Centrum voor Wiskunde en Informatica
REPORT*RAPPORT*

A partial classification of primes in the positive matrices and in the doubly stochastic matrices

G. Picci, J.M. van den Hof and J.H. van Schuppen

Department of Operations Reasearch, Statistics, and System Theory

BS-R9535 1995

Report BS-R9535
ISSN 0924-0659

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

A Partial Classification of Primes in the Positive Matrices and in the Doubly Stochastic Matrices

G. Picci

Dipartimento di Elettronica e Informatica, Universitá di Padova,
Via Gradenigo 6/a, 35131 Padova, Italy
picci@dei.unipd.it

J.M. van den Hof and J.H. van Schuppen

CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
jmhof@cwi.nl and J.H.van.Schuppen@cwi.nl

Abstract

The algebraic structure of the set of square positive matrices is that of a semi-ring. The concept of a prime in the positive matrices has been introduced. A few examples of primes in the positive matrices are known but there is no general classification. In this paper a partial classification of primes in the positive matrices and in the doubly stochastic matrices is presented. The classification of primes in the doubly stochastic matrices is reduced to the classification of solutions to an index equation and a linear equation over a latin square.

AMS Subject Classification (1991): 15A48, 15A23, 15A51.
Keywords and Phrases: Semi-ring, prime, positive matrix, doubly stochastic matrix, latin square.
Note: Report has been submitted for publication elsewhere.

1 Introduction

The purpose of this paper is to present results on the classification of primes in the positive matrices and in the doubly stochastic matrices.

The motivation of the authors for the study of positive linear algebra lies in problems of the research area of control and systems theory. The stochastic realization problem for finite-valued processes, see [22], is of interest to signal processing. In the literature one also speaks of the realization problem for the hidden Markov model, for a partially observed Markov chain, and for a finite stochastic system. A positive linear system is a dynamical system as understood in systems and control in which inputs, states, and outputs take positive values. The realization problem for this class of linear systems is of interest to compartmental analysis and to economics. The main question for these problems is the characterization of minimality for these systems. This question reduces to a problem of positive linear algebra, see [22]. For an entry into the literature on the second class of systems see [1].

The concept of a prime in the positive matrices has been defined in a paper by D.J. Richman and H. Schneider in 1974, see [23]. The algebraic structure of a semi-ring, in particular that of a monoid with respect to multiplication, allows one to define a prime

in the positive matrices. Several examples and special classes of primes in the positive matrices have been published, see [2, Sec. 3.4] and [23]. Primes in the Boolean matrices were explored in [7]. No complete classification of primes in the positive matrices is known. There is thus a need for such a classification and for the development of the algebraic theory of positive matrices. The use of a classification of these primes for the questions of control and system theory requires further study.

A summary of the results follows. A prime in the positive matrices is shown to be monomially equivalent to the direct sum of an identity matrix and of an indecomposable doubly stochastic matrix. The classification of primes in the doubly stochastic matrices is reduced to the classification of solutions of an index equation and of a linear equation over a latin square. The index equation can be solved in a straightforward manner. The linear equation over a latin square requires analytic solvability conditions that grow in complexity with the dimensions of the problem. A procedure to construct all primes in the doubly stochastic matrices is described. Examples of primes in the doubly stochastic matrices are presented, some of which are doubly stochastic circulants. The algebraic structure of the subclass of positive matrices will be useful to positive linear algebra and to control and system theory.

An outline of the paper by sections follows. Section 2 contains definitions and a problem formulation. Results of the classification of primes in the positive matrices are presented in Section 3 and of primes in the doubly stochastic matrices in Section 4. Concluding remarks are made in Section 5. The appendices contain various results of a technical character. Definitions and results on permutation matrices are presented in Appendix A, on circulants in Appendix B, on latin squares in Appendix C, and on doubly stochastic matrices in Appendix F. The solvability of a linear equation over a latin square is discussed in Appendix D, that of index equations in Appendix E, and the proofs for primes in the doubly stochastic matrices are presented in Appendix G.

Primes in the doubly stochastic circulants are studied in the paper [21].

2 Problem formulation

In this section a prime in the positive matrices is defined and the problem is posed of classifying all such primes.

2.1 Definitions

Positive matrices may be regarded either as matrices, as elements of a semi-ring, or as convex polyhedral cones. The relationships between the matrix, the algebraic, and the geometric approach is extremely useful. Sources on positive matrices are [2, 3, 5, 17].

In this paper the set $R_+ = [0, \infty)$ is called the set of *positive real numbers* and $(0, \infty)$ the set of *strictly positive real numbers*. This terminology is used in [9, 2.2]. Let $Z_+ = \{1, 2, \ldots\}$ denote the set of the positive integers and $N = \{0, 1, \ldots\}$ the set of the *natural numbers*. For $n \in Z_+$ let $Z_n = \{1, 2, \ldots, n\}$ and $N_n = \{0, 1, 2, \ldots, n\}$. Denote by R_+^n the set of n-tuples of the positive real numbers. The tuple (R_+, R_+^n) will be called a vector space with the understanding that R_+ does not have an inverse with respect to addition. Denote the *simplex* in R_+^n by

$$S_+^n = \Big\{ x \in R_+^n | \sum_{i=1}^{n} x_i = 1 \Big\}.$$

The set $R_+^{k\times m}$ of matrices over R_+ will be called the set of *positive matrices* of size k by m.

Definition 2.1 *A vector $a \in R_+^n$ is said to be of* order k *and this is denoted by $n(a) = k$ if exactly k elements of a are strictly positive. The indices of the strictly positive elements of such a vector are denoted by*

$$i(a) = (i_1, i_2, \ldots, i_k) \subset Z_n.$$

Denote for $a \in R_+^n$ by $a_r = a|_{i(a)} \in R_+^{n(a)}$, the vector obtained by selection of the strictly positive elements of the vector a. Let

$$e = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \in R_+^{n\times n}.$$

Definitions of special positive matrices are stated below.

Definition 2.2 a. *A positive matrix is said to be a* permutation matrix *if every row and every column has exactly one element equal to* 1 *while all other elements are equal to zero. The set of permutation matrices in $R_+^{n\times n}$ is denoted by $P^{n\times n}$.*

b. *A matrix is said to be a* diagonal matrix *if all off-diagonal elements are zero. The set of diagonal matrices in $R_+^{n\times n}$ is denoted by $D_+^{n\times n}$. A* strictly positive diagonal matrix *is a diagonal matrix whose diagonal elements are strictly positive.*

c. *A positive matrix is said to be a* monomial matrix *if every row and every column contains exactly one strictly positive element. The set of monomial matrices in $R_+^{n\times n}$ is denoted by $M_+^{n\times n}$.*

d. *A positive matrix is said to be a* doubly stochastic matrix *if for every row the sum of the row elements and for every column the sum of the column elements equals one. The set of doubly stochastic matrices in $R_+^{n\times n}$ is denoted by $DS_+^{n\times n}$.*

e. *A matrix $A \in R^{n\times n}$ is said to be a* circulant *or* circular matrix *if*

$$\begin{aligned} A_{ij} &= A_{i+1,j+1}, \quad \forall i \in Z_{n-1}, j \in Z_{n-1}, && (1)\\ A_{nj} &= A_{1,j+1}, \quad \forall j \in Z_{n-1}, && (2)\\ A_{in} &= A_{i+1,1}, \quad \forall i \in Z_{n-1}, && (3)\\ A_{nn} &= A_{11}. && (4) \end{aligned}$$

It is said to be a positive circulant *if it is a circulant and if $A \in R_+^{n\times n}$, and it is said to be a* doubly stochastic circulant *if it is a circulant and doubly stochastic.*

If $A \in R_+^{n\times n}$ is a circulant then write

$$A = \begin{pmatrix} a_1 & a_n & \ldots & a_2 \\ a_2 & a_1 & & a_3 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & \ldots & a_1 \end{pmatrix} = circ(a), \quad a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

If $a \in R_+^{n\times n}$ then $A = \mathrm{circ}(a) \in R_+^{n\times n}$ and if $a \in S_+^n$ then $A = \mathrm{circ}(a) \in DS_+^{n\times n}$. A circulant $A = \mathrm{circ}(a)$ is said to be of order k *if the vector a is of order k. Denote the set of doubly stochastic circulants by*

$$DSC_+^{n\times n} = \left\{A \in DS_+^{n\times n} | A \text{ is circulant}\right\}.$$

The terminology used above is fairly standard, see [2]. A circulant is mentioned in [16, 2.H.2]. If $M \in M_+^{n\times n}$ is a monomial matrix then there exists a permutation matrix $P_1 \in P^{n\times n}$ and a strictly positive diagonal matrix $D_1 \in D_+^{n\times n}$ such that $M = P_1 D_1$. Similarly there exists a $D_2 \in D_+^{n\times n}$ with the same properties as D_1 such that $M = D_2 P_1$.

2.2 Algebraic theory of positive matrices

The algebraic structure of the set of positive matrices is what will be called a semi-ring. A formal definition follows. This definition is patterned on the concept of a ring, see for example [12, 2.1].

Definition 2.3 *A* semi-ring *is defined to be a structure consisting of a non-empty subset X together with two binary compositions $+, .$ called respectively addition and multiplication and two elements $0, 1$ such that*

1. *$(X, +, 0)$ is a commutative monoid;*
2. *$(X, ., 1)$ is a monoid;*
3. *the following distributive laws hold for all $a, b, c \in X$*

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca, \quad a0 = 0a = 0.$$

A semi-ring differs from a ring in that it does not have an inverse with respect to addition. A semi-ring is related to but different from a dioid as defined in [10, p. 86], see also [11]. Examples of a semi-ring are R_+ and the set of positive matrices $R_+^{n\times n}$ for any $n \in Z_+$.

Note that in general a positive matrix does not have an inverse with respect to multiplication. For any $n \in Z_+$ with $n \geq 2$ the semi-ring $R_+^{n\times n}$ is neither commutative with respect to multiplication nor an integral domain (there exist $A, B \in R_+^{n\times n}$ nonzero for which $AB = 0$).

A *sub-semi-ring* $(Y, +, ., 0, 1)$ of a semi-ring $(X, +, ., 0, 1)$ is a semi-ring such that $Y \subset X$ and the operations on Y are identical to those of X when these are restricted to Y. Similarly one may define a *sub-monoid* $(Y, ., 1)$ of the monoid $(X, ., 1)$ of a semi-ring $(X, +, ., 0, 1)$. Then the set of doubly stochastic matrices $(DS_+^{n\times n}, ., I)$ is a sub-monoid of $(R_+^{n\times n}, ., I)$ for any $n \in Z_+$. Moreover, the set of doubly stochastic circulants $(DSC_+^{n\times n}, ., I)$ is a sub-monoid of $(DS_+^{n\times n}, ., I)$ and of $(R_+^{n\times n}, ., I)$.

