on matrix rings, and in particular on matrix rings over division rings, is not as restrictive as it might appear. Indeed, as shown in [3, Theorem 4.7], every ring R which is right strongly prime of bound greater than 1 is prime right Goldie and therefore a right order in $\mathbb{M}_n(D)$ for some division ring D. Moreover, in this situation, R inherits uniform strong primeness from the overring $\mathbb{M}_n(D)$ and its bound is at most that of the overring. If R is also a left order in $\mathbb{M}_n(D)$(this is the case, for example, whenever $D = F$ is a field, for left and right orders coincide in $\mathbb{M}_n(F)$ by the Faith–Utumi Theorem), the bound of R is identical to that of $\mathbb{M}_n(D)$ [5, Corollary 7]. Thus the calculation of bounds of uniform strong primeness of a significant class of strongly prime rings reduces to a consideration of matrix rings over division rings. However, as earlier work on this project has shown, the determination of this index in such apparently “simple” rings turns out to be surprisingly difficult.

In this paper, a method is developed for the calculation of the bound of uniform strong primeness of the matrix ring $\mathbb{M}_n(R)$ that involves reduction to a system of bilinear equations over R. This method shall provide a tool for proving results that are new, as well as a simplifying perspective on some that are old.

2. Preliminaries

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ will denote the sets of positive integers (0 is excluded), integers, rationals, reals and complex numbers respectively.

For $n \in \mathbb{N} \cup \{0\}$, define $\mathbb{N}_n = \{k \in \mathbb{N} : k \leq n\} = \{1, 2, \dots, n\}$. For $k \in \mathbb{Z}$,

$$\operatorname{sgn}(k) = \left\{ \begin{array}{ll} k/|k| & \text{if } k \neq 0 \\ 0 & \text{if } k = 0 \end{array} \right\}.$$

For $a \in \mathbb{R}$, $\lfloor a \rfloor$ and $\lceil a \rceil$ are the floor and ceiling respectively of a.

Throughout R will denote a unitary ring (ring with identity), D a division ring and F a field.

For $n, m \in \mathbb{N}$, $\mathbb{M}_{n\times m}(R)$ is the ring of n by m matrices over R and $\mathbb{M}_n(R)$ means $\mathbb{M}_{n\times n}(R)$.

For $n \in \mathbb{N}$, $i \in \mathbb{N}_n$ and $x \in R^n$, x_i is the ith component of x, $\mathbf{0}$ is the zero vector in R^n and $e_{(i)}$ is the ith unit vector in R^n. (The brackets emphasise that $e_{(i)}$ does not mean the ith component of a vector e.)

For n, $m \in \mathbb{N}$, $i \in \mathbb{N}_n$, $j \in \mathbb{N}_m$ and $A \in \mathbb{M}_{n\times m}(R)$, A_{ij} is A’s ith-row, jth-column entry and $A_{i\cdot}$ and $A_{\cdot j}$ are A’s ith row vector and jth column vector respectively. Following [8], $\operatorname{vec} A$ is the vector in R^{nm} obtained from $A \in \mathbb{M}_{n\times m}(R)$ by putting A’s columns on top of one another in order, that is,

$$\operatorname{vec} A = \left(\begin{array}{c} A_{\cdot 1} \\ \hline A_{\cdot 2} \\ \hline \vdots \\ \hline A_{\cdot m} \end{array} \right).$$

For n, $m \in \mathbb{N}$ and p, $q \in \mathbb{N}_n$, $\mathbb{O}$ is the zero matrix in $\mathbb{M}_{n\times m}(R)$, $\mathbb{I}$ the identity matrix in $\mathbb{M}_n(R)$ and, adapting notation from [8], $E_{(pq)}$ is the matrix in $\mathbb{M}_{n\times m}(R)$ where for $i \in \mathbb{N}_n$, $j \in \mathbb{N}_m$,

$$(E_{(pq)})_{ij} = \left\{ \begin{array}{ll} 1 & \text{if } p = i \text{ and } q = j \\ 0 & \text{otherwise.} \end{array} \right\}$$

(As with vectors, the brackets emphasise that $E_{(pq)}$ does not mean the entry in the pth row and qth column of a matrix E.)

Using and adapting notation in [6], if R is a ring for which the indicated index exists, the bound of uniform (respectively right, left) strong primeness of R will be denoted by $m(R)$ (respectively $m_r(R)$, $m_l(R)$) and if $n \in \mathbb{N}$, the bound of uniform strong primeness of the matrix ring $\mathbb{M}_n(R)$ will be denoted by $m_n(R)$. If R is right (respectively left) strongly prime but not right (respectively left) strongly prime of any bound $m \in \mathbb{N}$, take $m_r(R) = \infty$ (respectively $m_l(R) = \infty$).

3. Bilinear equations

The first re-interpretation of types of strong primeness for matrix rings in this paper involves homogeneous linear and bilinear equations. "(Bi)linear equation" will always mean "homogeneous (bi)linear equation". The notation used here is adapted from [8].

Proposition 1. *Suppose $n, m \in \mathbb{N}$, $X \in \mathbb{M}_n(R)\backslash\{\mathbb{O}\}$ and $S = \{A_{(p)} : p \in \mathbb{N}_m\}$ is a nonempty finite subset of $\mathbb{M}_n(R)$ with R a unitary ring. Consider the following conditions:*

(i) For $x, y \in R^n$, $(y^T A_{(p)}x = 0$ for $p \in \mathbb{N}_m) \Rightarrow (y = \mathbf{0}$ or $x = \mathbf{0})$.
(ii) For $x \in R^n$, $(X_{i\cdot}A_{(p)}x = 0$ for $p \in \mathbb{N}_m$, $i \in \mathbb{N}_n) \Rightarrow x = \mathbf{0}$.
(iii) For $y \in R^n$, $(y^T A_{(p)}X_{\cdot j} = 0$ for $p \in \mathbb{N}_m$, $j \in \mathbb{N}_n) \Rightarrow y = \mathbf{0}$.

S is a uniform insulator for $\mathbb{M}_n(R)$ (respectively right insulator for X, left insulator for X) iff (i) (respectively (ii), (iii)) holds.

Proof. The argument is an application of the definitions of uniform, right and left insulators and the fact that for $A, B, C \in \mathbb{M}_n(R)$,

$$BAC = \mathbb{O} \quad \Leftrightarrow \quad (\text{for } i, j \in \mathbb{N}_n,\ B_{i\cdot}AC_{\cdot j} = 0);$$

see the proof of [6, Lemma 2.2]. □

A matrix A corresponds to the bilinear equation $y^T Ax = 0$. A set of matrices is a uniform insulator precisely when the corresponding system of bilinear equations has no nontrivial solutions, and it is a right or left insulator when a system of linear equations that comes from restricting the bilinear equations to specific y or x has no nontrivial solutions. The question "What is $m_n(R)$?" is thus equivalent to the question "What is the smallest number of bilinear equations $y^T A_{(p)} x = 0$ that one needs to force $y = \mathbf{0}$ or $x = \mathbf{0}$?".

In the following result, parts (i) and (ii) without the conditions on the bounds come from [4, Proposition II.1] and [9, Lemma 9] respectively; the conditions on the bounds are obtained by adapting proofs from and using ideas in those articles and [7].

Theorem 2. *Let $n \in \mathbb{N}$ and let R be a unitary ring.*

(i) $\mathbb{M}_n(R)$ is right (respectively left) strongly prime precisely when R is right (respectively left) strongly prime, in which case $m_r(R) \leq m_r(\mathbb{M}_n(R)) \leq nm_r(R)$ (respectively $m_l(R) \leq m_l(\mathbb{M}_n(R)) \leq nm_l(R)$).

(ii) $\mathbb{M}_n(R)$ is uniformly strongly prime precisely when R is uniformly strongly prime, in which case $m(R) \leq m_n(R) \leq n^2 m(R)$.

Proof. (i) Suppose R is right strongly prime. Given $A \in \mathbb{M}_n(R) \backslash \{\mathbb{O}\}$, take $i, p \in \mathbb{N}_n$ with $A_{ip} \neq 0$; then A_{ip} has a right insulator $S \subseteq R$ of size at most $m_r(R)$. Consider the set $T = \{E_{(pq)}a : a \in S,\ q \in \mathbb{N}_n\} \subseteq \mathbb{M}_n(R)$. For $a \in R$, $q \in \mathbb{N}_n$, $x \in R^n$ one has $A_{i\cdot}(E_{(pq)}a)x = A_{ip}ax_q$. Hence

$$\begin{aligned} & A_{i\cdot}Tx = \{0\} \\ & \quad \Rightarrow \quad \big(\text{for } q \in \mathbb{N}_n,\ A_{ip}Sx_q = \{0\}\big) \\ & \quad \Rightarrow \quad (\text{for } q \in \mathbb{N}_n,\ x_q = 0) \\ & \quad \Rightarrow \quad x = \mathbf{0}. \end{aligned}$$

Thus by Proposition 1, T is a right insulator for A of size at most $nm_r(R)$.

