2019 Sixth Indian Control Conference (ICC)
December 18-20, 2019. IIT Hyderabad, India

On circulant Lyapunov operators, two-variable polynomials, and DFT

Chayan Bhawal, Debasattam Pal, and Madhu N. Belur

Abstract— **In this paper we deal with a special class of Lyapunov equations which we call *circulant Lyapunov equations*. These are Lyapunov equations arising from system matrices that are circulant. Here we bring out new theoretical insights into such Lyapunov operators. We show that, under a suitable projection map, two-variable polynomials are related to circulant Lyapunov operators. We also give necessary and sufficient conditions for the solvability of a circulant Lyapunov equation using two dimensional Fourier transform operation (2D-DFT) performed on a specially constructed matrix. Using these links among circulant Lyapunov operators, two-variable polynomials and 2D-DFT, an algorithm to solve circulant Lyapunov equations using 2D-DFT is developed in this paper.**
Keywords: Circulant matrices, Two dimensional discrete Fourier transform, Lyapunov equations.

1. Introduction

Lyapunov equations and operators arise in many areas of physics and mathematics. They find applications in stability theory of systems [7], linear-quadratic optimization and filtering [11], model order reduction [1], and many other fields of mathematics and control: see [8] and references therein. This has resulted in an interest in the theoretical and numerical aspects of Lyapunov equations and operators. In this paper, we focus on a special class of Lyapunov operators, which we call *circulant Lyapunov operators*. Circulant Lyapunov operators $\mathscr{L}_A(P) := AP + PA^T$ are those operators where A is a circulant matrix, that is, $A \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ has its (m,n)-th element given by $a_{mn} = c_{(n-m)\mathrm{mod}\,\mathtt{N}}$, where $c_k \in \mathbb{R}$ for $k = 0,1,\dots,\mathtt{N}-1$. In most applications, where linear matrix equations of the form $AP + PA^T = Q$ are studied, matrices A and Q are known and matrix P needs to be computed. Further, P and Q matrices in such cases are considered to be Hermitian. However, since the results presented in this paper are applicable to non-Hermitian P and Q as well, we do not assume P and Q to be Hermitian. Note that matrix A, in general, is related to the system under investigation and is called the *system matrix*. There are various examples in which the matrix A representing the system dynamics is circulant in nature: for example rings of identically coupled systems [12, Section 5.3], multiagent systems with circulant interconnection [9] etc. Stability analysis of such systems results in circulant Lyapunov operators.

In general, there are numerous methods to solve Lyapunov equations. However, none of these methods are well-suited for exploiting the structure present in circulant Lyapunov operators. In this paper, we achieve faster algorithm for solving circulant Lyapunov equations by associating Fourier analysis to these equations. We first show that circulant Lyapunov operators are intricately linked to two-variable polynomials under a suitable projection map. Fourier analysis and their one-variable polynomial interpretations are well-known in the literature: see [10, Section 2.4]. Analogously, two-variable polynomials are related to two dimensional discrete Fourier transform (2D-DFT). Using these links among circulant Lyapunov operators, two-variable polynomials and 2D-DFT, we give necessary and sufficient conditions for the solvability of circulant Lyapunov equations. These conditions help us devising an algorithm (Algorithm 4.1) to compute solutions of circulant Lyapunov equations using 2D-DFT.

It is important to note here that the results presented in this paper are a generalization of the results in [3], in the sense that this paper deals with all classes of circulant Lyapunov operators as opposed to the *unit cyclic* case (a special case of circulant Lyapunov operators) in [3]. The rest of the paper is organized as follows. Section 2 contains notation and preliminaries required for the paper. In Section 3, we establish the link between two-variable polynomials and circulant Lyapunov operators. The main results of the paper that link Lyapunov operator, 2D-DFT and two-variable polynomials are presented in Section 4. Concluding remarks are presented in Section 5.

Corresponding author email: chayanbhawal@ee.iitb.ac.in. The corresponding author is currently in the Computational Methods in Systems and Control Theory group of Max Planck Institute for Dynamics of Complex Technical Systems Magdeburg. This work was done when he was a Ph.D. student in the Department of Electrical Engineering, Indian Institute of Technology Bombay (IIT Bombay), India. The coauthors are in the Department of Electrical Engineering, IIT Bombay.

2. Notation and Preliminaries

We follow standard notation in this paper: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the sets of real numbers, complex numbers, integers and natural numbers, respectively. The symbol $\mathbb{C}[x_1,x_2,\dots,x_{\mathtt{n}}]$ denotes the ring of polynomials in $\mathtt{n}$ variables with complex coefficients. We use the notation $\langle p_1,p_2,\dots,p_{\mathtt{n}}\rangle$ to denote the ideal generated by $p_1,p_2,\dots,p_{\mathtt{n}}$: the ring usually being clear from the context. We represent the variety of an ideal $\mathbb{I}$ as $\mathbb{V}(\mathbb{I})$. The symbol j represents $\sqrt{-1}$, unless otherwise specified. We use $A = [a_{mn}]_{m,n=0,1,\dots\mathtt{N}-1}$ to represent a matrix A with element a_{mn} in the $(m+1)$-st row and $(n+1)$-st column. Conventionally, the elements of any matrix A i.e. a_{mn} are indexed as $m,n = 1,2,\dots,\mathtt{N}$. However, since we are dealing with polynomials, their degrees and DFT in this paper, we use 0 as the starting index for m and n. This means that the element in the 1-st row and 1-st column of matrix A is represented as a_{00}. A matrix of the form $\begin{bmatrix} B_1^T & B_2^T \end{bmatrix}^T$ is represented as $\mathrm{col}(B_1,B_2)$. The symbol $\mathbf{0}_{\mathtt{N}\times\mathtt{M}}$ denotes the zero matrix of dimension $\mathtt{N}\times\mathtt{M}$. The symbol $I_{\mathtt{N}}$ represents an $\mathtt{N}\times\mathtt{N}$ identity matrix. We use the symbols $\mathbf{X}$ and $\mathbf{Y}$ to represent column vectors of the form $\mathrm{col}(1,x,x^2,\dots,x^{\mathtt{N}-1}) \in \mathbb{R}^{\mathtt{N}}[x]$ and $\mathrm{col}(1,y,y^2,\dots,y^{\mathtt{N}-1}) \in \mathbb{R}^{\mathtt{N}}[y]$, respectively. The following symbols $A \star B$, $A \oslash B$ and $A \odot B$ represent 2D-convolution, entry-wise division and entry-wise product operation (also known as Hadamard product) between matrices A and B, respectively. We use $\mathfrak{f}(\bullet)$ to denote the 1D-DFT operator. The symbol $\mathscr{F}(\bullet)$ represents the 2D-DFT operator and $\mathscr{F}^{-1}(\bullet)$ represents the inverse 2D-DFT operator. Further, we use the following symbol for the Vandermonde matrix related to DFT (see [3] for preliminaries on DFT and two-variable polynomials).

$$\Omega_{\mathtt{N}} := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{\mathtt{N}-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(\mathtt{N}-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{\mathtt{N}-1} & \omega^{2(\mathtt{N}-1)} & \cdots & \omega^{(\mathtt{N}-1)^2} \end{bmatrix}, \omega := e^{-j\frac{2\pi}{\mathtt{N}}}, \mathtt{N} \in \mathbb{N}. \quad (1)$$

Matrices of the form

$$E := \begin{bmatrix} \mathbf{0}_{1\times(\mathtt{N}-1)} & 1 \\ I_{\mathtt{N}-1} & \mathbf{0}_{(\mathtt{N}-1)\times 1} \end{bmatrix} \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}} \quad (2)$$

are used extensively in this paper. For easy reference, we call such a matrix *the unit cyclic matrix* of order $\mathtt{N}$. Note that the matrix E is also in controller canonical form with characteristic polynomial $\mathscr{X}_E(s) := s^{\mathtt{N}} - 1$. Further, the eigenvalues of the unit cyclic matrix of order $\mathtt{N}$ are the $\mathtt{N}^{th}$ roots of unity i.e. $\{1, \omega, \omega^2, \dots, \omega^{\mathtt{N}-1}\}$, where $\omega := e^{-j\frac{2\pi}{\mathtt{N}}}$.