2.3 Primes

Consider a monoid $(M, ., 1)$. An element $u \in M$ is said to be a *unit* or *invertible* if there exists a $v \in M$ such that $uv = 1 = vu$. Such a v is unique, denoted by u^{-1}, and said to be the *inverse* of u. Denote by $U \subset M$ the set of units of M. The triple $(U, ., I)$ is a group and said to be the *group of units* of M.

Let X be a semi-ring and $x, y \in X$, $x \neq 0$. One says that x is *left divisor* of y or that y is a *left multiple* of x if there exists a $z \in X$ such that $y = xz$. A *right divisor* and a *right multiple* are defined correspondingly. A *divisor* of $x \in X$ is either a left or a right divisor.

If X is a semi-ring then $x \in X$ is called a *right associate* of $y \in X$ if there exists a unit $u \in U$ such that $x = yu$. The relation of right association is an equivalence relation. A *left associate* of $y \in X$ is defined correspondingly. An *associate* of $y \in X$ is an $x \in X$ such that there exists $u_1, u_2 \in U$ such that $x = u_1 y u_2$.

A *prime* of a semi-ring X is defined to be a nonzero element $p \in X$ that is not a unit and the only divisors of p are either units or associates of p. Equivalently, $p \in X$ is a prime iff it is not a unit and if $p = xy$ then either x or y is a unit. From the definition of a prime it is clear that one can define a prime in any monoid $(X, ., I)$ with a multiplicative operation.

Proposition 2.4 *Let $A \in R_+^{n\times n}$. Then A has an inverse in the positive matrices iff A is a monomial matrix.*

Proof This may be deduced form [2, 3.4.3]. □

Thus the group of units in the set of positive matrices is the set of mononial matrices.

Definition 2.5 *A* prime in the set of positive matrices $R_+^{n\times n}$ *is a positive matrix $A \in R_+^{n\times n}$ such that*

1. *A is not a monomial matrix;*
2. *if $A = BC$ with $B, C \in R_+^{n\times n}$ then either B or C is a monomial matrix.*

The above definition of a prime was introduced by D.J. Richmann and H. Schneider in 1974 [23]. For an exposition on primes in $R_+^{n\times n}$ see [2, Section 3.4].

Example 2.6 A few examples of primes in the positive matrices are known. In $R_+^{2\times 2}$ there is no prime. The matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in R_+^{3\times 3} \tag{5}$$

is a prime in the positive matrices. In $R_+^{4\times 4}$ several primes are known such as

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 5 & 0 \\ 0 & 1 & 1 & 5 \\ 5 & 0 & 1 & 1 \\ 1 & 5 & 0 & 1 \end{pmatrix}, \tag{6}$$

see [23] and [2, p. 79]. There is no classification of all primes in $R_+^{4\times 4}$. For $n \in Z_+$ with $n \geq 3$ let

$$a = \begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in R_+^n, \quad A = \mathrm{circ}(a).$$

Then A is a prime in the positive matrices. This follows from [2, 3.4.1].

Recall that $(DS_+^{n\times n}, ., I)$ is a monoid. Let $A \in DS_+^{n\times n}$. Then A^{-1} exists and $A^{-1} \in DS_+^{n\times n}$ iff A is a permutation matrix. This statement follows from Proposition 2.4. The group of units in $DS_+^{n\times n}$ is therefore the set of permutation matrices. One may then define a prime in the set of doubly stochastic matrices.

Definition 2.7 *A matrix $A \in DS_+^{n\times n}$ is called a* prime in the set of doubly stochastic matrices *if*

1. *A is not a permutation;*
2. *if $A = BC$ with $B, C \in DS_+^{n\times n}$ then either B or C is a permutation.*

The problem addressed in this paper can now be formulated.

Problem 2.8 *Classify all primes in the positive matrices and those in the doubly stochastic matrices.*

2.4 Equivalences

Definition 2.9 *The positive matrices $A_1, A_2 \in R_+^{n\times n}$ are said to be* permutation equivalent *if*

$$A_1 = X_1 A_2 X_2 \tag{7}$$

for permutation matrices $X_1, X_2 \in P^{n\times n}$. They are said to be diagonally equivalent *if in (7) $X_1, X_2 \in D_+^{n\times n}$ are strictly positive diagonal matrices. They are said to be* monomially equivalent *if in (7) $X_1, X_2 \in M_+^{n\times n}$ are monomial matrices. They are said to be* unitary *equivalent with respect to a semi-ring if X_1, X_2 are units of the semi-ring.*

They are said to be cogredient *if $A_1 = PA_2P^{-1}$ for a $P \in P^{n\times n}$.*

The relation of permutation equivalence is reflexive, symmetric, and transitive, hence an equivalence relation. The same remark applies to diagonal and monomial equivalence. If A_1, A_2 are, for example, monomially equivalent, then this is denoted by $A_1 \cong A_2$ while it is mentioned that this refers to monomial equivalence. The same notation will be used for permutation and diagonal equivalence. Note that in the definition of equivalence one does not require that $X_2 = X_1^{-1}$.

Canonical forms for a positive matrix under permutation, diagonal, and monomial equivalance are of interest. Below such forms are developed only as far as is relevant for the subject of the paper.

Definition 2.10 a. *A positive matrix $A \in R_+^{n\times n}$ is said to be* decomposable *if $n \geq 2$ and it is permutation equivalent to*

$$\begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}, \tag{8}$$

in which A_{11}, A_{22} are either a positive number or a square matrix. It is said to be reducible *if it is cogredient to (8).*

b. *A positive matrix $A \in R_+^{n\times n}$ is said to be* indecomposable *if $n \geq 2$ and it is not decomposable. It is said to be* irreducible *if $n \geq 2$ and it is not reducible.*

c. *A positive matrix $A \in R_+^{n\times n}$ is said to be* completely decomposable *if it is permutation equivalent to a direct sum of zero, one or more indecomposable matrices and, possibly, a diagonal matrix, or*

$$A \cong (A_1 \oplus A_2 \oplus \ldots \oplus A_{m-1} \oplus D),$$

with $m \in Z_+$, $n_i \geq 2$ $\forall i \in Z_{m-1}$, $n_1, \ldots, n_m \in Z_+$, $n_1 + n_2 + \ldots + n_m = n$, for all $i \in Z_{m-1}$ $A_i \in R_+^{n_i\times n_i}$ is an indecomposable matrix, and $D \in D_+^{n_m\times n_m}$ is a diagonal matrix.

The terms introduced above differ slightly from those used in [2].

3 Primes in the positive matrices

In this section results are presented on the classification of primes in the positive matrices.

3.1 Decomposition of primes in the positive matrices

Theorem 3.1 a. *The matrix $A \in R_+^{n\times n}$ is a prime in the set of positive matrices iff it is monomially equivalent to the direct sum of an indecomposable doubly stochastic matrix that is a prime in the positive matrices and an identity matrix, or iff*

$$A = M_1 \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} M_2 \cong S \oplus I, \tag{9}$$

with $M_1, M_2 \in M_+^{n\times n}$, $n_1, n_2 \in N$, $n_1 \geq 2$, $n_1 + n_2 = n$, $S \in DS_+^{n_1\times n_1}$ an indecomposable doubly stochastic matrix that is a prime in the positive matrices, and $I \in R_+^{n_2\times n_2}$ the identity matrix.

b. *Algorithm 3.2 transforms a prime in the positive matrices to the form (9).*

c. *If*

$$A = M_1 \begin{pmatrix} S_1 & 0 \\ 0 & I_{n_2} \end{pmatrix} M_2 = M_3 \begin{pmatrix} S_2 & 0 \\ 0 & I_{n_4} \end{pmatrix} M_4 \tag{10}$$

are two factorizations as defined in a with $S_1 \in DS_+^{n_1\times n_1}$ and $S_2 \in DS_+^{n_3\times n_3}$, then $n_1 = n_3$ and

$$S_1 = P_1 S_2 P_2 \tag{11}$$

for $P_1, P_2 \in P^{n_1\times n_1}$. Thus the matrix A determines the matrix S_1 up to permutation equivalence.

Algorithm 3.2 *Transformation of a prime in the set of positive matrices to the form of Theorem 3.1.a. Given a matrix $A \in R_+^{n\times n}$ that is a prime in the positive matrices.*

1. *Construct permutation matrices $P_1, P_2 \in P^{n\times n}$ such that*

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & D \end{pmatrix} P_2, \tag{12}$$

in which $n_1, n_2 \in N$, $n_1 + n_2 = n$, $A_1 \in R_+^{n_1\times n_1}$ is an indecomposable matrix and $D \in R_+^{n_2\times n_2}$ is a strictly positive diagonal matrix.

2. *Determine strictly positive diagonal matrices $D_1, D_2 \in D_+^{n_1\times n_1}$ such that*

$$A_1 = D_1 S D_2$$

for a doubly stochastic matrix $S \in DS_+^{n_1\times n_1}$. See [19] for numerical algorithms.

3. *Set*

$$M_1 = P_1 \begin{pmatrix} D_1 & 0 \\ 0 & D \end{pmatrix}, \quad M_2 = \begin{pmatrix} D_2 & 0 \\ 0 & I \end{pmatrix} P_2.$$

Then

$$A = M_1 \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix} M_2,$$

in which $M_1, M_2 \in M_+^{n\times n}$ are monomial matrices and $S \in DS_+^{n_1\times n_1}$ is indecomposable, doubly stochastic, and a prime in the positive matrices.

Definition 3.3 *The* doubly stochastic pseudo-canonical form *of a prime in the positive matrices is defined to be the matrix $(S \oplus I) \in R_+^{n\times n}$ in (9). One may call the matrix I the tail of the form.*

It follows from Theorem 3.1.a and Algorithm 3.2 that for every prime $A \in R_+^{n\times n}$ in the positive matrices one can determine a matrix of the form $(S \oplus I)$ in which S is doubly stochastic, indecomposable, and a prime in the positive matrices. It follows from Theorem 3.1.c that such a matrix S is unique up to permutation equivalence. Hence one may call the matrix $(S \oplus I)$ a doubly stochastic pseudo-canonical form of the prime A.

Proof of theorem 3.1

b The successive steps of the algorithm 3.2 are proven.

1 This step follows from [2, 4.2.3].

2 The existence of D_1, D_2, S follows from the fact that A_1 is indecomposable and [4, Th. 6.2]. The latter theorem is a major result in positive linear algebra.