Suppose $\mathbb{M}_n(R)$ is right strongly prime and choose $a \in R \backslash \{0\}$. The matrix $E_{(11)}a$ has a right insulator $\{A_{(p)} : p \in \mathbb{N}_m\}$ with $m \leq m_r(\mathbb{M}_n(R))$. Let $S = \{(A_{(p)})_{11} : p \in \mathbb{N}_m\}$. For $b \in R$,

$$\begin{aligned} & aSb = \{0\} \\ & \quad \Rightarrow \quad \big(\text{for } p \in \mathbb{N}_m,\ a(A_{(p)})_{11}b = 0\big) \\ & \quad \Rightarrow \quad \big(\text{for } p \in \mathbb{N}_m,\ (E_{(11)}a)A_{(p)}(E_{(11)}b) = \mathbb{O}\big) \\ & \quad \Rightarrow \quad E_{(11)}b = \mathbb{O} \\ & \quad \Rightarrow \quad b = 0. \end{aligned}$$

Thus S is a right insulator for a of size at most $m_r(\mathbb{M}_n(R))$.

The proof for left strong primeness is dual to this one.

(ii) Suppose R is uniformly strongly prime; then there is a nonempty finite set S with $|S| = m(R)$ and $(a, b \in R,\ aSb = \{0\}) \Rightarrow (a = 0 \text{ or } b = 0)$. Take $T = \{E_{(pq)}a : a \in S,\ p, q \in \mathbb{N}_n\} \subseteq \mathbb{M}_n(R)$. For $p, q \in \mathbb{N}_n$, $x, y \in R^n$, $a \in R$, one has $y^T(E_{(pq)}a)x = y_p a x_q$. Hence

$$\begin{aligned}
&y^T T x = \{0\} \\
&\quad \Rightarrow \quad \big(\text{for } p, q \in \mathbb{N}_n,\ y_p S x_q = \{0\}\big) \\
&\quad \Rightarrow \quad (\text{for } p, q \in \mathbb{N}_n,\ y_p = 0 \text{ or } x_q = 0) \\
&\quad \Rightarrow \quad \big((\text{for some } p \in \mathbb{N}_n,\ y_p \neq 0) \Rightarrow (\text{for } q \in \mathbb{N}_n,\ x_q = 0)\big) \\
&\quad \Rightarrow \quad (y \neq \mathbf{0} \Rightarrow x = \mathbf{0}).
\end{aligned}$$

Thus by Proposition 1, T is a uniform insulator for $\mathbb{M}_n(R)$ of size $n^2 m(R)$.

Suppose $\mathbb{M}_n(R)$ is uniformly strongly prime; then there is a nonempty finite set $\{A_{(p)} : p \in \mathbb{N}_{m_n(R)}\}$ with $(B, C \in \mathbb{M}_n(R)$ and for $p \in \mathbb{N}_{m_n(R)},\ BA_{(p)}C = \{\mathbb{O}\}) \Rightarrow (B = \mathbb{O}$ or $C = \mathbb{O})$. This is a right insulator for each nonzero matrix in $\mathbb{M}_n(R)$, so it is a right insulator for each $E_{(11)}a$ where $a \in R\backslash\{0\}$. Applying the argument from the proof of (i), $\{(A_{(p)})_{11} : p \in \mathbb{N}_{m_n(R)}\}$ is a uniform insulator for R of size at most $m_n(R)$. □

The result [7, Theorem 4] that $m_n(D) \leq 2n - 1$ for division rings D is generalised below.

Theorem 3. *Suppose $n, n' \in \mathbb{N}$ and R is a unitary ring. Then $m_{nn'}(R) \leq (2n-1)m_{n'}(R)$.*

Proof. Take a uniform insulator $S' = \{A_{(p)} : p \in \mathbb{N}_{m_{n'}(R)}\}$ for $\mathbb{M}_{n'}(R)$. Let $B_{(p)} = \sum_{k=\max\{1,p-n+1\}}^{\min\{p,n\}} E_{(k,p+1-k)} \in \mathbb{M}_n(R)$ for $p \in \mathbb{N}_{2n-1}$ (these matrices are used in the proof of [7, Theorem 4]), that is, $B_{(1)} = E_{(1,1)}$, $B_{(2)} = E_{(1,2)} + E_{(2,1)}$, $B_{(3)} = E_{(1,3)} + E_{(2,2)} + E_{(3,1)}, \ldots, B_{(n)} = E_{(1,n)} + E_{(2,n-1)} + \ldots + E_{(n,1)}$, $B_{(n+1)} = E_{(2,n)} + E_{(3,n-1)} + \ldots + E_{(n,2)}, \ldots, B_{(2n-1)} = E_{(n,n)}$. It is shown that $S = \{A_{(p,q)} : p \in \mathbb{N}_{2n-1},\ q \in \mathbb{N}_{m_{n'}(R)}\}$ is a uniform insulator for $\mathbb{M}_{nn'}(R)$, where each $A_{(p,q)} \in S$ is the nn' by nn' matrix obtained from $B_{(p)}$ by replacing each entry 0 with the zero n' by n' matrix and replacing each entry 1 with $A_{(q)}$.

For $x, y \in R^{n'n}$, write $y = (y_{(1)}^T \mid y_{(2)}^T \mid \ldots \mid y_{(n)}^T)^T$ with each $y_{(j)} \in R^{n'}$ and similarly for x. The bilinear equation $y^T A_{(p,q)} x = 0$ corresponding to each $A_{(p,q)} \in S$ is $\sum_{k=\max\{1,p-n+1\}}^{\min\{p,n\}} (y_{(k)}^T A_{(q)} x_{(p+1-k)}) = 0$ (given $A_{(p,q)}$, take the sum expressing $B_{(p)}$ in terms of $E_{(k,l)}$ and replace each $E_{(k,l)}$ with $y_{(k)}^T A_{(q)} x_{(l)}$ to obtain the left hand side of $A_{(p,q)}$'s equation).

One uses Proposition 1 repeatedly in the rest of the proof. Assume the equations $y^T A_{(p,q)} x = 0$ hold for some $y \in R^{nn'}\backslash\{\mathbf{0}\}$, $x \in R^{nn'}$. Let $p \in \mathbb{N}_n$ be minimal with $y_{(p)} \neq \mathbf{0}$. By the equations of the matrices $A_{(p,q)}$, $y_{(p)}^T A_{(q)} x_{(1)} = 0$ for $q \in \mathbb{N}_{m_{n'}(R)}$, so $x_{(1)} = \mathbf{0}$ (S' is a uniform insulator). If $x_{(1)}, x_{(2)}, \ldots, x_{(j)} = \mathbf{0}$ for some $j \in \mathbb{N}_{n-1}$ then by the equations of the matrices $A_{(p+j,q)}$, $y_{(p)}^T A_{(q)} x_{(j+1)} = 0$ for $q \in \mathbb{N}_{m_{n'}(R)}$, so $x_{(j+1)} = \mathbf{0}$

(S' is a uniform insulator). By induction, $x = \mathbf{0}$. Therefore S is a uniform insulator for $\mathbb{M}_{nn'}(R)$. □

Example 4. The set $\{A, B\}$ with

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is easily shown to be a uniform insulator for $\mathbb{M}_2(\mathbb{R})$, so $m_6(\mathbb{R}) = m_{3(2)}(\mathbb{R}) \leq (2(3) - 1)m_2(\mathbb{R}) \leq 10$. The proof of Theorem 3 above yields a uniform insulator for $\mathbb{M}_6(\mathbb{R})$ consisting of the following ten matrices, where each $\mathbb{O}$ is the 2 by 2 zero matrix:

$$\left(\begin{array}{c|c|c} A & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} B & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & A & \mathbb{O} \\ \hline A & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & B & \mathbb{O} \\ \hline B & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \end{array}\right),$$

$$\left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & A \\ \hline \mathbb{O} & A & \mathbb{O} \\ \hline A & \mathbb{O} & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & B \\ \hline \mathbb{O} & B & \mathbb{O} \\ \hline B & \mathbb{O} & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & A \\ \hline \mathbb{O} & A & \mathbb{O} \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & B \\ \hline \mathbb{O} & B & \mathbb{O} \end{array}\right),$$

$$\left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & A \end{array}\right), \quad \left(\begin{array}{c|c|c} \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & \mathbb{O} \\ \hline \mathbb{O} & \mathbb{O} & B \end{array}\right).$$

(Later in this article, it is shown that $m_6(\mathbb{R}) = 8$.)

