

The University of Texas at El Paso  
Department of Mathematical Sciences  
Research Reports Series

El Paso, Texas

Research Report No. 2006-06

# Multiplicative bases in matrix algebras

Carlos de la Mora, Piotr J. Wojciechowski





The University of Texas at El Paso  
Department of Mathematical Sciences  
Research Reports Series

El Paso, Texas

Research Report No. 2006-06

# Multiplicative bases in matrix algebras

Carlos de la Mora, Piotr J. Wojciechowski

**Carlos de la Mora, Piotr J. Wojciechowski:**

*Multiplicative bases in matrix algebras*

**Abstract:** *In a finite-dimensional algebra over a field  $\mathbf{F}$ , a basis  $\mathbf{B}$  is called a multiplicative basis provided that  $\mathbf{B} \cup \{0\}$  forms a semigroup. We will describe all multiplicative bases of  $\mathbf{F}_n$ , the full algebra of  $n \times n$  matrices over a subfield  $\mathbf{F}$  of the real numbers. Every such basis is associated with a nonsingular zero-one matrix via a lattice order on  $\mathbf{F}_n$ . This association is a one-to-one correspondence after identification of isomorphic semigroups and identification of the zero-one matrices that have just permuted rows and columns. This correspondence yields an enumeration method for nonequivalent multiplicative bases of  $\mathbf{F}_n$ . The enumeration is done for  $n \leq 5$ .*

**AMS subject classification:** 15A48; 06F25

**Keywords:** Matrix algebra, zero-one matrix, multiplicative basis, lattice order, conjugacy class, simultaneous similarity

### **Correspondence**

piotrw@utep.edu

### **Acknowledgment**

Partial support of the grant NIH-MARC 3T34 GM008048-20

The University of Texas at El Paso  
Department of Mathematical Sciences  
500 West University, El Paso, TX 79968  
Email: mathdept@math.utep.edu  
URL: <http://www.math.utep.edu>  
Phone: 1.915.747.5761  
Fax: 1.915.747.6502

# 1 Introduction

Let  $R$  be a finite-dimensional algebra over a field  $\mathbf{F}$ . In this paper we will consider special bases of  $R$  that shall be called *multiplicative bases*.

**Definition 1.1.** *A multiplicative basis of a finite-dimensional algebra is a basis  $\mathbf{B}$  such that  $\mathbf{B} \cup \{0\}$  is closed under multiplication.*

In section 2 we will describe all (up to equivalence) multiplicative bases for  $\mathbf{F}_n$ , the full algebra of  $n \times n$  matrices over a subfield  $\mathbf{F}$  of the real numbers. Corollary 2.2 will enable us to set up a strategy to enumerate the multiplicative bases of  $\mathbf{F}_n$ . The general strategy will then be described in section 3. We will use it to find the number of nonequivalent multiplicative bases for  $n = 1, 2, 3, 4$  and 5.

It is worth noticing that in the most general setting of an arbitrary finite-dimensional algebra, if additionally  $\mathbf{B} \cap \mathbf{J}$  is a basis for  $\mathbf{J}$ , the Jacobson radical of the algebra, then we have a *filtered* or *Cartan* basis. The major work on the topic is considered to be Bautista, Gabriel, Roiter and Salmeron [1]. Since the full matrix algebra  $\mathbf{F}_n$  is semisimple, the multiplicative bases considered here are also the filtered bases.

**Example 1.1.** One obvious multiplicative basis is the standard unit basis  $E_{ij}$  of matrices having 1 in the  $ij^{\text{th}}$  entry and zeros elsewhere.

**Example 1.2.** Every finite-dimensional (semi)group-algebra  $\mathbf{F}G$  has a multiplicative basis,  $G$ .

The next example is a generalization of the semigroup algebra. Introduced and discussed by Conrad in [3] and by Conrad and McCarthy in [6] are *generalized semigroup algebras*,  $\Sigma(\Delta, \mathbf{R})$ , for some finite set  $\Delta$  endowed with a *partial associative multiplication*.  $\Sigma(\Delta, \mathbf{R})$  is a real vector space of functions from  $\Delta$  to  $\mathbf{R}$ . The multiplicative structure is inherited from the partial multiplication on  $\Delta$ . Precise definitions can be found in Conrad and McCarthy [6]. We have:

**Example 1.3.** Every finite-dimensional generalized semigroup algebra  $\Sigma(\Delta, \mathbf{R})$ , has a multiplicative basis, namely the set of characteristic functions  $\chi_\delta$ ,  $\delta \in \Delta$ .

Not all finite-dimensional algebras have multiplicative bases.

**Example 1.4.** A  $2n^2$ -dimensional *real* algebra of  $n \times n$  matrices with *complex* entries does not have a multiplicative basis for any  $n = 1, 2, \dots$

This result easily follows from Ma [8]. Should the algebra have a multiplicative basis, it would yield a lattice order of the algebra, which is there proven impossible.

The work in section 2 is based on previous results of *lattice-ordered algebras of matrices* that is mainly contained in Ma and Wojciechowski [11]. We will recall some necessary terms from the theory of *lattice-ordered rings*. The pioneering work in this field is Birkhoff and Pierce [2].