3 The representation follows directly from Steps 1 and 2. Because A_1 is indecomposable and $D_1, D_2 \in D_+^{n_1\times n_1}$ are strictly positive, one concludes that $S \in DS_+^{n_1\times n_1}$ is indecomposable.

a $\Rightarrow$. It follows from b that the prime matrix $A \in R_+^{n\times n}$ has a factorization of the form (9) in which $S \in DS_+^{n_1\times n_1}$ is indecomposable. The matrix S indecomposable implies that $n_1 \geq 2$ and S is not a monomial. It remains to show that S is a prime in the positive matrices. Suppose S is not a prime. Since S is not a monomial, it follows that there exists a factorization $S = BC$ with neither B nor C a monomial. Then

$$A = B_1 C_1, \quad B_1 = M_1 \begin{pmatrix} B & 0 \\ 0 & I \end{pmatrix}, \quad C_1 = \begin{pmatrix} C & 0 \\ 0 & I \end{pmatrix} M_2$$

is a factorization of A with neither B_1 nor C_1 a monomial. This contradicts the assumption that A is a prime.
$\Leftarrow$. It follows from the fact that S is a prime in the positive matrices and [2, 3.4.24] that $(S \oplus I)$ is a prime in the positive matrices. Hence $A = M_1(S \oplus I)M_2$ is prime in the positive matrices.

c The equation (10) is equivalent to

$$\begin{pmatrix} S_1 & 0 \\ 0 & I \end{pmatrix} = M_5 \begin{pmatrix} S_2 & 0 \\ 0 & I \end{pmatrix} M_6,$$

for $M_5, M_6 \in M_+^{n\times n}$. Consider factorizations $M_5 = P_1 D_1$, $M_6 = D_2 P_2$ with $D_1, D_2 \in D_+^{n\times n}$ strictly positive diagonal matrices, $P_1, P_2 \in P^{n\times n}$,

$$D_1 = \begin{pmatrix} D_{11} & 0 \\ 0 & D_{12} \end{pmatrix}, \quad D_2 = \begin{pmatrix} D_{21} & 0 \\ 0 & D_{22} \end{pmatrix},$$

$D_{11}, D_{21} \in D_+^{n_3\times n_3}$, $D_{12}, D_{22} \in D_+^{n_4\times n_4}$. Then

$$\begin{pmatrix} S_1 & 0 \\ 0 & I \end{pmatrix} = P_1 \begin{pmatrix} D_{11}S_2D_{21} & 0 \\ 0 & D_{12}D_{22} \end{pmatrix} P_2.$$

From the assumption follows that S_1, S_2 are indecomposable. Because $D_{11}, D_{21} \in D_+^{n_3\times n_3}$ are strictly positive diagonal matrices $D_{11}S_2D_{21}$ is also indecomposable. The definition of indecomposability then implies that $n_1 = n_3$, $n_2 = n_4$,

$$P_1 = \begin{pmatrix} P_{11} & 0 \\ 0 & P_{12} \end{pmatrix}, \quad P_2 = \begin{pmatrix} P_{21} & 0 \\ 0 & P_{22} \end{pmatrix},$$

$$S_1 = P_{11}D_{11}S_2D_{21}P_{21}, \quad I = P_{12}D_{12}D_{22}P_{22},$$

with $P_{11}, P_{21} \in P_+^{n_1\times n_1}$, $P_{12}, P_{22} \in P_+^{n_2\times n_2}$. Hence

$$S_1 = D_3 \left(P_{11}S_2P_{21}\right) D_4$$

for strictly positive diagonal matrices $D_3, D_4 \in DS_+^{n_1\times n_1}$. Now S_1, S_2, and $(P_{11}S_2P_{21})$ are indecomposable and doubly stochastic matrices. It follows from the uniqueness of the transformation to doubly stochastic form [4, Th. 6.2.] that D_3, D_4 are multiples of the identity and satisfy $D_3D_4 = I$. Thus $S_1 = P_{11}S_2P_{21}$ for $P_{11}, P_{21} \in P^{n_1\times n_1}$. □

3.2 Indecomposable doubly stochastic matrices that are primes in the positive matrices

Theorem 3.1 reduces the classification of primes in the positive matrices to the classification of indecomposable doubly stochastic matrices which are primes in the positive matrices. The latter problem is pursued below. Assume in the following that attention is restricted to matrices in $R_+^{n\times n}$ with $n \geq 2$.

Proposition 3.4 *A prime in the positive matrices that is also doubly stochastic is a prime in the doubly stochastic matrices.*

Proof Let $A \in DS_+^{n\times n}$ be a prime in the positive matrices. Suppose it is not a prime in the doubly stochastic matrices. Then it is either a permutation or there exists a factorization $A = BC$ with neither B nor C a permutation. If A is a permutation then it is a monomial matrix hence a unit in the positive matrices. This is a contradiction of the assumption that it is a prime in the positive matrices. Suppose that there exists a factorization of A as $A = BC$ with $B, C \in DS_+^{n\times n}$ neither of which is a permutation. Because B is not a permutation and doubly stochastic, there exists a column of B with two nonzero elements. Thus B is not a monomial. Similarly, $C \in DS_+^{n\times n}$ is not a monomial matrix. Then the

above factorization of A implies that A is not a prime in the positive matrices. This is a contradiction of the assumption. □

The following example shows that a doubly stochastic matrix that is a prime in the doubly stochastic matrices is not necessarily a prime in the positive matrices.

Example 3.5 Consider the matrix

$$A = \sum_{i=1}^{6} a_i P_i = a_1 I + a_2 P_2 + a_5 P_5 = \begin{pmatrix} a_1 & 0 & a_2 + a_5 \\ a_2 & a_1 + a_5 & 0 \\ a_5 & a_2 & a_1 \end{pmatrix} \in DS_+^{3\times 3}. \tag{13}$$

with $a \in S_+^6$ and $i(a) = (1, 2, 5)$. It follows from Theorem 4.4 that A is a prime in the doubly stochastic matrices. It follows from [2, Cor. 3.4.20] that it is not a prime in the positive matrices.

The classification of indecomposable doubly stochastic matrices that are primes in the positive matrices is unsolved. In the next section attention is focused on primes in the doubly stochastic matrices.

3.3 Examples of primes in the positive matrices

Theorem 3.6 *Consider the matrix*

$$\sum_{i=1}^{n!} a_i P_i \in R_+^{n\times n}, \tag{14}$$

in which $n \geq 3$, $\{P_i, i \in Z_n\}$ is an enumeration of the permutations in $P^{n\times n}$, and $a \in R_+^{n!}$ is of order 2. This matrix is an indecomposable prime in the positive matrices iff it is monomially equivalent to the matrix

$$sI + (1-s)W_n = \begin{pmatrix} s & 0 & \dots & 0 & 1-s \\ 1-s & s \dots & 0 & 0 & \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & & s & 0 \\ 0 & 0 & \dots & 1-s & s \end{pmatrix} \tag{15}$$

for some $s \in (0, 1)$ and $W_n \in P^{n\times n}$ the shift.

Proof $\Leftarrow$. That (15) is a prime in the positive matrices follows from [23, Th. 2.6]. That this matrix is indecomposable follows from Proposition F.2.
$\Rightarrow$. Note that

$$B = \frac{1}{\sum_{i=1}^{n!} a_i} \sum a_i P_i \in DS_+^{n\times n}$$

and that B is monomially equivalent to A. From Proposition 3.4 follows that B is a prime in the doubly stochastic matrices. From Theorem 4.3 follows that B is permutation equivalent to (15). Hence A is monomially equivalent to (15). □

4 Primes in the doubly stochastic matrices

4.1 Equivalent condition for a prime in the doubly stochastic matrices

The set of doubly stochastic matrices decomposes nicely with respect to permutation equivalence.

Proposition 4.1 *Any doubly stochastic matrix is completely decomposable hence is permutation equivalent to the direct sum of zero, one, or more indecomposable doubly stochastic matrices and, possibly, a unit matrix.*

Proof The elementary proof is omitted. □

For questions that involve doubly stochastic matrices up to permutation equivalence the above result implies that attention in the search for primes in the doubly stochastic matrices may be restricted to indecomposable doubly stochastic matrices. Denote the indecomposable doubly stochastic matrices by $INDS_+^{n\times n}$. It follows from [13] that this set is closed with respect to multiplication. Note that the set of indecomposable doubly stochastic matrices does neither contain the identity matrix nor the permutations because these are not indecomposable. Therefore $(INDS_+^{n\times n}, ., I)$ is not a monoid.

It is first established that primes in the doubly stochastic matrices have an even more specific structure than that indicated in Proposition 4.1.

Theorem 4.2 a *The matrix $A \in DS_+^{n\times n}$ with $n \geq 2$ is a prime in the doubly stochastic matrices iff it is permutation equivalent to the direct sum of an indecomposable prime in the doubly stochastic matrices and an identity matrix, or*

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} P_2 \cong A_1 \oplus I, \tag{16}$$

with $P_1, P_2 \in P^{n\times n}$, $n_1, n_2 \in N$, $n_1 \geq 2$, $n_1 + n_2 = n$, $A_1 \in DS_+^{n_1\times n_1}$ an indecomposable prime in the doubly stochastic matrices, and $I \in R_+^{n_2\times n_2}$.

b *If*

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} P_2 = P_3 \begin{pmatrix} A_2 & 0 \\ 0 & I \end{pmatrix} P_4$$

with $A_1 \in DS_+^{n_1\times n_1}$ and $A_2 \in DS_+^{n_3\times n_3}$ are two factorizations as defined in (16) then $n_1 = n_3$ and $A_1 = P_5 A_2 P_6$ for $P_5, P_6 \in P^{n_1\times n_1}$.

The proof of Theorem 4.2 is provided in Appendix G.

A procedure follows by which one can determine whether a doubly stochastic matrix is a prime in the doubly stochastic matrices. The details of this procecure are provided in the appendices D, E, and F.

First decompose the given doubly stochastic matrix by permutation equivalence as stated in Proposition 4.1. Only if the resulting matrix has the form displayed in (16) can the given matrix be a prime in the doubly stochastic matrices.

Second, consider an indecomposable doubly stochastic matrix $A \in DS_+^{n\times n}$. It follows from [2, 2.5.6] that the matrix has a representation as a convex sum of permutations

$$A = \sum_{i=1}^{n!} a_i P_i, \tag{17}$$

The matrix A being indecomposable implies that the vector $a \in S_+^{n!}$ is of order at least two. It follows from Lemma G.2 under a condition stated there that A is a prime in the doubly stochastic matrices iff there do not exist $b, c \in S_+^{n!}$ both of order at least two such that

$$a = L_m(b)c, \tag{18}$$

where L_m is the latin square induced by multiplication. See Appendix C for the definition of this particular latin square. The equivalence follows from the factorization

$$\sum a_i P_i = A = BC = (\sum b_i P_i)(\sum c_i P_i). \tag{19}$$

Third, let $a \in S_+^n$ be of order ≥ 2. It follows from Lemma D.4 that there exist $b, c \in S_+^n$ both of order at least two such that (18) holds iff

$$\begin{aligned} i(a) &= \cup_{j \in i(c)} i(L_m(b)_{.j}), & (20) \\ a_r &= L_{mr}(b)c_r, & (21) \end{aligned}$$

where (20) is called an index equation and (21) is a Latin square in which $a_r \in S_+^{n(a)}$ is of full order.

