Centrum voor Wiskunde en Informatica
REPORT*RAPPORT*

Primes in the doubly stochastic circulants

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

Department of Operations Reasearch, Statistics, and System Theory

BS-R9536 1995

Report BS-R9536
ISSN 0924-0659

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

Primes in the Doubly Stochastic Circulants

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 doubly stochastic circulants is that of a semi-ring. The concept of a prime in the doubly stochastic circulants is introduced in this paper and examples are given. The classification of a prime in the doubly stochastic circulants is equivalent to the solvability of a linear equation over a doubly stochastic circulant. A representation of doubly stochastic circulants as polynomials in the quotient semi-ring of $R_+[z]$ is presented.

AMS Subject Classification (1991): 15A48, 15A23, 15A51.
Keywords and Phrases: Prime, positive matrix, doubly stochastic circulant, semi-ring.
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 doubly stochastic circulants.

The motivation of the authors for the study of positive linear algebra lies in problems of the research area of control and system theory. The stochastic realization problem for finite-valued processes, see [12], and the realization problem for positive linear systems, see [8], are not completely solved. In the literature the first problem is also called the realization problem for the hidden Markov model, for a partially observed Markov chain, and for a finite stochastic system. The second problem is related to systems in which inputs, states, and outputs take positive values. The main question for both related problems is the characterization of minimality. This question reduces to a problem of positive linear algebra, see [8, 12].

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 [13]. 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 [1, Sec. 3.4] and [13]. Primes in the Boolean matrices were explored in [2].

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. It is expected that the structure theory for positive matrices, that will result from a classification of primes in the positive matrices may be useful for the research area of systems and control.

The problem studied in this paper is the classification of primes in the doubly stochastic circulants. Doubly stochastic circulants is a class of doubly stochastic matrices with a special structure. Doubly stochastic matrices, for their part, form a class of positive matrices. The primes in the positive matrices and in the doubly stochastic matrices are discussed in [11].

The classification of the primes in the doubly stochastic circulants can be reduced to the solvability of a linear equation over a doubly stochastic circulant. The solvability problem reduces to (1) a discrete problem that may be phrased in terms of shifts and (2) an analytic problem of a quadratic character. The second problem is studied in Appendix A. The results of the paper are the classification of primes for small size matrices, such as for 3×3 and 4×4, and of primes described by vectors of low order.

The outline of the paper is as follows. Section 2 contains definitions and a problem formulation. In Section 3 primes in the doubly stochastic circulants are compared to primes in a quotient semi-ring of polynomials. Results of the classification of primes in the doubly stochastic circulants are presented in Section 4 and concluding remarks are made in Section 5. The solvability of a linear equation over a doubly stochastic circulant is discussed in Appendix A.

2. Definitions and problem formulation

In this section a prime in the doubly stochastic circulants is defined and the problem is posed of classifying all such primes. The presentation in this section starts with definitions.

2.1 Definitions

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 [4, 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. Denote the *simplex* in R_+^n by

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

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 if exactly k elements of a are strictly positive. Notation $n(a) = k$. The indices of the strictly positive elements of such a vector are denoted by

$$i(a) = \{i_1, i_2, \ldots, i_k\} \subset Z_n. \qquad \square$$

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 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 $DS_+^{n\times n}$.

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

$$A_{ij} = A_{i+1,j+1}, \quad \text{for all } i \in Z_{n-1}, j \in Z_{n-1}, \tag{2.1}$$
$$A_{nj} = A_{1,j+1}, \quad \text{for all } j \in Z_{n-1}, \tag{2.2}$$
$$A_{in} = A_{i+1,1}, \quad \text{for all } i \in Z_{n-1}, \tag{2.3}$$
$$A_{nn} = A_{11}. \tag{2.4}$$

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

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

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

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

The terminology used above is fairly standard, see [1]. A circulant is mentioned in [10, 2.H.2]. Above structures are related according to

$$DSC_+^{n\times n} \subset DS_+^{n\times n} \subset R_+^{n\times n}.$$

These structures are semi-rings. A unit in a semi-ring is an element whose inverse exists in the semi-ring. These concepts will be explained in Subsection 2.2.1

Example 2.3 Consider

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}.$$

Then $A \in R_+^{3\times 3}$ is a positive circulant and $A/6$ is a doubly stochastic circulant. $\square$

Another notion that will be used in this paper is permutation equivalence, defined below.

Definition 2.4 The positive matrices $A_1, A_2 \in R_+^{n\times n}$ are said to be *permutation equivalent* if

$$A_1 = X_1 A_2 X_2 \tag{2.5}$$

for permutation matrices $X_1, X_2 \in P^{n\times n}$. □

2.1.1 Shifts

Definition 2.5 For $n \in Z_+$ define the *shift* as the permutation matrix

$$W_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in R_+^{n\times n}. \tag{2.6}$$

□

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

Proposition 2.6 *Let $n \in Z_+$ and $W_n \in P^{n\times n}$ be the shift defined above.*

a. *For any $m = 0, 1, \dots, n-1$, $W_n^m \in P^{n\times n}$ corresponds to a shift of length m applied to a set with n elements.*

b. $W_n^n = I$.

c. $W_n^i W_n^j = W_n^{i+j|n}$, *where $i + j|n$ denotes that $i + j$ is taken modulo n.*

d. $(W_n^i)^{-1} = W_n^{n-i|n}$.

Proof The elementary proof is omitted. □

A circulant or circular matrix can be written as a convex combination of shifts, as given in the following proposition.

Proposition 2.7 *The matrix $A \in R^{n\times n}$ is a circulant if and only if there exists a vector $a \in R^n$ such that*

$$A = \sum_{i=1}^{n} a_i W_n^{i-1}, \tag{2.7}$$

where $W_n \in P^{n\times n}$ is the shift, see Definition 2.5.

Proof The elementary proof is omitted. □

More results on circulants can be found in [3].

2.2 Primes

In this subsection primes are introduced. First a general algebraic definition is given, and then this will be applied to primes in doubly stochastic circulants.

2.2.1 Algebraic definition of a prime The algebraic structure of the set of doubly stochastic circulants 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 [9, 2.1].

Definition 2.8 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 $a, b, c \in X$

$$a.(b + c) = a.b + a.c, \quad (b + c).a = b.a + c.a, \quad a.0 = 0.a = 0.$$

□

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 [6, p. 86], see also [7]. Examples of a semi-ring are R_+, the set of positive matrices $R_+^{n\times n}$ and the set of doubly stochastic circulants $DSC_+^{n\times n}$ for any $n \in Z_+$, by Proposition 2.9 below.

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 and denoted by u^{-1}. It is 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. It is 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 exist $u_1, u_2 \in U$ 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 such that the only divisors of p are either units or associates of p. Equivalently, $p \in X$ is a prime if and only if 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 multiplicative monoid $(X, ., I)$.