A ring  $R$  is called a lattice-ordered ring if  $R$  is also a lattice, and if the two structures are compatible in the sense that for any  $a, b, c \in R$ ,  $a \leq b \Rightarrow a + c \leq b + c$  (that is to say that  $R$  is an Abelian lattice-ordered group with respect to the addition), and if  $c \geq 0$ , then  $ac \leq bc$  and  $ca \leq cb$ . If additionally  $R$  is an algebra over a totally-ordered field  $\mathbf{F}$ , and  $R \ni a \geq 0$  and  $\mathbf{F} \ni k \geq 0$ , then  $ka \geq 0$ , then  $R$  is a *lattice-ordered algebra over  $\mathbf{F}$* . The *positive cone* of a lattice-ordered ring  $R$  is the set  $R^+ = \{a \in R : a \geq 0\}$ . The positive cone completely determines the order structure. Following the notation from Ma and Wojciechowski [11], by  $(\mathbf{F}_n, P)$  is denoted the lattice-ordered algebra  $\mathbf{F}_n$  with the positive cone  $P$ . If  $R$  and  $S$  are lattice-ordered algebras over the same totally-ordered field, then by a *lattice-ordered algebra isomorphism* (or shortly, an *isomorphism*) between  $R$  and  $S$  we understand an isomorphism between the algebras  $R$  and  $S$  also preserving the order structure. The algebra isomorphism  $\phi : R \rightarrow S$  is the lattice-ordered algebra isomorphism if and only if  $\phi(R^+) = S^+$ .

It is well-known (e.g. Jacobson [7]) that every algebra isomorphism  $\phi : \mathbf{F}_n \rightarrow \mathbf{F}_n$  is *inner*, i.e. is given by  $\phi(A) = CAC^{-1}$  for some nonsingular matrix  $C \in \mathbf{F}_n$ .

Finally, in section 2 we need the idea of an *order-basic* (or shortly, *basic*) element of a lattice-ordered ring. A positive element  $a \in R$  is called *basic* if the set  $\{x \in R : 0 \leq x \leq a\}$  is totally-ordered in  $R$ .

## 2 Structure of multiplicative bases

Let  $\mathbf{B}$  be a multiplicative basis on  $\mathbf{F}_n$ . If we let  $P = \{\sum \alpha_i B_i : \alpha_i \in \mathbf{F}^+, B_i \in \mathbf{B}\}$ , then  $P$  becomes a positive cone of a lattice order on  $\mathbf{F}_n$ . Moreover, the elements of  $\mathbf{B}$  are disjoint order-basic elements. By Theorem 2.1 in Ma and Wojciechowski [11], there exists a nonsingular matrix  $A$  such that the lattice-ordered algebras  $(\mathbf{F}_n, P_A)$  and  $(\mathbf{F}_n, P)$  are isomorphic, where  $P_A$  is the positive cone defined by (II) in section 2 in Ma and Wojciechowski [11], i.e.  $P_A = \sum_{i,j=1}^n \mathbf{F}^+ A_{ij}$  and  $A_{ij} = E_{ij} A^T$ ,  $1 \leq i, j \leq n$  (so the  $i^{\text{th}}$  row of  $A_{ij}$  consists of the  $j^{\text{th}}$  column of  $A$  and other rows consist of zeros.)

Recall that the matrices  $A_{ij}$  multiply according to the rule:

$$A_{ij} A_{rs} = a_{rj} A_{is}$$

**Definition 2.1.** We say that a multiplicative basis  $\mathbf{B}$  and a nonsingular matrix  $A$  are associated when the lattice-ordered algebras described above,  $(\mathbf{F}_n, P_A)$  and  $(\mathbf{F}_n, P)$ , are isomorphic.

Let  $\phi : (\mathbf{F}_n, P_A) \rightarrow (\mathbf{F}_n, P)$  be an isomorphism between the two structures. Then  $\phi(P_A) = P$ , and it is known that an order-basic element has to go on an order-basic element, so for every  $1 \leq i, j \leq n$ ,  $\phi(A_{ij})$  is a positive multiple of an element from  $\mathbf{B}$ . We use this fact to index the elements of  $\mathbf{B}$  and, at the same time, to define the positive constants  $\beta_{ij}$ :

$$\text{let } \phi(A_{ij}) = \beta_{ij}B_{ij} \text{ for every } 1 \leq i, j \leq n \quad (2.1)$$

**Lemma 2.1.** If  $a_{ij} \neq 0$  then  $a_{ij} = \beta_{ij}$ .

*Proof.* We have

$$a_{ij}\beta_{ij}B_{ij} = a_{ij}\phi(A_{ij}) = \phi(A_{ij}^2) = (\phi(A_{ij}))^2 = \beta_{ij}^2B_{ij}^2$$

Since  $\mathbf{B}$  is a multiplicative basis,  $B_{ij}^2$  is in  $\mathbf{B}$  or it is 0. The latter case is impossible since  $a_{ij} \neq 0$ , therefore by the above equality  $B_{ij}^2$  is a scalar multiple of  $B_{ij}$ , and since  $\mathbf{B}$  is a multiplicative basis,  $B_{ij}^2 = B_{ij}$ . Therefore we have  $\beta_{ij}^2B_{ij} = a_{ij}\beta_{ij}B_{ij}$ , and so  $\beta_{ij}^2 = a_{ij}\beta_{ij}$  and thus  $a_{ij} = \beta_{ij}$ .  $\square$

**Lemma 2.2.** For every  $1 \leq i, j, r, s \leq n$ ,  $\frac{\beta_{rj}}{\beta_{rs}} = \frac{\beta_{ij}}{\beta_{is}}$ .

*Proof.* Suppose that  $j$  and  $r$  are given and consider two cases.