Corollary 5. *Suppose R is a unitary domain and $n \in \mathbb{N}$. Then $m_n(R) \leq 2n - 1$.*

Proof. Take $n' = 1$ in Theorem 3, noting that $m_1(R) = 1$ since $\{1\}$ is a uniform insulator for R. □

3.1. Division rings

Little is known about the value of $m_n(D)$ in the case where D is a noncommutative division ring. This section sheds some light on the case $n = 2$.

The ideas of Proposition 1 are used in the proof of [7, Theorem 3]. The result and argument are adapted here, using ideas from [8].

Proposition 6. *Suppose $A_{(p)}$ ($p \in \mathbb{N}_m$) are matrices in $\mathbb{M}_n(D)$ with D a division ring. Then the following statements are equivalent:*

(i) $\{A_{(p)} : p \in \mathbb{N}_m\}$ is a uniform insulator for $\mathbb{M}_n(D)$.

(ii) For $y \in D^n \backslash \{\mathbf{0}\}$, the matrix

$$Y(y) = \begin{pmatrix} y^T A_{(1)} \\ \hline y^T A_{(2)} \\ \hline \vdots \\ \hline y^T A_{(m)} \end{pmatrix}$$

has right column rank n.

(iii) For $x \in D^n \backslash \{\mathbf{0}\}$, the matrix

$$X(x) = (\, A_{(1)}x \mid A_{(2)}x \mid \ldots \mid A_{(m)}x \,)$$

has left row rank n.

If D is a field, "right column rank" and "left row rank" may each be replaced with "rank".

Proof.

$$\begin{aligned} &\{A_{(p)} : p \in \mathbb{N}_m\} \text{ a uniform insulator for } \mathbb{M}_n(D) \\ \Leftrightarrow \quad & \big(y, x \in D^n,\ y \neq \mathbf{0},\ Y\,(y)x = \mathbf{0} \Rightarrow x = \mathbf{0} \big) \text{ (Proposition 1)} \\ \Leftrightarrow \quad & \left(y, x \in D^n,\ y \neq \mathbf{0},\ \sum_{k=1}^{n} \big(Y(y)_{\cdot k} x_k \big) = \mathbf{0} \Rightarrow x = \mathbf{0} \right) \\ \Leftrightarrow \quad & Y(y) \text{ has right column rank } n \text{ for } y \in D^n \backslash \{\mathbf{0}\}. \end{aligned}$$

Therefore (i) $\Leftrightarrow$ (ii). The proof of (i) $\Leftrightarrow$ (iii) is similar; it uses $y^T X(x)$ instead of $Y(y)x$. □

Theorem 7. *Let D be a division ring. Then $m_2(D)$ is 2 if some equation $wcw + wd - aw - b = 0$, $a, b, c, d \in D, c \neq 0$ has no solution $w \in D$ and is 3 otherwise.*

Proof. By [7, Theorem 4], $m_2(D) \in \{\ 2,\ 3\}$.

Let $A_{(1)}$, $A_{(2)} \in \mathbb{M}_2(D)$ be nonzero and consider the corresponding bilinear equations $y^T A_{(1)} x = 0$, $y^T A_{(2)} x = 0$.

One may assume $(A_{(1)})_{11} \neq 0$ without loss of generality: to achieve this, taking $J = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, one may replace $A_{(1)}$, $A_{(2)}$, y^T, x with $J^r A_{(1)} J^s$, $J^r A_{(2)} J^s$, $y^T J^r$, $J^s x$ respectively, where r, $s \in \mathbb{N}_2$. (The choice $r = s = 2$ leaves everything unchanged; $r = 1$ swaps the rows in each $A_{(p)}$ and swaps the elements of y; $s = 1$ swaps the columns in each $A_{(p)}$ and swaps the elements of x.)

Also, one may assume $A_{(1)} \in \{E_{(11)}, \mathbb{I}\}$ without loss of generality: taking $q' = (A_{(1)})_{22} - (A_{(1)})_{21} (A_{(1)})_{11}^{-1} (A_{(1)})_{12}$ and

$$q = \left\{ \begin{matrix} 1 & q' = 0 \\ q' & q' \neq 0, \end{matrix} \right\}$$

one may replace $A_{(1)}$, $A_{(2)}$, y^T, x with

$$\begin{gathered} \begin{pmatrix} (A_{(1)})_{11}^{-1} & 0 \\ -(A_{(1)})_{21}(A_{(1)})_{11}^{-1} & 1 \end{pmatrix} A_{(1)} \begin{pmatrix} 1 & -(A_{(1)})_{11}^{-1}(A_{(1)})_{12}q^{-1} \\ 0 & q^{-1} \end{pmatrix}, \\ \begin{pmatrix} (A_{(1)})_{11}^{-1} & 0 \\ -(A_{(1)})_{21}(A_{(1)})_{11}^{-1} & 1 \end{pmatrix} A_{(2)} \begin{pmatrix} 1 & -(A_{(1)})_{11}^{-1}(A_{(1)})_{12}q^{-1} \\ 0 & q^{-1} \end{pmatrix}, \\ y^T \begin{pmatrix} (A_{(1)})_{11} & 0 \\ (A_{(1)})_{21} & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & (A_{(1)})_{11}^{-1}(A_{(1)})_{12} \\ 0 & q \end{pmatrix} x \end{gathered}$$

respectively, so that the original $A_{(1)}$ is replaced with $E_{(11)}$ if $q' = 0$ and $\mathbb{I}$ otherwise. (These transformations may be obtained by adapting standard Gaussian elimination to division rings.)

Now let $A_{(2)} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Case I: $A_{(1)} = E_{(11)}$: The bilinear equations are $y_1x_1 = 0$, $y_1ax_1 + y_1bx_2 + y_2cx_1 + y_2dx_2 = 0$. If $y_1 = 0$ ($x_1 = 0$) then the second equation becomes $y_2(cx_1 + dx_2) = 0$ ($(y_1b + y_2d)x_2 = 0$), so the solution set is

$$\left\{ (y, x) \in D^2 \times D^2 : \mathbf{0} \in \left\{ y, x, \begin{pmatrix} y_1 \\ cx_1 + dx_2 \end{pmatrix}, \begin{pmatrix} x_1 \\ y_1b + y_2d \end{pmatrix} \right\} \right\}.$$

There is a nontrivial solution

$$y = e_{(2)}, \qquad x = \left\{ \begin{matrix} (\, -c^{-1}d \quad 1\,)^T & c \neq 0 \\ e_{(1)} & c = 0 \end{matrix} \right\}$$

and so $\{A_{(1)}, A_{(2)}\}$ is not a uniform insulator for $\mathbb{M}_2(D)$.

Case II: $A_{(1)} = \mathbb{I}$: The bilinear equations are $y_1x_1 + y_2x_2 = 0$, $y_1ax_1 + y_1bx_2 + y_2cx_1 + y_2dx_2 = 0$. If $c = 0$ then there is the nontrivial solution $y = e_{(2)}$, $x = e_{(1)}$, so suppose $c \neq 0$. If $y_1 = 0$ then the equations become $y_2x_2 = 0$, $y_2(cx_1 + dx_2) = 0$ and this gives $y_2 = 0$ or $x_2 = 0 = cx_1 + dx_2$, which implies $y = \mathbf{0}$ or $x = \mathbf{0}$; therefore all nontrivial solutions have $y_1 \neq 0$.

Suppose (y, x) is a nontrivial solution and let $w = -y_1^{-1}y_2$. The first equation becomes $x_1 = wx_2$, which implies $x_2 \neq 0$. Substituting $x_1 = wx_2$ into the second equation, one has $wcw + wd - aw - b = 0$. If this equation has a solution w then any (y, x) with $y_2 = -y_1w$, $x_1 = wx_2$ is a solution, there are nontrivial solutions and $\{A_{(1)}, A_{(2)}\}$ is not a uniform insulator for $\mathbb{M}_2(D)$; otherwise there are no nontrivial solutions and $\{A_{(1)}, A_{(2)}\}$ is a uniform insulator for $\mathbb{M}_2(D)$.

Therefore there is a uniform insulator for $\mathbb{M}_2(D)$ of size 2 (that is, $m_2(D) = 2$) iff some equation $wcw + wd - aw - b = 0, a, b, c, d \in D, c \neq 0$ has no solution $w \in D$. □

Observe that if the division ring D of Theorem 7 is commutative (and therefore a field), then the condition of Theorem 7 reduces to the existence of an irreducible polynomial of degree 2 over D which in turn implies the existence of a field extension of dimension 2 over D. This is known to imply $m_2(D) = 2$ [7, Theorem 11].