2.2.2 Matrix definition of a prime

Proposition 2.9 *The set of doubly stochastic circulants with the multiplication operation $(DSC_+^{n\times n}, ., I)$ is a monoid for any $n \in Z_+$.*

Proof Let $A, B \in DSC_+^{n\times n}$ say, by Proposition 2.7, with representations

$$A = \sum a_i W_n^{i-1}, \quad B = \sum b_i W_n^{i-1}.$$

Then

$$\begin{aligned} AB &= (\sum a_i W_n^{i-1})(\sum b_i W_n^{i-1}) = \sum_i \sum_j a_i b_j W_n^{i+j-2} \\ &= \sum_k \left(\sum_i a_i b_{k+1-i|n} \right) W_n^{k-1} \in DSC_+^{n\times n}, \quad \text{with } k = i+j-1. \end{aligned}$$

□

Before defining the prime in the doubly stochastic circulants, the units in the doubly stochastic circulants must be determined.

Proposition 2.10 *Let $A \in DSC_+^{n\times n}$. Then A has an inverse in the doubly stochastic circulants if and only if A is a shift.*

Proof ($\Rightarrow$) Let $A \in DSC_+^{n\times n}$ have an inverse in the doubly stochastic circulants, i.e., A^{-1} exists and $A^{-1} \in DSC_+^{n\times n}$. But also $A \in R_+^{n\times n}$ and $A^{-1} \in DSC_+^{n\times n} \subset R_+^{n\times n}$. Hence A is a unit of the positive matrices. From [1, 3.4.3] may be deduced that A is a monomial matrix. Because $A \in DSC_+^{n\times n}$, A is a permutation. But by Proposition 2.7 $A = \sum a_i W_n^{i-1}$. Therefore the fact that A is a permutation implies that $A = W_n^i$ for one $i \in \{0, 1, \ldots, n-1\}$. Thus A is a shift.
($\Leftarrow$) Let A be a shift, say $A = W_n^i$, for some $i \in \{0, 1, \ldots, n-1\}$. Then $A^{-1} = (W_n^i)^{-1} = W_n^{n-i} \in DSC_+^{n\times n}$ by Proposition 2.6.d. Thus A has an inverse in $DSC_+^{n\times n}$. □

It follows that in the set of doubly stochastic circulants the group of units is

$$U = \left\{ W_n^0, W_n^1, \ldots, W_n^{n-1} \right\}, \tag{2.8}$$

where W_n is the shift and $W_n^0 = I$.

Definition 2.11 A *prime in the set of doubly stochastic circulants* $DSC_+^{n\times n}$ is a doubly stochastic circulant $A \in DSC_+^{n\times n}$ such that

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

The problem in this paper is:

Problem 2.12 Classify all primes in the doubly stochastic circulants.

3. Polynomial representation of doubly stochastic circulants

Recall that any $n \times n$ circulant matrix A has a *unique* representation as a polynomial of degree $n-1$ in the shift operator W_n, see Proposition 2.7,

$$A = \sum_{i=0}^{n-1} a_i W_n^i.$$

The map associated to A,

$$a(z) = \sum_{i=0}^{n-1} a_i z^i,$$

is called its *representer* or *incidence polynomial*. It is a *ring homomorphism*, [3, p. 68-70]. Since $W_n^n = I$, in all operations involving representers of $n \times n$ circulant matrices, the nth power z^n must be treated as 1, i.e. the polynomial $z^n - 1$ is equivalent to the zero polynomial. The homomorphism above becomes a ring isomorphism if the ring of polynomials is substituted by the quotient ring $R[z]/(z^n - 1)$.

From these general facts it follows in particular that the representer of a doubly stochastic circulant $A \in DSC_+^{n\times n}$ is a polynomial in z with positive coefficients summing up to one, i.e. with the property $a(1) = 1$. The semi-ring of polynomials with positive coefficients will be denoted by $R_+[z]$, the semi-ring of polynomials $p(z)$ with positive coefficients normalized such that $p(1) = 1$ by $S_+[z]$, and the quotient semi-ring of $R_+[z]$ ($S_+[z]$ respectively) modulo $z^n - 1$ by $R_+[z]/(z^n - 1)$ ($S_+[z]/(z^n - 1)$ respectively). Clearly $DSC_+^{n\times n}$ and $S_+[z]/(z^n - 1)$ are isomorphic as semi-rings. A matrix $A \in DSC_+^{n\times n}$ is a unit if and only its representer $a(z)$ is a monomial in $S_+[z]/(z^n - 1)$, i.e. $a(z) = z^k$.

Definition 3.1 A *prime* in the quotient semi-ring $S_+[z]/(z^n - 1)$ is a polynomial $a(z)$ in the quotient semi-ring $S_+[z]/(z^n - 1)$ such that

1. $a(z)$ is not a monomial, i.e. $a(z) \neq z^k$;
2. if $a(z) = b(z)c(z)$ with $b(z), c(z) \in S_+[z]/(z^n - 1)$, then either $b(z)$ or $c(z)$ is a monomial. □

Whenever $a(z) = b(z)c(z)$ with $b(z), c(z) \in S_+[z]/(z^n - 1)$, neither of them being monomial, $b(z)$ (or $c(z)$) is said to *divide* $a(z)$ *strongly*.

It is obvious that for a positive factorization $a(z) = b(z)c(z)$, $a(z) \in S_+[z]/(z^n - 1)$, the factors $b(z), c(z) \in R_+[z]/(z^n - 1)$ can both be normalized by dividing them by positive numbers $b(1), c(1)$ such that $a(1) = 1 = b(1)c(1)$. Therefore, taking as group of units the set $\{\alpha z^k \mid \alpha \in R_+,\ k \in \mathbb{N}\}$, primes in $R_+[z]/(z^n - 1)$ are essentially the same as primes in $S_+[z]/(z^n - 1)$, up to multiplication with a constant.

Proposition 3.2 *A matrix $A \in DSC_+^{n\times n}$ is a prime in the doubly stochastic circulants if and only if its representer is a prime in the quotient semi-ring $S_+[z]/(z^n - 1)$.*

Proof. Let

$$A = \sum_{i=0}^{n-1} a_i W_n^i.$$

The representer of A is

$$a(z) = \sum_{i=0}^{n-1} a_i z^i.$$

A is a prime in the doubly stochastic circulants if and only if

1. A is not a monomial;

2. if $A = BC$, with $B, C \in DSC_+^{n\times n}$ then B or C is a monomial.

1 is equivalent to '$a(z)$ is not a monomial'. Let $B = \sum b_i W_n^i$ and $C = \sum c_i W_n^i$. Their representers are $b(z) = \sum b_i z^i$ and $c(z) = \sum c_i z^i$ respectively. It follows that $A = BC$ is equivalent to $a(z) = b(z)c(z)$, so 2 is equivalent to 'if $a(z) = b(z)c(z)$, with $b(z), c(z) \in S_+[z]/(z^n - 1)$ then $b(z)$ or $c(z)$ is a monomial'. So A is a prime in the doubly stochastic circulants if and only if $a(z)$ is a prime in the quotient semi-ring $S_+[z]/(z^n - 1)$. □

The following example shows that prime in $R_+[z]/(z^n - 1)$ is not the same as prime in $R_+[z]$.