A. Circulant matrices and Lyapunov operators

A matrix $H = [h_{mn}] \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ is said to be a *circulant matrix* of order $\mathtt{N}$ if it has the following form

$$H = \operatorname{circ}(\mathtt{c}_0, \mathtt{c}_1, \dots, \mathtt{c}_{\mathtt{N}-1}) = \begin{bmatrix} \mathtt{c}_0 & \mathtt{c}_1 & \cdots & \mathtt{c}_{\mathtt{N}-1} \\ \mathtt{c}_{\mathtt{N}-1} & \mathtt{c}_0 & \cdots & \mathtt{c}_{\mathtt{N}-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathtt{c}_1 & \mathtt{c}_2 & \cdots & \mathtt{c}_0 \end{bmatrix}, \quad (3)$$

i.e., $h_{mn} = \mathtt{c}_{(n-m)\bmod \mathtt{N}}$. Note that the unit cyclic matrix E, defined in equation (2), is also a circulant matrix. The set of circulant matrices forms a vector space over $\mathbb{C}$ of dimension $\mathtt{N}$: see [6, Chapter 3]. A set of basis matrices for circulants of order $\mathtt{N}$ is given by $\{I_{\mathtt{N}}, E, E^2, \cdots, E^{\mathtt{N}-1}\}$, where E is the unit cyclic matrix of order $\mathtt{N}$. In other words, any circulant matrix $H \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ can be written as $H = \sum_{k=0}^{\mathtt{N}-1} \mathtt{c}_k E^k$, where $\mathtt{c}_k \in \mathbb{R}$. Further, the eigenvalues of the matrix H, defined in equation (3), are given by the elements of the 1D-DFT vector $\mathfrak{f}([\mathtt{c}_0 \ \mathtt{c}_1 \ \cdots \ \mathtt{c}_{\mathtt{N}-1}])$.

Another important object of focus in this paper is the special linear matrix equation (operator) called the Lyapunov equation (operator). We review some basic properties of such an equation (operator) next. Given a matrix $A \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$, the continuous-time Lyapunov operator $\mathscr{L}_A : \mathbb{C}^{\mathtt{N}\times\mathtt{N}} \to \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ is defined as $\mathscr{L}_A(P) := AP + PA^T$.

In this paper two standard results on Lyapunov operators is often used. One among them is in [3, Proposition 2.1] and other dealing with the solvability of Lyapunov equations is stated below for the ease of reference.

Proposition 2.1. *Consider a Lyapunov equation $AP + PA^T = Q$, where $A \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}, P, Q \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$. Let $\Lambda := \{\lambda_0, \lambda_1, \dots, \lambda_{\mathtt{N}-1}\} \subset \mathbb{C}$ be the set of eigenvalues (counted with multiplicities) of A. Suppose $\lambda_m + \lambda_n = 0$ for some $m, n = 0, \dots, \mathtt{N}-1$. Then, exactly one of the following is true.*

1) There exist infinitely many P such that $AP + PA^T = Q$.
2) There exists no P such that $AP + PA^T = Q$.

Further, if $\lambda_m + \lambda_n \neq 0$ for all $m, n = 0, 1, \dots, \mathtt{N}-1$ then there exists a unique $P \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $AP + PA^T = Q$.

We call the Lyapunov operator $\mathscr{L}_A(\bullet)$ *singular* when a pair of eigenvalues of A sums to zero. The name stems from the fact that in such a case there exists a nonzero matrix $V \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathscr{L}_A(V) = 0$.

In this paper, we deal with Lyapunov operators of a special structure. For the ease of reference, we call such operators *circulant* Lyapunov operators. We define it next.

Definition 2.2. *Consider $A \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ and $P \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$. Suppose A is circulant. Then the Lyapunov operator $\mathscr{L}_A : P \mapsto AP + PA^T$ is called a circulant Lyapunov operator.*

3. Link to two-variable polynomials

In this section we show that two-variable polynomials are related to circulant Lyapunov operators under a suitable projection map.

Let $E \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ be the unit cyclic matrix as discussed in Section 2, $\mathscr{X}_E(s) := s^{\mathtt{N}} - 1$ is the characteristic polynomial of E. Consider the polynomial ring $\mathbb{C}[x,y]$ and the ideal $\mathbb{A} := \langle \mathscr{X}_E(x), \mathscr{X}_E(y) \rangle \subset \mathbb{C}[x,y]$. Define the map

$$\Pi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[x,y]/\mathbb{A}. \quad (4)$$

Under the action of Π, an element $p \in \mathbb{C}[x,y]$ goes to $[p]$. Note that the Gröbner basis corresponding to the ideal $\mathbb{A}$ is the set $\{\mathscr{X}_E(x), \mathscr{X}_E(y)\}$ itself. Hence, $[p]$ is uniquely represented by the remainder obtained on division of p by $\mathscr{X}_E(x)$ and $\mathscr{X}_E(y)$ (see [3, Section E] for preliminaries on Gröbner basis). According to [3, Proposition 2.2], this remainder's leading monomial will have multidegree that is less than that of $x^{\mathtt{N}}$ and $y^{\mathtt{N}}$. Therefore, every remainder upon division by $x^{\mathtt{N}} - 1$ and $y^{\mathtt{N}} - 1$ is going to be a polynomial with monomials being $x^k y^\ell$, where $0 \leqslant k, \ell \leqslant \mathtt{N}-1$. Hence, any element $g(x,y)$ in $\mathbb{C}[x,y]/\mathbb{A}$ can be written as $g(x,y) = \sum_{m,n=0}^{\mathtt{N}-1} \alpha_{mn} x^m y^n$, where $\alpha_{mn} \in \mathbb{C}$. Consider $G = [g_{mn}]_{m,n=0,1,\dots,\mathtt{N}-1} \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $g(x,y) = \mathbf{X}^T G \mathbf{Y}$. Then it is easy to see that $\alpha_{mn} = g_{mn}$ for every $m, n = 0, 1, \dots, \mathtt{N}-1$. Thus $g(x,y)$ and G has a one-to-one correspondence and we call G the *coefficient matrix* of $g(x,y)$. This one-to-one correspondence between $g(x,y)$ and its coefficient matrix G is crucially used in this paper.

