



# Uniqueness of rank-one auto-correlation matrix polynomials factorization

Konstantin Usevich, Julien Flamant, Marianne Clausel, David Brie

## ► To cite this version:

Konstantin Usevich, Julien Flamant, Marianne Clausel, David Brie. Uniqueness of rank-one auto-correlation matrix polynomials factorization. 2023. hal-04062934v1

**HAL Id: hal-04062934**

**<https://hal.science/hal-04062934v1>**

Preprint submitted on 7 Apr 2023 (v1), last revised 28 Aug 2023 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Uniqueness of rank-one auto-correlation matrix polynomials factorization

Konstantin Usevich<sup>a</sup>, Julien Flamant<sup>a</sup>, Marianne Clausel<sup>b</sup>, David Brie<sup>a</sup>

<sup>a</sup>CNRS, Université de Lorraine, CRAN, F-54000 Nancy France

<sup>b</sup>CNRS, Université de Lorraine, Institut Elie Cartan de Lorraine, F-54000 Nancy France

---

## Abstract

This article characterizes the rank-one factorization of auto-correlation matrix polynomials. We establish a sufficient and necessary uniqueness condition for uniqueness of the factorization based on the greatest common divisor (GCD) of multiple polynomials. In the unique case, we show that the factorization can be carried out explicitly using GCDs. In the non-unique case, the number of non-trivially different factorizations is given and all solutions are enumerated.

*Keywords:* matrix auto-correlation polynomial, rank-one factorization, uniqueness, greatest common divisor of polynomials

---

## 1. Introduction

Let  $\mathbf{\Gamma}(z) = [\Gamma_{ij}(z)]_{i,j=1}^{R,R}$  be an  $R \times R$  matrix polynomial of degree at most  $2(N-1)$ , with complex coefficients. The goal of this paper is to characterize the matrix polynomials that have the following rank-one factorization:

$$\mathbf{\Gamma}(z) = \begin{bmatrix} \Gamma_{11}(z) & \cdots & \Gamma_{1R}(z) \\ \vdots & & \vdots \\ \Gamma_{R1}(z) & \cdots & \Gamma_{RR}(z) \end{bmatrix} = \begin{bmatrix} X_1(z) \\ \vdots \\ X_R(z) \end{bmatrix} \begin{bmatrix} \tilde{X}_1(z) & \cdots & \tilde{X}_R(z) \end{bmatrix}, \quad (1)$$

where  $X_r(z), r \in \{1, \dots, R\}$  are polynomials with degree at most  $N-1$  and  $\tilde{X}_r$  are their complex conjugate reversals with the complex reversal operation defined as

$$\tilde{Y}(z) = z^{N-1} \overline{Y(\bar{z}^{-1})} = \sum_{n=0}^{N-1} \bar{y}_{N-1-n} z^n \quad (2)$$

for a polynomial  $Y(z) = \sum_{n=0}^N \bar{y}_n z^n$  of degree at most  $N-1$ . In this paper we address the following questions:

- is the factorization (1) unique?
- if it is not unique, how to find all possible factorizations (1)?

The polynomial factorization problem arises in several applications in signal processing, such as phase retrieval problems [1] and blind system identification [2]. In such applications, one is interested to reconstruct a number of signals (vectors)  $\mathbf{x}_r = [x_r[0] \ \cdots \ x_r[N-1]]^\top \in \mathbb{C}^N, r \in \{1, \dots, R\}$ , given a set of

---

*Email addresses:* `konstantin.usevich@univ-lorraine.fr` (Konstantin Usevich), `julien.flamant@cnrs.fr` (Julien Flamant), `marianne.clausel@univ-lorraine.fr` (Marianne Clausel), `david.brie@univ-lorraine.fr` (David Brie)

auto-correlations  $[\gamma_{ij}[n]]_{i,j=1,n=-N+1}^{R,R,N-1}$  sequences

$$\gamma_{ij}[n] = \sum_{m=0}^{N-1-n} x_i[m+n] \overline{x_j[m]}. \quad (3)$$

It can be shown (see Appendix A) that the elements in (3) corresponds exactly to the coefficients of the polynomial  $\Gamma_{ij}(z)$  factorized as (1). Thus the problem of recovery of the vectors  $\mathbf{x}_r$  from auto-correlations is equivalent to the problem of factorizing<sup>1</sup> a given matrix polynomial as (1).

In this paper we provide a complete characterization of all possible rank-one factorizations of the form (1); in fact, these factorizations are entirely characterized by the greatest common divisor of the polynomials  $\Gamma_{ij}(z)$ . In particular, we prove the following theorem.

**Theorem 1.** *The factorization (1) is unique up to global scaling if and only if the polynomial  $H(z) = \gcd\{\Gamma_{ij}\}_{i,j=1}^R$  may have only roots on the unit circle  $\mathbb{T}$ .*

By uniqueness up to global scaling in (1) we mean that any alternative factorization  $\Gamma_{ij}(z) = Y_i(z) \tilde{Y}_j(z)$  satisfies  $Y_i(z) = cX_i(z)$  with  $c \in \mathbb{C}$ ,  $|c| = 1$ . Moreover, in the non-unique case, we provide all possible factorizations modulo the global scaling, which again depend on roots and their multiplicities of the polynomial  $H(z)$ .

*Related work.* Factorizations of matrix polynomials and matrix functions are a classic topic in linear algebra and operator theory. In fact, it can be shown that the matrix polynomials factorized as (1) have the so-called  $*$ -palindromic structure [3]. Several previous works have addressed the spectral properties or the Smith normal form of palindromic matrix polynomials, but, up to the authors knowledge, none of them discussed in detail uniqueness and characterization of solutions, which is a very important question in applications mentioned above. The factorization (1) also resembles the problem of spectral factorization of matrix functions [4], however, unlike the latter problem, in the factorization (1) there is no restriction on location of zeros of the polynomials. Finally, the uniqueness problem was studied in the literature on (algebraic) phase retrieval problems. In fact, the case  $R = 1$  ( $1 \times 1$  matrices) was analyzed in [5], where a characterization of the solutions has been given. The characterization that we propose here supersedes the one given in [5], as we treat the  $R > 1$  case. Moreover, we use the formalism which employs the polynomials with roots at infinity, which simplifies the proofs and allows for a complete characterization.