Fourth, it turns out that the latter two equations can be solved. Solvability of the index equation is tedious but easy. Solvability of the equation over a latin square depends on inequalities having a solution.

In the next subsection examples of primes in the doubly stochastic matrices are described. The examples are structured by the order of the vector $a \in S_+^{n!}$ in (17). All such primes for the orders of a being 2 or 3 are classified. For the order of a being 4 or larger a condition on the real values of the vector is required for the existence of a solution to (21). The analytic solvability conditions have been derived in connection with the classification of the primes in the doubly stochastic circulants, see [21].

The partial classification of primes in the doubly stochastic matrices has herewith been reduced to solvability of equations. The solutions to these equations is described below for special cases. Apparently the classification of the primes in the doubly stochastic matrices cannot be described analytically.

4.2 Examples of primes in the doubly stochastic matrices

Theorem 4.3 *Consider a doubly stochastic matrix $A \in DS_+^{n \times n}$ with the convex sum representation $A = \sum_{i=1}^{n!} a_i P_i$ in which $n \geq 3$ and $a \in S_+^{n!}$ is of order 2. This matrix is an indecomposable prime in the doubly stochastic matrices iff it is permutation equivalent to*

$$sI + (1-s)W_n = \begin{pmatrix} s & 0 & \dots & 0 & 1-s \\ 1-s & s & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & s & 0 \\ 0 & 0 & \dots & 1-s & s \end{pmatrix} \in DS_+^{n \times n} \tag{22}$$

for some $s \in (0,1)$ and $W_n \in P^{n \times n}$ the shift.

Note that each element of the family of primes in the doubly stochastic matrices of the above mentioned theorem is a circulant. Therefore it seems of interest to investigate also the primes in the doubly stochastic circulants. See the paper [21] for results on that class.

Proof $\Rightarrow$. Let $A = \sum a_i P_i \in DS_+^{n\times n}$ be a prime in the doubly stochastic matrices with $a \in S_+^n$ of order 2. By premultiplication transform A to the form $a_1 I + a_j P_j$ for some $j \in Z_n$. From Lemma G.2.b follows that there do not exist $b, c \in S_+^{n!}$ both of order at least two such that $a = L_m(b)c$.

From Theorem 4.2 follows that A is permutation equivalent to a matrix of the form $A_1 \oplus I$. By assumption the identity part cannot be present because A is indecomposable. From Proposition F.2 follows that $a_1 I + a_j P_j$ is indecomposable iff the permutation P_j has only one cycle. By relabeling the elements of Z_n, or, equivalently, by applying a permutation $Q \in P^{n\times n}$, $QP_jQ^T = W_n$. Hence A is permutation equivalent to $a_1 I + a_j W_n$.
$\Leftarrow$. This follows by retracing the steps of the proof in the converse direction. The map $(a_1 I + a_2 W_n \mapsto a \in S_+^n$ is a bijection as is needed in Lemma G.2.a. From Lemma D.4 follows that then either Equation (40) or (41) does not hold. From Proposition D.5 follows that (41) always has a solution. From Proposition D.7 follows that Equation (40) has no solution iff $P_j \neq P_j^T$. □

Theorem 4.4 *Consider the family of doubly stochastic matrices*

$$A = \sum_{i=1}^{6} a_i P_i \in DS_+^{3\times 3}, \tag{23}$$

in which $\{P_i, i \in Z_6\}$ *is as defined in Example A.5 and* $a \in S_+^6$ *is of order 3. Then* A *is an indecomposable prime in the doubly stochastic matrices iff* A *equals*

$$\sum_{i=1}^{6} a_i P_i = a_1 I + a_2 P_2 + a_5 P_5 = \begin{pmatrix} a_1 & 0 & a_2 + a_5 \\ a_2 & a_1 + a_5 & 0 \\ a_5 & a_2 & a_1 \end{pmatrix} \in DS_+^{3\times 3}. \tag{24}$$

in which $a \in S_+^6$ *satisfies* $i(a) = (1, 2, 5) \subset Z_6$ *or is permutation equivalent to such a matrix.*

Note that each element of the family of primes in the doubly stochastic matrices is not a circulant.

Proof $\Rightarrow$. Let $A = \sum_{i=1}^{6} a_i P_i \in DS_+^{3\times 3}$ be a prime in the doubly stochastic matrices. From Lemma G.2.b follows that there do not exist $b, c \in S_+^6$ both of order at least two such that $a = L_m(b)c$. From Proposition D.8 then follows that the ordered triple $i(a) \subset Z_6$ is different from $(1, 2, 3)$ and $(4, 5, 6)$. Any matrix $\sum_{i=1}^{6} a_i P_i$ with $i(a)$ one of the cases mentioned is permutation equivalent to the matrix of the statement of the theorem, which corresponds to $i(a) = (1, 2, 5)$. This can be proved because for any of the matrices A with $i(a)$ one of the cases mentioned the matrix has one column with no zero and two columns with one zero. By pre and past multiplication by a permutation the matrix of any of the cases can be transformed to the form given in the theorem.
$\Leftarrow$. Note that $a \in S_+^6$ is of order 3 with $i(a) = (1, 2, 5)$. For the matrix $A = a_1 I + a_2 P_2 + a_5 P_5$ the map of A to $a \in S_+^6$ is a bijection. From Proposition D.8 follows that there do not exist $b, c \in S_+^6$ both of order at least two such that $a = L_m(b)c$. From Lemma G.2.a follows that A is a prime in the doubly stochastic matrices. □

The procedure to determine whether or not a given matrix is a prime in the doubly stochastic matrices can then be followed for other matrices than the cases discussed above. The doubly stochastic matrices of the form

$$A = \sum a_i P_i \in DS_+^{3\times 3}$$

in which $a \in S_+^6$ with order $n(a) \geq 4$ have not been analyzed on whether they contain primes. It is conjectured that they do not. For the case in which $A = \sum a_i P_i \in DS_+^{n\times n}$ with $n(a) = 3$ the solvability of the index equation is characterized by Lemma E.6. The solvability of the induced latin square is not yet characterized.

5 Concluding remarks

A decomposition has been presented of a prime in the positive matrices, see Theorem 3.1. A particular class of primes in the positive matrices has subsequently been characterized in Theorem 3.6.

A decomposition has been presented of a prime in the doubly stochastic matrices, see Theorem 4.2. A procedure to determine whether a given doubly stochastic matrix is a prime in the doubly stochastic matrices has been outlined. Special classes of primes in the doubly stochastic matrices have been described in Theorem 4.3 and in Theorem 4.4.

A major open problem is to characterize those primes in the indecomposable doubly stochastic matrices that are also primes in the positive matrices.

A Permutations

A.1 Definitions

In this section definitions and results for permutation matrices are collected. A permutation matrix was defined in Section 2. The set of permutation matrices in $R_+^{n\times n}$ is denoted by $P^{n\times n}$.

Definition A.1 *For $n \in Z_+$ define the* shift *as the circulant and permutation matrix*

$$W_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in R_+^{n\times n}. \tag{25}$$

The shift $W_n \in R_+^{n\times n}$ corresponds to a cyclic shift by one element on a set with n elements.

A.2 Cycles of permutations

Terminology on cycles of permutations follows, see [12, Section 1.6]. A permutation γ of Z_n which permutes a sequence of elements $i_1, i_2, \dots, i_r$, $r > 1$, cyclically, or

$$\gamma(i_1) = i_2, \gamma(i_2) = i_3, \dots, \gamma(i_{r-1}) = i_r, \gamma(i_r) = i_1,$$

and leaves unchanged the other elements of Z_n is said to be a *cycle*. The integer r is said to be the *order* of the cycle. A cycle is denoted by $\gamma = (i_1, i_2, \dots, i_r)$ and considered as an ordered subset of Z_n. This notation differs from that in [12] by the comma's. Two

cycles are said to be *disjoint* if their symbols contain no common elements. Any two permutations with disjoint cycles commute. A *cycle decomposition* of a permutation is the list of all its cycles. It is denoted by $c(P)$. An example is

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad c(P) = (1,2)(3)(4,6,5).$$

Note that P transforms 1 into 2, or $\gamma(1) = 2$, or $1 \mapsto 2$, and $\gamma(2) = 1$, hence the cycle $(1,2)$.

Proposition A.2 *Let $P \in P^{n\times n}$. For any $Q \in P^{n\times n}$, $Qc(P) = c(QPQ^T)$, or, in words, the cycles of P transformed by Q equal the cycles of QPQ^T.*

Proof Denote by $j = P(i)$ that $i \mapsto^P j$ or $P_{ji} = 1$. Let $j = P(i)$ and $k = Q(i)$. Then $i = Q^T(k)$ and $Q(j) = Q(P(i)) = Q(P(Q^T(k)))$. Thus $i \mapsto^P j$ implies that $k = Q(i) \mapsto^{QPQ^T} Q(j)$. From this the result follows. □

From Proposition A.2 follows that the cycles of the permutations of P and QPQ^T are the same except for relabeling of the elements of Z_n. Two permutations are said to be *cycle equivalent* if they have the same cycle decomposition except for relabeling of the elements of sets. Thus $P_1, P_2 \in P^{5\times 5}$ with $c(P_1) = (1,2,3)(4,5)$ and $c(P_2) = (2,5)(1,3,4)$ are cycle equivalent. Two permutations are cycle equivalent iff they are cogredient.

Definition A.3 *A permutation is said to be in the pseudo-canonical form for cycle equivalence if its cycle decomposition has the form*

$$c(P) = (i_1, i_2, \ldots, i_{r_1})(j_1, \ldots, j_{r_2}) \ldots (k_1, k_2, \ldots, k_{r_m}), \tag{26}$$

where $m \in Z_+$, $r_1, \ldots, r_m \in Z_+$, $r_1 \geq r_2 \geq r_m \geq 1$, $i_1 = 1$, $i_{k+1} = i_k + 1$, $j_1 = i_{r_1} + 1$, etc.

For example,

$$P = W_4 \oplus W_3 \oplus W_2 \oplus 1 \oplus 1, \quad c(P) = (1,2,3,4)(5,6,7)(8,9)(10)(11),$$

is a cycle decomposition of the matrix P in the pseudo-canonical form. In such a pseudo-canonical form the cycles are ordered in decreasing order. Because there may be two or more cycles with the same order such a form is invariant under relabeling the elements of Z_n that appear in cycles of such orders. Hence it is called a pseudo-canonical form.