Consider $P \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ and $p(x,y) \in \mathbb{C}[x,y]$ such that $p(x,y) := \mathbf{X}^T P \mathbf{Y}$. We prove that the operation $\Pi\Big((x^k + y^k)p(x,y)\Big)$ has an interesting link with the circulant Lyapunov operator $\mathscr{L}_A(\bullet)$, where $A = E^k$. Note that the summands of $(x^k + y^k)p(x,y) = x^k p(x,y) + y^k p(x,y)$ can be rewritten as

$$x^k \mathbf{X}^T P \mathbf{Y} = \begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{X}} \end{bmatrix}^T \begin{bmatrix} \mathbf{0}_{k\times\mathtt{N}} & \mathbf{0}_{k\times k} \\ P & \mathbf{0}_{\mathtt{N}\times k} \end{bmatrix} \begin{bmatrix} \mathbf{Y} \\ \hat{\mathbf{Y}} \end{bmatrix},$$

$$y^k \mathbf{X}^T P \mathbf{Y} = \begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{X}} \end{bmatrix}^T \begin{bmatrix} \mathbf{0}_{\mathtt{N}\times k} & P \\ \mathbf{0}_{k\times k} & \mathbf{0}_{k\times\mathtt{N}} \end{bmatrix} \begin{bmatrix} \mathbf{Y} \\ \hat{\mathbf{Y}} \end{bmatrix},$$

where $\hat{\mathbf{X}} := \operatorname{col}\left(x^{\mathtt{N}}, x^{\mathtt{N}+1}, \dots, x^{\mathtt{N}+k-1}\right)$ and $\hat{\mathbf{Y}} := \operatorname{col}\left(y^{\mathtt{N}}, y^{\mathtt{N}+1}, \dots, y^{\mathtt{N}+k-1}\right)$. Action of the map Π defined in (4) is equivalent to substituting $x^{\mathtt{N}}$ and $y^{\mathtt{N}}$ in the polynomial $(x^k + y^k)p(x,y)$ by 1. Hence, $\Pi\Big(x^k p(x,y)\Big) + \Pi\Big(y^k p(x,y)\Big) = \begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{X}} \end{bmatrix}^T \begin{bmatrix} \mathbf{0}_{\mathtt{N}\times k} & E^k \\ \mathbf{0}_{k\times k} & \mathbf{0}_{k\times\mathtt{N}} \end{bmatrix} \begin{bmatrix} \mathbf{0}_{k\times\mathtt{N}} & \mathbf{0}_{k\times k} \\ P & \mathbf{0}_{\mathtt{N}\times k} \end{bmatrix} \begin{bmatrix} \mathbf{Y} \\ \hat{\mathbf{Y}} \end{bmatrix} + \begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{X}} \end{bmatrix}^T \begin{bmatrix} \mathbf{0}_{\mathtt{N}\times k} & P \\ \mathbf{0}_{k\times k} & \mathbf{0}_{k\times\mathtt{N}} \end{bmatrix} \begin{bmatrix} \mathbf{0}_{k\times\mathtt{N}} & \mathbf{0}_{k\times k} \\ (E^k)^T & \mathbf{0}_{\mathtt{N}\times k} \end{bmatrix} \begin{bmatrix} \mathbf{Y} \\ \hat{\mathbf{Y}} \end{bmatrix} = \mathbf{X}^T\Big(E^k P + P(E^k)^T\Big)\mathbf{Y}$. Thus, we have

$$\Pi\Big(x^k p(x,y)\Big) + \Pi\Big(y^k p(x,y)\Big) = \mathbf{X}^T \mathscr{L}_{E^k}(P)\mathbf{Y}. \quad (5)$$

Thus, the coefficient matrix of the polynomial $\Pi\big((x^k + y^k)p(x,y)\big)$ is $\mathscr{L}_{E^k}(P)$. This leads us to the first main result of this paper.

Theorem 3.1. *Consider the Lyapunov operator $\mathscr{L}_A(\bullet)$, where $A \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ is a circulant matrix i.e. $A := \sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k E^k \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ and $\mathsf{a}_k \in \mathbb{R}$. Suppose $V \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}\backslash 0$ and $\gamma \in \mathbb{C}$. Define the two-variable polynomial associated with V as $v(x,y) := \mathbf{X}^T V \mathbf{Y}$. Consider the map $\Pi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[x,y]/\mathbb{A}$ where the ideal $\mathbb{A} \subset \mathbb{C}[x,y]$ is defined as $\mathbb{A} := \langle x^{\mathtt{N}}-1, y^{\mathtt{N}}-1\rangle$. Then the following are equivalent*
(1) $\mathscr{L}_A(V) = \gamma V$. (2) $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)v(x,y)\Big) = \gamma v(x,y)$.

Proof. Define $P \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathbf{X}^T P \mathbf{Y} := p(x,y)$. Since Π is a linear operator, we have

$$\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)p(x,y)\Big) = \sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k \Pi\Big((x^k+y^k)p(x,y)\Big) \quad (6)$$

Using equation (5) in equation (6), we have $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k + y^k)p(x,y)\Big) = \sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k \mathbf{X}^T\Big(E^k P + P(E^k)^T\Big)\mathbf{Y} = \mathbf{X}^T\Big(\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k E^k\Big)P + P\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k E^k\Big)^T\Big)\mathbf{Y} = \mathbf{X}^T\Big(AP + PA^T\Big)\mathbf{Y}$, i.e.,

$$\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)p(x,y)\Big) = \mathbf{X}^T \mathscr{L}_A(P)\mathbf{Y}. \quad (7)$$

This shows that $\mathscr{L}_A(P)$ is the coefficient matrix of the polynomial $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)p(x,y)\Big)$.
$(\mathbf{1} \Rightarrow \mathbf{2})$: From equation (7) we therefore have $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)v(x,y)\Big) = \mathbf{X}^T\mathscr{L}_A(V)\mathbf{Y} = \mathbf{X}^T\Big(\gamma V\Big)\mathbf{Y} = \gamma\Big(\mathbf{X}^T V\mathbf{Y}\Big) = \gamma v(x,y)$.
$(\mathbf{2} \Rightarrow \mathbf{1})$ Using equations (7), we have $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k + y^k)v(x,y)\Big) = \gamma v(x,y) \Rightarrow \mathbf{X}^T\mathscr{L}_A(V)\mathbf{Y} = \mathbf{X}^T\gamma V\mathbf{Y} \Rightarrow \mathscr{L}_A(V) = \gamma V$. This completes the proof of Theorem 3.1. □

From Theorem 3.1 we have a two-variable polynomial interpretation of eigenmatrices of circulant Lyapunov operators. This is the polynomial version of [3, Proposition 2.1] for circulant Lyapunov operators. Next we propose a theorem which provides a solvability condition for a circulant Lyapunov equation from two-variable polynomial perspective.

Theorem 3.2. *Consider the polynomial ring $\mathbb{C}[x,y]$ and the ideal $\mathbb{A} := \langle x^{\mathtt{N}}-1, y^{\mathtt{N}}-1\rangle$. Define the map $\Pi : \mathbb{C}[x,y] \to \mathbb{C}[x,y]/\mathbb{A}$. Given $G, R \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ define $g(x,y) := \mathbf{X}^T G\mathbf{Y}$, $r(x,y) := \mathbf{X}^T R\mathbf{Y}$. Then the following statements are true.*

(a) Suppose $g(x,y), r(x,y) \in \mathbb{C}[x,y]$ satisfy $\Pi\Big((x^k + y^k)g(x,y)\Big) = r(x,y)$, where $k \in \mathbb{N}$ and $k < \mathtt{N}$. Suppose $\Big((2\ell+1)\mathtt{N}\Big)\mathrm{mod}(2k) \neq 0$ for some $\ell \in \mathbb{Z}$. Then $g(x,y)$ is unique.
(b) Suppose $g(x,y), r(x,y) \in \mathbb{C}[x,y]$ satisfy $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k + y^k)g(x,y)\Big) = r(x,y)$, where $k \in \mathbb{N}$ and $k < \mathtt{N}$. Suppose $\sum_{k=0}^{\mathtt{N}-1} 2\mathsf{a}_k \cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}} \neq 0$ for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$. Then $g(x,y)$ is unique.