Example 3.3 Consider the polynomial $f(z) = z^3 + z + 10$. This polynomial can be factorized as $f(z) = (z+2)(z^2 - 2z + 5) = (z+2)(z-1+2i)(z-1-2i)$. There are no factors of $f(z)$ in $R_+[z]$, unequal to a monomial, so $f(z)$ is prime in $R_+[z]$. But in $R_+[z]/(z^4 - 1)$,

$$f(z) = (z^3 + \lambda z^2)(z^2 + \mu z)$$

with $\lambda = 5 + 2\sqrt{6} > 0$ and $\mu = 5 - 2\sqrt{6} = 5 - \sqrt{24} > 0$. So $f(z)$ is not prime in $R_+[z]/(z^4 - 1)$. It follows that $f(z)/12$ is not prime in $S_+[z]/(z^4 - 1)$ and hence

$$A = \frac{1}{12}\begin{pmatrix} 10 & 1 & 0 & 1 \\ 1 & 10 & 1 & 0 \\ 0 & 1 & 10 & 1 \\ 1 & 0 & 1 & 10 \end{pmatrix}$$

is not prime in $DSC_+^{4\times 4}$. □

The problem is to find for a polynomial $a(z) \in R_+[z]/(z^n - 1)$ a factorization with factors in $R_+[z]/(z^n - 1)$.

Lemma 3.4 *Consider $a(z) \in R_+[z]/(z^n - 1)$. There exist $b(z), c(z) \in R_+[z]/(z^n - 1)$, neither of which is a monomial, such that*

$$a(z) = b(z)c(z) \pmod{z^n - 1},$$

if and only if there exists a polynomial $g(z) \in R_+[z]$ of degree less than $n-1$, such that

$$a(z) + (z^n - 1)g(z) \in R_+[z]$$

can be factorized into $h(z)k(z)$ in $R_+[z]$ with neither $h(z) \pmod{z^n - 1}$ nor $k(z) \pmod{z^n - 1}$ monomial.

Proof. ($\Rightarrow$) Assume there exist polynomials $b(z), c(z) \in R_+[z]/(z^n - 1)$, neither of which is a monomial, such that

$$a(z) = b(z)c(z) \pmod{z^n - 1}.$$

This is equivalent to

$$a(z) + (z^n - 1)g(z) = b(z)c(z)$$

for a polynomial $g(z) \in R[z]$. Since $b(z), c(z) \in R_+[z]/(z^n-1)$, their degrees are less than or equal to $n-1$, so $\deg((z^n-1)g(z)) \leq \deg(b(z)c(z)) \leq 2n-2$, i.e. $\deg(g(z)) \leq n-2$. Let $g(z) = g_0 + g_1 z + \cdots + g_{n-2}z^{n-2}$, for $g_i \in R$. Then $b(z)c(z) = a(z) - g(z) + g_0 z^n + g_1 z^{n+1} + \cdots + g_{n-2}z^{2n-2}$. Now $g_i \geq 0$, since $\deg(a(z) - g(z)) \leq n-1$ and $b(z)c(z) \in R_+[z]$. From this it follows that $g(z) \in R_+[z]$ and $a(z) + (z^n-1)g(z)$ can be factorized into $b(z)c(z)$ with $b(z) \pmod{z^n-1}$ and $c(z) \pmod{z^n-1}$ not monomials.
($\Leftarrow$) Assume there exists a polynomial $g(z) \in R_+[z]$ of degree less than $n-1$, such that for

$$f(z) = a(z) + (z^n-1)g(z) \in R_+[z]$$

there exist polynomials $h(z), k(z) \in R_+[z]$, such that $f(z) = h(z)k(z)$. Let $b(z) = h(z) \pmod{z^n-1}$ and $c(z) = k(z) \pmod{z^n-1}$. Then

$$a(z) = f(z) \pmod{z^n-1} = h(z)k(z) \pmod{z^n-1} = b(z)c(z) \pmod{z^n-1}.$$

From the assumptions it follows that $b(z)$ and $c(z)$ are not monomials. This completes the proof. □

To start the classification of primes in $S_+[z]/(z^n-1)$, or equivalently, the classification of primes in the doubly stochastic circulants, the following result can be stated.

Proposition 3.5 *The polynomial*

$$p(z) = \sum_{i=0}^{n-1} p_i z^i \in R_+[z]/(z^n-1), \tag{3.1}$$

with $p_i > 0$ for all $i \in \boldsymbol{N}_{n-1}$, is not prime in the quotient semi-ring $R_+[z]/(z^n-1)$.

Proof. Consider first the polynomial $p(z)$ with $p_i = p_j = \bar{p}$ for all $i, j \in \boldsymbol{N}_{n-1}$. Then

$$p(z) = \sum_{i=0}^{n-1} p_i z^i = \sum_{i=0}^{n-1} \bar{p} z^i = \frac{1}{2}(z+1)\sum_{i=0}^{n-1} \bar{p} z^i = \frac{1}{2}(z+1)p(z) \pmod{z^n-1}.$$

So $p(z)$ is not prime in the quotient semi-ring $R_+[z]/(z^n-1)$.
Otherwise, if there exist $i, j \in \boldsymbol{N}_{n-1}$ such that $p_i \neq p_j$, choose

$$0 < a < \min\{\frac{p_0}{p_{n-1}}, \frac{p_i}{p_{i-1}},\ i \in Z_{n-1}\}.$$

Since $p_i > 0$ for all $i \in \boldsymbol{N}_{n-1}$, the minimum mentioned above is strictly positive, so such an a exists. The claim is that $a < 1$. Indeed, suppose $a \geq 1$. Then $p_0/p_{n-1} > a \geq 1$ and $p_i/p_{i-1} > a \geq 1$ for all $i \in Z_{n-1}$, so

$$1 \leq a^{n-1} < \frac{p_0}{p_{n-1}} \prod_{i=1}^{n-1} \frac{p_i}{p_{i-1}} = 1.$$

This is a contradiction, so $a < 1$. Now $p(z)$ can be factorized in $b(z)c(z)$ in $R_+[z]/(z^n-1)$ with

$$\begin{aligned} b(z) &= \frac{1}{1-a^n}\sum_{i=0}^{n-1} a^i z^i, \\ c(z) &= p_0 - a p_{n-1} + \sum_{i=1}^{n-1}(p_i - a p_{i-1}) z^i. \end{aligned}$$

Indeed,

$$b(z)c(z) = \sum_{i=0}^{n-1} b_i z^i \sum_{j=0}^{n-1} c_j z^j = \sum_{k=0}^{n-1} \Big(\sum_{i=0}^{n-1} b_{k-i|n} c_i \Big) z^k \pmod{z^n - 1}.$$