The following technical result is used in Proposition F.2.

Proposition A.4 *Let $P \in P^{n\times n}$. There exist $Q_1, Q_2 \in P^{n\times n}$ such that $Z_n = C_1 \cup C_2$, where the union is a disjoint union and where C_1, $C_2 \subset Z_n$ are either cycles of both Q_1Q_2 and Q_1PQ_2 or the unions of such cycles, iff $P \in P^{n\times n}$ has at least two cycles.*

Proof $\Leftarrow$. Suppose that P has at least two cycles, say

$$c(P) = (i_1, i_2, \ldots, i_{r_1})(j_1, \ldots, j_{r_2})(k_1, k_2, \ldots, k_{r_m}).$$

Let

$$C_1 = (i_1, i_2, \ldots, i_{r_1}), \quad C_2 = (j_1, \ldots, j_{r_2})(k_1, k_2, \ldots, k_{r_m}),$$

$Q_1 = Q_2 = I \in P^{n\times n}$. Then $c(Q_1Q_2) = c(I) = (1)(2)\dots(n)$, and both C_1 and C_2 are unions of cycles of $c(Q_1Q_2)$ and of $c(P)$.
$\Rightarrow$. Let $Q_3 = Q_1Q_2 \in P^{n\times n}$. Then $Q_1PQ_2 = Q_1PQ_1^TQ_1Q_2 = P_1Q_3$ with $P_1 = Q_1PQ_1^T$. Thus $Z_n = C_1 \cup C_2$ where C_1 and C_2 are cycles or unions of cycles of Q_3 and P_1Q_3. Suppose that $C_1 = (i_1, \dots, i_{r_1})$ is both a cycle of Q_3 and P_1Q_3. Then it is also a cycle of Q_3^T, of $P_1 = (P_1Q_3)Q_3^T$, and finally of $P = Q_1^TP_1Q_1$. Thus, in this case, P has at least two cycles. In the case in which C_1 is the union of two or more cycles of Q_3 and P_1Q_3 the proof goes similarly. Then C_1 may be a cycle or a union of cycles of P. □

A.3 Multiplication of permutations

In the main body of the paper the multiplication of two permutations plays a major role. In this subsection results for this point are collected.

Example A.5 Consider the following enumeration of the elements of $P^{3\times3} = \{P_1, \dots, P_6\}$:

$$P_1 = I, \quad P_2 = W_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad P_3 = W_3^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \tag{27}$$

$$P_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{28}$$

The multiplication table for $P^{3\times3}$ is then given by

		j					
		1	2	3	4	5	6
i	1	1	2	3	4	5	6
	2	2	3	1	6	4	5
	3	3	1	2	5	6	4
	4	4	5	6	1	2	3
	5	5	6	4	3	1	2
	6	6	4	5	2	3	1

(29)

where, if $P_iP_j = P_k$, then the entry in the table corresponds to k, and the enumeration of $P^{3\times3}$ is that defined above.

A.4 Permutation covering

Definition A.6 *A subset*

$$PC = \{P_i,\ i \in I\} \subset P^{n\times n} \tag{30}$$

is said to be a permutation covering *of* $R_+^{n\times n}$ *if*

$$\sum_{i\in I} P_i = E_n,$$

where $E_n \in R_+^{n\times n}$ *is such that* $(E_n)_{ij} = 1$ *for all* $i, j \in Z_n$.

A permutation covering consists of exactly n permutations. Which subsets of $P^{n\times n}$ form a permutation covering?

Example A.7 The set of multiple shifts

$$\left\{W_n^0, W_n^1, \ldots, W_n^{n-1}\right\} \subset P^{n\times n}$$

is a permutation covering of $R_+^{n\times n}$.

B Circulants

In this section results on circulants are collected. A circulant or circular matrix is defined in Definition 2.2. A source on circulants is [6].

The matrix $A \in R^{n\times n}$ is a circulant iff there exists a vector $a \in R^n$ such that

$$A = \sum_{i=1}^{n} a_i W_n^{i-1}, \tag{31}$$

where $W_n \in P^{n\times n}$ is the shift, see Definition A.1. The set of doubly stochastic circulants with the multiplication operation $(DSC_+^{n\times n}, ., I)$ is a monoid for any $n \in Z_+$.

The group of units of the doubly stochastic circulants $DSC_+^{n\times n}$ is given by

$$U = \left\{W_n^0, W_n^1, \ldots, W_n^{n-1}\right\}. \tag{32}$$

C Latin squares

A latin square is a well known concept, see [8]. In this paper another definition is presented that seems more suitable than one of the definitions of the literature.

Definition C.1 *A matrix $A \in R_+^{n\times n}$ will be called a* positive latin square *if there exists a permutation covering $\{P_i, i \in I\} \subset P^{n\times n}$ of $R_+^{n\times n}$ and a vector $a \in R_+^n$ such that*

$$A = \sum_{i=1}^{n} a_i P_i. \tag{33}$$

In this case define the map $L : R_+^n \to R_+^{n\times n}$ by $A = L(a) = \sum a_i P_i$. The matrix $A \in R_+^{n\times n}$ is called a doubly stochastic latin square *if it is a positive latin square and doubly stochastic. In this case it admits a representation as (33) where $a \in S_+^n$.*

It follows from the definition of a positive latin square, in particular from a permutation covering, that every row and every column of such a matrix $A = \sum a_i P_i$ is a permutation of the elements of the vector $a \in R_+^n$.

A characterization of the set of latin squares follows from a characterization of the set of permutation coverings.

Definition C.2 *The* latin square induced by multiplication of permutation *in $P^{n\times n}$ is defined as*

$$L_m : R_+^{n!} \to R_+^{n!\times n!}, \quad L_m(x)_{kj} = x_i, \quad \text{if } P_i P_j = P_k, \tag{34}$$

where P_i, P_j, P_k are elements of an enumeration of $P^{n\times n}$.

It is proven below that L_m is a positive latin square.

Example C.3 The latin square in $R^{3!\times 3!}$ induced by multiplication of permutations in $P^{3\times 3}$ is given by

$$L_m(x) = \begin{pmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_6 & x_4 & x_5 \\ x_3 & x_2 & x_1 & x_5 & x_6 & x_4 \\ x_4 & x_6 & x_5 & x_1 & x_2 & x_3 \\ x_5 & x_4 & x_6 & x_3 & x_1 & x_2 \\ x_6 & x_5 & x_4 & x_2 & x_3 & x_1 \end{pmatrix}, \tag{35}$$

where the enumeration of $P^{3\times 3}$ is as stated in A.5. This matrix may be represented as

$$L_m(x) = \sum_{i=1}^{6} x_i P_i,$$

where the permutation covering is given by the following permuations

$$\begin{aligned} P_1 &= I = (1)(2)(3)(4)(5)(6), \quad P_2 = (2,3,1)(6,5,4), \quad P_3 = (3,2,1)(5,6,4), \\ P_4 &= (4,1)(5,2)(6,3), \quad P_5 = (5,1)(6,2)(4,3), \quad P_6 = (6,1)(4,2)(5,3). \end{aligned}$$

Proposition C.4 *A latin square induced by multiplication as defined in C.2 is a latin square as defined in C.1.*

Proof By definition C.2

$$L_m(x)_{kj} = x_i, \quad \text{if } P_i P_j = P_k.$$

Fix x_1 say. Define $Q_1 \in R_+^{n\times n}$

$$(Q_1)_{kj} = \begin{cases} 1, & \text{if } P_1 P_j = P_k, \\ 0, & \text{else.} \end{cases}$$

For all $k \in Z_n$ there exists an unique $j \in Z_n$ such that $P_1 P_j = P_k$ namely $P_j = P_1^T P_k$. Therefore every row of Q_1 contains exactly one element equal to 1. Similarly every column contains exactly one element equal to 1. Thus $Q_1 \in P^{n\times n}$ is a permutation matrix. Similarly define $Q_2, \ldots, Q_n$. Then $\{Q_i, i \in I\}$ is permutation covering and

$$L_m(x) = \sum x_i Q_i.$$

□

D Linear equation over a doubly stochastic latin square

The classification of primes in the doubly stochastic matrices has been shown to be equivalent to the solvability of a linear equation over a latin square in Section 4. In this section results for the latter problem are collected.

D.1 Problem formulation

Problem D.1 *Let $a \in S_+^n$ be a vector of order at least 2 and let $L : S_+^n \to R_+^{n\times n}$ be the map of a doubly stochastic latin square. Determine conditions on $a \in S_+^n$ such that there do exist $b, c \in S_+^n$ both of order at least two such that the following equality holds*

$$a = L(b)c. \tag{36}$$

In Section 4 this problem is formulated for the case where $L = L_m$, the latin square induced by multiplication of permutations, see Definition C.2.

D.2 General solvability conditions

Notation and a result on the specialization order are stated below. Sources on this are [17, Ch. V] and [16]. For $x \in R_+^n$ let

$$x_\downarrow = \begin{pmatrix} x_{[1]} \\ \vdots \\ x_{[n]} \end{pmatrix} \in R_+^n, \quad x_{[1]} \geq x_{[2]} \geq \ldots \geq x_{[n]}, \tag{37}$$

denote the vector with the components of x in decreasing order.

Definition D.2 *For $x, y \in R_+^n$ one says that x is* majorized *by y or that y* majorizes *x, if*

$$\sum_{i=1}^{k} x_{[i]} \leq \sum_{i=1}^{k} y_{[i]}, \quad k = 1, 2, \ldots, n-1, \quad \sum_{i=1}^{n} x_{[i]} = \sum_{i=1}^{n} y_{[i]}. \tag{38}$$

Denote by $x \preceq y$ that x is majorized by y and call $\preceq$ the specialization order *on R_+^n.*

It follows from [16, X] that, with $x, y \in R_+^n$, $x \preceq y$ iff there exists a $S \in DS_+^{n\times n}$ such that $x = Sy$.