Proof. **(a)**: Let $h(x,y) := \mathbf{X}^T H\mathbf{Y}$, $H \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ be a polynomial such that $\Pi\Big((x^k+y^k)h(x,y)\Big) = r(x,y)$. Then

$$(x^k+y^k)g(x,y) = a(x,y)(x^{\mathtt{N}}-1) + b(x,y)(y^{\mathtt{N}}-1) + r(x,y) \quad (8)$$

$$(x^k+y^k)h(x,y) = c(x,y)(x^{\mathtt{N}}-1) + d(x,y)(y^{\mathtt{N}}-1) + r(x,y) \quad (9)$$

for some $a(x,y), b(x,y), c(x,y), d(x,y) \in \mathbb{C}[x,y]$. Subtracting equation (9) from (8), we have

$$(x^k+y^k)\,[g(x,y)-h(x,y)] = [a(x,y)-c(x,y)]\,(x^{\mathtt{N}}-1) + [b(x,y)-d(x,y)]\,(y^{\mathtt{N}}-1) \quad (10)$$

Define $p(x,y) := [g(x,y)-h(x,y)]$ and $q_1(x,y) := [a(x,y)-c(x,y)]$ and $q_2(x,y) := [b(x,y)-d(x,y)]$. Rewriting equation (10), we have

$$(x^k+y^k)p(x,y) = q_1(x,y)(x^{\mathtt{N}}-1) + q_2(x,y)(y^{\mathtt{N}}-1) \quad (11)$$

Let $\omega := e^{-j\frac{2\pi}{\mathtt{N}}}$. Using the fact that $\omega^{m\mathtt{N}} = \omega^{n\mathtt{N}} = 1$ and evaluating the right hand side of equation (11) at $x = \omega^m$ and $y = \omega^n$, for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$, we have

$$q_1(\omega^m,\omega^n)(\omega^{m\mathtt{N}}-1) + q_2(\omega^m,\omega^n)(\omega^{n\mathtt{N}}-1) = 0. \quad (12)$$

Therefore, the left hand side of equation (11) becomes

$$(\omega^{mk}+\omega^{nk})p(\omega^m,\omega^n) = 0 \text{ for every } m,n = 0,1,\ldots,\mathtt{N}-1. \quad (13)$$

It can be easily verified that

$$\omega^{mk}+\omega^{nk} = e^{-j\frac{2\pi}{\mathtt{N}}mk} + e^{-j\frac{2\pi}{\mathtt{N}}nk} = 2\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}}.$$

Since $|\omega^{\frac{(m+n)k}{2}}| \neq 0$, we have $\omega^{mk}+\omega^{nk}$ is zero if and only if $\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right) = 0$ i.e. for some $\ell \in \mathbb{Z}$, we have

$$\frac{\pi(m-n)k}{\mathtt{N}} = \frac{(2\ell+1)\pi}{2} \Rightarrow m-n = \frac{(2\ell+1)\mathtt{N}}{2k} \quad (14)$$

Since $\Big((2\ell+1)\mathtt{N}\Big)\mathrm{mod}(2k) \neq 0$ for all $\ell \in \mathbb{Z}$, therefore $\omega^{mk} + \omega^{nk} \neq 0$. Hence, from equation (13), we conclude that for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$, we have

$$p(\omega^m,\omega^n) = 0 \Rightarrow g(\omega^m,\omega^n) = h(\omega^m,\omega^n). \quad (15)$$

Rewriting equation (15) in terms of Vandermonde matrix $\Omega_{\mathtt{N}}$ shown in equation (1), we have $\Omega_{\mathtt{N}}^T G\Omega_{\mathtt{N}} = \Omega_{\mathtt{N}}^T H\Omega_{\mathtt{N}}$. Since the elements of the set $\{1,\omega,\omega^2,\ldots,\omega^{\mathtt{N}-1}\}$ are distinct in $\mathbb{C}$, we have $\Omega_{\mathtt{N}}$ to be a nonsingular matrix. Therefore, we conclude that $G = H$, i.e., $g(x,y) = h(x,y)$. This completes the proof of statement (a) of Theorem 3.2.
(b): Here we replace $(x^k + y^k)$ in equations (8)-(11) by $\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(x^k+y^k)$. Then equation (13) becomes $\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(\omega^{mk} + \omega^{nk})p(\omega^m,\omega^n) = 0$. Under the assumptions given in statement (b), we have $\sum_{k=0}^{\mathtt{N}-1} \mathsf{a}_k(\omega^{mk}+\omega^{nk}) \neq 0$ for every $m,n = 0,1,\ldots,\mathtt{N}-1$. This leads us to equation (15) of the proof of statement (a). Rest of the proof is exactly the same as that of statement (a). Finally, we have $g(x,y) = h(x,y)$. □

The next theorem reveals the relation between nonsingularity of circulant Lyapunov operator $\mathscr{L}_A(\bullet)$ and the uniqueness of the polynomial $g(x,y)$ dealt with in Theorem 3.2.

Theorem 3.3. *Consider the polynomial ring $\mathbb{C}[x,y]$ and the ideal $\mathbb{A} := \langle x^{\mathtt{N}}-1, y^{\mathtt{N}}-1\rangle$. Define the map $\Pi : \mathbb{C}[x,y] \to$*

$\mathbb{C}[x,y]/\mathbb{A}$. *Consider the circulant Lyapunov operator* $\mathscr{L}_A(\bullet)$, *where* $A := \sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k E^k$. *Let* $g(x,y), r(x,y) \in \mathbb{C}[x,y]$ *be such that* $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k+y^k)g(x,y)\Big) = r(x,y)$. *Then* $\mathscr{L}_A(\bullet)$ *is nonsingular if and only if* $g(x,y)$ *is unique.*

Proof. Let $R, G \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ be such that $r(x,y) =: \mathbf{X}^T R\mathbf{Y}, g(x,y) =: \mathbf{X}^T G\mathbf{Y}$.

(**If:**) From equation (7), we have $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k)g(x,y)\Big) = \mathbf{X}^T \mathscr{L}_A(G)\mathbf{Y}$. Therefore, $\mathbf{X}^T \mathscr{L}_A(G)\mathbf{Y} = \mathbf{X}^T R\mathbf{Y}$. Since $g(x,y)$ and its coefficient matrix G has a one-to-one correspondence, we have $g(x,y)$ unique means there exists a unique G such that $\mathscr{L}_A(G) = R$. Therefore, $\mathscr{L}_A(\bullet)$ is an injective operator. Since $\mathscr{L}_A(\bullet) : \mathbb{C}^{\mathtt{N}\times\mathtt{N}} \to \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ and $\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ is a finite dimensional vector space, we have $\mathscr{L}_A(\bullet)$ is not only injective but surjective as well. Hence, $\mathscr{L}_A(\bullet)$ is a bijective operator. This means that $\mathscr{L}_A(\bullet)$ is nonsingular.