Since for all $\in \boldsymbol{N}_{n-1}$

$$\begin{aligned}
\sum_{i=0}^{n-1} b_{k-i|n} c_i &= \sum_{i=0}^{k} b_{k-i} c_i + \sum_{i=k+1}^{n-1} b_{n+k-i} c_i \\
&= \frac{1}{1-a^n} \Big\{ (p_0 - a p_{n-1}) a^k + \sum_{i=1}^{k} a^{k-i} (p_i - a p_{i-1}) + \sum_{i=k+1}^{n-1} a^{n+k-i} (p_i - a p_{i-1}) \Big\} \\
&= \frac{1}{1-a^n} (a^k p_0 - a^{k+1} p_{n-1} + a^{k-1} p_1 - a^k p_0 + \ldots + a^0 p_k - a p_{k-1} + \\
&\quad + a^{n-1} p_{k+1} - a^n p_k + \ldots + a^{k+1} p_{n-1} - a^{k+2} p_{n-2}) \\
&= \frac{1}{1-a^n} (1 - a^n) p_k = p_k,
\end{aligned}$$

it follows that $p(z) = b(z)c(z) \pmod{z^n - 1}$. Because $a < 1$, $b_i = a^i/(1-a^n) > 0$, and since $a < p_0/p_{n-1}$ and $a < p_i/p_{i-1}$ for $i \in Z_{n-1}$, also $c_0 = p_0 - a p_{n-1} > 0$ and $c_i = p_i - a p_{i-1} > 0$. So $b(z)$ and $c(z)$ in $R_+[z]/(z^n - 1)$ are not monomials, from which it follows that $p(z)$ is not a prime in the quotient semi-ring $R_+[z]/(z^n - 1)$. □

4. Primes in the doubly stochastic circulants

In this section results are presented on the classification of primes in the doubly stochastic circulants.

Proposition 4.1 *If $A \in DSC_+^{n \times n}$ is a prime in the doubly stochastic circulants with*

$$A = \mathrm{circ}(a),$$

then $n(a) < n$.

Proof. This follows from Proposition 3.5. □

Theorem 4.2 *Let $A \in DSC_+^{n \times n}$ be a doubly stochastic circulant of order two, for $n \geq 3$. Then A is a prime in the doubly stochastic circulants.*

Proof This follows directly form Lemma A.1 and Proposition A.6. □

Corollary 4.3 *Let $A \in DSC_+^{4 \times 4}$ be a doubly stochastic circulant of order 2. Then this matrix is a prime in the doubly stochastic circulants if and only if*

1. *either*

$$A = W_4^k \begin{pmatrix} a_1 & 0 & 0 & a_2 \\ a_2 & a_1 & 0 & 0 \\ 0 & a_2 & a_1 & 0 \\ 0 & 0 & a_2 & a_1 \end{pmatrix} W_4^j \cong \mathrm{circ}(a) = \sum_i a_i W_4^{i-1}, \quad a = \begin{pmatrix} a_1 \\ a_2 \\ 0 \\ 0 \end{pmatrix}, \qquad (4.1)$$

where $a \in S_+^4$, $n(a) = 2$, $i(a) = (1, 2)$;

2. or

$$A = W_4^k \begin{pmatrix} a_1 & 0 & a_3 & 0 \\ 0 & a_1 & 0 & a_3 \\ a_3 & 0 & a_1 & 0 \\ 0 & a_3 & 0 & a_1 \end{pmatrix} W_4^j \cong \mathrm{circ}(a) = \sum_i a_i W_4^{i-1}, \quad a = \begin{pmatrix} a_1 \\ 0 \\ a_3 \\ 0 \end{pmatrix}, \tag{4.2}$$

where $a \in S_+^4$, $n(a) = 2$, $i(a) = (1, 3)$.

Theorem 4.4 *Let* $A \in DSC_+^{4\times 4}$ *be a doubly stochastic circulant of order* 3. *This matrix is a prime in the doubly stochastic circulants if and only if*

$$A = W_4^k \begin{pmatrix} a_1 & 0 & a_3 & a_2 \\ a_2 & a_1 & 0 & a_3 \\ a_3 & a_2 & a_1 & 0 \\ 0 & a_3 & a_2 & a_1 \end{pmatrix} W_4^j \cong \mathrm{circ} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \mathrm{circ}(a) = \sum_{i=1}^{4} a_i W_4^{i-1}, \tag{4.3}$$

where $a \in S_+^4$ *and* $a_2^2 < 4a_1a_3$.

Proof Let $A \in DSC_+^{4\times 4}$ with $n(a) = 3$ and representation

$$A = \sum a_i W_4^{i-1} = \mathrm{circ}(a).$$

By Lemma A.1 A is a prime in the doubly stochastic circulants if and only if there do not exist $b, c \in S_+^4$ of order at least two such that $a = \mathrm{circ}(b)c$. By Proposition A.11 there do not exist such $b, c \in S_+^4$ if and only if $a_2^2 < 4a_1a_3$, since the only possible form of a up to permutation equivalence by a unit is

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} \in S_+^4.$$

Thus (4.3) represents the only family of primes in the doubly stochastic circulants of $DSC_+^{4\times 4}$. □

Example 4.5 The matrix

$$A = \frac{1}{3} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in DSC_+^{4\times 4} \tag{4.4}$$

is a prime in the doubly stochastic circulants. This follows from Example A.10, Proposition A.11, and Theorem 4.4. □

Theorem 4.6 *Let* $A \in DSC_+^{5\times 5}$ *be a doubly stochastic circulant of order* 4. *Then this matrix is not a prime in the doubly stochastic circulants.*

Proof This follows from Lemma A.1 and Proposition A.12. □

The preceding result motivates the following conjecture.

Conjecture 4.7 *Let $n \in Z_+$, $n \geq 6$, and let $A \in DSC_+^{n\times n}$ be of order $n-1$. Then A is not a prime in the doubly stochastic circulants.*

Enlarging the size of the matrix but keeping the order 3 or 4 gives the following result.

Proposition 4.8 *Let $A \in DSC_+^n$ be a doubly stochastic circulant of order $3 \leq n(a) \leq 4$, such that*

$$A = W_n^{k-1}\mathrm{circ}\begin{pmatrix} a_1 \\ \vdots \\ a_{n(a)} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

for some $k \in Z_n$. Assume $n(a) < n$. A is prime in the doubly stochastic circulants if and only if

1. *$a_2^2 < 4a_1a_3$ for $n(a) = 3$;*
2. *never for $n(a) = 4$, $n = 5$;*
3. *$a_1a_4 > a_2a_3$ for $n(a) = 4$, $n \geq 6$.*

Proof. This follows from Lemma A.1 and Proposition A.13. □

There exist doubly stochastic circulants of order e.g. 3 that are prime, independent of the values of the nonzero elements. An example is $A = \mathrm{circ}(a) \in DSC_+^{9\times 9}$ with

$$a = \begin{pmatrix} a_1 & 0 & a_3 & 0 & 0 & a_6 & 0 & 0 & 0 \end{pmatrix}^T \in S_+^9, \quad a_1 > 0,\ a_3 > 0,\ a_6 > 0.$$

From the nonzero pattern and Lemma A.5 it follows that there do not exist $b, c \in S_+^9$ of order at least two such that $a = \mathrm{circ}(b)c$.

5. Concluding remarks

The problem of the classification of primes in the doubly stochastic circulants has been studied. For low order doubly stochastic circulants a characterization has been given. For higher order the problem cannot generally be solved, since the solvability of a linear equation over a doubly stochastic circulant becomes complicated. The polynomial representation of doubly stochastic circulants turns out to be a nice compact way of representing the doubly stochastic circulants, but unfortunately it does not simplify the calculations.

