CLOSED-FORM EXPRESSION OF SMITH FORMS FOR PSEUDO-CIRCULANTS

Yuan-Pei Lin[†], *and See-May Phoong*[‡]

[†]Dept. Elect. and Control Engr., National Chiao Tung Univ., Hsinchu, Taiwan
[‡]Dept. of EE & Grad. Inst. of Comm Engr.,National Taiwan Univ.,Taipei, Taiwan

ABSTRACT

The pseudo-circulant matrices arise naturally in the block filtering application of multirate systems. More recently, there has been considerable interests in pseudo-circulants for the applications of precoding and discrete multitone communications systems. In these systems, a scalar FIR channel $P(z)$ is cast as a pseudo-circulant channel matrix. Many important channel properties have been derived from the Smith form and the decomposition of pseudo-circulants. In this paper, we will show that the Smith form of an FIR pseudo-circulant matrix can be given in terms of the zeros of the underlying scalar filter $P(z)$. Once the zeros of $P(z)$ are known, the Smith form of the corresponding pseudo-circulant matrix can be obtained in closed form.

1. INTRODUCTION

Pseudo-circulant matrices have found many applications in signal processing and communication systems [1]-[8]. There matrices arise from block filtering implementation of scalar LTI filters [1][3]. Fig. 1 shows the block filtering representation of $P(z)$ in terms of an $N \times N$ pseudo-circulant matrix $\mathbf{C}(z)$. A first detailed study of pseudo-circulants is made in [3]. One very useful property shown in [3] is that pseudo-circulants can be diagonalized using simple orthonormal matrices. More recently there is growing interest in pseudo-circulants due to their applications in communication systems such as precoding systems, discrete multitone systems or transmultiplexers [2]. In these systems, a scalar FIR channel $P(z)$ is recast into a FIR pseudo-circulant matrix $\mathbf{C}(z)$. The matrix formulation greatly facilitates the analysis of the transmitting and receiving systems.

It is well-known that, polynomial matrices in z^{-1} can be diagonalized using unimodular matrices, called Smith form decomposition. The decomposition has been demonstrated to be a very important tool for channel analysis [4]. As the decomposition is given in terms of FIR matrices, it is also useful for the design of FIR transceivers. Smith form decomposition is employed in [5][6][8] for the design of ISI free FIR transceivers. Important properties of the underlying scalar filter $P(z)$ can be directly linked to the Smith form of the pseudo-circulant channel matrix $\mathbf{C}(z)$, [6][7]. For example, the minimum redundancy for the existence of FIR DMT transceivers is equal to the number of nontrivial terms in the Smith form.

In this paper we show that, given the scalar filter $P(z)$, the Smith form of its corresponding $N \times N$ pseudo-circulant matrix $\mathbf{C}(z)$ can be given in closed form. In particular, the zeros of $P(z)$ can be grouped into sets of the so-called *congruous zeros*. Using congruous sets, we will see that the Smith form of $\mathbf{C}(z)$ can be determined by inspection.

2. PSEUDO-CIRCULANTS AND KNOWN RESULTS

Let $P(z)$ be an FIR filter of order L. We can obtain the polyhphase representation of $P(z)$ with respect to an integer N, where N is not necessarily larger than L. Let the polyphase representation of $P(z)$ be given by,

$$P(z) = \sum_{\ell=0}^{N} P_\ell(z^N) z^{-\ell}.$$

The scalar filter $P(z)$ can be represented using block filtering of block size N as shown in Fig. 1. The corresponding $N \times N$ block filter is given by,

$$\mathbf{C}(z) = \begin{pmatrix} P_0(z) & z^{-1}P_{N-1}(z) & \cdots & z^{-1}P_1(z) \\ P_1(z) & P_0(z) & \cdots & z^{-1}P_2(z) \\ \vdots & \vdots & \ddots & \vdots \\ P_{N-1}(z) & P_{N-2}(z) & \cdots & P_0(z) \end{pmatrix}. \quad (1)$$

Matrices in the above form are known as pseudo-circulant matrices [1]. In what follows, we briefly review Smith form decomposition for polynomial matrices [1] and two results of pseudo-circulant matrices known in the literature [3][6].