*Organization of the paper.* Our results rely on the formalism of the polynomials with roots at infinity (used in [6, §I.0] to build the algebraic theory of Hankel matrices). The main notation regarding polynomials is given in Section 2. In Section 3, we provide the main result on uniqueness of the factorization, which is a slight generalization of Theorem 1. Finally, in Section 4 we discuss the complete description of the set of solutions.

## 2. Background and main notations

### 2.1. Polynomials and multiplications

We borrow some notation from [7]. Let  $\mathbb{C}$  denote the complex field,  $\mathbb{T} = \{z \in \mathbb{C} | |z| = 1\}$  denote the unit circle, and let  $\mathbb{C}_{\leq D}[z]$  denote the space of univariate polynomials with complex coefficients of degree at most  $D$ . For a polynomial  $A \in \mathbb{C}_{\leq D}[z]$  we will use the following notation for its coefficients:

$$A(z) = \sum_{n=0}^D a[n]z^n. \quad (4)$$

---

<sup>1</sup>This is the reason why in [1] we refer to (1) as the polynomial auto-correlation factorization (PAF).

Thus  $\mathbb{C}_{\leq D}[z]$  is a  $(D+1)$ -dimensional vector space that is isomorphic to  $\mathbb{C}^{D+1}$  via the following one-to-one map:

$$\mathbf{a} = [a[0] \ a[1] \ \cdots \ a[D]]^\top \mapsto A(z) = a[0] + za[1] + \cdots + z^D a[D]. \quad (5)$$

The conjugate reversal  $\tilde{A}(z)$  of the polynomial in (4) is given by (2) and corresponds to the conjugated and reversed vector of coefficients

$$[\overline{a[D]} \ \cdots \ \overline{a[1]} \ \overline{a[0]}]^\top.$$

Next, when multiplying polynomials, we always keep in mind to which space it belongs to.

**Definition 1.** We define the multiplication as map from  $\mathbb{C}_{\leq D_1}[z] \times \mathbb{C}_{\leq D_2}[z]$  to  $\mathbb{C}_{\leq (D_1+D_2)}[z]$ :

$$(A(z), B(z)) \mapsto C(z) = A(z)B(z),$$

which in coordinates (i.e., for the vectors of coefficients  $\mathbf{a} \in \mathbb{C}^{D_1+1}$  and  $\mathbf{b} \in \mathbb{C}^{D_2+1}$ ) can be expressed as

$$(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{c} = \mathbf{M}_{D_1}(\mathbf{b})\mathbf{a} = \mathbf{M}_{D_2}(\mathbf{a})\mathbf{b}, \quad (6)$$

where  $\mathbf{M}_L(\mathbf{a})$  is the multiplication matrix

$$\mathbf{M}_L(\mathbf{a}) := \underbrace{\begin{bmatrix} a_0 & & & \\ \vdots & \ddots & & \\ a_D & & & a_0 \\ & \ddots & \vdots & \\ & & & a_D \end{bmatrix}}_{\in \mathbb{C}^{(D+L+1) \times (L+1)}}, \quad (7)$$

defined for any nonnegative integer  $L$  and a vector of coefficients

$$\mathbf{a} = [a[0] \ a[1] \ \cdots \ a[D]] \in \mathbb{C}^{D+1}.$$

Note that via isomorphism (5), the multiplication of polynomials corresponds essentially to the convolution of vectors.

**Remark 1.** The space  $\mathbb{C}_{\leq D}[z]$  can be also identified with the space of homogeneous bivariate polynomials of degree  $D$ , see [7] for a discussion. Homogeneous polynomials are very common in, for example, algebraic geometry [8, Ch. 8]. In this paper, however, for simplicity we prefer to work with univariate polynomials in  $\mathbb{C}_{\leq D}[z]$  instead.

## 2.2. Roots at infinity

An important tool used in this paper is that we operate with  $\infty$  roots. We will say that the polynomial  $A \in \mathbb{C}_{\leq D}[z]$  in (4) has root at  $\infty$  (with multiplicity  $\mu_k$ ) if its leading coefficient vanishes (i.e., if  $a[D] = \cdots = a[D - \mu_k + 1] = 0$ ). We will formally write  $(z - \infty)^d B(z)$  to denote that  $d$  zero leading coefficients are appended to the polynomial.

**Example 1.** Consider the following polynomial from  $\mathbb{C}_{\leq 5}[z]$ :

$$A(z) = 0 \cdot z^5 + 0 \cdot z^4 + \frac{1}{2}z^3 + \frac{1}{2}z^2 - z \in \mathbb{C}_{\leq 5}[z]. \quad (8)$$

This polynomial has roots  $\{\infty, -2, 1, 0\}$ , where the root  $\infty$  has multiplicity 2. Hence it has the following factorization

$$A(z) = \frac{1}{2}(z - \infty)^2(z - 1)(z + 2)z. \quad (9)$$

**Remark 2.** The root at infinity can be formally defined as:

$$(z - \infty) := 0 \cdot z + 1 \in \mathbb{C}_{\leq 1}[z].$$

Then the multiplication by such polynomial in the sense of the definition in (6) corresponds exactly to adding a zero leading coefficient. In particular,

$$(z - \infty)^d := 0 \cdot z^d + 0 \cdot z^{d-1} + \cdots + 0 \cdot z + 1 \in \mathbb{C}_{\leq d}[z].$$

With such a convention, the following extended version of the fundamental theorem of algebra holds true: any nonzero polynomial  $A \in \mathbb{C}_{\leq D}[z] \setminus \{\mathbf{0}\}$  can be uniquely factorized (up to permutation of roots) as

$$A(z) = \lambda \prod_{i=1}^m (z - \alpha_i)^{\mu_i}, \quad (10)$$

where  $\lambda \in \mathbb{C}$ ,  $\alpha_i \in \mathbb{C} \cup \{\infty\}$  are distinct roots and  $\mu_i$  are the multiplicities of  $\alpha_i$ , so that their sum is

$$\mu_1 + \cdots + \mu_m = D.$$

Finally, we remark that the conjugate reflection (2) leads to reflection of roots.