Appendix

A. Linear equation over a doubly stochastic circulant

In Subsection A.1 it will be shown that the classification of a prime in the doubly stochastic circulants is equivalent to solvability of a linear equation over a doubly stochastic circulant. The latter problem is analyzed in Subsection A.2.

A.1 Problem formulation

Lemma A.1 *Let $A \in DSC_+^{n\times n}$ be of order larger or equal than 2, say with representation*

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

Then the following statements are equivalent.

a. *The matrix $A \in DSC_+^{n\times n}$ is a prime in the doubly stochastic circulants.*

b. *There do not exist $b, c \in S_+^n$ each of which is of order at least two such that*

$$a = \mathrm{circ}(b)c. \tag{A.2}$$

Proof a. $\Rightarrow$ b. Suppose there do exist $b, c \in S_+^n$ of order at least two such that $a = \mathrm{circ}(b)c$. Then

$$\begin{aligned} A &= \sum a_i W_n^{i-1} = \sum_i \left(\sum_j b_{i-j+1|n} c_j \right) W_n^{i-1} \\ &= \sum_j \sum_k b_k c_j W_n^{k-1} W_n^{j-1} = \left(\sum_k b_k W_n^{k-1} \right) \left(\sum_j c_j W_n^{j-1} \right) = BC. \end{aligned}$$

Because $b, c \in S_+^n$ are of order at least two, $B, C \in DSC_+^{n\times n}$ are not units. Thus A is not a prime in the $DSC_+^{n\times n}$. This is a contradiction of the assumption.
b. $\Rightarrow$ a. Suppose that $A \in DSC_+^{n\times n}$ is not a prime in the doubly stochastic circulants. Then there do exist $B, C \in DSC_+^{n\times n}$ which are not units, thus of order larger or equal than two, such that $A = BC$. Then

$$\begin{aligned} \sum a_i W_n^{i-1} &= A = BC = \left(\sum b_i W_n^{i-1} \right) \left(\sum c_j W_n^{j-1} \right) \\ &= \sum_i \sum_j b_i c_j W_n^{i+j-2} = \sum_k \left(\sum_j b_{k-j+1|n} c_j \right) W_n^{k-1}, \end{aligned}$$

hence

$$a_i = \sum_j b_{i-j+1|n} c_j, \quad \text{for all } i \in Z_n,$$

which is equivalent to $a = \mathrm{circ}(b)c$. Thus there exist $b, c \in S_+^n$ of order at least two such that $a = \mathrm{circ}(b)c$. This is a contradiction of assumption b. □

Problem A.2 *Solvability of a linear equation over a doubly stochastic circulant.* Let $a \in S_+^n$ be a vector of order at least two. Determine conditions on this vector such that there exist vectors $b, c \in S_+^n$, each of which is of order at least two, such that

$$a = \mathrm{circ}(b)c. \tag{A.3}$$

As mentioned in Definition 2.1 the orders of a, b, and c are denoted respectively by $n(a)$, $n(b)$, and $n(c)$, and the set of indices of the strictly positive elements of the vector a by $i(a) \subset Z_n$.

For $x \in R_+^n$ let

$$x_{[1]} \geq x_{[2]} \geq \ldots \geq x_{[n]}, \tag{A.4}$$

denote the components of x in decreasing order.

Definition A.3 For $x, y \in R_+^n$ one says that x is *majorized* by y or that y *majorizes* x, if

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

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

Let $x, y \in R_+^n$. The following statements are equivalent:

a. $x \preceq y$.

b. There exists an $S \in DS_+^{n \times n}$ such that $x = Sy$.

c. $\sum_{i=1}^{n} f(x_i) \leq \sum_{i=1}^{n} f(y_i)$ for all convex functions $f : R_+^n \to R$.

A source on the specialization order is [10].

Proposition A.4 *Let $n \in Z_+$, $n \geq 2$, and $a \in S_+^n$. Assume that there exist $b, c \in S_+^n$ such that*

$$a = \mathrm{circ}(b)c.$$

Then $n(b) \leq n(a)$ or the order of b is less than or equal to that of a, and similarly $n(c) \leq n(a)$.

Proof The assumptions that $b \in S_+^n$ and $\mathrm{circ}(b)$ is a circulant imply that $\mathrm{circ}(b) \in DS_+^{n \times n}$. It then follows from above and equation (A.3) 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, so $n(c) \leq n(a)$. By symmetry of the equation (A.3) in b, c, the inequality $n(b) \leq n(a)$ follows. □

Lemma A.5 *Let $a \in S_+^n$ be a vector with order $n(a) \geq 2$. If there exist $b, c \in S_+^n$ each of which is of order at least two such that*

$$a = \mathrm{circ}(b)c \tag{A.5}$$

then

$$i(a) = \cup_{j=1, c_j>0}^{n} i(W_n^{j-1}b).$$

Proof Let $a \in S_+^n$ with $n(a) \geq 2$ and suppose there exist $b, c \in S_+^n$ each of which is of order at least two such that $a = \mathrm{circ}(b)c$. Note that $a = \mathrm{circ}(b)c$ is equivalent to

$$a_k = \sum_{j=1}^{n} (W_n^{j-1}b)_k c_j, \quad \text{for } k \in Z_n.$$

Now $a_k > 0$ if and only if there exists a $j_1 \in Z_n$ such that $(W_n^{j_1-1}b)_k > 0$ and $c_{j_1} > 0$. This is equivalent to $k \in i(W_n^{j_1-1}b)$ for $c_{j_1} > 0$, which implies

$$k \in \cup_{j=1, c_j>0}^{n} i(W_n^{j-1}b).$$

This completes the proof. □

A.2 Small size linear equations over a doubly stochastic circulant

Below solutions are presented to several special cases of Problem A.2. The results are ordered by the order of the vector $a \in S_+^n$. It follows from Proposition 4.1 that only a matrix in $DSC_+^{n\times n}$ of order smaller or equal than $n-1$ is eligible to be a prime.

Proposition A.6 *Let $n \in Z_+$, $n \geq 3$, and $a \in S_+^n$ with order $n(a) = 2$. Then there do not exist $b, c \in S_+^n$ of order at least two such that*

$$a = \mathrm{circ}(b)c. \tag{A.6}$$

Proof Assume there exist $b, c \in S_+^n$ of order at least two such that (A.6) holds. Then by Proposition A.4, $n(b) \leq n(a) = 2$ and $n(c) \leq n(a) = 2$, hence $n(b) = n(c) = 2$. From Lemma A.5 it follows that

$$i(a) = \cup_{j=1, c_j>0}^{n} i(W_n^{j-1}b), \tag{A.7}$$

while

$$2 = n(a) < 3 \leq n(\cup_{j=1, c_j>0}^{n} i(W_n^{j-1}b)), \tag{A.8}$$

where the last inequality follows because the union is exactly over two values of j, say j_1, j_2, with $n(W_n^{j_1-1}b) = 2$, $i(W_n^{j_1-1}b) \neq i(W_n^{j_2-1}b)$, and there may be overlap between $i(W_n^{j_1-1}b)$, $i(W_n^{j_2-1}b)$. The equations (A.7) and (A.8) are incompatible. This is a contradiction. □

The above result is illustrated by the following two examples.