(**Only if:**) Given $\mathscr{L}_A(\bullet)$ is nonsingular and $\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ being a finite dimensional vector space, we can infer that $\mathscr{L}_A(\bullet)$ is bijective. Therefore, for each $R \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ there exists a unique $G \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathscr{L}_A(G) = R \Rightarrow \mathbf{X}^T \mathscr{L}_A(G)\mathbf{Y} = \mathbf{X}^T R\mathbf{Y}$. Recall that $\mathscr{L}_A(G)$ is the coefficient matrix of $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k)g(x,y)\Big)$, where $g(x,y) = \mathbf{X}^T G\mathbf{Y}$. The polynomial corresponding to R is $r(x,y) = \mathbf{X}^T R\mathbf{Y}$. Therefore, $\mathbf{X}^T \mathscr{L}_A(G)\mathbf{Y} = \Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k+y^k)g(x,y))\Big) = r(x,y)$.

Since G is unique and we know that there is a one-to-one correspondence between polynomials in $\mathbb{C}[x,y]/\mathbb{A}$ and matrices in $\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$, we conclude that $g(x,y)$ is unique. □

Thus, Theorem 3.3 is a polynomial analogue of Proposition 2.1. As discussed in Section 2-A, the periodic structure of circulant matrices ties these matrices to Fourier analysis: see [6, Chapter 3]. The natural question that arises now is: are circulant Lyapunov operators linked to Fourier analysis? We answer this in the next section using the insights obtained in Theorem 3.3.

4. Link to 2D-DFT

In this section, we bring out the link between circulant Lyapunov operators and 2D-DFT using the polynomial link we established with circulant Lyapunov operators in Section 3. The next theorem is one of the main results of this paper and it is the basis for a 2D-DFT based algorithm to solve circulant Lyapunov equations.

Theorem 4.1. *Consider the polynomial ring* $\mathbb{C}[x,y]$ *and the ideal* $\mathbb{A} := \langle x^{\mathtt{N}} - 1, y^{\mathtt{N}} - 1\rangle$. *Define the map* $\Pi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[x,y]/\mathbb{A}$. *Let* $P,Q,R \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ *be such that* $p(x,y) := \mathbf{X}^T P\mathbf{Y}$, $q(x,y) := \mathbf{X}^T Q\mathbf{Y}$ *and* $r(x,y) := \mathbf{X}^T R\mathbf{Y}$. *Let* $\mathscr{F}(P), \mathscr{F}(Q)$ *and* $\mathscr{F}(R)$ *be the 2D-DFT matrices of* P, Q *and* R*, respectively. Then the following are equivalent: (i)* $\Pi\Big(p(x,y)q(x,y)\Big) = r(x,y)$. *(ii)* $\mathscr{F}(P) \odot \mathscr{F}(Q) = \mathscr{F}(R)$.

Proof. (**i**) $\Rightarrow$ (**ii**) : Given $\Pi\Big(p(x,y)q(x,y)\Big) = r(x,y)$, there exists $a(x,y), b(x,y) \in \mathbb{C}[x,y]$ such that

$$p(x,y)q(x,y) = a(x,y)(x^{\mathtt{N}} - 1) + b(x,y)(y^{\mathtt{N}} - 1) + r(x,y). \quad (16)$$

Now, we evaluate equation (16) at $x = \omega^m$ and $y = \omega^n$ for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$, where $\omega = e^{-j\frac{2\pi}{\mathtt{N}}}$. As shown in the proof of Theorem 3.2, $a(x,y)(x^{\mathtt{N}} - 1) + b(x,y)(y^{\mathtt{N}} - 1) = 0$ at $x = \omega^m$ and $y = \omega^n$ for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$. Therefore, for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$ we have

$$p(\omega^m,\omega^n)q(\omega^m,\omega^n) = r(\omega^m,\omega^n) \quad (17)$$

Let $\mathscr{F}(P) =: [e_{mn}], \mathscr{F}(Q) =: [f_{mn}]$ and $\mathscr{F}(R) =: [g_{mn}]$, where $m,n = 0,1,\ldots,\mathtt{N}-1$. As discussed in [3, Section B], computation of 2D-DFT of a matrix $U \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ is essentially the computation of $\mathbf{X}^T U\mathbf{Y}$ at $x = \omega^m$ and $y = \omega^n$ for every $m,n = 0,1,2,\ldots,\mathtt{N}-1$. Hence, it is clear that $e_{mn} = p(\omega^m,\omega^n)$, $f_{mn} = q(\omega^m,\omega^n)$ and $g_{mn} = r(\omega^m,\omega^n)$. Rewriting equation (17) in matrix form, we have $\mathscr{F}(P) \odot \mathscr{F}(Q) = \mathscr{F}(R)$.

(**ii**) $\Rightarrow$ (**i**) : Given $\mathscr{F}(P) \odot \mathscr{F}(Q) = \mathscr{F}(R)$. Therefore, for every $m,n = 0,1,\ldots,\mathtt{N}-1$ and $\omega := e^{-j\frac{2\pi}{\mathtt{N}}}$, we have

$$p(\omega^m,\omega^n)q(\omega^m,\omega^n) = r(\omega^m,\omega^n). \quad (18)$$

Note that the variety of $\mathbb{A}$, denoted by $\mathbb{V}(\mathbb{A})$, is the set $\big\{(\alpha,\beta) \in \mathbb{C}^2 | \alpha^{\mathtt{N}} = 1 \text{ and } \beta^{\mathtt{N}} = 1\big\}$. Let $\mathscr{I}\Big(\mathbb{V}(\mathbb{A})\Big)$ be the ideal consisting of all polynomials $g(x,y) \in \mathbb{C}[x,y]$ such that $g(\alpha,\beta) = 0$ for all $(\alpha,\beta) \in \mathbb{V}(\mathbb{A})$. Since equation (18) is true for every $m,n = 0,1,\ldots,\mathtt{N}-1$, we have $p(\alpha,\beta)q(\alpha,\beta) - r(\alpha,\beta) = 0$ for all $(\alpha,\beta) \in \mathbb{V}(\mathbb{A})$. Therefore, $p(x,y)q(x,y) - r(x,y) \in \mathscr{I}\Big(\mathbb{V}(\mathbb{A})\Big)$.

By Hilbert's Nullstellensatz[1], we infer that $p(x,y)q(x,y) - r(x,y) \in \mathscr{I}\Big(\mathbb{V}(\mathbb{A})\Big) = \sqrt{\mathbb{A}}$. Note that $\mathbb{V}(\mathbb{A}) \subset \mathbb{C}^2$ is a finite set and therefore $\mathbb{A}$ is a zero-dimensional ideal[2]. Hence using [5, Proposition 2.7], we can verify that $\mathbb{A}$ is a radical ideal i.e. $\sqrt{\mathbb{A}} = \mathbb{A}$. Therefore,

$$\begin{aligned} &p(x,y)q(x,y) - r(x,y) \in \sqrt{\mathbb{A}} \Rightarrow p(x,y)q(x,y) - r(x,y) \in \mathbb{A} \\ &\Rightarrow \Pi\Big(p(x,y)q(x,y) - r(x,y)\Big) = 0. \end{aligned} \quad (19)$$

Since[3] $LM\Big(r(x,y)\Big) \preceq (xy)^{\mathtt{N}-1}$, we have $\Pi\Big(r(x,y)\Big) = r(x,y)$. It therefore follows from equation (19) that

$$\Pi\Big(p(x,y)q(x,y)\Big) = \Pi\Big(r(x,y)\Big) \Rightarrow \Pi\Big(p(x,y)q(x,y)\Big) = r(x,y).$$

This completes the proof of Theorem 4.1. □

Using Theorem 4.1 and results from Section 3, we can now, not only establish a relation between 2D-DFT and circulant Lyapunov operators but also formulate an algorithm to solve circulant Lyapunov equations using 2D-DFT. The next corollary and the discussion thereafter reveal this.