Proposition D.3 *Let $a, b, c \in S_+^n$ and $L : S_+^n \to R_+^{n\times n}$ be the map of a doubly stochastic latin square. Assume that (36) holds. If $a \in S_+^n$ is a vector of order $n(a) \in N_n$ then both b and c are vectors of orders at most $n(a)$, or $n(b) \leq n(a)$ and $n(c) \leq n(a)$.*

Proof The assumptions that $b \in S_+^n$ and L is a latin square imply that $L(b) \in DS_+^{n\times n}$. It then follows from the characterization of the specialization order and equation (36) that $a \preceq c$, or that

$$\sum_{i=1}^{k} a_{[i]} \leq \sum_{i=1}^{k} c_{[i]}, \quad k = 1, 2, \ldots, n-1, \quad \sum_{i=1}^{n} a_{[i]} = \sum_{i=1}^{n} c_{[i]} = 1.$$

If a is a vector of order m then

$$1 = \sum_{i=1}^{m} a_{[i]} \leq \sum_{i=1}^{m} c_{[i]}$$

and hence, because $c \in S_+^n$, $\sum_{i=1}^{m} c_{[i]} = 1$. Thus c is a vector of order at most m. Because $a = L(b)c$ there also holds $a = L_1(c)b$ for another positive latin square L_1. The result for c then follows by symmetry. □

Lemma D.4 *Let $a \in S_+^n$ be a vector of order $n(a) \geq 2$. Let $L : S_+^n \to R_+^{n\times n}$ be the map of a latin square. There exist $b, c \in S_+^n$ both of order at least two such that*

$$a = L(b)c, \tag{39}$$

iff there exist $b, c \in S_+^n$ such that $2 \leq n(b) \leq n(a)$, $2 \leq n(c) \leq n(a)$, and the following conditions both hold:

1. $$i(a) = \cup_{j \in i(c)} i(L(b)_{.j}); \tag{40}$$

   in words, the rows indexed by the strictly positive elements of the vector a equal the rows indexed by the strictly positive elements of the columns $L(b)_{.j}$ for all j indexed by the strictly positive elements of the vector c;

2. and

$$a_r = L_r(b)c_r, \tag{41}$$

where $a_r = a|_{i(a)} \in S_+^{n(a)}$ *is of order* $n(a)$, $c_r = c|_{i(c)} \in S_+^{n(c)}$ *is of order* $n(c)$, *and* $L_r(b) = L(b)|_{i(a)\times i(c)}$.

Proof $\Leftarrow$. Let $P_1, P_2 \in P^{n\times n}$ be such that

$$P_1 a = \begin{pmatrix} a_r \\ 0 \end{pmatrix}, \quad P_2 c = \begin{pmatrix} c_r \\ 0 \end{pmatrix}.$$

Then

$$\begin{aligned} P_1 a &= \begin{pmatrix} a_r \\ 0 \end{pmatrix} = \begin{pmatrix} L_r(b) & * \\ 0 & * \end{pmatrix} \begin{pmatrix} c_r \\ 0 \end{pmatrix} \text{ by conditions 1 and 2,} \\ &= P_1 L(b) P_2^T \begin{pmatrix} c_r \\ 0 \end{pmatrix} \text{ by condition 1,} \\ &= P_1 L(b) c, \end{aligned}$$

hence $a = L(b)c$.
$\Rightarrow$. It follows from Proposition D.3 that $2 \leq n(b) \leq n(a)$ and $2 \leq n(c) \leq n(a)$. Let $P_1, P_2 \in P^{n\times n}$ be such that

$$\begin{pmatrix} a_r \\ 0 \end{pmatrix} = P_1 a, \quad \begin{pmatrix} c_r \\ 0 \end{pmatrix} = P_2 c,$$

$a_r \in S_+^{n(a)}$ and $c_r \in S_+^{n(c)}$ both of full order. Then

$$\begin{pmatrix} a_r \\ 0 \end{pmatrix} = P_1 a = P_1 L(b) P_2^T P_2 c = \begin{pmatrix} L_r(b) & * \\ 0 & * \end{pmatrix} \begin{pmatrix} c_r \\ 0 \end{pmatrix}, \tag{42}$$

where the decomposition of the matrix follows form the definitions of $L_r(b)$, a_r, c_r, P_1, and P_2. That the (2,1)-block is zero follows from the facts that c_r contains the strictly positive elements of the vector c. Then (42) implies that

$$i(a) = \cup_{j\in i(c)} i(L(b)_{\cdot j}), \tag{43}$$

and $a_r = L_r(b)c_r$. The fact that $i(a)$ indexes the strictly positive elements of the vector a implies that in (43) equality holds. □

D.3 Specific linear equations over a doubly stochastic latin square

Proposition D.5 *Let* $a \in S_+^n$ *be of order* n *and let* $L : S_+^n \to S_+^n$ *be a circulant. Then there exists* $b, c \in S_+^n$ *both of order at least two such that that* $a = L(b)c$.

Proof This follows from [21, Proposition 3.5]. □

For the sake of clarity the proof of the above proposition is presented for the case $n = 2$. Suppose that $a = (a_1 \ a_2)^T$ with $a_1 \geq 1/2$; otherwise permute the elements of the vector a. Because $a \in S_+^2$ is a vector of order 2, $a_1 < 1$. Define

$$b_1 = (1 + a_1)/2, \quad c_1 = (3a_1 - 1)/(2a_1).$$

Then $0 < b_1 < 1$ and $0 < c_1 < 1$ because $3a_1 - 1 \geq \frac{1}{2} > 0$ and $c_1 < 1 \Leftrightarrow a_1 < 1$. Thus $b = (b_1 \; 1 - b_1)^T \in S_+^2$ and $c = (c_1 \; 1 - c_1)^T \in S_+^2$ are vectors of order two. Finally $a = \mathrm{circ}(b)c$. □

Proposition D.6 *Let $a \in S_+^{3!} = S_+^6$ be of order two. Then there do* not *exist $b, c \in S_+^6$ both of order at least two such that*

$$a = L_m(b)c \tag{44}$$

iff the indices of the strictly positive elements of the vector a are given by

$$i(a) = (1,2),\ (1,3),\ (2,3),\ (4,5),\ (4,6),\ or\ \ (5,6). \tag{45}$$

Note that the values of the strictly positive components of a are otherwise unconstrained.

Proof By Lemma D.4 there exist $b, c \in S_+^6$ both of order at least two such that (44) holds iff

$$i(a) \;=\; \cup_{j \in i(c)} i(L_m(b))_{\cdot j}), \tag{46}$$

$$a|_{i(a)} \;=\; L_m(b)|_{i(b) \times i(c)} c|_{i(c)}. \tag{47}$$

From Proposition D.5 follows that (47) always has a solution. By Proposition E.1 and Example E.2 there do not exist solutions b, c of (46) iff the index set $i(a)$ is one the cases mentioned in (45). □

Proposition D.7 *Let $a \in S_+^n$ be of order 2 with $i(a) = (i_1, i_2) \subset Z_n$, $i_1 \neq i_2$. Then there do exist $b, c \in S_+^n$ both of order at least two such that $a = L_m(b)c$ iff*

$$P_{i_1} P_{i_2}^T = P_{i_2} P_{i_1}^T. \tag{48}$$

Proof From Proposition D.3 follows that if there exist $b, c \in S_+^n$ satisfying $a = L_m(b)c$ both of order at least two then both b and c are of order at most two, hence precisely two. From Lemma D.4 follows that there exist $b, c \in S_+^n$ both of order two such that $a = L_m(b)c$ iff (40) and (41) both hold. From Proposition E.1 follows that (40) holds iff (48) holds. From Proposition D.5 follows that in this case (41) always has a solution. □

Proposition D.8 *Let $a \in S_+^6$ be of order 3. There do exist $b, c \in S_+^6$ both of order at least two such that $a = L_m(b)c$ iff either $i(a) = (1,2,3)$ or $i(a) = (4,5,6)$.*

Proof From Lemma D.4 follows that $b, c \in S_+^6$ as formulated in the statement of the proposition do exist iff the Equations (40) and (41) both hold. From Proposition E.7 follows that Equation (40) has a solution iff $i(a) = (1,2,3)$ or $i(a) = (4,5,6)$. If $i(a) = (1,2,3)$ then it follows from Proposition E.5 that $i(c) = (1,2,3)$ and the Equation $a_r = L_r(b)c_r$ reduces to

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = circ \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

It then follows from [21, Proposition 3.5] that this equation has a solution. If $i(a) = (4,5,6)$ then a permutation must be applied to transform (41) to the form of [21, Proposition 3.5]. Thus in this case (41) also has a solution. □

Proposition D.9 *Let $a \in S_+^3$ be of order 3. Then there exists $b, c \in (0,1)$ such that*

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 1-b & b \\ 0 & 1-b \end{pmatrix} \begin{pmatrix} c \\ 1-c \end{pmatrix},$$

iff $a_2^2 \geq 4a_1a_3$.

Proof [21, Proposition A.9]. □

E Index equations over a latin square

In this appendix necessary and sufficient conditions are provided for the existence of a solution to the index equation over a latin square of Lemma D.4.

Proposition E.1 *Given $a \in S_+^n$ with $n(a) = 2$ and $i(a) = (i_1, i_2)$.*

a *There exist $b, c \in S_+^n$ with $n(b) = n(c) = 2$ such that $i(a) = \cup_{k \in i(c)} i(L_m(b)_{.k})$ iff $P_{i_1} P_{i_2}^T = P_{i_2} P_{i_1}^T$.*

b *If the condition of a holds then all solutions are given by*

$$\begin{aligned} &P_{j_1} \in P^{n \times n}, \quad \textit{arbitrary}, \quad P_{j_2} = (P_{i_1} P_{i_2}^T) P_{j_1}, \\ &P_{k_1} = P_{j_1}^T P_{i_1}, \quad P_{k_2} = P_{j_1}^T P_{i_2}, \\ &i(b) = (j_1, j_2), \quad i(c) = (k_1, k_2). \end{aligned}$$

Proof Suppose that $b, c \in S_+^n$ exist. Let $i(b) = (j_1, j_2)$ and $i(c) = (k_1, k_2)$. Then the index relation holds iff, case 1,

$$L_m(b)_{i_1,k_1} = b_{j_1}, \quad L_m(b)_{i_1,k_2} = b_{j_2}, \quad L_m(b)_{i_2,k_1} = b_{j_2}, \quad L_m(b)_{i_2,k_2} = b_{j_1},$$

or, case 2, the assignment with the indices j_1 and j_2 interchanged holds. In case 1 there follows from the definition of L_m that the relations equal

$$P_{j_1} P_{k_1} = P_{i_1}, \quad P_{j_2} P_{k_1} = P_{i_2}, \quad P_{j_2} P_{k_2} = P_{i_1}, \quad P_{j_1} P_{k_2} = P_{i_2}.$$

From this follows that

$$P_{k_1} = P_{j_1}^T P_{i_1} = P_{j_2}^T P_{i_2}, \quad P_{k_2} = P_{j_2}^T P_{i_1} = P_{j_1}^T P_{i_2}, \quad P_{j_2} = P_{i_1} P_{k_2}^T = P_{i_1} P_{i_2}^T P_{j_1} \tag{49}$$

$$P_{i_1} P_{i_2}^T = P_{j_1} P_{j_2}^T = P_{i_2} P_{i_1}^T. \tag{50}$$

In case 2 the same conclusion results. Part b. follows immediately from (49). □

Example E.2 Let $a \in S_+^6$ with $n(a) = 2$ and $i(a) = (i_1, i_2)$. For which tuples $(i_1, i_2) \subset Z_6$ do there *not* exist $b, c \in S_+^6$ with $n(b) = 2 = n(c)$ such that $i(a) = \cup_{k \in i(c)} i(L_m(b)_{.k})$. According to Proposition E.1 such b, c do not exist iff $P_{i_1} P_{i_2}^T \neq P_{i_2} P_{i_1}^T = P_x$. The only possible choices for $P_x \in P^{6 \times 6}$ such that $P_x \neq P_x^T$ are $P_x = P_2$ and $P_x = P_3$. From $P_x = P_{i_2} P_{i_1}^T$ follows $P_{i_2} = P_x P_{i_1}$. For $P_x = P_2$ the possible tuples (i_1, i_2) are $(1,2)$, $(2,3)$, $(3,1)$, $(4,6)$, $(5,4)$, and $(6,5)$. For $P_x = P_3$ one obtains the same tuples. Because the ordering of i_1 and i_2 is unimportant the tuples may also be written as $(1,2)$, $(2,3)$, $(1,3)$, $(4,5)$, $(4,6)$, and $(5,6)$.