**Lemma 1.** The conjugate reflection of the polynomial (10) admits a factorization

$$\tilde{A}(z) = \tilde{\lambda} \prod_{i=1}^m \left( z - \overline{\alpha_i^{-1}} \right)^{\mu_i}, \quad \text{where } \tilde{\lambda} := \bar{\lambda} \prod_{\substack{i=1 \\ \alpha_i \neq \infty}}^m (-\bar{\alpha_i})^{\mu_i},$$

i.e., the roots  $\alpha_i$  are mapped to  $\overline{\alpha_i^{-1}}$ , where 0 is formally assumed to be the inverse of  $\infty$  and vice versa.

**Example 2.** For Example 1, the conjugate reflection  $\tilde{A}(z) \in \mathbb{C}_{\leq 5}[z]$ , as well as its factorization becomes:

$$\tilde{A}(z) = 0 \cdot z^5 - z^4 + \frac{1}{2}z^3 + \frac{1}{2}z^2 = (-1)(z - \infty)(z + \frac{1}{2})(z - 1)z^2.$$

which has roots  $\{\infty, 1, -\frac{1}{2}, 0\}$ , where the root 0 has multiplicity 2.

Graphically, the conjugate reflection of the roots has a nice interpretation in terms of the Riemann sphere: the mapping of the root under conjugate reflection becomes simply a reflection with respect to the plane passing through the equator, see Fig. 1.

**Remark 3.** When dealing with homogeneous polynomials, the roots in fact belong to the projective space  $\mathbb{P}^1$  which corresponds exactly to  $\mathbb{C} \cup \{\infty\}$ .

### 2.3. Divisors and greatest common divisors

Finally, we need to be careful when speaking about multiplication and divisors, as we need to take into account the possible roots at infinity. We define the divisibility according to Definition 1.

**Definition 2.** We say that the polynomial  $A \in \mathbb{C}_{\leq (D)}[z]$  has a divisor  $B \in \mathbb{C}_{\leq D'}[z] \setminus \{\mathbf{0}\}$  if there is a polynomial  $C \in \mathbb{C}_{\leq D-D'}[z]$  such that  $A(z) = B(z)C(z)$  in the sense of Definition 1.

Note that the zero leading coefficients need to be taken into account.

**Example 3.** The polynomial  $0 \cdot z^3 + 0 \cdot z^2 + z + 2 = (z - \infty)^2(z + 2) \in \mathbb{C}_{\leq 3}[z]$  is a divisor of the polynomial  $A(z)$  in from Example 1, but the polynomial  $0 \cdot z^4 + 0 \cdot z^3 + 0 \cdot z^2 + z + 2 = (z - \infty)^3(z + 2) \in \mathbb{C}_{\leq 4}[z]$  is not, because there are not enough infinite roots in the expansion of  $A(z)$ .

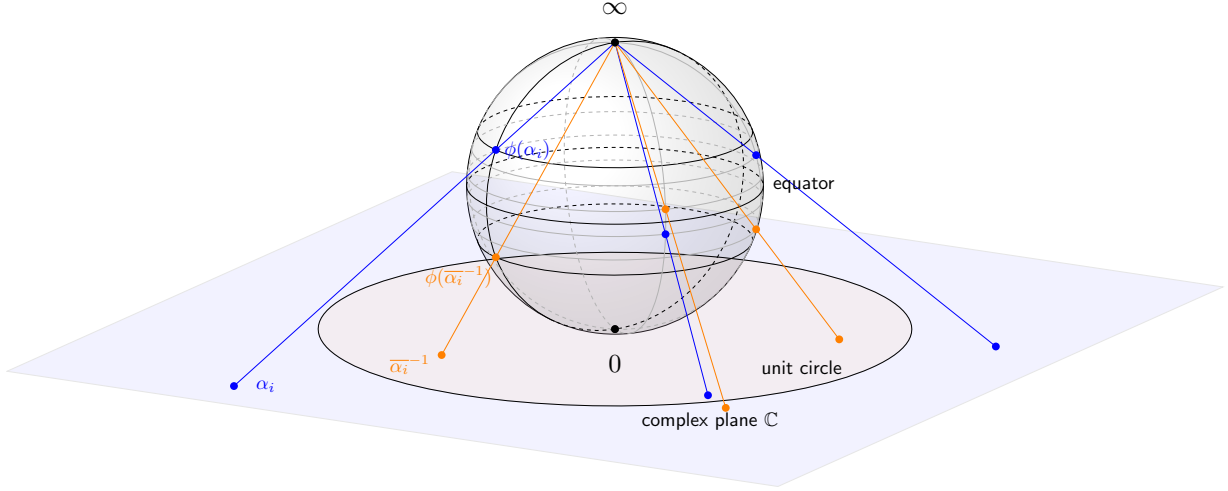


Figure 1: Complex plane and the Riemann sphere (the preimage under the stereographic projection). The conjugate inversion corresponds to reflection with respect to the equator on the Riemann sphere. Here  $\phi : \mathbb{C} \rightarrow \mathcal{S}^2$  denote the inverse stereographic mapping onto the sphere  $\mathcal{S}^2$ .

**Remark 4.** Let (10) be the factorization of a polynomial  $A \in \mathbb{C}_{\leq(D)}[z]$ . Then  $B \in \mathbb{C}_{\leq(D')}[z] \setminus \{0\}$  is a divisor of  $A$  if and only if it can be factorized as

$$B(z) = \lambda' \prod_{i=1}^m (z - \alpha_i)^{\nu_i}, \quad (11)$$

where  $\nu_i \geq 0$ ,  $\nu_1 + \dots + \nu_m = D'$ .

Finally, we make a remark on the notion of the greatest common divisor, which, for two nonzero polynomials  $A_1, A_2 \in \mathbb{C}_{\leq D}[z]$  is a polynomial  $H \in \mathbb{C}_{\leq D'}[z]$  with highest possible  $D'$ , which is a divisor of both  $A_1(z)$  and  $A_2(z)$ . The GCD is defined uniquely up to a multiplication by a scalar in  $\mathbb{C} \setminus \{0\}$ , so when we write  $C(z) = \gcd(A(z), B(z))$ , the equality is meant up to the multiplication by a non-zero scalar. The same notion can be defined for several polynomials, see [7, Section 2] for more details. In fact, for any non-zero tuple of polynomials, the GCD exists and is unique.

### 3. Uniqueness of factorizations

The main goal of this section is to provide a proof of Theorem 1, thus giving a characterization of the uniqueness properties of the polynomial factorization problem (1). In fact, we will prove a generalized version of Theorem 1.