1. *Smith form decomposition.* An $N \times N$ polynomial matrix $\mathbf{C}(z)$ in z^{-1} can be represented using the Smith

THE WORK WAS SUPPORTED IN PARTS BY NSC 90-2213-E-009-108, NSC 90-2213-E-002-097, MINISTRY OF EDUCATION, UNDER CONTRACT NUMBER 89-E-FA06-2-4, TAIWAN, R.O.C., AND THE LEE AND MTI CENTER FOR NETWORKING RESEARCH.

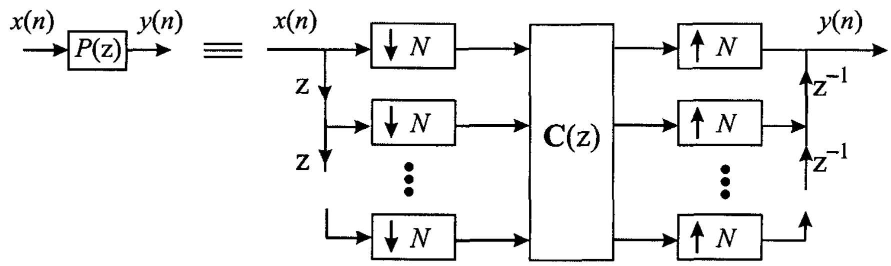

Figure 1: Block filtering representation of a scalar filter $P(z)$.

form decomposition [1]

$$\mathbf{C}(z) = \mathbf{U}(z)\mathbf{\Gamma}(z)\mathbf{V}(z), \tag{2}$$

where all three matrices in the decomposition are matrix polynomials in the variable z^{-1}. The matrices $\mathbf{U}(z)$ and $\mathbf{V}(z)$ are unimodular matrices, i.e., matrices with determinants equal to a constant; $\mathbf{\Gamma}(z)$ is a diagonal matrix,

$$\mathbf{\Gamma}(z) = \text{diag}\begin{pmatrix}\gamma_0(z) & \gamma_1(z) & \cdots & \gamma_{N-1}(z)\end{pmatrix}. \tag{3}$$

Moreover the unimodular matrices $\mathbf{U}(z)$ and $\mathbf{V}(z)$ can be so chosen that the polynomials $\gamma_k(z)$ are monic (i.e., highest power has unity coefficient) and $\gamma_k(z)$ is a factor of $\gamma_{k+1}(z)$, i.e., $\gamma_k(z)$ divides $\gamma_{k+1}(z)$. The matrix $\mathbf{\Gamma}(z)$, called the *Smith form* of $\mathbf{A}(z)$, is unique. But the matrices $\mathbf{U}(z)$ and $\mathbf{V}(z)$ are not unique. The decomposition can be obtained using a finite number of elementary row and column operations [1].

2. *Diagonalizaion using orthonormal matrices, [3].* Let $\mathbf{C}(z)$ be a pseudo circulant matrix of the form in (1). The the matrix $\mathbf{C}(z^N)$ be can diagonalized using orthonormal matrices [1][3]. In particular,

$$\mathbf{C}(z^N) = \mathbf{D}(z)\mathbf{W}\mathbf{\Sigma}(z)\mathbf{W}^\dagger\mathbf{D}(z^{-1}), \tag{4}$$

where

$$\mathbf{\Sigma}(z) = \text{diag}\begin{pmatrix}P(z) & P(zW^{-1}) & \cdots & P(zW^{-N+1})\end{pmatrix}$$

and

$$\mathbf{D}(z) = \text{diag}\begin{pmatrix}1 & z^{-1} & \cdots & z^{-N+1}\end{pmatrix}.$$

The matrix $\mathbf{W}$ is the $N \times N$ DFT matrix given by,

$$[\mathbf{W}]_{kn} = \frac{1}{\sqrt{N}}W^{kn} \quad \text{where} \quad W = e^{-j2\pi/N}.$$

The k-th diagonal entry of $\mathbf{\Sigma}(z)$ is $P(zW^{-k})$.