A version of the Fundamental Theorem of Algebra for the division ring $\mathbb{H}$ of quaternions, proved by Eilenberg and Niven [10, Theorem 1], says that for $n \in \mathbb{N}$, each equation in $\mathbb{H}$ of the form $c_0wc_1w \ldots c_n$ +(finite sum of terms of the form $d_0wd_1w \ldots d_k$ with $k <$
n) $= 0$ is satisfied by some w if the constants c_i are all nonzero. Taking $n = 2$ and $c_0 = c_2 = 1$ in this result and applying Theorem 7, one obtains

Corollary 8. $m_2(\mathbb{H}) = 3$.

3.2. Commutative rings

If R is a commutative ring and $A \in \mathbb{M}_n(R)$, then

$$y^T Ax = \sum_{k=1}^{n} \sum_{l=1}^{n} \big(A_{kl}(y_k x_l)\big) = (\operatorname{vec} A) \cdot \big(\operatorname{vec} yx^T\big),$$

so the equation $y^T Ax = 0$ is equivalent to (vec A) $\cdot z = 0$, which can be seen as a linear equation in the components $z_{n(l-1)+k} = y_k x_l$ of $z = \operatorname{vec} yx^T$ (see [8]). By interpreting bilinear equations as linear ones in this way, one finds an alternative characterisation of $m_n(F)$, F a field.

The following lemma and theorem and the proof of the theorem are adapted from the results and proofs of [6, Theorem 1.3, Lemma 2.2]. Some ideas are rephrased in light of Proposition 1 and the previous paragraph to illustrate a new perspective on the argument.

Lemma 9. *Suppose $n \in \mathbb{N}$, F is a field and $S = \{A_{(k)} : k \in \mathbb{N}_{m_n(F)}\}$ is a uniform insulator for $\mathbb{M}_n(F)$ of smallest possible size. Then S is a linearly independent set.*

Proof. If $n = 1$ the result is trivial ($m_1(F) = 1$ and for $y, x \in F\backslash\{0\}$, $y0x = 0$), so let $n > 1$. Take $A_{(1)} = \sum_{k=2}^{m_n(F)} a_{(k)} A_{(k)}$ where $a_{(k)} \in F$ for $k \in \mathbb{N}_{m_n(F)}\backslash\{1\}$. If $y^T A_{(k)} x = 0$ for $k \in \mathbb{N}_{m_n(F)}\backslash\{1\}$ then $y^T A_{(1)} x = \sum_{k=2}^{m_n(F)} a_{(k)}(y^T A_{(k)} x) = 0$. Thus $\{A_{(k)} : k \in \mathbb{N}_{m_n(F)}\backslash\{1\}\}$ is a uniform insulator for $\mathbb{M}_n(F)$, contradicting the definition of $m_n(F)$. □

Theorem 10. *(See [6, Theorem 1.3].) Suppose $n \in \mathbb{N}$ and F is a field. Then the highest dimension of a subspace S of $\mathbb{M}_n(F)$ such that no matrices in S are of rank 1 is $n^2 - m_n(F)$.*

Proof. Take an arbitrary subspace S of $\mathbb{M}_n(F)$. $\mathbb{M}_n(F)$ is isomorphic to F^{n^2} as a vector space under the isomorphism vec, so $S' = \operatorname{vec} S$ is a subspace of F^{n^2} with

$\dim S' = \dim S = d$. Let B be any matrix in $\mathbb{M}_{(n^2-d)\times n^2}(F)$ with linearly independent rows such that S' is the null space of B. The matrices in $\mathbb{M}_n(F)$ of rank 1 are precisely the matrices of the form vw^T with $v, w \in F^n\backslash\{\mathbf{0}\}$. Letting $y, x \in F^n$ and $z = \operatorname{vec} yx^T$,

$$\begin{aligned}
&(S \text{ has no matrices of rank } 1)\\
\Leftrightarrow\quad &\big(S' \text{ has no vectors of the form vec } vw^T \text{ with } v, w \in F^n\backslash\{\mathbf{0}\}\big)\\
\Leftrightarrow\quad &\big(Bz = \mathbf{0} \Rightarrow (y = \mathbf{0} \text{ or } x = \mathbf{0})\big)\\
\Leftrightarrow\quad &\big((\text{for } i \in \mathbb{N}_{n^2-d},\ B_{i\cdot}z = 0) \Rightarrow (y = \mathbf{0} \text{ or } x = \mathbf{0})\big)\\
\Leftrightarrow\quad &\Big(\big(\text{for } i \in \mathbb{N}_{n^2-d},\ \big(\operatorname{vec}\big(\operatorname{vec}^{-1} B_{i\cdot}^T\big)\big)\cdot z = 0\big) \Rightarrow (y = \mathbf{0} \text{ or } x = \mathbf{0})\Big)\\
\Leftrightarrow\quad &\big(\big\{\operatorname{vec}^{-1} B_{i\cdot}^T : i \in \mathbb{N}_{n^2-d}\big\} \text{ is a uniform insulator for } \mathbb{M}_n(F)\big).
\end{aligned}$$

Thus there is a correspondence between subspaces S of $\mathbb{M}_n(F)$ with no matrices of rank 1 and sets of linearly independent uniform insulators for $\mathbb{M}_n(F)$, where each uniform insulator corresponding to a subspace S of dimension d has size n^2-d. From the definition of $m_n(F)$, $n^2-d \geq m_n(F)$, so $d \leq n^2-m_n(F)$. By Lemma 9, any uniform insulator of size $m_n(F)$ is linearly independent, so it corresponds to a subspace of $\mathbb{M}_n(F)$ of dimension $n^2 - m_n(F)$ with no matrices of rank 1. □

3.3. Involutive fields and formally real fields

It will be proved that the upper bound of $2n-1$ for $m_n(F)$ can be lowered if F is a formally real field.

Recall that an *involution* on a field F is a field automorphism $* : F \to F : a \mapsto a^*$ which is its own inverse. Such a function $*$ has an *associated norm* $\|\cdot\| : F \to F : a \mapsto aa^*$, which will be called *definite* if for any family $\{a_{(k)} : k \in \mathbb{N}_n\} \subseteq F$, $\sum_{k=1}^n \|a_{(k)}\| = 0$ iff for $k \in \mathbb{N}_n$, $a_{(k)} = 0$. The classical prototype of involution with definite associated norm is the conjugate map on $\mathbb{C}$.

Lemma 11. *Suppose $n \in \mathbb{N}$ is given. For each $p \in \mathbb{N}_{2n-2}\backslash\{1\}$, let $C_p = \{(i, j) : i, j \in \mathbb{N}_n,\ i < j,\ i + j = p + 1\}$. Suppose $Z \subseteq \mathbb{N}_n$ and a relation $\sim$ on $\mathbb{N}_n$ satisfy the following conditions:*

(i) $\sim$ is reflexive and symmetric.
(ii) Partial transitivity: $(i, j, k \in \mathbb{N}_n,\ j \notin Z,\ i \sim j,\ j \sim k) \Rightarrow i \sim k$.
(iii) $(i \in Z,\ j \notin Z,\ k \in \mathbb{N}_n,\ i \sim j) \Rightarrow i \sim k$.
(iv) $i, j \in Z \Rightarrow i \sim j$.
(v) For $p \in \mathbb{N}_{2n-2}\backslash\{1\}$, if $i \nsim j$ for at most one $(i, j) \in C_p$ then $i \sim j$ for $(i, j) \in C_p$.

Then for $i, j \in \mathbb{N}_n$, $i \sim j$.

Proof. One inducts on $n \in \mathbb{N}$. For $n = 1$, if $\sim$ satisfies (i) then $1 \sim 1$ and so $i \sim j$ for $i, j \in \mathbb{N}_1$ (whatever Z is).

Assume the result for a particular $n = n_1 \in \mathbb{N}$; the result is shown for $n = n_1 + 1$. Suppose $Z \subseteq \mathbb{N}_{n_1+1}$ and a relation $\sim$ on $\mathbb{N}_{n_1+1}$ satisfy (i) to (v). Three cases are considered.