#### 3.1. Polynomial factorization and common divisors

We will need a few lemmas that help to reduce the matrix case to the univariate factorization.

**Lemma 2.** Let  $Q(z) := \gcd\{X_1, X_2, \dots, X_R\}$  where  $Q \in \mathbb{C}_{\leq D}[z]$  and  $R_1, R_2, \dots, R_R \in \mathbb{C}_{\leq N-D-1}[z]$  be the corresponding quotients, i.e.,  $X_r(z) = Q(z)R_r(z)$  for  $r = 1, \dots, R$  with  $\gcd\{R_1, R_2, \dots, R_R\} = 1$ . Then we have that

1) the GCD  $H(z) := \gcd\{\Gamma_{ij}\}_{i,j=1}^{R,R}$  must have the form

$$H(z) = cQ(z)\tilde{Q}(z), \quad c \neq 0; \quad (12)$$

2) given the quotients  $R_{ij}(z)$  (i.e.,  $\Gamma_{ij}(z) = H(z)R_{ij}(z)$ ,  $\gcd\{R_{ij}\}_{i,j=1}^R = 1$ ), the quotients of  $X_1, X_2, \dots, X_R$  are determined up to a multiplicative constant as

$$R_r(z) = \gcd\{R_{r1}, R_{r2}, \dots, R_{rR}\}. \quad (13)$$

*Proof.* Start by 1). Direct calculations show that, for  $i, j = 1, \dots, R$ ,

$$\Gamma_{ij}(z) = X_i(z)\tilde{X}_j(z) = R_i(z)\tilde{R}_j(z)Q(z)\tilde{Q}(z).$$

Then the GCD of polynomials  $\Gamma_{ij}(z)$  can be explicitly computed as

$$\begin{aligned} H(z) &= \gcd\{\Gamma_{ij}\}_{i,j=1}^R \\ &= \gcd\left\{\gcd\{\Gamma_{1j}\}_{j=1}^R, \gcd\{\Gamma_{2j}\}_{j=1}^R, \dots, \gcd\{\Gamma_{Rj}\}_{j=1}^R\right\} \\ &= \gcd\left\{R_1Q\tilde{Q}, R_2Q\tilde{Q}, \dots, R_RQ\tilde{Q}\right\} && \text{since } \gcd\{\tilde{R}_1, \tilde{R}_2, \dots, \tilde{R}_R\} = 1 \\ &= cQ(z)\tilde{Q}(z) && \text{since } \gcd\{R_1, R_2, \dots, R_R\} = 1 \end{aligned}$$

Proof of 2). From 1), we have that  $R_{ij}(z) = c^{-1}R_i(z)\tilde{R}_j(z)$ . The determination (13) of  $R_r(z)$  is then straightforward using that  $\gcd\{R_1, R_2, \dots, R_R\} = \gcd\{\tilde{R}_1, \tilde{R}_2, \dots, \tilde{R}_R\} = 1$  by assumption.  $\square$

Lemma 2 shows that the study of the uniqueness properties of (1) is directly related to uniqueness of the univariate polynomial factorization (12), i.e., the recovery of  $Q(z)$  given  $H(z) = cQ(z)\tilde{Q}(z)$ . Indeed, if  $Q(z)$  can be uniquely recovered from  $H(z)$ , then the polynomials  $X_1(z), X_2(z), \dots, X_R(z)$  can be found by multiplying  $Q(z)$  with the respective quotients  $R_1(z), R_2(z), \dots, R_R(z)$  obtained thanks to (13). Before giving the sufficient and necessary uniqueness condition, we make a remark about the roots of the product  $Q(z)\tilde{Q}(z)$  which are key to understanding uniqueness.

**Lemma 3.** Let  $Q(z) = \lambda \prod_{i=1}^D (z - \alpha_i)$  (with possibly repeating  $\alpha_i$ ). Then  $H(z) = cQ(z)\tilde{Q}(z)$  has the following factorization

$$H(z) = c\lambda\tilde{\lambda} \prod_{i=1}^D (z - \alpha_i)(z - \overline{\alpha_i^{-1}}). \quad (14)$$

Furthermore, if  $\alpha \in \mathbb{T}$ , then  $\alpha = \overline{\alpha^{-1}}$ . Therefore, a unit-modulus  $\alpha$  is a root of  $Q(z)$  of multiplicity  $\mu$  if and only if it is a root of  $H(z)$  of multiplicity  $2\mu$ .

*Proof.* Follows by straightforward calculation.  $\square$

**Remark 5.** From Lemma 3, we see that the unit-modulus roots of  $H(z)$  do not contribute to non-uniqueness of the factorization (1). Indeed, all unit-modulus roots of  $Q(z)$  can be uniquely retrieved from  $H(z)$ . This helps us to establish a necessary and sufficient condition for uniqueness of the problem (1), as it will be shown next.

We will also need the following lemma

**Lemma 4.** *The coefficient of the polynomial  $X(z)\tilde{Y}(z)$  at the monomial  $z^{N-1}$  is equal to the inner product between the vectors of coefficients, that is:*

$$(X(z)\tilde{Y}(z))\Big|_{z^{N-1}} = \langle X, Y \rangle = \sum_{n=0}^{N-1} x_n \bar{y}_n.$$

In particular,

$$(X(z)\tilde{X}(z))\Big|_{z^{N-1}} = \langle X, X \rangle = \|X\|_2.$$

*Proof.* Follows from the relation between (1) and autocorrelation, see Appendix A □

### 3.2. The main uniqueness result

Finally, before proving the theorem, we clarify what we mean by uniqueness.

**Remark 6.** *If  $\Gamma(z)$  can be factorized as (1). Then any simultaneous rescaling of the polynomials by  $\beta \in \mathbb{C}$ ,  $|\beta| = 1$  provides an alternative factorization since  $\beta\bar{\beta} = 1$*

$$\begin{bmatrix} \beta X_1(z) \\ \vdots \\ \beta X_R(z) \end{bmatrix} \begin{bmatrix} \bar{\beta}\tilde{X}_1(z) & \cdots & \bar{\beta}\tilde{X}_R(z) \end{bmatrix} = \begin{bmatrix} X_1(z) \\ \vdots \\ X_R(z) \end{bmatrix} \begin{bmatrix} \tilde{X}_1(z) & \cdots & \tilde{X}_R(z) \end{bmatrix},$$

i.e. polynomials  $Y_i(z) = \beta X_i(z)$  provide an equivalent factorization. In what follows, we refer to essential uniqueness of the solution (1) as uniqueness up to a global scaling by a unimodular constant.