3. *Zeros of Pseudo-Circulants [6].* Suppose the underlying scalar filter $P(z)$ is a causal FIR filter of order L. Let the zeros be α_ℓ, for $\ell = 1, 2, \cdots, L$ and $P(z) = p_0 \prod_{\ell=1}^{L}(1 - \alpha_\ell z^{-1})$. Then $\det \mathbf{C}(z)$ is also a causal FIR filter of order L. The zeros of $\det \mathbf{C}(z)$ are α_ℓ^N, for $\ell = 1, 2, \cdots, L$. In particular,

$$\det \mathbf{C}(z) = p_0^N \prod_{\ell=1}^{L}(1 - \alpha_\ell^N z^{-1}). \tag{5}$$

Remarks. Note that, the diagonalization in (4) gives us the following decomposition of $\mathbf{C}(z)$,

$$\mathbf{C}(z) = \mathbf{D}(z^{1/N})\mathbf{W}\mathbf{\Sigma}(z^{1/N})\mathbf{W}^\dagger\mathbf{D}(z^{-1/N}).$$

The expression contains $z^{-1/N}$, a fraction of a delay, which can not be realized with a finite cost. Nonetheless the diagonalization is important from a theoretical viewpoint as it is a link of $\mathbf{C}(z)$ and the underlying scalar filter $P(z)$. It is very useful for the derivation in Section 3. On the other hand, notice that the matrices in the Smith decomposition $\mathbf{U}(z)$, $\mathbf{V}(z)$ and $\mathbf{\Gamma}(z)$ are all FIR and causal matrices. They can be used in the analysis of FIR transceivers [4][5]. They can also be incorporated directly in the design of FIR transceivers for channel equalization [8].

3. SMITH FORM OF PSEUDO-CIRCULANTS

In this section, we will derive the Smith form $\mathbf{\Gamma}(z)$ of the pseudo-circulant matrix $\mathbf{C}(z)$. We will see that given the zeros $\{\alpha_\ell\}_{\ell=1}^{L}$ of the scalar filter $P(z)$, the diagonal terms $\gamma_k(z)$ of the Smith form in (3) can be given in terms of α_ℓ in closed form.

Consider the Smith form decomposition in (2). Since $\det \mathbf{U}(z)$ and $\det \mathbf{V}(z)$ are both constants; we have

$$\det \mathbf{C}(z) = c \det \mathbf{\Gamma}(z) = c\Pi_{k=0}^{N-1}\gamma_k(z),$$

where

$$c = \det \mathbf{U}(z) \det \mathbf{V}(z).$$

This means that the collection of zeros of $\gamma_k(z)$ forms the zeros of $\det \mathbf{C}(z)$.

Definition 1 *Congruous zeros. A set of zeros*

$$\mathbf{B} = \{\alpha_{k_1}, \alpha_{k_2}, \cdots \alpha_{k_q}\}$$

of $P(z)$ are congruous with respect to N if

(i) $\alpha_{k_1}, \alpha_{k_2}, \cdots \alpha_{k_q}$ *are distinct and,*

(ii) $\alpha_{k_1}^N = \alpha_{k_2}^N = \cdots = \alpha_{k_q}^N$.

The zeros that are congruous are distinct but their magnitudes are the same and their angles differ by an integer multiple of $2\pi/N$. They can be expressed as the rotation of each other by integer multiples of $2\pi/N$, i.e.,

$$\alpha_{k_j} = \alpha_{k_1} W^{-n_j}, \tag{6}$$

$$\text{where } W = e^{-j2\pi/N}, 1 \le n_j < N, j = 1, 2, \cdots, q.$$

As congruous zeros are distinct, the numbers n_j are distinct. The results in (5) show that the zeros of $\det \mathbf{C}(z)$ are obtained by raising the zeros of $P(z)$ to the power N. So, when $P(z)$ has a set of q congruous zeros, $\det \mathbf{C}(z)$ has a zero of multiplicity q.