Case 1: $1 \notin Z$*:* By (i), $1 \sim 1$. Suppose that for some $n_2 \in \mathbb{N}_{n_1}$ and all $i, j \in \mathbb{N}_{n_2}$, $i \sim j$ (this was established for $n_2 = 1$; one inducts on n_2). Then $1 \sim n_2 + 1$ by (v) with $p = n_2 + 1$ and by (i), $n_2 + 1 \sim 1$. Also, $1 \sim i$ for $i \in \mathbb{N}_{n_2}$. By (ii), $n_2 + 1 \sim i$ (and $i \sim n_2 + 1$ by (i)) for $i \in \mathbb{N}_{n_2}$. By (i), $n_2 + 1 \sim n_2 + 1$. Hence $i \sim j$ for $i, j \in \mathbb{N}_{n_2+1}$. By induction on n_2, $i \sim j$ for $i, j \in \mathbb{N}_{n_1+1}$.

Case 2: $1 \in Z$ *and for* $j \notin Z$*,* $1 \nsim j$*:* Suppose that for some $n_2 \in \mathbb{N}_{n_1}$, $\mathbb{N}_{n_2} \subseteq Z$ (this is true for $n_2 = 1$ by assumption; one inducts on n_2). By (iv), $i \sim j$ for $i, j \in \mathbb{N}_{n_2}$. Again by (v) with $p = n_2 + 1$, $1 \sim n_2 + 1$. Since $1 \nsim j$ for $j \notin Z$, $n_2 + 1 \in Z$. Thus $\mathbb{N}_{n_2+1} \subseteq Z$. By induction on n_2, $Z = \mathbb{N}_{n_1+1}$, so by (iv), $i \sim j$ for $i, j \in \mathbb{N}_{n_1+1}$.

Case 3: $1 \in Z$ *and for some* $j \notin Z$*,* $1 \sim j$*:* By (iii), $1 \sim k$ for $k \in \mathbb{N}_{n_1+1}$. Define $Z' = \{i \in \mathbb{N}_{n_1} : i + 1 \in Z\}$ and define a relation $\sim'$ on $\mathbb{N}_{n_1}$ by $i \sim' j \Leftrightarrow (i+1) \sim (j+1)$ for $i, j \in \mathbb{N}_{n_1}$. Then Z' and $\sim'$ satisfy (i) to (v) with "Z", "$\sim$" replaced with "Z'", "$\sim'$" respectively. By the inductive hypothesis, $i \sim' j$ for $i, j \in \mathbb{N}_{n_1}$, that is, $i \sim j$ for $i, j \in \mathbb{N}_{n_1+1} \backslash \{1\}$. Hence $i \sim j$ for $i, j \in \mathbb{N}_{n_1+1}$.

Thus in all cases, the result holds for $n = n_1 + 1$. By induction, the result holds for $n \in \mathbb{N}$. □

Lemma 12. *Let* $n \in \mathbb{N}$*,* $n > 1$ *and let* F *be a field with involution* $*$ *whose associated norm* $\|\cdot\|$ *is definite. For* $x \in F^n$*, let* $x^* \in F^n$ *be the vector with each* $(x^*)_k = (x_k)^*$*. Take* $B_{(p)} = \sum_{k=\max\{1,p-n+1\}}^{\min\{p,n\}} E_{(k,p+1-k)} \operatorname{sgn}(p + 1 - 2k) \in \mathbb{M}_n(F)$ *for* $p \in \mathbb{N}_{2n-2} \backslash \{1\}$*, that is,* $B_{(2)} = E_{(1,2)} - E_{(2,1)}$*,* $B_{(3)} = E_{(1,3)} - E_{(3,1)}$*,* $B_{(4)} = E_{(1,4)} + E_{(2,3)} - E_{(3,2)} - E_{(4,1)}$*,* $B_{(5)} = E_{(1,5)} + E_{(2,4)} - E_{(4,2)} - E_{(5,1)}$*, . . . ,* $B_{(2n-2)} = E_{(n-1,n)} - E_{(n,n-1)}$*. (These are close variants of matrices used in the proof of [7, Theorem 4].) For* $x \in F^n$*, define* $M(x) = (\, x^* \mid B_{(2)}x \mid B_{(3)}x \mid \ldots \mid B_{(2n-2)}x \,) \in \mathbb{M}_{n\times(2n-2)}(F)$*. Then for* $x \in F^n$*, one has* rank $M(x) = n$ *iff* $x \neq \mathbf{0}$*.*

Proof. Given $x \in F^n \backslash \{\mathbf{0}\}$, one has rank $M(x) = n$ iff for $y \in F^n$, $y^T M(x) = \mathbf{0}^T$ implies $y = \mathbf{0}$. It thus suffices to show that for y, $x \in F^n$, $y^T M(x) = \mathbf{0}^T$ implies $y = \mathbf{0}$ or $x = \mathbf{0}$.

Suppose y, $x \in F^n$ satisfy $y^T M(x) = \mathbf{0}^T$. This matrix equation corresponds to

$$\left(y^T M(x)\right)_1^T = y^T x^* = \sum_{k=1}^{n} (y_k x_k^*) = 0,$$

$$\left(y^T M(x)\right)_p^T = y^T B_{(p)} x = \sum_{k=\max\{1,p-n+1\}}^{\min\{p,n\}} \left(y_k x_{p+1-k} \operatorname{sgn}(p + 1 - 2k)\right) = 0$$

(for $p \in \mathbb{N}_{2n-2} \backslash \{1\}$). The equation $(y^T M(x))_p^T = 0$, $p \in \mathbb{N}_{2n-2} \backslash \{1\}$ is equivalent to

$$\sum_{k=\max\{1,p-n+1\}}^{\lfloor p/2\rfloor} \begin{vmatrix} y_k & x_k \\ y_{p+1-k} & x_{p+1-k} \end{vmatrix} = 0.$$

(Here, each pair $y_k x_{p+1-k}$, $-y_{p+1-k} x_k$ in the equation for $(y^T M(x))_p^T$ is combined to form the determinant appearing in the sum. For instance, if $n \geq 5$ then the equation $y_1x_5 + y_2x_4 - y_4x_2 - y_5x_1 = 0$ for $(y^T M(x))_5^T$ becomes $(y_1x_5 - y_5x_1) + (y_2x_4 - y_4x_2) = 0$, that is, $\left|\begin{smallmatrix} y_1 & x_1 \\ y_5 & x_5 \end{smallmatrix}\right| + \left|\begin{smallmatrix} y_2 & x_2 \\ y_4 & x_4 \end{smallmatrix}\right| = 0$.)

Let $Z = \{i \in \mathbb{N}_n : y_i = 0\}$ and define the relation $\sim$ on $\mathbb{N}_n$ by:

$$\text{For } i, j \in \mathbb{N}_n, \quad \left(i \sim j \Leftrightarrow \begin{vmatrix} y_i & x_i \\ y_j & x_j \end{vmatrix} = 0 \right).$$

Z and $\sim$ satisfy conditions (i) to (v) of Lemma 11, so $i \sim j$ for $i, j \in \mathbb{N}_n$ and $(y \mid x)$ has rank at most 1, i.e., there are $a, b \in F$ and $w \in F^n$ with $y = aw$, $x = bw$. Substituting these into $(y^T M(x))^T_1 = 0$, one finds $ab^* \sum_{k=1}^{n} \|w_k\| = 0$. This gives three possibilities:

- $a = 0$, in which case $y = \mathbf{0}$.
- $b = 0$, in which case $x = \mathbf{0}$.
- $\sum_{k=1}^{n} \|w_k\| = 0$, in which case $w = \mathbf{0}$ (since $\|\cdot\|$ is definite) and so $y = x = \mathbf{0}$. □

Theorem 13. *Let F be a field with involution $*$ whose associated norm is definite. Let K be a subfield of F such that K is fixed by $*$ and $[F : K] = n' \in \mathbb{N}$. Also let $n \in \mathbb{N}$, $n > 1$. Then $m_{nn'}(K) \leq (2n-2)n'$.*

Proof. One may assume without loss of generality that the K-vector space $F \subseteq \mathbb{M}_{n'}(K)$ (identify each element of F with its image under some representation $F \to \mathbb{M}_{n'}(K)$). Let $\{\mathbf{B}_{(k)} : k \in \mathbb{N}_{n'}\} \subseteq \mathbb{M}_{n'}(K)$ be a K-basis for F.

Take $w \in K^{nn'}$. For each $i \in \mathbb{N}_n$, define $X_{(i)} = \sum_{k=1}^{n'} \mathbf{B}_{(k)} w_{(i-1)n'+k} \in F$. Since $*$ is a K-algebra automorphism on F, it follows from the Noether–Skolem Theorem that there exists $C \in \mathbb{M}_{n'}(K)$ such that $A^* = CAC^{-1}$ for all $A \in F$; so for $i \in \mathbb{N}_n$, $X_{(i)}^* = \sum_{k=1}^{n'} (C\mathbf{B}_{(k)}C^{-1}) w_{(i-1)n'+k}$.