**Theorem 2.** *The following equivalences are true:*

1. The problem (1) admits a unique solution (in the sense of Remark 6);
2.  $X_1(z), X_2(z), \dots, X_R(z)$  have no common roots in  $(\mathbb{C} \cup \{\infty\}) \setminus \mathbb{T}$  (common roots may be only on the unit circle);
3.  $H(z) = \gcd\{\Gamma_{ij}\}_{i,j=1}^R$  has no common roots in  $\mathbb{C} \setminus \mathbb{T}$

*Proof.* The proof is organized in several parts.

- 2  $\Leftrightarrow$  3 By Lemma 2,  $H(z) = cQ(z)\tilde{Q}(z)$ , where  $c$  is a constant and  $Q(z) = \gcd\{X_i(z)\}_{i=1}^R$ . Therefore, by Lemma 3,  $H(z)$  does not have roots outside unit circle if and only if  $Q(z)$  does not. Note that by Lemma 3, the roots of  $H(z)$  appear in pairs, and therefore  $H(z)$  has an  $\infty$  root if and only 0 is a root. Thus, we can look at common roots in  $\mathbb{C}$  instead of the whole  $\mathbb{C} \cup \{\infty\}$ .
- 1  $\Rightarrow$  2 Suppose that the solution of (1) is essentially unique, but the polynomial  $Q(z)$  has a root  $\alpha$  outside the unit circle. Then easy calculations show that polynomial  $S(z) = \frac{Q(z)(z-\bar{\alpha}^{-1})}{(z-\alpha)}$  satisfies

$$S(z)\tilde{S}(z) = Q(z)\tilde{Q}(z).$$

Note that  $S(z)$  is not proportional to  $Q(z)$ , because

$$\frac{(z - \bar{\alpha}^{-1})}{(z - \alpha)} \neq \text{const.}$$

Therefore the polynomial vector

$$(Y_1(z), \dots, Y_R(z)) := (S(z)R_1(z), \dots, S(z)R_R(z)),$$

is not proportional to the vector  $(X_1(z), \dots, X_R(z))$ , but gives an alternative factorization  $\Gamma_{ij}(z) = Y_i(z)Y_j(z)$  (a contradiction).



- 1  $\Leftarrow$  2 We begin by noting that there is an equivalence

$$\Gamma_{ij}(z) \equiv 0 \iff X_i(z) \equiv 0 \text{ or } X_j(z) \equiv 0 \iff \Gamma_{ii}(z) \equiv 0 \text{ or } \Gamma_{jj}(z) \equiv 0$$

Thus we can determine the cases when  $X_k(z) \equiv 0$  and otherwise assume without loss of generality that  $\Gamma_{ij}(z) \neq 0$  for all  $i, j$ .

Assume that  $H(z)$  has only unit-modulus roots. By Lemma 3, there is a unique monic polynomial  $Q(z)$  such that  $H(z) = cQ(z)\tilde{Q}(z) = c(Q(z))^2$ . Therefore, by Lemma 2, we can find the quotients  $R_1(z), \dots, R_R(z)$  up to a multiplicative constants. Therefore, we can determine the polynomials  $X_k(z) = R_k(z)Q(z)$  up to a multiplicative constant, i.e.,

$$W_1(z) = c_1 X_1(z), \quad \dots, \quad W_R(z) = c_R X_R(z),$$

where  $c_k \in \mathbb{C} \setminus \{0\}$ . Note that we recovered  $X_k(z)$  up to individual scalings. In what follows, we show how to remove these scalings.

We assume that one of them is nonzero, i.e.  $W_k(z) \not\equiv 0$ . First, we determine  $|c_k|$ , and for that we invoke Lemma 4. We note that

$$\gamma_{kk}[0] = (\Gamma_{kk}(z))|_{z^{N-1}} = (X_k(z)\tilde{X}_k(z))|_{z^{N-1}} = \|X_k\|_2^2$$

Therefore, we have that

$$|c_k| = \frac{\|W_k\|_2}{\sqrt{\gamma_{kk}[0]}}.$$

Therefore, we conclude that for all  $j$

$$\frac{|W_k|}{\sqrt{\gamma_{kk}[0]}} \frac{\Gamma_{jk}(z)}{\tilde{W}_k(z)} = \frac{|W_k|}{\sqrt{\gamma_{kk}[0]}} \frac{X_j(z)}{\bar{c}_k} = \beta X_j(z)$$

where  $\beta \in \mathbb{T}$  does not depend on  $j$ .

□

**Remark 7.** Note that the uniqueness condition given in Theorem 2 clarifies previous statements made in the literature [9, 2] for the case of two polynomials ( $R = 2$ ). In particular, in [9, Theorem 1] it was claimed that a necessary and sufficient for uniqueness of the solution of (1) is the coprimeness of the polynomials  $X_1(z)$  and  $X_2(z)$ . Theorem 2 shows that it was just a sufficient condition, because unimodular roots do not affect uniqueness. This agrees with a similar behavior observed for uniqueness in univariate 1D phase retrieval, see e.g., [5].

### 3.3. The coprime case

In the case where the polynomials are coprime, the reconstruction algorithm considerably simplifies, which we show in this paper. But before that, we will need the following lemma.

**Corollary 1** (GCD solution of (1) for the coprime case). *Suppose that  $\gcd(\Gamma_{ij}(z)) = 1$  (equivalently,  $\gcd(X_k(z)) = 1$ ). Then the polynomials  $X_k(z)$  can be obtained up to a global unimodular constant as follows:*

- Choose  $k$  such that  $\Gamma_{kk}(z) \not\equiv 0$ .
- Compute the polynomial  $W_k(z)$  as GCDs:

$$W_k(z) := \gcd\{\Gamma_{k1}, \Gamma_{k2}, \dots, \Gamma_{kR}\};$$

note that  $W_j(z) = c_k X_k(z)$  (i.e.  $X_k(z)$  is recovered up to a multiplicative constant).