Case 1:  $a_{rj} \neq 0$ . We have

$$a_{rj}\beta_{is}B_{is} = \phi(a_{rj}A_{is}) = \phi(A_{ij} \cdot A_{rs}) = \beta_{ij}\beta_{rs}B_{ij} \cdot B_{rs}$$

Since  $a_{rj} \neq 0$ , and since  $\mathbf{B}$  is a multiplicative basis,  $B_{ij}B_{rs} = B_{is}$  and so  $a_{rj}\beta_{is} = \beta_{ij}\beta_{rs}$  and by Lemma 2.1  $\frac{\beta_{rj}}{\beta_{rs}} = \frac{\beta_{ij}}{\beta_{is}}$ .

Case 2:  $a_{rj} = 0$ . Since  $A$  is nonsingular, there is  $k$  such that  $a_{kj} \neq 0$ . By Case 1, for all  $1 \leq i, s \leq n$ ,  $\frac{\beta_{ki}}{\beta_{ks}} = \frac{\beta_{ij}}{\beta_{is}}$ . In particular, for  $i = r$  we have for every  $1 \leq s \leq n$ :  $\frac{\beta_{rj}}{\beta_{rs}} = \frac{\beta_{kj}}{\beta_{ks}}$ . Therefore, for arbitrary  $1 \leq i, s \leq n$ ,  $\frac{\beta_{rj}}{\beta_{rs}} = \frac{\beta_{ij}}{\beta_{is}}$ .  $\square$

**Corollary 2.1.** The matrices  $\{\frac{1}{\beta_{ij}}A_{ij}\}_{i,j=1}^n$  form a multiplicative basis.

*Proof.* For every  $1 \leq i, j \leq n$ , if  $a_{rj} \neq 0$ ,

$$\frac{1}{\beta_{ij}}A_{ij} \cdot \frac{1}{\beta_{rs}}A_{rs} = \frac{1}{\beta_{ij}\beta_{rs}}A_{ij}A_{rs} = \frac{a_{rj}}{\beta_{ij}\beta_{rs}}A_{is} = \frac{\beta_{rj}}{\beta_{ij}\beta_{rs}}A_{is} = \frac{1}{\beta_{is}}A_{is}$$

If  $a_{rj} = 0$ , we obtain the 0 matrix.  $\square$

Now we can prove the fundamental theorem about the multiplicative bases in  $\mathbf{F}_n$ .

**Theorem 2.1.** *Every multiplicative basis of  $\mathbf{F}_n$  is associated with some nonsingular zero-one matrix. Conversely, every nonsingular zero-one matrix is associated with some multiplicative basis.*

*Proof.* Let the multiplicative basis  $\mathbf{B}$  be associated with a nonsingular matrix  $A$ , and let us consider the matrix  $B = (\beta_{ij})$ . Fix  $j, s$  and  $r$  and let  $i = 1, \dots, n$ . By Lemma 2.2 we obtain  $n$  equalities:  $\beta_{ij} = (\frac{\beta_{rj}}{\beta_{rs}})\beta_{is}$ . This shows that the  $j^{\text{th}}$  and the  $s^{\text{th}}$  columns of  $B$  are dependent. Therefore, every two columns of  $B$  are dependent and thus  $B$  has rank 1. Let us rename row one to be:  $\beta_1, \beta_2, \dots, \beta_n$ . We have that for some positive constants  $\lambda_1 = 1, \lambda_2, \dots, \lambda_n$ ,  $\beta_{ij} = \lambda_i \beta_j$ . Now if  $a_{ij} \neq 0$ , by Lemma 2.1  $a_{ij} = \beta_{ij} = \lambda_i \beta_j$ . Let  $M = (m_{ij})$  where  $m_{ij} = 0$  if  $a_{ij} = 0$ , otherwise  $m_{ij} = 1$ . Then the following holds:

$$A = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) M \text{diag}(\beta_1, \beta_2, \dots, \beta_n)$$

Since  $A$  and the diagonal matrices are nonsingular, then the zero-one matrix  $M$  is nonsingular, too. By Theorem 2.2 in Ma and Wojciechowski [11],  $(\mathbf{F}_n, P_A)$  is isomorphic to  $(\mathbf{F}_n, P_M)$ , and thus the multiplicative basis  $\mathbf{B}$  is associated with a nonsingular zero-one matrix.

For the converse, if  $A$  is a nonsingular zero-one matrix, then the matrices  $A_{ij}$ ,  $1 \leq i, j \leq n$  form a multiplicative basis. □

There is no uniqueness of the nonsingular zero-one matrix associated with a given multiplicative basis. Nevertheless there is a unique *class* of nonsingular zero-one matrices associated with a given multiplicative basis.

Let  $\sim$  be a relation on the set of all nonsingular zero-one  $n \times n$  matrices defined by:  $A \sim B$  if and only if there exist  $n \times n$  permutation matrices  $M$  and  $N$  such that  $MAN = B$ . It is easy to check that this is an equivalence relation. Let  $[A]$  denote the equivalence class represented by the matrix  $A$ , and let  $\mathcal{N}_n$  denote the quotient space. We have the following.