Corollary 4.2. *Consider the circulant Lyapunov equation* $AP + PA^T = Q$ *with* $A := \sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k E^k \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ *and* $P,Q \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$. *Define* $J \in \mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ *such that* $\mathbf{X}^T J\mathbf{Y} = \sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k)$. *Then, the following are equivalent:*

(i) $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k)p(x,y)\Big) = q(x,y)$,

(ii) $\mathscr{F}(J) \odot \mathscr{F}(P) = \mathscr{F}(Q)$.

[1] Hilbert's Nullstellensatz: If $\mathbb{F}$ is an algebraically closed field and $\mathbb{J}$ is an ideal in $\mathbb{F}[x_1,x_2,\ldots,x_{\mathtt{n}}]$, then $\mathscr{I}(\mathbb{V}(\mathbb{J})) = \sqrt{\mathbb{J}}$. $\sqrt{\mathbb{J}}$ is the *radical* of $\mathbb{J}$. The radical of $\mathbb{J}$, denoted by $\sqrt{\mathbb{J}}$, is the set $\{g \in \mathbb{F}[x_1,\ldots,x_2] : g^m \in \mathbb{J}$ for some $m \geqslant 1\}$. Further, an ideal $\mathbb{J}$ is said to be a *radical ideal* if $\sqrt{\mathbb{J}} = \mathbb{J}$.

[2] An ideal $\mathbb{J} \subset \mathbb{C}[x_1,x_2,\ldots,x_{\mathtt{n}}]$ is a *zero-dimensional* ideal if $\mathbb{V}(\mathbb{J}) \subset \mathbb{C}^{\mathtt{n}}$ is a finite set: see [5, Chapter 2, Finiteness Theorem] for details.

[3] Let $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{C}[x_1,x_2,\ldots,x_{\mathtt{n}}]$ and let $\succ$ be a term ordering. Then the leading monomial of f is $LM(f) := x^{d(f)}$ (with coefficient 1), where the multidegree $d(f)$ of f is defined as $d(f) := \max(\alpha \in \mathbb{Z}^{\mathtt{n}}_{\geq 0} : a_\alpha \neq 0)$: see [4, Chapter 2].

Proof. Define $g(x,y) = \mathbf{X}^T J\mathbf{Y}$. Then from Theorem 4.1 we conclude that $\Pi\Big(g(x,y)p(x,y)\Big) = q(x,y)$ if and only if $\mathscr{F}(J)\odot\mathscr{F}(P) = \mathscr{F}(Q)$. □

This means that given matrices A and Q in the equation $AP+PA^T = Q$, computation of P is possible using the formula $P = \mathscr{F}^{-1}(\mathscr{F}(Q)\oslash\mathscr{F}(J))$. However, for the operation $\oslash$ i.e. element-wise division to be well-defined, *every* element of $\mathscr{F}(J)$ needs to be nonzero. Therefore, a relevant question to ask here is: when will every element of $\mathscr{F}(J)$ be nonzero? The next few results formulate the condition under which every entry of $\mathscr{F}(J)$ is nonzero. Although a complete characterization of the class of J matrices that results in every element of $\mathscr{F}(J)$ being nonzero requires further investigation, the next theorem and corollary throw some light on this question. For ease of exposition, we state Theorem 4.4 after the following corollary.

Corollary 4.3. *Define $J\in\mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathbf{X}^T J\mathbf{Y} := \mathsf{a}(x^k+y^k)$, where $\mathsf{a}\in\mathbb{R}\backslash\{0\}$, $k\in\mathbb{N}\backslash\{0\}$ and $k<\mathtt{N}$. Let $\mathscr{F}(J)$ be the 2D-DFT matrix of J. Assume $A := \mathsf{a}E^k$. Then, every element of $\mathscr{F}(J)$ is nonzero if and only if $\Big((2\ell+1)\mathtt{N}\Big)\mathrm{mod}(2k)\neq 0$ for each $\ell\in\mathbb{Z}$.*
Further, if the above condition holds then the Lyapunov equation $AP+PA^T = Q$ is solvable for each $Q\in\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$.

The proof of Corollary 4.3 directly follows from that of Theorem 4.4 next and hence we skip that. Before we formulate necessary and sufficient conditions for the general case of all circulant matrices A (in Theorem 4.4), we first link the case of *singular* Lyapunov equation (i.e. Proposition 2.1) with division by zero. More precisely, Lyapunov operator singularity is equivalent to encountering a division by zero (during entry-wise division operation $\oslash$) as mentioned in Corollary 4.3. Further, when dividing by zero, if the numerator also is zero, this is precisely the case when we *have solvability* for the singular Lyapunov operator, i.e. Case 1 of Proposition 2.1. Further, from Corollary 4.3 it is clear that for the case when $A = \mathsf{a}E^k$, entry-wise division is well-defined if $\mathtt{N}$ is odd. On the other hand, when $\mathtt{N}$ is even there can be instances when entry-wise division $\mathscr{F}(Q)\oslash\mathscr{F}(J)$ fails. The next theorem is a generalized version of Corollary 4.3.

Theorem 4.4. *Define $J\in\mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathbf{X}^T J\mathbf{Y} = \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)$, where $\mathsf{a}_k\in\mathbb{R}$. Let $\mathscr{F}(J)$ be the 2D-DFT matrix of J. Define $\omega := e^{-j\frac{2\pi}{\mathtt{N}}}$. Then every element of $\mathscr{F}(J)$ is nonzero if and only if for each $m,n = 0,1,2,\ldots,\mathtt{N}-1$*

$$\sum_{k=0}^{\mathtt{N}-1} 2\mathsf{a}_k\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}}\neq 0. \quad (20)$$

Further, if equation (20) holds then the Lyapunov equation $AP+PA^T = Q$ is solvable for each $Q\in\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$, with $A\in\mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ defined as $A := \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k E^k$.