- There exists  $\beta \in \mathbb{T}$  such that all other polynomials can be recovered up to multiplication by  $\beta$  as

$$\beta X_j(z) = \frac{|W_k|}{\sqrt{\gamma_{kk}[0]}} \frac{\Gamma_{jk}(z)}{\widetilde{W}_k(z)}.$$

*Proof.* The proof is based on the computation presented in the part  $\boxed{1 \Leftarrow 2}$  of the proof of Theorem 2.  $\square$

**Corollary 2** (Almost everywhere uniqueness of (1)). *In the generic case, the solution of (1) is essentially unique: there exists a set of (Lebesgue) measure zero in  $A \subset (\mathbb{C}_{\leq N}[z])^R$ , such that for all  $(X_1, \dots, X_R) \in (\mathbb{C}_{\leq N}[z])^R \setminus A$  the solution of (1) is essentially unique.*

*Proof.* It is a well-known results that the two polynomials  $X_1, X_2 \in \mathbb{C}_{\leq N}[z]$  do not have a common root in  $\mathbb{C} \cup \{\infty\}$  if and only if its  $2N \times 2N$  Sylvester matrix

$$S_1(X_1, X_2) = \begin{bmatrix} \mathbf{M}_{N-1}(\mathbf{X}_1) & \mathbf{M}_{N-1}(\mathbf{X}_2) \end{bmatrix}$$

is nonsingular. The equation  $\det(S_1(X_1, X_2)) = 0$  defines an algebraic variety  $V$  of dimension  $2N + 1 \leq \dim((\mathbb{C}_{\leq N}[z])^2)$ , thus it is a set of measure zero. Taking  $A = V \times \dim(\mathbb{C}_{\leq N}[z])^{R-2}$  concludes the proof.  $\square$

#### 4. Ambiguities and counting the number of solutions

In this section, we refine Theorem 2 by providing the number of solutions and describing the set of solutions of (1) in the non-uniqueness case. In essence, this description depends mainly on uniqueness properties of the factorization (12) (i.e., how to find all  $Q(z)$  such that  $H(z) = Q(z)\tilde{Q}(z)$ ). We begin this section by discussing the number of solutions of the factorization (12), and we conclude by enumerating the solutions to the matrix polynomial factorization problem (1).

##### 4.1. Univariate autocorrelation factorization

Uniqueness of the factorization (12) is known to be equivalent to the uniqueness of the so called univariate phase retrieval problem [5, 10]. We adapt these results to the formalism used here of polynomial with  $\infty$  roots.

**Theorem 3** (Number of solutions of (1)). *Let  $H(z) = Q(z)\tilde{Q}(z)$  and  $\mu_1, \dots, \mu_{N_D}$  be the respective multiplicities of the  $N_D$  non-unit-modulus roots pairs  $(\delta_1, \bar{\delta}_1^{-1}), \dots, (\delta_{N_D}, \bar{\delta}_{N_D}^{-1})$  of  $H(z)$ . Then the problem (1) admits exactly*

$$\prod_{i=1, |\delta_i| \neq 1}^{N_D} (\mu_i + 1) \tag{15}$$

*different solutions, where only non-unimodular common roots of  $X_1$  and  $X_2$  contribute to the total number of solutions. In particular, when common roots are all simple and outside the unit circle, there is exactly  $2^{N_D}$  different solutions.*

*Proof.* Lemma 2 shows that the number of solutions of (1) is exactly the number of different (up to multiplication by a scalar) polynomials  $Q(z)$  such that  $H(z) = Q(z)\tilde{Q}(z)$ . This *spectral factorization* problem is equivalent to selecting the roots of  $Q(z)$  amongst the root pairs  $(\delta_i, \bar{\delta}_i^{-1})$  of  $H(z)$ . Since  $\mu_1, \dots, \mu_{N_D}$  are the multiplicities of the root pairs of  $H(z)$ , then for each root pair  $(\delta_i, \bar{\delta}_i^{-1})$  one has to select exactly  $\mu_i$  roots among those pairs, leading to a polynomial  $Q(z)$  of degree  $D = \mu_1 + \dots + \mu_{N_D}$ .

Consider a non-unit root pair  $(\delta_i, \bar{\delta}_i^{-1})$  with multiplicity  $\mu_i$ ; then the number of different combinations of  $\mu_i$  roots is that of a random draw of  $k = \mu_i$  items with replacement in a set of  $n = 2$  elements, i.e.,  $(n+k-1)!/(k!(n-1)!) = \mu_i + 1$ . Repeating the same process for each root pair gives the total number (15) of solutions to the problem (1).  $\square$

**Remark 8** (Counting multiplicities). *The number of solutions (15) depends in fact on the multiplicities of pairs of roots of  $Q(z)$ . This means in particular that if  $\delta$  and  $\bar{\delta}^{-1}$  are roots of  $Q(z)$  with multiplicities  $\mu_1$  and  $\mu_2$ , then the multiplicity of the pair  $(\delta, \bar{\delta}^{-1})$  of  $H(z)$  is equal to  $\mu_1 + \mu_2$ . The same applies to 0 and  $\infty$  roots.*

**Example 4.** *Consider  $Q(z) = A(z)$  that is the polynomial from Example 1 having double  $\infty$  root and simple roots  $\{-2, 1, 0\}$ . Then the polynomial  $H(z) = A(z)\tilde{A}(z)$  is given by*

$$H(z) = Q(z)\tilde{Q}(z) = -\frac{1}{2}(z - \infty)^3 \left(z + \frac{1}{2}\right) (z + 2)(z - 1)^2 z^3.$$

*The multiplicity of the root pair  $(0, \infty)$  is 3, while the root pair  $(-2, -\frac{1}{2})$  have multiplicity 1. This yields a total of  $4 \cdot 2 = 8$  solutions, where the other factorizations are given by permuting 0 and  $\infty$  roots or/and replacing root  $-2$  with  $-\frac{1}{2}$ . For example, some of possible alternative factorisations are given by  $Q(z) = \frac{1}{2}(z + 2)(z - 1)z^3$  or  $Q(z) = (z + \frac{1}{2})(z - 1)z^3$ .*

#### 4.2. Enumerating all solutions

We conclude the study of uniqueness properties of (1) in Theorem 4 below.