Example A.7 Let $a \in S_+^4$ and assume there exist $b, c \in S_+^4$ of order 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_2 \\ b_2 & b_1 & 0 & 0 \\ 0 & b_2 & b_1 & 0 \\ 0 & 0 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \end{pmatrix}.$$

Then

$$i(a) = \{1,2\}, \quad \cup_{j=1, c_j>0}^n i(W_4^{j-1}b) = i(b) \cup i(W_4 b) = \{1,2\} \cup \{2,3\} = \{1,2,3\}.$$

Hence such b, c cannot exist. The other possibilities for a, b, c similarly result in impossibilities. □

Example A.8 Let $a \in S_+^4$ with order $n(a) = 3$ and assume there exist $b, c \in S_+^4$ of order 2 such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_2 \\ b_2 & b_1 & 0 & 0 \\ 0 & b_2 & b_1 & 0 \\ 0 & 0 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \end{pmatrix} = \mathrm{circ}(b)c.$$

Then

$$i(a) = \{1,2,3\} \subset Z_4, \quad \cup_{j=1,\, c_j>0}^n i(W_4^{j-1}b) = \{1,2,3\}. \qquad \square$$

To determine whether a matrix

$$A = \sum_{i=1}^n a_i W_n^{i-1} \in DSC_+^{n\times n}, \quad a \in S_+^n, \quad 2 < n(a) < n,$$

is prime, it has to be proved that there do not exist $b, c \in S_+^n$ with $2 \leq n(b) \leq n(a)$ and $2 \leq n(c) \leq n(a)$ such that $a = \mathrm{circ}(b)c$. Examples on how to solve this problem follow below.

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

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 1-b & b \\ 0 & 1-b \end{pmatrix} \begin{pmatrix} c \\ 1-c \end{pmatrix} \tag{A.9}$$

if and only if $a_2^2 \geq 4a_1a_3$.

Proof Let $a \in S_+^3$ be of order 3. Then $a_2 = 1 - a_1 - a_3$. Note that (A.9) is equivalent to

$$\begin{aligned} a_1 &= bc, && \text{(A.10)} \\ a_2 &= (1-b)c + b(1-c), && \text{(A.11)} \\ a_3 &= (1-b)(1-c). && \text{(A.12)} \end{aligned}$$

It is claimed that (A.10,A.11,A.12) is equivalent to (A.10,A.12). This is proven by showing that (A.10,A.12) implies (A.11). Indeed, using (A.10) and (A.12),

$$(1-b)c + b(1-c) = c - bc + b - bc = 1 - bc - (1-b)(1-c) = 1 - a_1 - a_3 = a_2.$$

Consider the calculations

$$\begin{aligned} a_1 &= bc \\ a_3 &= (1-b)(1-c) = 1 - b - c + bc = 1 - (b+c) + a_1 \\ b + c &= 1 + a_1 - a_3. \end{aligned}$$

Thus (A.10) and (A.12) are equivalent to

$$\begin{aligned} bc &= a_1 && \text{(A.13)} \\ b + c &= 1 + a_1 - a_3. && \text{(A.14)} \end{aligned}$$

Consider the polynomial

$$(z+b)(z+c) = z^2 + (b+c)z + bc = z^2 + (1 + a_1 - a_3)z + a_1. \qquad \text{(A.15)}$$

$b, c \in R$ exist if and only if $D := (1 + a_1 - a_3)^2 - 4a_1 \geq 0$. Now

$$\begin{aligned} D &= (1 + a_1 - a_3)^2 - 4a_1 = (2a_1 + a_2)^2 - 4a_1 \\ &= 4a_1^2 + 4a_1a_2 + a_2^2 - 4a_1 = a_2^2 + 4a_1(a_1 + a_2 - 1) = a_2^2 - 4a_1a_3. \end{aligned}$$

So if $b, c \in (0,1)$ exist, then $a_2^2 \geq 4a_1a_3$. Conversely, assume $a_2^2 \geq 4a_1a_3$. Then D defined above is nonnegative, so the roots of the polynomial (A.15) are real, i.e. there exist $b, c \in R$ such that (A.10), (A.11), and (A.12) hold. The question is whether $b, c \in (0,1)$. Since $bc = a_1 > 0$ and $b + c = 1 + a_1 - a_3 = 2a_1 + a_2 > 0$, also $b > 0$ and $c > 0$. It follows from $bc = a_1 < 1$ that $b < 1$ or $c < 1$. If $b < 1$, then from (A.12) it follows that

$$1 - c = \frac{a_3}{1-b} > 0,$$

so $c < 1$. The same reasoning gives that if $c < 1$, then also $b < 1$. It follows that there exist $b, c \in (0,1)$ such that (A.10), (A.11), and (A.12) hold. □

Example A.10 For the vector

$$a = \frac{1}{3}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in S_+^3$$

there do not exist $b, c \in (0,1)$ such that a can be written in the form (A.9). This follows because the inequality $a_2^2 \geq 4a_1a_3$ is equivalent to $(1/3)^2 \geq 4(1/3)^2$, which is false. □

Proposition A.11 *Let $a \in S_+^4$ be of order 3. There exist $b, c \in S_+^4$ of order at least two such that*

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \mathrm{circ}(b)c$$

if and only if $a_1^2 + a_3^2 \geq 4a_2a_4 > 0$ or $a_2^2 + a_4^2 \geq 4a_1a_3 > 0$.

Proof Let $a \in S_+^4$ be of order 3. The possible patterns of the vector a are

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix}, \quad a^{(1)} = \begin{pmatrix} a_1 \\ a_2 \\ 0 \\ a_4 \end{pmatrix}, \quad a^{(2)} = \begin{pmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{pmatrix}, \quad a^{(3)} = \begin{pmatrix} 0 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}.$$

Note that $a^{(i)} = W_4^{4-i}a^{(0)}$, so there exist $b, c \in S_+^4$ of order at least two such that $a^{(0)} = \mathrm{circ}(b)c$ if and only if $a^{(i)} = \mathrm{circ}(W_4^{4-i}b)c$. It will be proven that there exist $b, c \in S_+^4$ of order at least two such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \mathrm{circ}(b)c$$

if and only if $a_2^2 + a_4^2 \geq 4a_1a_3 > 0$.
($\Rightarrow$) Consider $a^{(0)}$. Assume there exist $b, c \in S_+^4$ of order at least two such that $a^{(0)} = \mathrm{circ}(b)c$. From Proposition A.4 it follows that $n(b) \leq n(a) = 3$ and $n(c) \leq n(a) = 3$. The possible values of the pair $(n(b), n(c))$ are $(3,3), (3,2), (2,3), (2,2)$. The first three possibilities cannot occur as can be seen from the nonzero pattern of the vectors. There remains the case $(n(b), n(c)) = (2,2)$. The possible choices for nonzero patterns of c, $i(c)$, are $\{1,2\}$, $\{2,3\}$, $\{3,4\}$, and $\{1,4\}$. The patterns $\{1,3\}$ and $\{2,4\}$ are not possible, as can be seen from the nonzero pattern of b. It follows that the possible choices for b and c are