Suppose $w \neq \mathbf{0}$. Since $\{\mathbf{B}_{(k)} : k \in \mathbb{N}_{n'}\}$ is a K-basis for F, some $X_{(i)} \neq \mathbb{O}$. Put $x \in F^n$ with each $x_i = X_{(i)}$; then $x \neq \mathbf{0}$, so rank $M(x) = n$ by Lemma 12.

From now on, interpret $M(x)$ as a block matrix in $\mathbb{M}_{nn' \times (2n-2)n'}(K)$. Since $[F : K] = n'$, the rank of the block matrix $M(x)$ is nn'.

Since each entry of $M(x)$ is a K-linear combination of the components of w, it follows that each column of $M(x)$ can be expressed in the form Aw for a suitable nn' by nn' matrix A. One can therefore choose a set of matrices $S = \{A_{(p)} : p \in \mathbb{N}_{(2n-2)n'}\} \subseteq \mathbb{M}_{nn'}(K)$ such that $M(x) = (A_{(1)}w \mid A_{(2)}w \mid \dots \mid A_{((2n-2)n')}w)$. Since rank $M(x) = nn'$ whenever $w \neq \mathbf{0}$, one concludes from Proposition 6 that S is a uniform insulator for $\mathbb{M}_{nn'}(K)$ and $m_{nn'}(K) \leq (2n-2)n'$ as required. □

Recall that a field F is called *formally real* if for every family $\{a_{(k)} : k \in \mathbb{N}_n\} \subseteq F$, $\sum_{k=1}^{n} a_{(k)}^2 = 0$ iff for $k \in \mathbb{N}_n$, $a_{(k)} = 0$. Observe that a field F is formally real precisely if the norm associated with the identity involution on F is definite.

Corollary 14. *Suppose F is a formally real field and $n \in \mathbb{N}$, $n > 1$. Then:*

(i) $m_n(F) \leq 2n - 2$. (In particular, $m_2(F) = 2$.)
(ii) $m_{2n}(F) \leq 4n - 4$. (In particular, $m_4(F) = 4$.)

Proof. (i) Take $K = F$ with the identity involution and $n' = 1$ in Theorem 13.

(ii) Apply the Cayley–Dickson construction to the formally real F to obtain a field $E = \{a + b\mathbf{i} : a, b \in F\}$ of dimension 2 over F with $\mathbf{i}^2 = -1$, an involution $* : E \to E : a + b\mathbf{i} \mapsto a - b\mathbf{i}$ that fixes F, and an associated norm $\| \cdot \| : E \to E : a + b\mathbf{i} \mapsto (a + b\mathbf{i})(a + b\mathbf{i})^* = a^2 + b^2$. Since F is formally real, the norm $\| \cdot \|$ on E is easily seen to be definite. Now in Theorem 13, take F, E for K, F respectively and take $n' = 2$.

The special cases $m_2(F) = 2$, $m_4(F) = 4$ are a consequence of the fact that $m_{n'}(D) \geq n'$ for all n' and all division rings D [7, Theorem 4]. □

Remark 15. With reference to the proof of Corollary 14(ii) above, one could try to extend this further, applying the Cayley–Dickson construction again to obtain a division ring $F[\mathbf{i}, \mathbf{j}]$ for an attempted proof that $m_{4n}(F) \leq 8n - 8$ for integers $n > 1$. Unfortunately, this fails. The above results depend on applying Lemma 11 to a relation $\sim$ defined via 2 by 2 determinants. Although determinants are not well defined in division rings which are not fields, the reasonable definition of the 2 by 2 determinant would be $|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}| = ad - cb$ identically, because of the structure of $M(x)$ and the associated bilinear equations. But then the partial transitivity condition (ii) of Lemma 11 fails: consider $(y \mid x)$ with $y_1 = \mathbf{i}$, $y_2 = \mathbf{j}$, $y_3 = \mathbf{ij}$, $x_1 = \mathbf{j}$, $x_2 = \mathbf{i}$, $x_3 = \mathbf{1}$.

4. Multiplication of vectors

There is another interpretation of the types of strong primeness for matrix rings that involves a multiplication operation of vectors.

Proposition 16. *Suppose $n, m \in \mathbb{N}$ and R is a unitary ring. Consider the following conditions for a multiplication function $\odot : (R^n)^2 \to R^m$.*

(i) $\odot$ is left linear in its first argument and right linear in its second argument. That is, for $a \in R, w, x, y \in R^n$,
   - *$(aw + y) \odot x = a(w \odot x) + (y \odot x)$.*
   - *$y \odot (wa + x) = (y \odot w)a + (y \odot x)$.*

(ii) For $y, x \in R^n$, $y \odot x = \mathbf{0} \Rightarrow (y = \mathbf{0}$ or $x = \mathbf{0})$.

(iii) For $x \in R^n$ and $X \in \mathbb{M}_n(R)\backslash\{\mathbb{O}\}$, $(X_{i.} \odot x = \mathbf{0}$ for $i \in \mathbb{N}_n) \Rightarrow x = \mathbf{0}$.
(iv) For $y \in R^n$ and $X \in \mathbb{M}_n(R)\backslash\{\mathbb{O}\}$, $(y \odot X_{.j} = \mathbf{0}$ for $j \in \mathbb{N}_n) \Rightarrow y = \mathbf{0}$.

$m_n(R) \leq m$ (respectively $m_r(\mathbb{M}_n(R)) \leq m$, $m_l(\mathbb{M}_n(R)) \leq m$) iff there is a multiplication function $\odot : (R^n)^2 \to R^m$ such that (i) and (ii) hold (respectively (i) and (iii) hold, (i) and (iv) hold).

Proof. The proof is an application of Proposition 1 and the fact that the functions $\odot : (R^n)^2 \to R^m$ satisfying (i) are precisely the functions $\odot : (R^n)^2 \to R^m$ of the form $(y \odot x)_p = y^T A_{(p)} x$ for y, $x \in R^n$, $p \in \mathbb{N}_m$ for some matrices $A_{(p)} \in \mathbb{M}_n(R)$ (where each $(A_{(p)})_{ij} = (e_{(i)} \odot e_{(j)})_p$). □

The result [6, Theorem 1.2(ii)] that there is an n-dimensional (not necessarily associative) division algebra over a field F precisely when $m_n(F) = n$ is generalised to division rings. Define a *division pseudoalgebra* over a division ring D to be a D-bimodule ${}_DM_D$ with a multiplication $\odot : M^2 \to M$ which is left linear in its first argument, right linear in its second and such that for $y \in M\backslash\{\mathbf{0}\}$, $x \in M$, each of the equations $y \odot w = x$, $w \odot y = x$ has exactly one solution $w \in M$. For $D = F$ a field, this idea coincides with the usual concept of a (not necessarily associative) division algebra over F [7].

Theorem 17. *Suppose $n \in \mathbb{N}$ and D is a division ring. Then there is a division pseudoalgebra over D which is isomorphic to D^n as a D-bimodule precisely when $m_n(D) = n$.*

Proof. By [7, Theorem 4], $m_n(D) = n$ iff $m_n(D) \leq n$. By Proposition 16, $m_n(D) \leq n$ iff there is an operation $\odot : (D^n)^2 \to D^n$, left linear in its first argument and right linear in its second, such that

$$y, x \in D^n, \quad y \odot x = \mathbf{0} \quad \Rightarrow \quad (y = \mathbf{0} \text{ or } x = \mathbf{0}). \tag{1}$$

Suppose $\odot : (D^n)^2 \to D^n$ is left linear in its first argument and right linear in its second. It will be shown that (1) is equivalent to

$$y \in D^n\backslash\{\mathbf{0}\}, \quad x \in D^n \quad \Rightarrow \quad \begin{pmatrix} \text{each of the equations } y \odot w = x,\ w \odot y = x \\ \text{has exactly one solution } w \in D^n \end{pmatrix}. \tag{2}$$

If (2) holds and $y \in D^n\backslash\{\mathbf{0}\}$, $x \in D^n$ satisfy $y \odot x = \mathbf{0}$ then $y \odot \mathbf{0} = y \odot (0\mathbf{0}) = 0\ (y \odot \mathbf{0}) = \mathbf{0}$, so $x = \mathbf{0}$ by (2). Hence (2) $\Rightarrow$ (1).