**Theorem 4** (Expression of the solutions of (1)). *Let  $H(z) = \gcd(\{\Gamma_{ij}\}) = Q(z)\tilde{Q}(z)$  and suppose  $H(z)$  has  $D$  pairs of roots  $(\delta_i, \bar{\delta}_i^{-1})$  (possibly repeating). Let  $R_k(z) \in \mathbb{C}_{N-D-1}[z]$ ,  $k = 1, \dots, R$  be determined as in (13), and denote by  $\alpha_{ki}$  the roots of  $R_k(z)$ . Then all solutions  $X'_1(z), \dots, X'_R(z)$  to the problem (1) can be expressed as*

$$X'_1(z) = e^{j\theta} \lambda_1 \prod_{i=1}^D (z - \beta_i) \prod_{i=1}^{N-D-1} (z - \alpha_{1i}), \quad (16)$$

$$\vdots \quad (17)$$

$$X'_R(z) = e^{j\theta} \lambda_R \prod_{i=1}^D (z - \beta_i) \prod_{i=1}^{N-D-1} (z - \alpha_{Ri}), \quad (18)$$

where each  $\beta_i$  is chosen among zeros pairs  $(\delta_i, \bar{\delta}_i^{-1})$  of  $H(z)$ ; the angle  $\theta \in (-\pi, \pi)$  accounts for the global phase trivial ambiguity.

*Proof.* Denote by  $\alpha_{ki}$  the  $N - D - 1$  roots of  $R_k(z)$  and assume that we can write

$$R_k(z) = c_k \prod_{i=1}^{N-D-1} (z - \alpha_{ki}),$$

where  $c_k \in \mathbb{C}$  are constants. Then we have that, by Lemma 2,  $\Gamma_{ij}(z) = X'_i(z)\tilde{X}'_j(z)$ , where

$$X'_k(z) = \lambda_k Q(z) R_k(z),$$

where  $Q(z)$  is such that  $H(z) = cQ(z)\tilde{Q}(z)$  and  $\lambda_k$  can be determined in the same fashion as the constants in Theorem 2.

Thus all possible solution depends on the solution of the factorization problem  $H(z) = cQ(z)\tilde{Q}(z)$ . Denoting by  $(\delta_i, \bar{\delta}_i^{-1})$  the pair roots of  $H(z)$ , then  $Q(z)$  can be written as

$$Q(z) = \prod_{i=1}^D (z - \beta_i), \quad \beta_i \in \{\delta_i, \bar{\delta}_i^{-1}\}. \quad (19)$$

As explained in Theorem 3, the number of different solutions for  $Q(z)$  dictates the number of solutions for problem (1). Thus, if polynomials  $(X'_1(z), \dots, X'_R(z))$  are solutions of (1) then they can be expressed as

$$X'_1(z) = \lambda_1 \prod_{i=1}^D (z - \beta_i) \prod_{i=1}^{N-D-1} (z - \alpha_{1i}) \quad (20)$$

$$\vdots \quad (21)$$

$$X'_R(z) = \lambda_R \prod_{i=1}^D (z - \beta_i) \prod_{i=1}^{N-D-1} (z - \alpha_{Ri}). \quad (22)$$

where  $\lambda_1, \dots, \lambda_R$  can be determined in a similar fashion as in Theorem 2.  $\square$

The next proposition provides an explicit expression of solutions of (1) in the simplified case of  $R = 2$  and where there are no 0 or  $\infty$  roots in common, meaning that  $\mathbf{x}[0] \neq \mathbf{0}$  and  $\mathbf{x}[N-1] \neq \mathbf{0}$ . This setting is relevant to the context of polarimetric phase retrieval [1].

**Proposition 1.** *For the case of two polynomials ( $R = 2$ ), such that  $H(z)$  does not have roots  $\{0, \infty\}$ , the constants  $\lambda_1, \lambda_2 \in \mathbb{C}$  in (4) are given by*

$$\lambda_1 = \sqrt{|\gamma_{11}[N-1]| \prod_{i=1}^D |\beta_i|^{-1} \prod_{i=1}^{N-D-1} |\alpha_{1i}|^{-1}}, \quad (23)$$

$$\lambda_2 = e^{j\Delta} \sqrt{|\gamma_{22}[N-1]| \prod_{i=1}^D |\beta_i|^{-1} \prod_{i=1}^{N-D-1} |\alpha_{2i}|^{-1}}, \quad (24)$$

where  $\Delta$  reads

$$\Delta = \pi(N-1) + \arg \gamma_{12}[N-1] + \sum_{i=1}^D \arg \beta_i + \sum_{i=1}^{N-D-1} \arg \alpha_{2i}. \quad (25)$$

*Proof.* To determine  $\lambda_1$  and  $\lambda_2$ , one writes the expression of the measurements polynomials in terms of  $X'_1(z)$  and  $X'_2(z)$  above. For instance:

$$\begin{aligned} \Gamma_{11}(z) &= X'_1(z) z^{N-1} \overline{X'_1(\bar{z}^{-1})} \\ &= |\lambda_1|^2 \prod_{i=1}^D (z - \beta_i) \prod_{i=1}^{N-D-1} (z - \alpha_{1i}) \prod_{i=1}^D (1 - \bar{\beta}_i z) \prod_{i=1}^{N-D-1} (1 - \bar{\alpha}_{1i} z) \end{aligned} \quad (26)$$

Using that  $\Gamma_{11}(z) := \sum_{n=0}^{2N-2} \gamma_{11}[n-N+1] z^n$ , identifying leading order coefficients yields

$$\gamma_{11}[N-1] = |\lambda_1|^2 (-1)^{N-1} \prod_{i=1}^D \bar{\beta}_i \prod_{i=1}^{N-D-1} \bar{\alpha}_{1i} \quad (27)$$

Similarly, one gets

$$\gamma_{22}[N-1] = |\lambda_2|^2 (-1)^{N-1} \prod_{i=1}^D \bar{\beta}_i \prod_{i=1}^{N-D-1} \bar{\alpha}_{2i} \quad (28)$$

$$\gamma_{12}[N-1] = \lambda_1 \bar{\lambda}_2 (-1)^{N-1} \prod_{i=1}^D \bar{\beta}_i \prod_{i=1}^{N-D-1} \bar{\alpha}_{2i} \quad (29)$$