Lemma 1 *Let $\mathbf{C}(z)$ be a pseudo-circulant matrix with Smith form decomposition as given in (2) and diagonalization of $\mathbf{C}(z^N)$ in (4). Then,*

$$\text{rank}(\mathbf{C}(z^N)) = \text{rank}(\mathbf{\Sigma}(z)) = \text{rank}(\mathbf{\Gamma}(z^N)), \forall z.$$

Proof: The rank of $\mathbf{C}(z^N)$ is the same as the rank of $\mathbf{\Sigma}(z)$ as $\mathbf{W}$ and $\mathbf{D}(z)$ in (4) are nonsingular. On the other hand, the matrices $\mathbf{U}(z)$ and $\mathbf{V}(z)$ in the Smith form decomposition (2) are unimodular; they are nonsingular for all z. Therefore the rank of $\mathbf{C}(z^N)$, $\mathbf{\Sigma}(z)$ and $\mathbf{\Gamma}(z^N)$ are the same for all z.

$\Delta\Delta\Delta$

Lemma 2 *Let $B = \{\alpha_{k_1}, \alpha_{k_2}, \cdots, \alpha_{k_q}\}$ be a set of congruous zeros. Suppose no other zeros can be included in B to form a larger congruous set. Then,*

1. $\text{rank}(\mathbf{C}(\alpha_{k_1}^N)) = N - q$;
2. *The diagonal terms $\gamma_k(z)$ in the Smith form of $\mathbf{C}(z)$ satisfy the property that exactly q terms have the factor $(1-\alpha_{k_1}^N z^{-1})$. The q terms are $\gamma_{N-q}(z)$, $\gamma_{N-q+1}(z)$, $\cdots$, $\gamma_{N-1}(z)$.*

Proof: Consider the terms on the diagonal of $\mathbf{\Sigma}(z)$ in (4). Observe that

$$P(zW^{-n_j})|_{z=\alpha_{k_1}} = P(\alpha_{k_1} W^{-n_j})$$

As the zeros $\alpha_{k_1}, \alpha_{k_2}, \cdots, \alpha_{k_q}$ are congruous, they can be expressed as in (6) and

$$P(zW^{-n_j})|_{z=\alpha_{k_1}} = P(\alpha_{k_j}) = 0,$$

$$j = 1, 2, \cdots, q.$$

Therefore, we have

$$\text{rank}(\mathbf{\Sigma}(z))|_{z=\alpha_{k_1}} = N - q.$$

By Lemma 1, this implies that

$$\text{rank}(\mathbf{C}(\alpha_{k_1}^N)) = \text{rank}(\mathbf{\Gamma}(\alpha_{k_1}^N)) = N - q.$$

This means that q of the diagonal terms $\{\gamma_k(z)\}$ contain the factor $(1 - \alpha_{k_1}^N z^{-1})$. Because $\gamma_k(z)$ divides $\gamma_{k+1}(z)$, we conclude that the last q terms contain the factor $(1 - \alpha_{k_1}^N z^{-1})$; we arrive at the second result of the Lemma.

$\Delta\Delta\Delta$

In other words, whenever $P(z)$ have a set of q congruous zeros $\{\alpha_{k_1}, \alpha_{k_2}, \cdots, \alpha_{k_q}\}$, the scalar filter $\det \mathbf{C}(z)$ has a zero of multiplicity q at $\alpha_{k_1}^N$. The q zeros at $\alpha_{k_1}^N$ spread out into q diagonal terms of the Smith form. Notice that, when $P(z)$ has double zeros at α, $\det \mathbf{C}(z)$ has double zeros at α^N. However, double zeros of $P(z)$ are not considered congruous zeros by definition; the double zeros of $\det \mathbf{C}(z)$ at α^N do not spread out into two diagonal terms of the Smith form.