Assume (1); take $\odot$ to be defined using a uniform insulator $S = \{A_{(p)} : p \in \mathbb{N}_n\}$ for $\mathbb{M}_n(D)$ of size n as in the proof of Proposition 16. Choose $y \in D^n\backslash\{\mathbf{0}\}$. For x, w_1, $w_2 \in D^n$, if $y \odot w_1 = y \odot w_2 = x$ then $y \odot (w_1 - w_2) = \mathbf{0}$, so $w_1 = w_2$ by (1). Using $\odot$'s definition via S and Proposition 6's notation, for $w \in D^n$ one has $y \odot w = Y(y)w$. By Proposition 6, $Y(y)$ has right column rank n, so every $x \in D^n$ can be written as $Y(y)w$

for some $w \in D^n$. Hence $y \odot w = x$ has exactly one solution $w \in D^n$ for $y \in D^n \backslash \{\mathbf{0}\}$, $x \in D^n$. Similarly, the same is true for $w \odot y = x$. Thus (1) ⇒ (2).

Hence $m_n(D) = n$ iff there is an operation $\odot : (D^n)^2 \to D^n$, left linear in its first argument and right linear in its second, satisfying (2); that is, iff D^n can be made into a division pseudoalgebra over D by defining a vector multiplication on it. □

For $D = F$ a field, every n-dimensional vector space over F is isomorphic to F^n, so every n-dimensional division algebra over F is isomorphic to F^n with an appropriate vector multiplication; this proves [6, Theorem 1.2(ii)].

Proposition 16 can be used to obtain an alternative proof of Theorem 13 which is presented below.

Proof. One may assume without loss of generality that the K-vector space $F = K^{n'}$(identify each element of F with its co-ordinate vector with respect to some K-basis for F). The multiplication of the field F is then a commutative operation $\odot : F^2 \to F$ satisfying conditions (i) and (ii) of Proposition 16, so $(y \odot x)_p = y^T X_{(p)} x$ identically for some $X_{(1)}, X_{(2)}, \ldots, X_{(n')} \in \mathbb{M}_{n'}(K)$. Also, $* : F \to F$ is a K-vector space homomorphism, so some $C \in \mathbb{M}_{n'}(K)$ satisfies $x^* = Cx$ identically.

Let $B'_{(1)}$, $B_{(1)}$ be the identity matrices in $\mathbb{M}_n(K)$, $\mathbb{M}_n(F)$ respectively. For $p \in \mathbb{N}_{2n-2} \backslash\{1\}$, take the matrix $B_{(p)} \in \mathbb{M}_n(F)$ from the proof of Lemma 12 and obtain $B'_{(p)} \in \mathbb{M}_n(K)$ by replacing the entries $\mathbf{0}$, $\mathbf{1}$, $-\mathbf{1} \in F$ with 0, 1, $-1 \in K$ respectively. Write $D_{(1)} = C$, $D_{(p)} = \mathbb{I} \in \mathbb{M}_{n'}(K)$ for $p \in \mathbb{N}_{2n-2} \backslash\{1\}$. Take the $(2n-2)n'$ matrices $A_{(p,q)} \in \mathbb{M}_{n'n}(K)$, $p \in \mathbb{N}_{2n-2}$, $q \in \mathbb{N}_{n'}$ with each $A_{(p,q)} = B'_{(p)} \otimes X_{(q)} D_{(p)}$, using the Kronecker tensor product $\otimes$ where for matrices X, Y, the matrix $X \otimes Y$ is obtained from X by replacing each entry X_{ij} with $X_{ij}Y$.

Take $y, x \in K^{n'n}$ and write $y = (y^T_{(1)} \mid y^T_{(2)} \mid \ldots \mid y^T_{(n)})^T$ with each $y_{(i)} \in K^{n'}$, and similarly for x. Consider $y', x' \in F^n$ with components $(y')_i = y_{(i)}$, $(x')_i = x_{(i)}$ for $i \in \mathbb{N}_n$. For $p \in \mathbb{N}_{2n-2}$, write $D_{(p)} \circ x' \in F^n$ where for $i \in \mathbb{N}_n$, $(D_{(p)} \circ x')_i = D_{(p)}(x')_i$.

Suppose y, x satisfy the $(2n-2)n'$ equations $y^T A_{(p,q)} x = 0$. For $p \in \mathbb{N}_{2n-2}$, the n' bilinear equations $y^T A_{(p,q)} x = 0$ together are equivalent to the equation $(y')^T B_{(p)}(D_{(p)} \circ x') = \mathbf{0}$ where matrix multiplication is defined using the field multipli-cation $\odot$ of F. (Each $y^T A_{(p,q)} x = ((y')^T B_{(p)}(D_{(p)} \circ x'))_q$.) Thus $y', x' \in F^n$ satisfy the $2n-2$ equations $(y')^T B_{(p)}(D_{(p)} \circ x') = \mathbf{0}$; that is, $(y')^T (x')^* = \mathbf{0}$ and for $p \in \mathbb{N}_{2n-2} \backslash\{1\}$,$(y')^T B_{(p)} x' = \mathbf{0}$. Taking the matrix $M(x') \in \mathbb{M}_{n \times (2n-2)}(F)$ from Lemma 12, one sees that $(y')^T M(x') = \mathbf{0}$, so by Lemma 12, $y' = \mathbf{0}$ or $x' = \mathbf{0}$. Thus $y = \mathbf{0}$ or $x = \mathbf{0}$.

By Proposition 1, the $(2n-2)n'$ matrices $A_{(p,q)}$ form a uniform insulator for $\mathbb{M}_{n'n}(K)$. □

4.1. The real numbers

A result shown by Bott and Milnor [11, Corollary 1] via deep algebraic–topological theorems says that every (not necessarily associative) division algebra over $\mathbb{R}$ has dimension

1, 2, 4 or 8. In the light of [6, Theorem 1.2(ii)] (or the more general Theorem 17) and a result of van den Berg [7, Theorem 15] which gives $n \in \{ 2, 4, 8\} \Rightarrow m_n(\mathbb{R}) = n$, this means that

Theorem 18. $m_n(\mathbb{R}) = n \Leftrightarrow n \in \{1, 2, 4, 8\}$.

It is proved that for $n \in \mathbb{N}$, $m_n(\mathbb{R}) \geq 2^{\lceil \log_2 n \rceil}$. The argument used is generalised from a proof due to Hatcher [12, Theorem 3.20] of Hopf's celebrated theorem: the dimension of every real division algebra is a power of 2. In the light of [6, Theorem 1.2(ii)] or Theorem 17, this corresponds to the statement that $m_n(\mathbb{R}) = n$ only if n is a power of 2. For easy comparison with Hatcher's proof of Hopf's theorem, notation from that proof is used here. Equivalence classes are denoted by $[\cdot]$.

A full introduction of all the algebraic–topological terms used in the proof of Theorem 19 below, such as projective space $\mathbb{R}P^{\,n}$, the unit sphere S^n and the cohomology ring $H^*(X;\, R)$, would lead this article too far astray. The reader is referred instead to a text such as [12] for the necessary background.

Theorem 19. *For $n \in \mathbb{N}$, $m_n(\mathbb{R}) \geq 2^{\lceil \log_2 n \rceil}$.*

Proof. The result is known for $n \in \{ 1, 2\}$ [7, Theorem 15(ii)]. Take an integer $n \geq 3$, let $m = m_n(\mathbb{R})$ and take the continuous map $u : \mathbb{R}^m \backslash \{\mathbf{0}\} \to S^{m-1} : x \mapsto x/|x|$.

There is a bilinear multiplication $\odot : (\mathbb{R}^n)^2 \to \mathbb{R}^m$ such that for $y, x \in \mathbb{R}^n$ one has the implication $y \odot x = \mathbf{0} \Rightarrow \mathbf{0} \in \{y, x\}$.

Take $g : (S^{n-1})^2 \to S^{m-1}$ so that for $y, x \in S^{n-1}$, $g(y, x) = u(y \odot x)$ (which exists because $y \odot x \neq \mathbf{0}$). Since $\odot$ is bilinear, it is continuous; u is also continuous, so g is continuous too.

Projecting the spheres onto their projective spaces, one has the continuous map $h : (\mathbb{R}P^{n-1})^2 \to \mathbb{R}P^{m-1}$ so that for $y, x \in S^{n-1}$, $h([y], [x]) = [g(y, x)]$. The function h is well defined since for $y, x \in S^{m-1}$, $g(y, -x) = u(y \odot (-x)) = u(-(y \odot x)) = -u(y \odot x) = -g(y, x)$ and similarly $g(-y, x) = -g(y, x)$.