These relations determine uniquely the amplitudes of  $\lambda_1, \lambda_2$  as well as the phase difference between  $\lambda_1$  and  $\lambda_2$ . Thus  $\lambda_1, \lambda_2$  are unique up to a global phase factor  $\exp(j\theta)$ ,  $\theta \in [-\pi, \pi)$ . One obtains eventually the following expressions

$$\lambda_1 = e^{j\theta} \left( |\gamma_{11}[N-1]| \prod_{i=1}^D |\beta_i|^{-1} \prod_{i=1}^{N-D-1} |\alpha_{1i}|^{-1} \right)^{1/2} \quad (30)$$

$$\lambda_2 = e^{j(\theta-\Delta)} \left( |\gamma_{22}[N-1]| \prod_{i=1}^D |\beta_i|^{-1} \prod_{i=1}^{N-D-1} |\alpha_{2i}|^{-1} \right)^{1/2} \quad (31)$$

with

$$\Delta = \arg(\lambda_1 \bar{\lambda}_2) \quad (32)$$

$$= \pi(N-1) + \arg \gamma_{12}[N-1] + \sum_{i=1}^D \arg \beta_i + \sum_{i=1}^{N-D-1} \arg \alpha_{2i}. \quad (33)$$

□

### A. Link between matrix polynomial factorization and autocorrelation

The matrix polynomial rank-one factorization problem (1) arises in multivariate instances of Fourier phase retrieval [1] and blind multichannel system identification [2]. In such applications, one is interested in recovering a deterministic discrete vector signal  $\mathbf{x} : \llbracket 0, N-1 \rrbracket \rightarrow \mathbb{C}^R$  from the different cross-correlations functions between the  $R$  signal channels. Now, define the polynomial representation of the  $i$ -th channel of  $\mathbf{x}$  as  $X_i(z) = \sum_{n=0}^{N-1} x_i[n]z^n$ . Similarly, define the correlation polynomial  $\Gamma_{ij}(z) := \sum_{n=0}^{2(N-1)} \gamma_{ij}[n-N+1]z^n$ . Then, a key result is that

$$\Gamma_{ij}(z) = X_i(z) \tilde{X}_j(z) \quad (34)$$

since

$$X_i(z) \tilde{X}_j(z) = \left( \sum_{n=0}^{N-1} x_i[n]z^n \right) \left( \sum_{m=0}^{N-1} \overline{x_j[N-1-m]}z^m \right) \quad (35)$$

$$= \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} x_i[n] \overline{x_j[N-1-m]} z^{n+m} \quad (36)$$

$$= \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} x_i[n] \overline{x_j[m]} z^{n+N-1-m} \quad (37)$$

$$= \sum_{n'=0}^{2(N-1)} \gamma_{ij}[n'-N+1] z^{n'} := \Gamma_{ij}(z). \quad (38)$$

Therefore, defining the matrix polynomial  $\mathbf{\Gamma}(z)$  such that

$$\mathbf{\Gamma}(z) = \begin{bmatrix} \Gamma_{11}(z) & \cdots & \Gamma_{1R}(z) \\ \vdots & & \vdots \\ \Gamma_{R1}(z) & \cdots & \Gamma_{RR}(z) \end{bmatrix} = \sum_{n=0}^{2N} \begin{bmatrix} \gamma_{11}[n-N+1] & \cdots & \gamma_{1R}[n-N+1] \\ \vdots & & \vdots \\ \gamma_{R1}[n-N+1] & \cdots & \gamma_{RR}[n-N+1] \end{bmatrix} z^n := \sum_{n=0}^{2(N-1)} \mathbf{\Gamma}[n] z^n \quad (39)$$

where  $\{\mathbf{\Gamma}[n] \in \mathbb{C}^{R \times R}\}_{n=-N+1}^N + 1$  is the auto-correlation matrix sequence of the  $D$ -dimensional vector signal  $\{\mathbf{x}[n] \in \mathbb{C}^R\}_{n=0}^{N-1}$ . Plugging (34) into (39) yields the rank-one autocorrelation matrix factorization problem (1).

## References

- [1] J. Flamant, K. Usevich, M. Clausel, D. Brie, [Polarimetric fourier phase retrieval](#), submitted (2023). URL <https://hal.science/hal-03613352>
- [2] K. Jaganathan, B. Hassibi, [Reconstruction of Signals From Their Autocorrelation and Cross-Correlation Vectors, With Applications to Phase Retrieval and Blind Channel Estimation](#), IEEE Transactions on Signal Processing 67 (11) (2019) 2937–2946. doi:10.1109/TSP.2019.2911254. URL <https://ieeexplore.ieee.org/document/8691612/>
- [3] D. Mackey, N. Mackey, C. Mehl, V. Mehrmann, Smith forms of palindromic matrix polynomials, The Electronic Journal of Linear Algebra 22 (2011) 53–91.
- [4] D. A. Bini, G. Fiorentino, L. Gemignani, B. Meini, Effective fast algorithms for polynomial spectral factorization, Numerical Algorithms 34 (2003) 217–227.
- [5] R. Beinert, G. Plonka, Ambiguities in one-dimensional discrete phase retrieval from fourier magnitudes, Journal of Fourier Analysis and Applications 21 (6) (2015) 1169–1198.
- [6] G. Heinig, K. Rost, Algebraic methods for Toeplitz-like matrices and operators, Birkhäuser, Basel, 1984.
- [7] K. Usevich, I. Markovsky, [Variable projection methods for approximate \(greatest\) common divisor computations](#), Theoretical Computer Science 681 (2017) 176–198. doi:10.1016/j.tcs.2017.03.028. URL <https://linkinghub.elsevier.com/retrieve/pii/S0304397517302505>
- [8] D. Cox, J. Little, D. O’Shea, Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 2nd Edition, Springer, 1997.
- [9] O. Raz, N. Dudovich, B. Nadler, [Vectorial Phase Retrieval of 1-D Signals](#), IEEE Transactions on Signal Processing 61 (7) (2013) 1632–1643. doi:10.1109/TSP.2013.2239994. URL <http://ieeexplore.ieee.org/document/6410442/>
- [10] T. Bendory, R. Beinert, Y. C. Eldar, [Fourier Phase Retrieval: Uniqueness and Algorithms](#), in: H. Boche, G. Caire, R. Calderbank, M. März, G. Kutyniok, R. Mathar (Eds.), Compressed Sensing and its Applications, Springer International Publishing, Cham, 2017, pp. 55–91, series Title: Applied and Numerical Harmonic Analysis. doi:10.1007/978-3-319-69802-1\_2. URL [http://link.springer.com/10.1007/978-3-319-69802-1\\_2](http://link.springer.com/10.1007/978-3-319-69802-1_2)