Proof. Let us write the 2D-DFT matrix $\mathscr{F}(J)$ as $\mathscr{F}(J) = [\mathscr{F}(J)_{mn}]_{m,n=0,1,\ldots,\mathtt{N}-1}$. Then we have (see [3, Section B]) $\mathscr{F}(J)_{mn} = \sum_{p=0}^{\mathtt{N}-1}\left(\sum_{q=0}^{\mathtt{N}-1}J_{pq}\omega^{qm}\right)\omega^{pn}$, i.e.,

$$\mathscr{F}(J) = \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(\omega^{mk}+\omega^{nk}) = \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(e^{-j\frac{2\pi}{\mathtt{N}}mk}+e^{-j\frac{2\pi}{\mathtt{N}}nk}) \quad (21)$$

$$= \sum_{k=0}^{\mathtt{N}-1}2\mathsf{a}_k\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}} \quad (22)$$

(**If**): Given $\sum_{k=0}^{\mathtt{N}-1}2\mathsf{a}_k\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}}\neq 0$ for each $m,n = 0,1,2,\ldots,\mathtt{N}-1$. Therefore, from equation (22) we infer that every entry of $\mathscr{F}(J)$ is nonzero.
(**Only if**): Since $\mathscr{F}(J)_{mn}\neq 0$, From equation (22), we conclude that $\sum_{k=0}^{\mathtt{N}-1}2\mathsf{a}_k\cos\left(\frac{\pi(m-n)k}{\mathtt{N}}\right)\omega^{\frac{(m+n)k}{2}}\neq 0$ for every $m,n = 0,1,\ldots,\mathtt{N}-1$.
Further, from Statement (b) of Theorem 3.2, it is clear that under condition (20), there exists a unique polynomial $p(x,y)$ with coefficient matrix $P\in\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ such that $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)p(x,y)\Big) = q(x,y)$ for a given $q(x,y) =: \mathbf{X}^T Q\mathbf{Y}$. From the discussion in Section 3, we know that coefficient matrix of $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)p(x,y)\Big)$ is $AP+PA^T$. Clearly, $\mathbf{X}^T(AP+PA^T)\mathbf{Y} = \mathbf{X}^T Q\mathbf{Y}$. Hence the Lyapunov equation $AP+PA^T = Q$ for each $Q\in\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ is solvable under condition (20). □

Theorem 4.4 customized to the special case when $A = \mathsf{a}E^k$ results in some interesting properties which we presented in Corollary 4.3. The next theorem shows that the eigenvalues of a circulant Lyapunov operator are the same as that of the elements of the 2D-DFT matrix corresponding to coefficient matrix J formed in Theorem 4.4. This theorem gives a check on the nonsingularity of circulant Lyapunov operators using the 2D-DFT matrix $\mathscr{F}(J)$ of J.

Theorem 4.5. *Consider a circulant Lyapunov operator $\mathscr{L}_A(\bullet)$, where $A := \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k E^k$ and define $J\in\mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ such that $\mathbf{X}^T J\mathbf{Y} := \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)$. Let Λ be the set of eigenvalues of $\mathscr{L}_A(\bullet)$ and let Γ be the set of elements of $\mathscr{F}(J)$. Then, $\Lambda = \Gamma$.*
In particular, $\mathscr{F}(J)$ has every element nonzero if and only if $\mathscr{L}_A(\bullet)$ is nonsingular.

Proof. We first prove that $\Lambda\supseteq\Gamma$. From equation (21), the elements of $\mathscr{F}(J) = [\mathscr{F}(J)]_{m,n=0,1,\ldots,\mathtt{N}-1}$ are given by

$$\mathscr{F}(J)_{mn} = \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k\Big(\omega^{mk}+\omega^{nk}\Big) \text{ where } \omega = e^{-j\frac{2\pi}{\mathtt{N}}}. \quad (23)$$

Note that ω^m and ω^n are eigenvalues of E for any $m,n = 0,1,\ldots,\mathtt{N}-1$. Let $v_m, v_n\in\mathbb{C}^{\mathtt{N}}$ be the eigenvectors of E corresponding to eigenvalues ω^m,ω^n, respectively. Note that $E^k v_m = \omega^{mk}v_m$ and $E^k v_n = \omega^{nk}v_n$. We construct the matrix $V_{mn} := v_m v_n^T\in\mathbb{C}^{\mathtt{N}\times\mathtt{N}}$. Note that $\mathscr{L}_A(V_{mn}) = \Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k E^k\Big)v_m v_n^T + v_m v_n^T\Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k E^k\Big)^T$. Hence, we have

$$\mathscr{L}_A(V_{mn}) = \Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(\omega^{mk}+\omega^{nk})\Big)V_{mn} \quad (24)$$

Note that equation (24) is true for all $m,n = 0,1,\ldots,\mathtt{N}-1$. This proves that each element of $\mathscr{F}(J)$ given by equation (23) is an eigenvalue of $\mathscr{L}_A(\bullet)$. Therefore, $\Lambda\supseteq\Gamma$.
Next we prove that $\Lambda\subseteq\Gamma$. Let γ be any eigenvalue of $\mathscr{L}_A(\bullet)$ and V be the corresponding eigenmatrix i.e $\mathscr{L}_A(V) = \gamma V$. Let $v(x,y) := \mathbf{X}^T V\mathbf{Y}$. Since $A = \sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k E^k$ and $\mathscr{L}_A(V) = \gamma V$, from Theorem 3.1, we have $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)v(x,y)\Big) = \gamma v(x,y)$. Let $J\in\mathbb{R}^{\mathtt{N}\times\mathtt{N}}$ be the coefficient matrix of $\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k)$ i.e. $\sum_{k=0}^{\mathtt{N}-1}\mathsf{a}_k(x^k+y^k) = \mathbf{X}^T J\mathbf{Y}$. Then by Theorem 4.1, we have $\mathscr{F}(J)\odot\mathscr{F}(V) = \gamma\mathscr{F}(V)$. Let $\mathscr{F}(J) =: [\alpha_{mn}]_{m,n=0,1,\ldots,\mathtt{N}-1}$ and $\mathscr{F}(V) =: [\beta_{mn}]_{m,n=0,1,\ldots,\mathtt{N}-1}$. Thus we

have $\alpha_{mn}\beta_{mn} = \gamma\beta_{mn}$ for each $m,n = 0,1,\ldots,\mathtt{N}-1$. Now, we claim that $\beta_{mn} \neq 0$ for at least one $m,n = 0,1,\ldots,\mathtt{N}-1$. Suppose this is not true, then $\beta_{mn} = 0$ for all $m,n = 0,1,\ldots \mathtt{N}-1$ i.e. $\mathscr{F}(V) = 0$. Then, we have $\mathscr{F}(V) = 0 \Rightarrow \Omega^T V \Omega = 0 \Rightarrow V = 0$ (Since Ω are nonsingular). But $V \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}\backslash 0$. Hence, $\mathscr{F}(V) \neq 0$. This means there exists at least one nonzero element in $\mathscr{F}(V)$. Let (p,q)-th component of $\mathscr{F}(V)$ is nonzero. Then, $\alpha_{pq}\beta_{pq} = \gamma\beta_{pq} \Rightarrow \alpha_{pq} = \gamma$. Thus for any eigenvalue γ of $\mathscr{L}_A(\bullet)$ there exists an index (p,q) such that $\alpha_{pq} = \gamma$, where $\alpha_{pq} \in \mathscr{F}(J)$. Thus $\Lambda \subseteq \Gamma$.
Therefore, $\Lambda = \Gamma$. This completes the proof of Theorem 4.5. Therefore, $\mathscr{F}(J)$ has every element nonzero if and only if $\mathscr{L}_A(\bullet)$ is nonsingular. □

From Theorem 4.5 it is clear that the matrix $\mathscr{F}(J)$ having at least one zero element means that the corresponding circulant Lyapunov operator is singular. Thus from Proposition 2.1, Theorem 4.4 and Theorem 4.5 it is clear that if equation (20) is false then a circulant Lyapunov equation $\mathscr{L}_A(P) = Q$ has either no solution or has infinitely many solutions. Note that a singular, circulant Lyapunov equation $\mathscr{L}_A(P) = Q$ have infinitely many solutions if $Q \in \operatorname{img}\Big(\mathscr{L}_A(\bullet)\Big)$ and no solutions if $Q \notin \operatorname{img}\Big(\mathscr{L}_A(\bullet)\Big)$. Therefore a relevant question is: Is there a relation between $\mathscr{F}(J)$ and Q that serves as an indication as to when $\mathscr{L}_A(P) = Q$ has no solutions or has infinitely many solutions. For ease of exposition, we explain this for the case when $A := \mathtt{a}E$. From Corollary 4.3 it is clear that $\mathscr{L}_{\mathtt{a}E}(P) = Q$ has either no solution or has infinitely many solutions when $\mathtt{N}$ is even.