Proposition E.3 *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset Z_n$.*

a *There exist $b, c \in S_+^n$ both of order two such that*

$$i(a) = \cup_{k \in i(c)} i(L_m(b)_{.k}), \tag{51}$$

iff one of the following three conditions holds:

$$P_{i_1} P_{i_2}^T = P_{i_2} P_{i_3}^T, \tag{52}$$

$$P_{i_1} P_{i_2}^T = P_{i_3} P_{i_1}^T, \tag{53}$$

$$P_{i_3} P_{i_1}^T = P_{i_2} P_{i_3}^T. \tag{54}$$

b *If one of the conditions of a holds then all combinations of the indices of b, c are constructed as follows, in case (52):*

$$P_{j_1} \in P^{n\times n} \text{ arbitrary}, \quad P_{j_2} = (P_{i_2} P_{i_1}^T) P_{j_1}, \quad P_{k_1} = P_{j_1}^T P_{i_1}, \quad P_{k_2} = P_{j_2}^T P_{i_3},$$
$$i(b) = (j_1, j_2), \quad i(c) = (k_1, k_2).$$

The solution in the other cases is easily deduced by symmetry.

The proof of Proposition E.3 is easily deduced from that of Proposition E.1. The same holds for the following results.

Proposition E.4 *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset Z_n$. There exist $b, c \in S_+^n$ with $n(b) = 3$ and $n(c) = 2$ such that (51) holds iff*

$$P_{i_1} P_{i_2}^T = P_{i_2} P_{i_3}^T = P_{i_3} P_{i_1}^T. \tag{55}$$

Proposition E.5 *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset Z_n$.*

a *There exist $b, c \in S_+^n$ with $n(b) = 3$ and $n(c) = 3$ such that (51) holds iff*

$$P_{i_1} P_{i_2}^T = P_{i_2} P_{i_3}^T = P_{i_3} P_{i_1}^T. \tag{56}$$

b *Assume that the condition of a holds. All solutions for b, c are constructed by:*

$$P_{j_1} \in P^{n\times n} \text{ arbitrary}, \quad P_{j_2} = P_{i_2} P_{i_1}^T P_{j_1}, \quad P_{j_3} = P_{i_1} P_{i_2}^T P_{j_1}, P_{k_1} = P_{j_1}^T P_{i_1},$$
$$P_{k_2} = P_{j_1}^T P_{i_2}, \quad P_{k_3} = P_{j_1}^T P_{i_3}, \quad i(b) = (j_1, j_2, j_3), \quad i(c) = (k_1, k_2, k_3).$$

Lemma E.6 *Let $a \in S_+^n$ with $n(a) = 3$ and $i(a) = (i_1, i_2, i_3) \subset Z_n$.*

a *There exist $b, c \in S_+^n$ both of order at least two such that (51) holds iff of the three products $P_{i_1} P_{i_2}^T$, $P_{i_2} P_{i_3}^T$, $P_{i_3} P_{i_1}^T$ two are equal or all three are equal.*

b *The conditions of a remain the same if the order of the indices in $i(a) = (i_1, i_2, i_3)$ is arbitrarily interchanged.*

Proof $\Rightarrow$. If $b, c \in S_+^n$ exist then it follows from (51) that $2 \le n(b) \le n(a) = 3$ and the same bounds on $n(c)$. The possible values of $(n(b), n(c))$ are thus $(2,2)$, $(2,3)$, $(3,2)$, and $(3,3)$. The result then follows from the three previous propositions.
$\Leftarrow$. This follows from the three previous propositions. □

Proposition E.7 *Let $a \in S_+^6$ be of order 3 with $i(a) = (i_1, i_2, i_3) \subset Z_6$. There exist $b, c \in S_+^6$ both of order at least two such that (51) holds iff either $i(a) = (1,2,3)$ or $i(a) = (4,5,6)$.*

Proof Lemma E.6 is applied. For $i(a) = (1,2,3)$ the products are all equal to P_3 while for $i(a) = (4,5,6)$ they are all equal to P_2. All other ordered triples in Z_6 with different elements are: $(1,2,4)$, $(1,2,5)$, $(1,2,6)$, $(1,3,4)$, $(1,3,5)$, $(1,3,6)$, $(1,4,5)$, $(1,4,6)$, $(2,3,4)$, $(2,3,5)$, $(2,3,6)$, $(2,4,5)$, $(2,4,6)$, $(2,5,6)$, $(3,4,5)$, $(3,4,6)$, and $(3,5,6)$. For $i(a) = (1,2,5)$, $P_1 P_2^T = P_3$, $P_2 P_5^T = P_4$, $P_5 P_1^T = P_5$ hence the three products are different. Similarly in all other cases the three products are each different. □

F Doubly stochastic matrices

A doubly stochastic matrix was defined in Definition 2.2. The set of such matrices of size $n \times n$ is denoted by $DS_+^{n\times n}$. Sources on doubly stochastic matrices are [17, Ch. V] and [14, 15, 16, 18, 20]. The set of doubly stochastic matrices in $DS_+^{n\times n}$ is a convex polyhedron of dimension $(n-1)^2$ whose extremal elements are the set of permutation matrices according to a theorem of G. Birkhoff [2, 2.5.6]. Therefore any doubly stochastic matrix may be represented as a convex sum of permutation matrices.

Definition F.1 *A matrix $A \in R_+^{n\times n}$ is said to have a representation as a* convex sum of permutations *if*

$$A = \sum_{i=1}^{n!} x_i P_i, \tag{57}$$

where $x \in S_+^{n!}$ and $\{P_i, i \in Z_{n!}\} = P^{n\times n}$ is the set of permutations of size $n \times n$. Such a matrix is said to be nontrivial if it is not itself a permutation, or, equivalently, if the vector x is of order two or larger.

Note that a circulant and a positive latin square in $R_+^{n\times n}$ have representations as convex sums of permutations in which the sum is only over n permutations and in the case of a doubly stochastic circulant the permutations are the shifts.

Given a matrix $A \in DS_+^{n\times n}$, its representation as a convex sum of permutations as in Equation (57) is not unique. An algorithm to obtain from A the decomposition may be constructed along the lines of ordinary linear algebra.

Proposition F.2 *Consider the family of doubly stochastic matrices*

$$a_1 I + a_2 P \in DS_+^{n\times n}, \tag{58}$$

where $a_1, a_2 \in (0,1)$, $a_1 + a_2 = 1$, $P \in P^{n\times n}$, $P \neq I$, $n \geq 2$. A matrix of this family is indecomposable iff the permutation matrix P has only one cycle, or, up to relabeling, $c(P) = (1, 2, \ldots, n)$.

Proof It will be proved first that any matrix of the form (58) is indecomposable iff there do not exist $Q_1, Q_2 \in P^{n\times n}$ such that $Z_n = C_1 \cup C_2$, a disjoint union, where $C_1,\ C_2 \subset Z_n$ are either cycles or union of cycles of both Q_1Q_2 and Q_1PQ_2. With this statement the proof follows from Proposition A.4.

$\Rightarrow$. Suppose there exist $Q_1, Q_2 \in P^{n\times n}$ such that $Z_n = C_1 \cup C_2$ with C_1 and C_2 having the properties stated above. It follows from the definition of a cycle that then Q_1Q_2 and Q_1PQ_2 have a decomposition of the form

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

where the diagonal blocks are square and the decomposition is conform the partition $Z_n = C_1 \cup C_2$. Hence $Q_1[a_1 I + a_2 P]Q_2$ has the same decomposition and $a_1 I + a_2 P$ is decomposable. This is a contradiction.

$\Leftarrow$. Suppose $a_1 I + a_2 P$ is not indecomposable, hence decomposable. From Proposition 4.1 follows that this matrix is completely decomposable, or there exist $Q_1, Q_2 \in P^{n\times n}$ such that

$$Q_1[a_1 I + a_2 P]Q_2 = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Hence $Z_n = C_1 \cup C_2$ where C_1 and C_2 are either cycles or unions of cycles of Q_1Q_2 and Q_1PQ_2 where the partition of Z_n is conform the partition in the above matrix. This is a contradiction of the statement made at the start of the proof. □

G Proofs for primes in the doubly stochastic matrices

The proof of Theorem 4.2 is based on a proposition that is first stated and proved.

Proposition G.1 *Let $n_1, n_2 \in Z_+$, $n = n_1 + n_2$, and $A_1 \in DS_+^{n_1 \times n_1}$ be an indecomposable prime in the doubly stochastic matrices. Then*

$$A = A_1 \oplus I = \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} \in DS_+^{n \times n}$$

is a prime in the doubly stochastic matrices.

Proof The proof is analogous to [2, Th. 3.4.24]. Suppose that A is a not a prime in the doubly stochastic matrices. Then there exists a factorization $A = BC$ with $B, C \in DS_+^{n \times n}$ neither of which is a permutation. Let

$$B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} \in R_+^{n \times n}, \quad B_1 \in R_+^{n_1 \times n}.$$

There exists a permutation matrix $Q \in P^{n \times n}$ such that, if B_1 has any zero column, these columns are placed on the right of B_1Q. Then

$$A_1 \oplus I = A = (BQ)(Q^TC) = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

where $B_{11} \in R_+^{n_1 \times r}$, $B_{12} \in R_+^{n_1 \times (n-r)}$, and the other matrices are conformingly. By the choice of Q, $B_{12} = 0$ and no column of B_{11} is zero. If $r = 0$ then $(B_{11}\ B_{12}) = B_{12} = 0$ hence $A_1 = 0$ but this contradicts that A_1 is indecomposable. Thus $r > 0$. Note that $B_{11}C_{12} = 0$. Because B_{11} has no zero columns, it follows that $C_{12} = 0$. If $r = n$ then

$$A_1 \oplus I = \begin{pmatrix} B_{11} \\ B_{12} \end{pmatrix} \begin{pmatrix} C_{11} & 0 \end{pmatrix}$$

but then $I = B_{12}0$ cannot hold. Thus $0 < r < n$.