**Theorem 2.2.** *If two nonsingular zero-one matrices  $A$  and  $B$  are associated with a multiplicative basis  $\mathbf{B}$ , then  $A \sim B$ . Conversely, if  $A \sim B$  and  $A$  is associated with a multiplicative basis  $\mathbf{B}$ , then so is  $B$ .*

*Proof.* Let  $\mathbf{B}$  be a multiplicative basis that is associated with nonsingular zero-one matrices  $A$  and  $B$ . Then both lattice-ordered algebras  $(\mathbf{F}_n, P_A)$  and  $(\mathbf{F}_n, P_B)$  are isomorphic to  $(\mathbf{F}_n, P)$ , and thus there is an isomorphism between them. Therefore, by Theorem 2.2 (2) from Ma and Wojciechowski [11], there are matrices  $C_1$  and  $C_2$ , each being a product of a permutation matrix and a

diagonal matrix with strictly positive diagonal entries, such that  $B = C_1AC_2$ . Without loss of generality we can further write  $B = EMANF$ , where  $M$  and  $N$  are permutation matrices and  $E$  and  $F$  are diagonal matrices with strictly positive diagonal entries. The matrix  $MAN$  is also a zero-one matrix. Let us use notation  $\text{ent}_{ij}X$  to denote the  $ij^{\text{th}}$  entry of a matrix  $X$ . We have:

$$e_{ii}\text{ent}_{ij}(MAN)f_{jj} = \text{ent}_{ij}E(MAN)F = \text{ent}_{ij}B$$

so  $\text{ent}_{ij}(MAN) = 0$  if and only if  $\text{ent}_{ij}B = 0$ , and thus  $\text{ent}_{ij}(MAN) = 1$  if and only if  $\text{ent}_{ij}B = 1$ . Therefore  $B = MAN$ .

For the converse, let a multiplicative basis  $\mathbf{B}$  be associated with  $A$  and let  $A \sim B$ , where  $A$  and  $B$  are nonsingular zero-one matrices. Again Theorem 2.2 (2) from Ma and Wojciechowski [11] guarantees that  $(\mathbf{F}_n, P_A)$  and  $(\mathbf{F}_n, P_B)$  are isomorphic, and since  $(\mathbf{F}_n, P_A)$  is isomorphic to  $(\mathbf{F}_n, P)$ ,  $(\mathbf{F}_n, P_B)$  is also isomorphic to  $(\mathbf{F}_n, P)$ . Thus  $B$  is also associated with  $\mathbf{B}$ .  $\square$

By the second part of Theorem 2.1, given a nonsingular zero-one matrix  $A$ , it is possible to associate a multiplicative basis. Again, the basis is not unique. Nevertheless we obtain uniqueness of a *class* of multiplicative bases associated with  $A$ .

Note first that if we adjoin a zero matrix to  $\mathbf{B}$ , by putting  $\mathbf{B}_0 = \mathbf{B} \cup \{0\}$ , then  $\mathbf{B}_0$  becomes a semigroup under the matrix multiplication. Let us write  $\mathbf{B} \approx \mathbf{B}'$  provided that the semigroups  $\mathbf{B}_0$  and  $\mathbf{B}'_0$  are isomorphic. The relation  $\approx$  is an equivalence relation on the set of all multiplicative bases, so let  $[\mathbf{B}]$  denote the equivalence class determined by  $\mathbf{B}$  and let  $\mathcal{M}_n$  be the quotient space. We have the following:

**Theorem 2.3.** *Let multiplicative bases  $\mathbf{B}$  and  $\mathbf{B}'$  be both associated with a nonsingular zero-one matrix  $A$ . Then  $\mathbf{B} \approx \mathbf{B}'$ . Conversely, if  $\mathbf{B} \approx \mathbf{B}'$  and a nonsingular zero-one matrix  $A$  is associated with  $\mathbf{B}$  then it is also associated with  $\mathbf{B}'$ .*

*Proof.* Let  $\phi : (\mathbf{F}_n, P_A) \rightarrow (\mathbf{F}_n, P)$  and  $\psi : (\mathbf{F}_n, P_A) \rightarrow (\mathbf{F}_n, P')$  be isomorphisms guaranteed by Theorem 2.1. If we use  $\phi$ ,  $A_{ij}$ ,  $1 \leq i, j \leq n$  and (2.1) to label the elements of  $\mathbf{B}$  as  $B_{ij}$ , and similarly  $\psi$  to define  $B'_{ij}$ , then we have that  $B_{ij}B_{rs} = 0$  if and only if  $A_{ij}A_{rs} = 0$  if and only if  $B'_{ij}B'_{rs} = 0$ , and otherwise, by the argument used in case 1 of the proof of Lemma 2.2,  $B_{ij}B_{rs} = B_{is}$  and  $B'_{ij}B'_{rs} = B'_{is}$ . Thus we obtain  $B_{ij}B_{rs} = B_{is}$  (respectively,  $B_{ij}B_{rs} = 0$ ) if and only if  $B'_{ij}B'_{rs} = B'_{is}$  (respectively,  $B'_{ij}B'_{rs} = 0$ ), which proves that the semigroups  $\mathbf{B}_0$  and  $\mathbf{B}'_0$  are isomorphic.