Lemma 2 provides us with the link between congruous zeros of the scalar filter $P(z)$ and the Smith form of $\mathbf{C}(z)$. Let us partition the zeros of $P(z)$ into sets of congruous zeros. Each set contains either congruous zeros or a single zero and no two sets can be combined to form a larger congruous set. In this case, the number of congruous sets is minimum. Say, there are total s congruous sets, $B_1, B_2, \cdots, B_s$. Denoting the cardinal of B_j as ℓ_j, we have

$$\sum_{j=1}^{s} \ell_j = L.$$

Without loss of generality, we assume

$$\ell_1 \le \ell_2 \cdots \le \ell_s.$$

Let

$$B_j = \{\alpha_{j,1}, \alpha_{j,2}, \cdots, \alpha_{j,\ell_j}\}, \; j = 1, 2, \cdots, s. \tag{7}$$

Using Lemma 2, we see that $\det \mathbf{C}(z)$ has a zero of multiplicity ℓ_j at $\alpha_{j,1}^N$. This means that $\gamma_{N-k}(z)$, for $k = 1, 2, \cdots, \ell_j$ contains the factor $(1 - \alpha_{j,1}^N z^{-1})$. Therefore $\gamma_{N-k}(z)$ contains every factor $(1 - \alpha_{j,1}^N z^{-1})$ with $\ell_j \ge k$. For $k > \ell_s$, we have $\gamma_{N-k}(z) = 1$. Summarizing, we have the following theorem.

Theorem 1 *Let the zeros of $P(z)$ be partitioned into minimum number of congruous sets, $B_1, B_2, \cdots, B_s$, where B_j are as given in (7). Then the Smith form $\mathbf{\Gamma}(z)$ of the pseudo-circulant $\mathbf{C}(z)$ has diagonal terms given by,*

$$\gamma_{N-k}(z) = \begin{cases} \prod_{\substack{j=1,\\ \ell_j \geq k}}^{s} (1-\alpha_{j,1}^{N} z^{-1}), & k = 1, 2, \cdots, \ell_s, \\ 1, & \text{otherwise.} \end{cases} \quad (8)$$

Using the above theorem, one can determine the Smith form of any $N \times N$ FIR pseudo circulant matrix $\mathbf{C}(z)$ by inspection once the zeros of the corresponding scalar filter $P(z)$ are known. Theorem 1 implies that the number of nontrivial terms in the Smith form is ℓ_s, i.e., the cardinal of the largest congruous set. This property has an important application in DMT transceiver design, where the minimum redundancy for the existence of FIR transceivers is equal to the number of nontrivial terms in the Smith form [6].

4. EXAMPLE

Suppose the scalar filter $P(z)$ have order $L = 5$ and $P(z)$ is given by

$$P(z) = 1 - z^{-1} - z^{-4} + z^{-5}.$$

The zeros of $P(z)$ are $\{1, 1, -1, j, -j\}$. Let us consider the Smith form $\mathbf{\Gamma}(z)$ of the pseudo-circulant matrix for $N = 2, 3, 4$.