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \\ 0 \\ 0 \end{pmatrix} \tag{A.16}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \end{pmatrix} \begin{pmatrix} 1-c_1 \\ 0 \\ 0 \\ c_1 \end{pmatrix} \tag{A.17}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ c_1 \\ 1-c_1 \end{pmatrix} \tag{A.18}$$

$$a^{(0)} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \\ b_1 & 0 & 0 & 1-b_1 \end{pmatrix} \begin{pmatrix} 0 \\ c_1 \\ 1-c_1 \\ 0 \end{pmatrix} \tag{A.19}$$

Note that (A.16), (A.17), (A.18), and (A.19) are all equivalent and they are also equivalent to

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b_1 & 0 \\ 1-b_1 & b_1 \\ 0 & 1-b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \end{pmatrix}. \tag{A.20}$$

With Proposition A.9 it follows that if $b_1, c_1 \in (0,1)$ exist, then $a_2^2 \geq 4a_1a_3$. Since $a_4 = 0$ and $a_1 > 0$, $a_3 > 0$, there holds $a_2^2 + a_4^2 \geq 4a_1a_3 > 0$.
($\Leftarrow$) Assume $a_2^2 + a_4^2 \geq 4a_1a_3 > 0$ and $a_4 = 0$. Then $a_2^2 \geq 4a_1a_3$ and from Proposition A.9 it follows that there exist $b_1, c_1 \in (0,1)$ such that (A.20) holds, from which it follows that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & 1-b_1 \\ 1-b_1 & b_1 & 0 & 0 \\ 0 & 1-b_1 & b_1 & 0 \\ 0 & 0 & 1-b_1 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ 1-c_1 \\ 0 \\ 0 \end{pmatrix} = \mathrm{circ}(b)c,$$

with $b, c \in S_+^4$ of order two.

For pattern $a^{(0)}$ the proposition has been proven. The proofs of the other patterns of a are analogously, but with (a_1, a_2, a_3) shifted:

$a^{(1)}$: There exist $b, c \in S_+^4$ of order at least two such that

$$\begin{pmatrix} a_1 \\ a_2 \\ 0 \\ a_4 \end{pmatrix} = \mathrm{circ}(b)c$$

if and only if $a_1^2 \geq 4a_2a_4$, or equivalently $a_1^2 + a_3^2 \geq 4a_2a_4 > 0$.

$a^{(2)}$: There exist $b, c \in S_+^4$ of order at least two such that

$$\begin{pmatrix} a_1 \\ 0 \\ a_3 \\ a_4 \end{pmatrix} = \mathrm{circ}(b)c$$

if and only if $a_4^2 \geq 4a_1a_3$, or equivalently $a_2^2 + a_4^2 \geq 4a_1a_3 > 0$.

$a^{(3)}$: There exist $b, c \in S_+^4$ of order at least two such that

$$\begin{pmatrix} 0 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \mathrm{circ}(b)c$$

if and only if $a_3^2 \geq 4a_2a_4$, or equivalently $a_1^2 + a_3^2 \geq 4a_2a_4 > 0$. □

Proposition A.12 *Let $a \in S_+^5$ be of order 4. Then there exist $b, c \in S_+^5$ of orders at least two such that*

$$a = \mathrm{circ}(b)c. \tag{A.21}$$

Proof It will be assumed that

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \end{pmatrix} \in S_+^5, \quad a_i > 0, \quad \text{for all } i \in Z_4.$$

If the vector a does not have this form then there exists a transformation of a to this form, say $W_5^m a$. If it is shown that there exist $b, c \in S_+^5$ with the necessary order properties such that $W_5^m a = \mathrm{circ}(b)c$, then it follows that $a = \mathrm{circ}(W_5^{5-m}b)c$. Therefore the assumption is no loss of generality.

Two cases are distinguished depending on a property of the vector a: (1) $a_1a_4 \leq a_2a_3$; (2) $a_1a_4 \geq a_2a_3$.

Case (1). Assume that $a_1a_4 \leq a_2a_3$. It will be shown that there exist a $b \in S_+^5$ of order two or three and a $c \in S_+^5$ of order two such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & 0 & b_3 & b_2 \\ b_2 & b_1 & 0 & 0 & b_3 \\ b_3 & b_2 & b_1 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{A.22}$$

This equation is equivalent to

$$a_1 = b_1c_1 \tag{A.23}$$
$$a_2 = b_2c_1 + b_1c_2 \tag{A.24}$$
$$a_3 = b_3c_1 + b_2c_2 \tag{A.25}$$
$$a_4 = b_3c_2 \tag{A.26}$$

Consider the polynomial

$$b(z)c(z) = (b_3z^2 + b_2z + b_1)(c_2z + c_1) = a_4z^3 + a_3z^2 + a_2z + a_1 = a(z).$$

Since $b_3c_2 = a_4 > 0$, assume without loss of generality that $b_3 > 0$ and $c_2 > 0$. One root of $a(z)$ is $\lambda_1 = -c_1/c_2$. Let λ_2, λ_3 denote the other roots of $a(z)$, i.e. the roots of $(b_3z^2 + b_2z + b_1)$. Then $\lambda_2 + \lambda_3 = -b_2/b_3$. Consider the Routh scheme, [5, Vol. II],

$$\begin{pmatrix} a_4 & a_2 \\ a_3 & a_1 \\ a_2 - \frac{a_4}{a_3}a_1 & \\ a_0 & \end{pmatrix}.$$

It follows from Routh's criterion that all roots of $a(z)$ have negative real parts, if and only if

$$a_2 - \frac{a_4}{a_3} a_1 > 0, \quad \text{or} \quad a_1 a_4 < a_2 a_3.$$

So if $a_1 a_4 < a_2 a_3$, then $\lambda_1 < 0$, $\mathrm{Re}(\lambda_2) < 0$, and $\mathrm{Re}(\lambda_3) < 0$. The consequences for b_1, b_2, and c_1 are

- $\lambda_1 < 0$, if and only if $c_1/c_2 > 0$, if and only if $c_1 > 0$, if and only if $b_1 > 0$. The last equivalence follows from $c_1 b_1 = a_1 > 0$.
- $\mathrm{Re}(\lambda_2) < 0$ and $\mathrm{Re}(\lambda_3) < 0$ imply $\mathrm{Re}(\lambda_2) + \mathrm{Re}(\lambda_3) = \lambda_2 + \lambda_3 < 0$, which is equivalent to $b_2/b_3 > 0$, or $b_2 > 0$.

So there exist strictly positive c_1, c_2, b_1, b_2, and b_3 such that (A.23), (A.24), (A.25), and (A.26) hold if $a_1 a_4 < a_2 a_3$. Since $a(1) = a_4 + a_3 + a_2 + a_1 = 1$, also $b(1)c(1) = 1$. Replacing b_i by $b_i/b(1)$ and c_i by $c_i/c(1)$, also $b(1) = b_3 + b_2 + b_1 = 1$ and $c(1) = c_1 + c_2 = 1$.