Let $\alpha \in H^1((\mathbb{R}P^{n-1})^2; \mathbb{Z}/2\mathbb{Z})$ (respectively $\beta \in H^1((\mathbb{R}P^{n-1})^2; \mathbb{Z}/2\mathbb{Z})$) be the equivalence class of cocycles from $C_1((\mathbb{R}P^{n-1})^2)$ to $\mathbb{Z}/2\mathbb{Z}$ which take cycles whose projections on the first (respectively second) $\mathbb{R}P^{n-1}$ factor are not boundaries to $[1]$ and all other cycles to $[0]$. Let $\gamma \in H^1(\mathbb{R}P^{m-1}; \mathbb{Z}/2\mathbb{Z})$ be a generator of $H^1(\mathbb{R}P^{m-1}; \mathbb{Z}/2\mathbb{Z})$; γ is the equivalence class of cocycles from $C_1(\mathbb{R}P^{m-1})$ to $\mathbb{Z}/2\mathbb{Z}$ which take boundaries (respectively cycles which are not boundaries) to $[0]$ (respectively $[1]$).

Consider the dual map $h^* : H^1(\mathbb{R}P^{m-1}; \mathbb{Z}/2\mathbb{Z}) \to H^1((\mathbb{R}P^{n-1})^2; \mathbb{Z}/2\mathbb{Z})$; it is shown that $h^*(\gamma) = \alpha + \beta$.

Consider the paths in S^n with opposite endpoints. Images of such paths under the standard quotient map from S^n to $\mathbb{R}P^n$ will be called nontrivial loops; other loops in $\mathbb{R}P^n$ will be called trivial loops.

Suppose the path $\lambda : [0,1] \to S^{n-1}$ has opposite endpoints in S^{n-1}. For $x \in S^{n-1}$, the path $[0,1] \to S^{m-1} : t \mapsto g(\lambda(t),x)$ has opposite endpoints $g(\lambda(0),x)$ and $g(\lambda(1),x) = g(-\lambda(0),x) = -g(\lambda(0),x)$; so h maps each loop in $(\mathbb{R}P^{n-1})^2$ whose projection onto the first (and, similarly, the second) of the two $\mathbb{R}P^{n-1}$ factors is nontrivial and whose projection onto the other $\mathbb{R}P^{n-1}$ factor is constant onto a nontrivial loop in $\mathbb{R}P^{m-1}$.

So the class $h^*(\gamma) \in H^1((\mathbb{R}P^{n-1})^2; \mathbb{Z}/2\mathbb{Z}) = \{0, \alpha, \beta, \alpha+\beta\} \cong (\mathbb{Z}/2\mathbb{Z})^2$ consists of cocycles from $C_1((\mathbb{R}P^{n-1})^2)$ to $\mathbb{Z}/2\mathbb{Z}$ which take each cycle in $(\mathbb{R}P^{n-1})^2$ whose projection onto one of the two $\mathbb{R}P^{n-1}$ factors is not a boundary and whose projection onto the other $\mathbb{R}P^{n-1}$ factor is constant to $[1]$; so $h^*(\gamma) = \alpha + \beta$.

Using the fact that the map h^* on $H^*(\mathbb{R}P^{m-1}; \mathbb{Z}/2\mathbb{Z})$ is a ring homomorphism, it follows that in $H^*((\mathbb{R}P^{n-1})^2; \mathbb{Z}/2\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})[\alpha,\beta]/(\alpha^n, \beta^n)$, one has $0 = h^*(0) = h^*(\gamma^m) = (h^*(\gamma))^m = (\alpha+\beta)^m = \sum_{k=0}^{m} \binom{m}{k} \alpha^k \beta^{m-k}$.

This is equivalent to the statement that $\binom{m}{k}$ is even for each integer $k \in (m-n, n)$, which is true iff $n \leq 2^{\lfloor \log_2 m \rfloor}$, that is, $\log_2 n \leq \lfloor \log_2 m \rfloor$. Now for $a, b \in \mathbb{R}$, $a \leq \lfloor b \rfloor \Leftrightarrow \lceil a \rceil \leq \lfloor b \rfloor \Leftrightarrow \lceil a \rceil \leq b$. Therefore $\lceil \log_2 n \rceil \leq \log_2 m$; hence $2^{\lceil \log_2 n \rceil} \leq m$. $\square$

In particular, taking $k \in \mathbb{N}$, one has $2^{k+1} \leq m_{2^k+1}(\mathbb{R})$ and $2^{k+1} \leq m_{2^k+2}(\mathbb{R})$. By Corollary 14, $m_{2^k+1}(\mathbb{R}) \leq 2^{k+1}$ and $m_{2^k+2}(\mathbb{R}) \leq 2^{k+1}$; so $m_{2^k+1}(\mathbb{R}) = m_{2^k+2}(\mathbb{R}) = 2^{\,k+1}$. Combining this with Corollary 14, [7, Proposition 6, Theorem 15], Theorem 18 and Theorem 3 with $n' \in \{\,2,\,4,\,8\}$, one has

Theorem 20. *For $n \in \mathbb{N}$, $k \in \mathbb{N}$ with $k \geq 4$:*

$$\begin{array}{rcl}
n \in [1, 10] & \Rightarrow & m_n(\mathbb{R}) = 2^{\lceil \log_2 n \rceil} \\
n \in \left[2^{k-1}+3, 2^k-1\right] & \Rightarrow & m_n(\mathbb{R}) \in \left[2^k, \left\{ \begin{array}{ll} 2n-8 & 8 \textit{ divides } n \\ 2n-6 & n \bmod 8 = 7 \\ 2n-4 & n \bmod 8 \in \{2,4,6\} \\ 2n-2 & n \bmod 8 \in \{1,3,5\} \end{array} \right\}\right] \\
n = 2^k & \Rightarrow & m_n(\mathbb{R}) \in \left[2^k+1, 2^{k+1}-8\right] \\
n \in \left\{2^k+1, 2^k+2\right\} & \Rightarrow & m_n(\mathbb{R}) = 2^{k+1}.
\end{array}$$

Remark 21. The fourth point of the previous theorem tells one that the set $\{m_n(\mathbb{R})/n : n \in \mathbb{N}\}$ (contained in $[1,2)$) has 2 as an accumulation point, because $\lim_{k\to\infty} 2^{k+1}/(2^k+1) = 2$. It would be interesting to know whether $\lim_{n\to\infty} m_n(\mathbb{R})/n$ exists. If it does, its value must be 2 in view of the earlier comment.

Acknowledgments

A majority of this article consists of verbatim, virtually verbatim and/or adapted extracts from an essay submitted in partial fulfilment of the requirements for the degree Bachelor of Science Honours in Mathematics in the Faculty of Natural and Agricultural

Sciences, University of Pretoria, 2013 by Henry R. Thackeray. Mr. Thackeray thanks the essay supervisor Prof. John E. van den Berg for his invaluable comments and advice, in particular his ideas in discussions which led to Theorem 3, Theorem 13, Corollary 14(ii) and their effect on Theorem 20, as well as a modification of Lemma 12.

References

[1] J. Lawrence, Primitive group rings, Master's thesis, McGill University, Montreal, Canada, 1973.

[2] J.E. Viola-Prioli, On absolutely torsion-free rings and kernel functors, PhD thesis, Rutgers, The State University of New Jersey, New Brunswick, New Jersey, 1973.

[3] K.R. Goodearl, D. Handelman, J. Lawrence, Strongly Prime and Completely Torsion-Free Rings, Carleton Univ. Math. Ser., vol. 109, Carleton University Press, 1974.

[4] D. Handelman, J. Lawrence, Strongly prime rings, Trans. Amer. Math. Soc. 211 (1975) 209–223.[5] J.E. van den Berg, On uniformly strongly prime rings, Math. Jpn. 38 (6) (1993) 1157–1166.

[6] K.I. Beidar, R. Wisbauer, On uniform bounds of primeness in matrix rings, J. Aust. Math. Soc. 76 (2004) 167–174.

[7] J.E. van den Berg, A note on uniform bounds of primeness in matrix rings, J. Aust. Math. Soc. (Ser. A) 65 (2) (1998) 212–223.

[8] C.R. Johnson, J.A. Link, Solution theory for complete bilinear systems of equations, Numer. Linear Algebra Appl. 16 (2009) 929–934.

[9] D.M. Olson, A uniformly strongly prime radical, J. Aust. Math. Soc. (Ser. A) 43 (1987) 95–102.

[10] S. Eilenberg, I. Niven, The "fundamental theorem of algebra" for quaternions, Bull. Amer. Math. Soc. 50 (1944) 246–248.

[11] J. Milnor, Some consequences of a theorem of Bott, Ann. of Math. 68 (2) (1958) 444–449.

[12] A. Hatcher, Algebraic Topology, Cambridge University Press, Cambridge, United Kingdom, 2002.