1. *N=2.* The two zeros at $1, -1$ are congruous and the two zeros at $j, -j$ are congruous. The minimum number of congruous sets is 3. The congruous sets are $\{1\}, \{1, -1\}$, and $\{j, j\}$. The zeros of $\det \mathbf{C}(z)$ corresponding to the congruous sets are $\{1\}, \{1, 1\}$, and $\{-1, -1\}$. We have $\gamma_0(z) = (1 - z^{-1})(1 + z^{-1})$, and $\gamma_1(z) = (1 + z^{-1})(1 - z^{-1})^2$. The Smith form $\mathbf{\Gamma}(z)$ of $\mathbf{C}(z)$ is
$$\mathbf{\Gamma}(z) = \begin{pmatrix} (1-z^{-1})(1+z^{-1}) & 0 \\ 0 & (1-z^{-1})^2(1+z^{-1}) \end{pmatrix}$$
2. *N=3.* In this case, no two zeros are congruous. Each congruous set has only one entry, $\{1\}$, $\{1\}$, $\{-1\}$, $\{j\}$, $\{-j\}$ and the zeros of $\det \mathbf{C}(z)$ corresponding to the congruous sets are $\{1\}$, $\{1\}$, $\{-1\}$, $\{-j\}$ and $\{j\}$. We have $\gamma_0(z) = \gamma_1(z) = 1$, and $\gamma_2(z) = (1-z^{-1})^2(1+z^{-1})(1+z^{-2})$. The Smith form $\mathbf{\Gamma}(z)$ of $\mathbf{C}(z)$ is
$$\mathbf{\Gamma}(z) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (1-z^{-1})^2(1+z^{-1})(1+z^{-2}) \end{pmatrix}$$
Although $\det \mathbf{C}(z)$ has double zeros at $z = 1$, these two zeros do not come from a congruous set; they do not spread out into two terms in the Smith form.
3. *N=4.* There are two congruous sets, $\{1\}$, and $\{1, -1, j, -j\}$. The corresponding zeros of $\det \mathbf{C}(z)$ are $\{1\}, \{1, 1, 1, 1\}$. Therefore, $\gamma_0(z) = \gamma_1(z) = \gamma_2(z) = 1 - z^{-1}$, and $\gamma_3(z) = (1 - z^{-1})^2$. The Smith form $\mathbf{\Gamma}(z)$ of $\mathbf{C}(z)$ is
$$\mathbf{\Gamma}(z) = \begin{pmatrix} 1-z^{-1} & 0 & 0 & 0 \\ 0 & 1-z^{-1} & 0 & 0 \\ 0 & 0 & 1-z^{-1} & 0 \\ 0 & 0 & 0 & (1-z^{-1})^2 \end{pmatrix}$$

The example demonstrates that the number of nontrivial terms in the Smith form varies with the dimension N. It may increase as N increases.

5. REFERENCES

[1] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Englewood Cliffs,Prentice-Hall, 1993.

[2] A. N. Akansu, et. al., "Orthogonal Transmultiplexers in Communication: A Review," *IEEE Trans. Signal Processing*, vol. 46, pp. 979-995, April 1998.

[3] P. P. Vaidyanathan, and S. K. Mitra, "Polyphase Networks, Block Digital Filtering, LPTV Systems, and Alias-Free QMF Banks: A Unified Approach Based on Pseudocirculants", *IEEE Trans. Acoustics, Speech, and Signal Proc.*, ASSP-36, no. 3, March 1988.

[4] Xiang-Gen Xia, "New Precoding For Intersymbol Interference Cancellation Using Nonmaximally Decimated Multirate FilterBanks with Ideal FIR Equalizers," *IEEE Trans. on Signal Processing*, vol. 45, pp. 2431 -2441, 1997.

[5] Hui Liu and Xiang-Gen Xia, "Precoding Techniques for Undersampled Multireceiver Communication Systems," *IEEE Trans. on Signal Processing*, vol. 48, pp. 1853-1863, July 2000.

[6] Yuan-Pei Lin and See-May Phoong, "Minimum Redundancy ISI Free FIR Filterbank Transceivers, Proc. Society of Photo-Optical Instrumentation Engineers, July 2000.

[7] Yuan-Pei Lin and See-May Phoong, "Minimum Redundancy for ISI Free FIR Filterbank Transceivers,to appear in *IEEE Trans. on Signal Processing*.

[8] T. Karp and G. Schuller, "Joint Transmitter/Receiver Design for Multicarrier Data Transmission with Low Latency Time,Proc. Int. Conf. Acoustic, Speech and Signal Processing, Salt Lake, May 2001.