Conversely, let  $\sigma : \mathbf{B}_0 \rightarrow \mathbf{B}'_0$  be a semigroup isomorphism, and let  $A$  be a nonsingular zero-one matrix associated with  $\mathbf{B}$ . Since  $\mathbf{B}$  is a multiplicative basis, as before, label its elements as  $B_{ij}$ ,  $i, j = 1, \dots, n$ . Extend  $\sigma$  linearly

from  $\mathbf{B}$  to the entire  $\mathbf{F}_n$  to obtain a vector space isomorphism  $\bar{\sigma} : \mathbf{F}_n \rightarrow \mathbf{F}_n$ . Since  $\bar{\sigma}(B_{ij}B_{rs}) = \bar{\sigma}(B_{ij})\bar{\sigma}(B_{rs})$ , for any two matrices  $M$  and  $N$ ,  $\bar{\sigma}(MN) = \bar{\sigma}(M)\bar{\sigma}(N)$ , and  $\bar{\sigma}$  is a ring homomorphism. Obviously  $\bar{\sigma}(\mathbf{B}) = \mathbf{B}'$ , so it is a lattice-ordered algebra isomorphism. Thus the algebras  $(\mathbf{F}_n, P)$  and  $(\mathbf{F}_n, P')$  are isomorphic, so  $(\mathbf{F}_n, P')$  is isomorphic to  $(\mathbf{F}_n, P_A)$ , and therefore  $\mathbf{B}'$  is associated with  $A$ . □

**Corollary 2.2.** *The number of pairwise nonequivalent multiplicative bases is equal to the number of pairwise nonequivalent nonsingular zero-one matrices, i.e.  $|\mathcal{M}_n| = |\mathcal{N}_n|$ .*

*Proof.* By Theorem 2.1 a nonsingular zero-one matrix is associated with some multiplicative basis  $\mathbf{B}$ .

Consider the assignment  $\Phi : \mathcal{N}_n \rightarrow \mathcal{M}_n$  defined by  $\Phi([A]) = [\mathbf{B}]$  provided that the nonsingular zero-one matrix  $A$  is associated with the multiplicative basis  $\mathbf{B}$ . By the second part of Theorem 2.3 if  $A$  is associated with  $\mathbf{B}$ , then  $A$  is also associated with every element from  $[\mathbf{B}]$ . Moreover, if  $A$  is associated with another basis  $\mathbf{B}'$ , then by the first part of Theorem 2.3,  $\mathbf{B}' \in [\mathbf{B}]$ . Therefore the mapping  $\phi(A) = [\mathbf{B}]$  is well-defined.

By the second part of Theorem 2.2, if  $A' \in [A]$ , then  $A'$  is associated with  $\mathbf{B}$ , so we have  $\phi(A') = [\mathbf{B}]$ . Therefore, the mapping  $\Phi$  is well-defined. It is onto by the first part of the Theorem 2.1. By the first part of Theorem 2.2, the mapping  $\Phi$  is one-to-one. □

We will end this section with a characterization of multiplicative bases by pairs of sets of linearly independent vectors.

**Theorem 2.4.**  *$\mathbf{B}$  is a multiplicative basis of  $\mathbf{F}_n$  if and only if there exist two sets of linearly independent vectors  $u_1, \dots, u_n$  and  $v_1, \dots, v_n$  such that*

$$\mathbf{B} = \{u_i v_j^T\} \text{ with } v_j^T u_i = 0 \text{ or } 1, \text{ for } i, j = 1, \dots, n$$

*Proof.* Let  $\mathbf{B}$  be a multiplicative basis. By Theorem 2.1,  $\mathbf{B}$  is associated with some nonsingular zero-one matrix  $A$ . Therefore there is an algebra isomorphism mapping the set  $\{A_{ij}\}$  onto  $\mathbf{B}$ . Recall that  $A_{ij} = e_i(\text{col}_j A)^T$  for  $i, j = 1, \dots, n$ . Since the isomorphism is an inner automorphism of  $\mathbf{F}_n$ , for some nonsingular matrix  $C$ ,  $\mathbf{B} = \{C e_i (\text{col}_j A)^T C^{-1} : i, j = 1, \dots, n\}$ . If we now let  $u_i = C e_i$  for  $i = 1, \dots, n$  and  $v_j = (C^{-1})^T (\text{col}_j A)$  for  $j = 1, \dots, n$ , then the sets  $\{u_i : i = 1, \dots, n\}$  and  $\{v_j : j = 1, \dots, n\}$  are linearly independent and

$$v_j^T u_i = (\text{col}_j A)^T C^{-1} C e_i = (\text{col}_j A)^T e_i \in \{0, 1\}$$

Conversely, if two linearly independent sets of vectors  $u_1, \dots, u_n$  and  $v_1, \dots, v_n$  are given, then it is well-known that the set of matrices  $\{u_i v_j^T : i, j = 1, \dots, n\}$  forms a basis in the vector space  $\mathbf{F}_n$ . If additionally,  $v_j^T u_i \in \{0, 1\}$  then

$$u_i v_j^T u_r v_s^T = (v_j^T u_r) u_i v_s^T \in \{0, u_i v_s^T\}$$

and thus the set  $\{u_i v_j^T : i, j = 1, \dots, n\}$  is a multiplicative basis in  $\mathbf{F}_n$  □

### 3 Enumeration of multiplicative bases

Theorem 2.2 from the last section enables us to determine the number of nonequivalent multiplicative bases in  $\mathbf{F}_n$ .

Let  $\Omega_n$  denote the set of all nonsingular zero-one  $n \times n$  matrices. Following the idea of Cherniavsky and Sklarz [5], allow the group  $S_n \times S_n$  act on  $\Omega_n$  by:

$$(\pi, \sigma) \cdot A = [\pi]A[\sigma]^{-1}$$

where  $\sigma, \pi \in S_n$  and  $[\pi]$  denotes the permutation matrix associated with the natural embedding of  $S_n$  into  $GL_n(\mathbf{F})$  and  $A \in \Omega_n$ .