Note that $A_1 = B_{11}C_{11}$ and $I = B_{22}C_{22}$. If $r < n_1$ then

$$A_1 = (B_{11}\ 0) \begin{pmatrix} C_{11} \\ 0 \end{pmatrix}$$

contradicts that A_1 is prime in the doubly stochastic matrices. If $r > n_1$ then $I = B_{22}C_{22}$, $n - r < n_2$, $B_{22} \in R_+^{n_2 \times (n-r)}$, and $C_{22} \in R_+^{(n-r) \times n_2}$, is a contradiction. Thus $r = n_1$ and $B_{11}, B_{22}, C_{11}, C_{22}$ are square matrices. Note that $B_{21}C_{11} + B_{22}C_{21} = 0$ hence $B_{21}C_{11} = 0$ and $B_{22}C_{21} = 0$. From $B_{22}C_{22} = I$ follows that B_{22} is nonsingular. This and $B_{22}C_{21} = 0$ imply that $C_{21} = 0$. From $A_{11} = B_{11}C_{11}$ follows that C_{11} is either an indecomposable prime or a permutation. In either case, this and $B_{21}C_{11} = 0$ imply that $B_{21} = 0$. From $B_{22}C_{22} = I$ and $B, C \in DS_+^{n \times n}$ follows that $B_{22}, C_{22} \in P^{n_2 \times n_2}$. Finally one obtains the factorization in $DS_+^{n \times n}$

$$A_1 \oplus I = \begin{pmatrix} B_{11} & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} C_{11} & 0 \\ 0 & I \end{pmatrix}.$$

Neither B nor C a permutation implies that neither B_{11} nor C_{11} is a permutation. Hence $A_{11} = B_{11}C_{11}$ is a factorization that contradicts that A_1 is a prime in the doubly stochastic matrices. □

Proof of Theorem 4.2 $\Rightarrow$. From Proposition 4.1 follows that A is permutation equivalent to the direct sum $A_1 \oplus I$ where $A_1 \in DS_+^{n_1 \times n_1}$ is a direct sum of indecomposable doubly stochastic matrices. Then A_1 is a prime in the doubly stochastic matrices. Because, if A_1 is not a prime then there exist $B_1, C_1 \in DS_+^{n_1 \times n_1}$ neither of them is a permutation such that $A_1 = B_1C_1$. Then

$$A = P_1 \begin{pmatrix} A_1 & 0 \\ 0 & I \end{pmatrix} P_2 = [P_1 \begin{pmatrix} B_1 & 0 \\ 0 & I \end{pmatrix}][\begin{pmatrix} C_1 & 0 \\ 0 & I \end{pmatrix} P_2] = BC$$

is a factorization of A such that $B, C \in DS_+^{n \times n}$ and neither of them is a permutation. This contradicts that A is a prime in the doubly stochastic matrices.

Suppose that A_1 is the direct sum of two or more indecomposable doubly stochastic matrices. Without loss of generality suppose that

$$A_1 = P_3 \begin{pmatrix} A_2 & 0 \\ 0 & A_3 \end{pmatrix} P_4,$$

with $P_3, P_4 \in P^{n_1 \times n_1}$ $A_2 \in DS_+^{n_2 \times n_2}$ and $A_3 \in DS_+^{n_3 \times n_3}$ indecomposable. Then consider the factorization

$$A_1 = [P_1 \begin{pmatrix} A_2 & 0 \\ 0 & I \end{pmatrix}][\begin{pmatrix} I & 0 \\ 0 & A_3 \end{pmatrix} P_2] = BC.$$

Because A_2 is indecomposable it is not a permutation, hence so are B and C. Thus A_1 is not a prime in the doubly stochastic matrices which is a contradiction.
$\Leftarrow$. This follows from Proposition G.1.
b. The proof is analogous to that of Theorem 3.1. □

Lemma G.2 *Let*

$$A = \sum_{i=1}^{n!} a_i P_i \in DS_+^{n \times n} \tag{59}$$

be a doubly stochastic matrix that is not a permutation. Hence $a \in S_+^{n!}$ is a vector of order at least two. Let $L_m : S_+^{n!} \to R_+^{n! \times n!}$ be the latin square induced by multiplication of the permutations, see Definition C.2.

a. *Assume that the relation between $A \in DS_+^{n \times n}$ and $a \in S_+^{n!}$ according to Equation (59) is a bijection. If there do not exist $b, c \in S_+^{n!}$ both of which are of order at least two such that*

$$a = L_m(b)c \tag{60}$$

then $A \in DS_+^{n \times n}$ defined above is a prime in the doubly stochastic matrices.

b. *If $A \in DS_+^{n \times n}$ is a prime in the doubly stochastic matrices then there do not exist $b, c \in S_+^{n!}$ both of order at least two such that (60) holds.*

The assumption on the bijection in Lemma G.2.a is satisfied if $A = \sum_{i \in Z_n} a_i P_i$, where $\{P_i, i \in Z_n\}$ is a permutation covering of $R_+^{n \times n}$. An example of a permutation covering is the collection of shifts $\{W_n^{m-1}, m \in Z_n\}$.

Proof of G.2 a. Suppose that A is not a prime in the doubly stochastic matrices. Because by assumption A is not a permutation, this implies that there exist $B, C \in DS_+^{n \times n}$ neither of which is a permutation such that $A = BC$. Because $B, C \in DS_+^{n \times n}$, they admit the representations $B = \sum b_i P_i$ and $C = \sum c_i P_i$, for $b, c \in S_+^{n!}$. Because neither B nor C is a permutation, b, c are vectors of order at least two. Now

$$\sum a_k P_k = A = BC = \left(\sum b_i P_i\right)\left(\sum c_i P_i\right) = \sum_k \left[\sum_{j=1}^{n!} L_m(b)_{kj} c_j\right] P_k,$$

by the definition of the latin square induced by multiplication of permutations. The assumption that the relation between A and a is a bijection now implies that

$$a_k = \sum_{j=1}^{n!} L_m(b)_{kj} c_j, \quad k = 1, 2, \ldots, n!, \quad \Leftrightarrow a = L_m(b)c. \tag{61}$$

Then there exist $b, c \in S_+^{n!}$ of order at least two such that $a = L_m(b)c$. This is a contradiction of the assumption that such b, c do not exist.
b. Suppose there do exist $b, c \in S_+^{n!}$ each of which is at least of order two such that $a = L_m(b)c$. Let $B = \sum b_i P_i$ and $C = \sum c_i P_i$. Then

$$\begin{aligned} BC &= (\sum b_i P_i)(\sum c_j P_j) = \sum_{k=1}^{n!} \left[\sum_i \sum_{j, P_i P_j = P_k} b_i c_j\right] P_k \\ &= \sum_{k=1}^{n!} \left[L_m(b)_{kj} c_j\right] P_k = \sum_k a_k P_k, \quad \text{by } a = L_m(b)c, \\ &= A \end{aligned}$$

Because $b, c \in S_+^{n!}$ are of order at least two, neither B nor C is a permutation. Then this and $A = BC$ imply that A is not a prime in the doubly stochastic matrices. This is a contradiction of the assumption. □

References

[1] A. Berman, M. Neumann, and R.J. Stern. *Nonnegative matrices in dynamic systems.* John Wiley & Sons, New York, 1989.

[2] A. Berman and R.J. Plemmons. *Nonnegative matrices in the mathematical sciences.* Academic Press, New York, 1979.

[3] A. Berman and R.J. Plemmons. *Nonnegative matrices in the mathematical sciences.* Number 9 in Classics in Applied Mathematics. SIAM, Philadelphia, 1993.

[4] R.A. Brualdi, S.V. Parter, and H. Schneider. The diagonal equivalence of a nonnegative matrix to a stochastic matrix. *J. Math. Anal. Appl.*, 16:31–50, 1966.

[5] R.A. Brualdi and H.J. Ryser. *Combinatorial matrix theory.* Cambridge University Press, Cambridge, 1991.

[6] P.J. Davis. *Circulant matrices.* Wiley, New York, 1979.

[7] D. de Caen and D.A. Gregory. Primes in the semigroup of boolean matrices. *Linear Algebra Appl.*, 37:119–134, 1981.

[8] J. Dénes and A.D. Keedwell. *Latin squares: New developments in the theory and applications.* North-Holland, Amsterdam, 1991.

[9] J. Dieudonné. *Foundations of modern analysis.* Academic Press, New York, 1969.

[10] M. Gondran and M. Minoux. *Graphs and algorithms.* John Wiley & Sons, Chichester, 1984.

[11] M. Gondran and M. Minoux. Linear algebra in dioids: a survey of recent results. *Ann. Discrete Math.*, 19:147–164, 1984.

[12] N. Jacobson. *Basic algebra, volumes 1, 2, 2nd edition.* W.H. Freeman and Company, New York, 1985.

[13] M. Lewin. On nonnegative matrices. *Pacific J. Math.*, 36:753–759, 1971.

[14] D. London. On matrices with a doubly stochastic pattern. *J. Math. Anal. Appl.*, 34:648–652, 1971.

[15] M. Marcus, K. Kidman, and M. Sandy. Products of elementary doubly stochastic matrices. *Linear and Multilinear Algebra*, 15:331–340, 1984.

[16] A.W. Marshall and I. Olkin. *Inequalities: Theory of majorization and its applications.* Academic Press, New York, 1979.

[17] H. Minc. *Nonnegative matrices.* Wiley, New York, 1988.

[18] L. Mirsky. Results and problems in the theory of doubly-stochastic. *Z. Wahrscheinlichkeitstheorie*, 1:319–334, 1963.

[19] B.N. Parlett and T.L. Landis. Methods for scaling to doubly stochastic form. *Linear Algebra Appl.*, 48:53–79, 1982.

[20] H. Perfect and L. Mirsky. The distribution of positive elements in doubly stochastic matrices. *J. London Math. Soc.*, 40:689–698, 1965.

[21] G. Picci, J.M. van den Hof, and J.H. van Schuppen. Primes in the doubly stochastic circulants. Preprint, CWI, Amsterdam, 1995.

[22] G. Picci and J.H. van Schuppen. Stochastic realization of finite-valued processes and primes in the positive matrices. In H. Kimura and S. Kodama, editors, *Recent advances in mathematical theory of systems, control, networks, and signal processing II - Proceedings of the International Symposium MTNS-91*, pages 227–232, Tokyo, 1992. Mita Press.

[23] D.J. Richman and H. Schneider. Primes in the semigroup of non-negative matrices. *Linear and Multilinear Algebra*, 2:135–140, 1974.

Contents