If $a_1 a_4 = a_2 a_3$, then a solution for (A.23), (A.24), (A.25), and (A.26) is $b_1 = a_1 + a_2$, $b_2 = 0$, $b_3 = a_3 + a_4$, $c_1 = a_1/(a_1 + a_2)$, and $c_2 = a_2/(a_1 + a_2)$.

Thus there exist $b, c \in S_+^5$ of order at least two such that (A.22) holds if $a_1 a_4 \leq a_2 a_3$.

Case (2). Assume that $a_1 a_4 \geq a_2 a_3$. It will be shown that there exist a $b \in S_+^5$ of order two or three and a $c \in S_+^5$ of order two such that

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ 0 \end{pmatrix} = \begin{pmatrix} b_3 & 0 & b_2 & 0 & b_1 \\ b_1 & b_3 & 0 & b_2 & 0 \\ 0 & b_1 & b_3 & 0 & b_2 \\ b_2 & 0 & b_1 & b_3 & 0 \\ 0 & b_2 & 0 & b_1 & b_3 \end{pmatrix} \begin{pmatrix} c_1 \\ 0 \\ c_2 \\ 0 \\ 0 \end{pmatrix} \tag{A.27}$$

This equation is equivalent to

$$a_1 = b_3 c_1 + b_2 c_2, \tag{A.28}$$
$$a_2 = b_1 c_1, \tag{A.29}$$
$$a_3 = b_3 c_2, \tag{A.30}$$
$$a_4 = b_2 c_1 + b_1 c_2. \tag{A.31}$$

Comparison of these equalities with those of (A.23,A.24,A.25,A.26) shows that these equalities are transformed according to $(a_1, a_2, a_3, a_4) \mapsto (a_3, a_1, a_4, a_2)$. The inequality $a_1 a_4 \geq a_2 a_3$ then becomes $a_3 a_2 \geq a_1 a_4$. The solution follows from the previous case. □

Proposition A.13 *Let $a \in S_+^n$ be a vector of order $3 \leq n(a) \leq 4$, such that*

$$a = W_n^{k-1} \begin{pmatrix} a_1 \\ \vdots \\ a_{n(a)} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

for some $k \in Z_n$, i.e. the $n(a)$ strictly positive elements are consecutive. Assume $n(a) < n$. There exist $b, c \in S_+^n$ both of order at least two such that

$$a = \mathrm{circ}(b)c \tag{A.32}$$

if and only if

1. $a_2^2 \geq 4a_1a_3$ *for* $n(a) = 3$;
2. *always for* $n(a) = 4$, $n = 5$;
3. $a_1a_4 \leq a_2a_3$ *for* $n(a) = 4$, $n \geq 6$.

Proof. Without loss of generality it may be assumed that $k = 1$.
1. $n(a) = 3$. From Proposition A.4 it follows that $n(b) \leq n(a) = 3$ and $n(c) \leq n(a) = 3$. The possible values of the pair $(n(b), n(c))$ are $(3,3), (3,2), (2,3), (2,2)$. The first three possibilities cannot occur as can be seen from the nonzero pattern of the vectors. So the remaining case is $(n(b), n(c)) = (2,2)$. The rest of the proof is equivalent to the proof of Proposition A.11
2. This is Proposition A.12.
3. $n(a) = 4$, $n \geq 6$. From Proposition 2.7 it follows that $n(b) \leq 4$ and $n(c) \leq 4$. The nonzero pattern of a gives the following possible values of $(n(b), n(c))$: $(3,2), (2,3), (2,2)$. By symmetry of (A.32) in b, c it is sufficient to consider only $(3,2)$ and $(2,2)$. Assume without loss of generality that $c_1 > 0$ and $c_j > 0$ for exactly one $j \in \{2, 3, \ldots, n\}$. From Lemma A.5 it follows that if there exist $b, c \in S_+^n$ both of order at least two such that $a = \mathrm{circ}(b)c$, then $i(b) \subset i(a) = \{1,2,3,4\}$. For $n(b) = n(c) = 2$, possible nonzero patterns of b and c are

$$(i(b), i(c)) \in \{(\{1,2\},\{1,3\}), (\{1,3\},\{1,2\}), (\{2,4\},\{1,n\}), (\{3,4\},\{1,n-1\})\}.$$

Writing out (A.32) it follows that those patterns are possible if and only if $a_1a_4 = a_2a_3$.

For $n(b) = 3$, $n(c) = 2$, $(\{1,2,3\},\{1,2\})$ and $(\{2,3,4\},\{1,n\})$ are the possible nonzero patterns for $(i(b), i(c))$. The first pattern gives equations equivalent to (A.22). If $a_1a_4 \leq a_2a_3$, then from case 1 in the proof of Proposition A.12 it follows that there exists a solution. But if $a_1a_4 > a_2a_3$, then it follows from Routh's algorithm, [5], that $a(z) = a_4z^3 + a_3z^2 + a_2z + a_1$ has two roots with $\mathrm{Re}(\lambda) > 0$. The notation of the proof of Proposition A.12 will be used. If $\mathrm{Re}(\lambda_1) = -c_1/c_2 > 0$, then c_1 and c_2 cannot both be positive. So suppose $\mathrm{Re}(\lambda_2) > 0$ and $\mathrm{Re}(\lambda_3) > 0$. Then $-b_2/b_3 = \lambda_2 + \lambda_3 = \mathrm{Re}(\lambda_2) + \mathrm{Re}(\lambda_3) > 0$, so also b_2 and b_3 cannot be both positive. It follows that if $a_1a_4 > a_2a_3$, a cannot be written as $a = \mathrm{circ}(b)c$ with b and c of order at least two. For the nonzero pattern $i(b) = \{2,3,4\}$ and $i(c) = \{1,n\}$ an analogous reasoning holds. □

References

1. A. Berman and R. J. Plemmons. *Nonnegative Matrices in the Mathematical Sciences.* Computer Science and Applied Mathematics. Academic Press, New York, 1979.
2. D. de Caen and D. A. Gregory. Primes in the semigroup of boolean matrices. *Linear Algebra & its Applications*, 37:119–134, 1981.
3. P. J. Davis. *Circulant Matrices.* Wiley, New York, 1979.

4. J. Dieudonné. *Foundations of Modern Analysis.* Academic Press, New York, 1969.

5. F. R. Gantmacher. *The Theory of Matrices.* Chelsea Publishing Company, New York, 1977.

6. M. Gondran and M. Minoux. *Graphs and Algorithms.* John Wiley & Sons, Chichester, 1984.

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

8. J. M. van den Hof. Realization of positive linear systems. Preprint, Accepted for publication in Linear Algebra and its Applications, 1995.

9. N. Jacobson. *Basic Algebra, volumes 1, 2, 2nd edition.* W.H. Freeman and Company, New York, 1985.

10. A. W. Marshall and I. Olkin. *Inequalities: Theory of Majorization and Its Applications.* Academic Press, 1979.

11. G. Picci, J. M. van den Hof, and J. H. van Schuppen. A partial classification of primes in the positive matrices and in the doubly stochastic matrices. Preprint, CWI, Amsterdam, 1995.

12. 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.

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