For the next theorem, we need the following notation:

$$c_{(\pi, \sigma)} = |\{A \in \Omega_n : [\pi]A[\sigma]^{-1} = A\}|$$

Also let  $\bar{\pi} = \{\rho\pi\rho^{-1} : \rho \in S_n\}$ , so that  $\bar{\pi}$  be the *conjugacy class* of the permutation  $\pi$ .

The following theorem serves as the enumeration means for the multiplicative bases in  $\mathbf{F}_n$ .

**Theorem 3.1.**

$$|\mathcal{N}_n| = \frac{1}{n!^2} \sum_{\bar{\pi}} |\bar{\pi}|^2 c_{(\pi, \pi)}$$

*Proof.* By theorem 2.2,  $|\mathcal{N}_n|$  is equal to the number of orbits of the action of the group  $S_n \times S_n$  on  $\Omega_n$  defined above. By the well-known Cauchy-Frobenius lemma,

$$|\mathcal{N}_n| = \frac{1}{|S_n \times S_n|} \sum_{(\tau, \sigma) \in S_n \times S_n} c_{(\tau, \sigma)} = \frac{1}{n!^2} \sum_{(\tau, \sigma) \in S_n \times S_n} c_{(\tau, \sigma)}$$

By Theorem 4.5 from Cherniavsky and Sklarz [5],  $c_{(\tau, \sigma)} = c_{(\pi, \pi)}$  if  $\tau$  and  $\sigma$  belong to the conjugacy class of  $\pi$ , and otherwise, when  $\tau$  and  $\sigma$  do not belong to a common conjugacy class,  $c_{(\tau, \sigma)} = 0$ . Therefore,

$$|\mathcal{N}_n| = \frac{1}{n!^2} \sum_{\bar{\pi}} \sum_{\tau, \sigma \in \bar{\pi}} c_{(\tau, \sigma)} = \frac{1}{n!^2} \sum_{\bar{\pi}} |\bar{\pi}|^2 c_{(\pi, \pi)}$$

□

With  $|\mathcal{N}_1|$  being obviously 1, we will apply the above theorem for the enumeration of the nonequivalent multiplicative bases for  $n = 2, 3, 4, 5$ .

Note first that for any  $n$ ,  $c_{(e,e)}$  is equal to the number of nonsingular  $n \times n$  zero-one matrices, so that  $c_{(e,e)} = A055165(n)$  (see [12]). Moreover, in order to compute  $c(\pi, \pi)$ , we must consider all non-singular zero-one matrices  $A = (a_{ij})$  satisfying  $[\pi]A[\pi]^{-1} = A$  and thus equivalently

$$a_{ij} = (a_{\pi(i)\pi(j)}) \text{ for } i, j = 1, \dots, n \quad (3.1)$$

**Case  $n = 2$ .**

We have two conjugacy classes  $\bar{e}$  and  $\overline{(1, 2)}$ , with  $|\bar{e}| = 1$ ,  $|\overline{(1, 2)}| = 1! \binom{2}{2} = 1$ ,  $c_{(e,e)} = A055165(2) = 6$ .

In order to find the value for  $c_{((1,2),(1,2))}$  the formula 3.1 applied to the permutation  $(1, 2)$  yields the matrices of the form

$$\begin{bmatrix} x & y \\ y & x \end{bmatrix}$$

which in turns gives two non-singular zero-one matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

so  $c_{((1,2),(1,2))} = 2$  and

$$|\mathcal{N}_2| = \frac{1^2 \cdot 6 + 1^2 \cdot 2}{2!^2} = 2$$

Two nonequivalent zero-one nonsingular matrices can be taken to be:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Note that every multiplicative basis in  $\mathbf{F}_2$  is associated with one of the above two matrices.

**Case  $n = 3$ .**

We have the following conjugacy classes  $\bar{e}$ ,  $\overline{(1, 2)}$  and  $\overline{(1, 2, 3)}$ , with  $|\bar{e}| = 1$ ,  $|\overline{(1, 2)}| = 1! \binom{3}{2} = 3$ ,  $|\overline{(1, 2, 3)}| = 2! \binom{3}{3} = 2$ , and  $c_{(e,e)} = A055165(3) = 174$ .

From the formula 3.1, the matrices invariant under the action of  $((1, 2), (1, 2))$  are of the form:

$$A = \begin{bmatrix} x & y & z \\ y & x & z \\ w & w & t \end{bmatrix}$$

In order to find  $c_{((1,2),(1,2))}$ , we used Mathematica 5.1 software to count the number of solutions of the inequality:

$$\det A \neq 0 \text{ with } x, y, z, t \in \{0, 1\}$$

by executing the code

```
Length[Solve[{Det[A] != 0, x==0 || x==1,y==0 || y==1,z==0 ||
z==1,w==0 || w==1,t==0 || t==1},{x,y,z,w,t}]]
```

The result is  $c_{((1,2),(1,2))} = 10$ .

The matrices invariant under the action of  $((1, 2, 3), (1, 2, 3))$  are of the form:

$$\begin{bmatrix} x & y & z \\ z & x & y \\ y & z & x \end{bmatrix}$$

Similarly as before we obtain  $c_{((1,2,3),(1,2,3))} = 6$ .