Further, it is clear that whenever $\mathscr{F}(J)$ has zero elements then either there is non-uniqueness in the solution of a Lyapunov equation or there are no solutions to the Lyapunov equation. Further, it also establishes that if there is a zero element in $\mathscr{F}(J)$ then the corresponding position of the matrix $\mathscr{F}(Q)$ must also be zero for the circulant Lyapunov equation to be solvable. In such a case we encounter a zero by zero division during element-wise division operation. This is precisely the condition when there are infinitely many solutions to the Lyapunov equation[4].

The next corollary reveals the link between two-variable polynomials, circulant Lyapunov operator and 2D-DFT.

Corollary 4.6. *Let* $A := \sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k E^k$ *and* $J \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ *be such that* $\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k) =: \mathbf{X}^T J \mathbf{Y}$. *Define* $\mathbb{A} := \langle x^{\mathtt{N}} - 1, y^{\mathtt{N}} - 1\rangle \subset \mathbb{C}[x,y]$. *Assume* $g(x,y), r(x,y) \in \mathbb{C}[x,y]$ *such that* $\Pi\Big(\sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k(x^k + y^k) g(x,y)\Big) = r(x,y)$. *Then the following are equivalent: (a)* $\mathscr{L}_A(\bullet)$ *is nonsingular. (b)* $g(x,y)$ *is unique. (c)* $\mathscr{F}(J)$ *has every element nonzero.*

Since this corollary is a direct consequence of Theorem 3.3 and Theorem 4.5, we skip the proof. All the results in the paper finally leads to the following algorithm.

[4]For the case when $\mathscr{F}(J)$ and $\mathscr{F}(Q)$ have zero in their corresponding position, e.g. say α_{mn} and β_{mn} are zero, where $\mathscr{F}(Q) =: [\alpha_{mn}]$ and $\mathscr{F}(J) =: [\beta_{mn}]$, then the Lyapunov equation has infinitely many solutions. Hence, one can choose an arbitrary value of α_{mn}/β_{mn} (say τ as given in Step 9 of Algorithm 4.1) to get to a solution of the Lyapunov equation.

Algorithm 4.1 A 2D-DFT based algorithm to solve circulant Lyapunov equation i.e. $\mathscr{L}_A(P) = Q$.

Input: $\mathtt{a}_0, \mathtt{a}_1, \ldots, \mathtt{a}_{\mathtt{N}-1} \in \mathbb{R}$, $Q \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ and $A = \sum_{k=0}^{\mathtt{N}-1} \mathtt{a}_k E^k$.
Output: Solution $P \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ of $AP + PA^T = Q$.

1: Construct $v := [\mathtt{a}_1\ \mathtt{a}_2\ \cdots\ \mathtt{a}_{\mathtt{N}-1}]$ and $J := \begin{bmatrix} 2\mathtt{a}_0 & v \\ v^T & \mathbf{0} \end{bmatrix}$.
2: Compute 2D-DFT of Q and J. **Result:** $\mathscr{F}(Q) =: [\alpha_{mn}]$ and $\mathscr{F}(J) =: [\beta_{mn}]$, respectively.
3: Construct $\mathscr{F}(P) = [\kappa_{mn}]$ as follows
4: **for** $m = 1 : \mathtt{N}$ **do**
5:     **for** $n = 1 : \mathtt{N}$ **do**
6:         **if** $\beta_{mn} \neq 0$ **then**
7:             $\kappa_{mn} = \alpha_{mn}/\beta_{mn}$.
8:         **else**
9:             $\kappa_{mn} = \tau$, where $\tau \in \mathbb{C}^{\mathtt{N}\times\mathtt{N}}$ (see Footnote 4).
10:         **end if**
11:     **end for**
12: **end for**
13: Use inverse 2D-DFT to find $P = \mathscr{F}^{-1}\Big(\mathscr{F}(P)\Big)$.

5. Conclusion

In this paper we have shown that under a suitable projection map Π, two-variable polynomials are related to circulant Lyapunov operators (Theorem 3.3 and Theorem 3.1). Using this two-variable polynomial interpretation of circulant Lyapunov operators, we showed that nonsingularity of Lyapunov operators is a necessary and sufficient condition for every element of the 2D-DFT matrix corresponding to a suitably constructed matrix to be nonzero (Theorem 4.5). These links among circulant Lyapunov operators, two-variable polynomials and 2D-DFT matrix formulated in Corollary 4.6 revealed how the solutions to circulant Lyapunov equations can be found using 2D-DFT. Using these results we devised an algorithm to solve circulant Lyapunov equations (Algorithm 4.1). The algorithm is not only an order of magnitude faster than the conventional algorithms, like that in [2], to compute Lyapunov equation solutions but can also be parallelized.

References

[1] P. Benner and T. Damm, Lyapunov equations, energy functionals, and model order reduction of bilinear and stochastic systems, *SIAM Journal on Control and Optimization*, vol. 49, no. 2, pages 686-711, 2011.
[2] G. Golub, S. Nash, and C. Van Loan, A Hessenberg-Schur method for the problem $AX + XB = C$, *IEEE Transactions on Automatic Control*, vol. 24, no. 6, pp. 909-913, 1979.
[3] C. Bhawal, D. Pal, and M.N. Belur, A 2D-DFT based method to solve Bezoutian and a link to Lyapunov equation, *In the Proceedings of Indian Control Conference, Guwahati, India,* 2017.
[4] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, New York, 1992.
[5] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Springer Science & Business Media, New York, 2004.
[6] P.J. Davis, *Circulant Matrices*, John Wiley and Sons, New York, 1979.
[7] Z. Gajić and M.T.J. Qureshi, *Lyapunov Matrix Equation in System Stability and Control*, Academic Press, San Diego, CA, 1995.
[8] M. Konstantinov, V. Mehrmann and P. Petkov, On properties of Sylvester and Lyapunov operators, *Linear Algebra and its applications*, vol. 312, no. 1-3, pages 35-71, 2000.
[9] J.A. Marshall and M.E. Broucke, Symmetry invariance of multiagent formations in self-pursuit, *IEEE Transactions on Automatic Control*, vol. 53, no. 9, pages 2022-2032, 2008.
[10] V.Y. Pan, *Structured Matrices and Polynomials: Unified Superfast Algorithms*, Birkhäuser, Boston, New York, 2001.
[11] P.H. Petkov, N.D. Christov and M.M. Konstantinov, *Computational Methods for Linear Control Systems*, Prentice-Hall, Herts, UK, 1991.
[12] A. Pogromsky, G. Santoboni and H. Nijmeijer, Partial synchronization: from symmetry towards stability, *Physica D: Nonlinear Phenomena*, vol. 172, no. 1, pages 65-87, 2002.