Therefore

$$|\mathcal{N}_3| = \frac{1^2 \cdot 174 + 3^2 \cdot 10 + 2^2 \cdot 6}{3!^2} = 8$$

Below we give a set of all representatives of the eight pairwise nonequivalent classes.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

In order to check that these matrices are indeed pairwise nonequivalent, following the idea of Cherniavsky and Bagno [4] section 4, one can calculate the number of nonzero entries in each row and column of the matrices. So let  $\text{rowset}(A) = \{k_1, k_2 \cdots k_n\}$  where  $k_i = \sum_{j=1}^n a_{ij}$ , and let  $\text{columnset}(A) = \{t_1, t_2 \cdots t_n\}$  where  $t_j = \sum_{i=1}^n a_{ij}$ . The *columnset* and *rowset* are easily seen to be invariant under the group action. In other words  $\text{rowset}((\pi, \sigma) \cdot A) = \text{rowset}(A)$  and  $\text{columnset}((\pi, \sigma) \cdot A) = \text{columnset}(A)$ . The pairs  $(\text{rowset}, \text{columnset})$  are different for each of the eight matrices.

Note that every multiplicative basis in  $\mathbf{F}_3$  is associated with one of the above eight matrices.

**Case  $n = 4$ .**

We have the following conjugacy classes  $\bar{e}$ ,  $\overline{(1, 2)}$ ,  $\overline{(1, 2, 3)}$ ,  $\overline{(1, 2)(3, 4)}$ ,  $\overline{(1, 2, 3, 4)}$ , with  $|\bar{e}| = 1$ ,  $|\overline{(1, 2)}| = 1!\binom{4}{2} = 6$ ,  $|\overline{(1, 2, 3)}| = 2!\binom{4}{3} = 8$ ,  $|\overline{(1, 2)(3, 4)}| = \frac{1}{2!}\binom{4}{2} = 3$ ,  $|\overline{(1, 2, 3, 4)}| = 3!\binom{4}{4} = 6$ , and  $c_{(e,e)} = A055165(4) = 22560$ .

From the formula 3.1, the matrices invariant under the corresponding actions are of the forms given below. The number of the zero-one nonsingular matrices of each of these forms, calculated using the analogous computer code as in the case  $n = 3$ , is written under the matrices.

The matrices invariant under the action of  $((1, 2), (1, 2))$  are of the form:

$$\begin{bmatrix} x & y & z & l \\ y & x & z & l \\ w & w & t & s \\ u & u & m & r \end{bmatrix}$$

$$c_{((1,2),(1,2))} = 264$$

The matrices invariant under the action of  $((1, 2, 3), (1, 2, 3))$  are of the form:

$$\begin{bmatrix} x & y & z & l \\ z & x & y & l \\ y & z & x & l \\ m & m & m & r \end{bmatrix}$$

$$c_{((1,2,3),(1,2,3))} = 30$$

The matrices invariant under the action of  $((1, 2)(3, 4), (1, 2)(3, 4))$  are of the form:

$$\begin{bmatrix} x & y & z & m \\ y & x & m & z \\ t & l & r & n \\ l & t & n & r \end{bmatrix}$$

$$c_{((1,2)(3,4),(1,2)(3,4))} = 96$$

The matrices invariant under the action of  $((1, 2, 3, 4), (1, 2, 3, 4))$  are of the form:

$$\begin{bmatrix} x & y & z & t \\ t & x & y & z \\ z & t & x & y \\ y & z & t & x \end{bmatrix}$$

$$c_{((1,2,3,4),(1,2,3,4))} = 8$$

We tabulate the results:

Permutation class	Number of elements in the class	Number of fixed matrices
$\bar{e}$	1	$A055165(4) = 22560$
$\overline{(1, 2)}$	$\binom{4}{2} = 6$	264
$\overline{(1, 2, 3)}$	$2! \binom{4}{3} = 8$	30
$\overline{(1, 2)(3, 4)}$	$\frac{1}{2!} \binom{4}{2} = 3$	96
$\overline{(1, 2, 3, 4)}$	$3! \binom{4}{4} = 6$	8

Therefore,

$$|\mathcal{N}_4| = \frac{22560 + 6^2 \cdot 264 + 8^2 \cdot 30 + 3^2 \cdot 96 + 6^2 \cdot 8}{4!^2} = 61$$

We conclude that there are 61 pairwise nonequivalent multiplicative bases.

**Case  $n = 5$ .**

We have tabulated the permutation classes and the corresponding numbers in the table below. The computations were done again using Mathematica with the code analogous to the ones before. This time we will not list the matrices invariant under the group action resulting from each permutation.

Permutation class	Number of elements in the class	Number of fixed matrices
$\bar{e}$	1	$A055165(5) = 12514320$
$\overline{(1, 2)}$	$1! \binom{5}{2} = 10$	31920
$\overline{(1, 2, 3)}$	$2! \binom{5}{3} = 20$	792
$\overline{(1, 2)(3, 4)}$	$\frac{1}{2!} \binom{5}{2} \binom{3}{2} = 15$	2256
$\overline{(1, 2, 3, 4)}$	$3! \binom{5}{4} = 30$	40
$\overline{(1, 2, 3, 4, 5)}$	$4! \binom{5}{5} = 24$	30
$\overline{(1, 2, 3)(4, 5)}$	$2! \binom{5}{3} = 20$	48

We conclude that the number of pairwise nonequivalent multiplicative bases in  $\mathbf{F}_5$  is:

$$|\mathcal{N}_5| = \frac{12514320 + 10^2 \cdot 31920 + 20^2 \cdot 792 + 15^2 \cdot 2256 + 30^2 \cdot 40 + 24^2 \cdot 30 + 20^2 \cdot 48}{5!^2} = 1153$$

## 4 Example of an extension to a multiplicative basis

It follows immediately from Theorem 2.1 that every element of a multiplicative basis is a rank one idempotent or a rank one nilpotent (of index 2). It is natural to ask whether one should expect that a linearly independent set

of rank one nilpotents and/or idempotents forming a semigroup with zero, extends to a full multiplicative basis of  $\mathbf{F}_n$ .

Generally, the answer is negative.

**Example 4.1.** In  $\mathbf{F}_4$  consider the following three matrices:  $e_1(e_3 + e_4)^T$ ,  $e_2e_3^T$  and  $(e_1 + e_2)e_4^T$ . The multiplication on the set of these matrices is zero, and they are linearly independent. However the set  $e_1, e_2, e_1 + e_2$  is linearly dependent. Since the presentation of a rank 1 matrix as an outer product  $uv^T$  is unique up to scalar multiples, the above three matrices cannot be extended to a multiplicative basis of  $\mathbf{F}_4$  by Theorem 2.4.

Nevertheless, extensions to multiplicative bases are possible under some more restrictive conditions.

**Lemma 4.1.** *Let  $k \leq n$  and  $S = \{A_1, A_2, \dots, A_k\}$  be a set of linearly independent matrices in  $\mathbf{F}_n$  having zeros everywhere except the first row and 1 in the  $(1, 1)$  entry. Then  $S$  can be extended to a multiplicative basis of  $\mathbf{F}_n$ .*

*Proof.* The nonzero rows of the matrices from  $S$  are linearly independent in  $\mathbf{F}^n$ . If the number  $k < n$ , then let us first complete this set of vectors to such basis of  $\mathbf{F}^n$  that each basic vector has 1 in the first component. Then without loss of generality, we can assume that  $k = n$ .

Let  $C = \sum_{i=1}^n E_{i1}A_i - (\sum_{i=2}^n E_{i1})A_1$ . Since  $C$  was obtained from a nonsingular matrix consisting of the linearly independent vectors beginning with 1 by an elementary column operation,  $\det C \neq 0$ . Since  $A_jA_i = A_i$  we have that  $CA_i = A_i$  for every  $i = 1, \dots, n$ . Also,  $E_{11}C = E_{11}A_1 = A_1$  and  $(E_{11} + E_{1i})C = A_1 + E_{1i}E_{i1}A_i - E_{1i}E_{i1}A_1 = A_1 + A_i - A_1 = A_i$ . This proves that the matrices  $A_i, i = 1, \dots, n$  are simultaneously similar with the matrices  $E_{11}, E_{11} + E_{1i}, i = 2, \dots, n$ . The latter ones extend to a multiplicative basis

of  $\mathbf{F}^n$  given by the nonsingular 0-1 matrix 
$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & 1 \end{bmatrix} \quad \square$$

**Theorem 4.2.** *Let  $S$  be a set of linearly independent idempotent matrices, each of rank 1, having a common eigenvector  $x$  associated with the eigenvalue 1. Then the set  $S$  can be extended to a multiplicative basis of  $\mathbf{F}_n$ .*

*Proof.* Let  $U$  be any orthogonal matrix with  $x$  as its first column. Then for every  $A \in S$  there exists a  $1 \times n - 1$  matrix  $P$  and a  $n - 1 \times n - 1$  matrix  $A'$  such that  $U^{-1}AU = \begin{bmatrix} 1 & P \\ 0 & A' \end{bmatrix}$  (cf. Mirsky [9], Ch. 10.6). But  $U^{-1}AU$  has rank 1, so  $A' = 0$ . Therefore the matrices  $\{U^{-1}AU : A \in S\}$  satisfy the assumptions of Lemma 4.1 and thus extend to a multiplicative basis, and thus so do the matrices from  $S$ .  $\square$

Note that we have also shown that there are at most  $n$  matrices in  $S$ , and that they multiply according to the rule  $AB = B$ .

## References

- [1] R. Bautista, P. Gabriel, A. Roiter and L. Salmeron, *Representation-finite algebras and multiplicative bases* Invent.-Math., (1985), 217-285.
- [2] G. Birkhoff and R. S. Pierce, *Lattice-ordered rings*, An. Acad. Brasil. Ci. 28 (1956), 41-69.
- [3] P. Conrad, *Generalized semigroup rings*, J. Indian Math. Soc. 21, 73-95 (1957).
- [4] Y. Cherniavsky and E. Bagno, *Permutation representations on invertible matrices*, arXiv:math.RT/0411556v1 24 NOV 2004.
- [5] Y. Cherniavsky and M. Sklarz, *On conjugation action of  $S_n$  on invertible matrices*, arXiv:math.CO/0411554v1 24 Nov 2004.
- [6] P. Conrad and P. McCarthy, *The structure of  $f$ -algebras*, Math. Nachr., 58 (1973), 169-191.
- [7] N. Jacobson, *Lectures in Abstract Algebra, Vol. II*, Van Nostrand, Princeton, N. J., (1952).
- [8] J. Ma, *Finite dimensional simple algebras that do not admit a lattice order*, Comm. in Algebra, 32 (2004), 1615-1617.
- [9] L. Mirsky *An Introduction to Linear Algebra*, Dover 1990.
- [10] J. Ma and P. Wojciechowski, *A proof of Weinberg's conjecture on lattice-ordered matrix algebras*, Pro. Amer. Math. Soc., 130 (2002) no. 10, 2845-2851.
- [11] J. Ma and P. Wojciechowski, *Lattice orders on matrix algebras*, Algebra Univers. 47 (2002), 435-441.
- [12] On-line Encyclopedia of Integer Sequences, <http://www.research.att.com/njas/sequences/A055165>