Paraunitary Filter Banks Over Finite Fields

See-May Phoong, *Member, IEEE,* and P. P. Vaidyanathan, *Fellow, IEEE*

***Abstract*—In real and complex fields, unitary and paraunitary (PU) matrices have found many applications in signal processing. There has recently been interest in extending these ideas to the case of finite fields. In this paper, we will study the theory of PU filter banks (FB's) in $GF(q)$ with q prime. Various properties of unitary and PU matrices in finite fields will be studied. In particular, a number of factorization theorems will be given. We will show that i) all unitary matrices in $GF(q)$ are factorizable in terms of Householder-like matrices and permutation matrices, and ii) the class of first-order PU matrices (the lapped orthogonal transform in finite fields) can always be expressed as a product of degree-one or degree-two building blocks. If $q > 2$, we do not need degree-two building blocks. While many properties of PU matrices in finite fields are similar to those of PU matrices in complex field, there are a number of differences. For example, unlike the conventional PU systems, in finite fields, there are PU systems that are *unfactorizable* in terms of smaller building blocks. In fact, in the special case of 2×2 systems, all PU matrices that are factorizable in terms of degree-one building blocks are diagonal matrices. We will derive results for both the cases of $GF(2)$ and $GF(q)$ with $q > 2$. Even though they share some similarities, there are many differences between these two cases.**

I. Introduction

FILTER BANKS (FB's) have found many successful applications in the subband coding of images and audio and video signals [1]–[6]. In the past, many researchers have contributed to the theory and design of FB's over real or complex field [1]–[8], especially for the class of paraunitary (PU) FB's that have the property of energy conservation. Consider Fig. 1(a) and (b), where an M-channel FB and its polyphase implementation are shown, respectively. In real or complex field, a FB is said to be PU if its polyphase matrix $\boldsymbol{E}(z) = \Sigma_k \boldsymbol{e}(k) z^{-k}$ satisfies [1]–[6]:

$$\boldsymbol{E}^{\dagger}(e^{j\omega})\boldsymbol{E}(e^{j\omega}) = \boldsymbol{I}, \quad \text{for all } \omega \tag{1.1}$$

where the superscript $\dagger$ represents transpose conjugate. Note that if we take $\boldsymbol{R}(e^{j\omega}) = \boldsymbol{E}^{\dagger}(e^{j\omega})$, then we have a perfect reconstruction (PR) FB. The class of PU FB's has the advantage [1]–[6] that PR can be obtained with FIR filters, and the synthesis filters are simply the time-reversed version of the analysis filters. What makes PU FB's so attractive in the application of subband coding is that both the analysis and synthesis banks have the energy preservation property. This property guarantees that the coding gain is greater than unity.

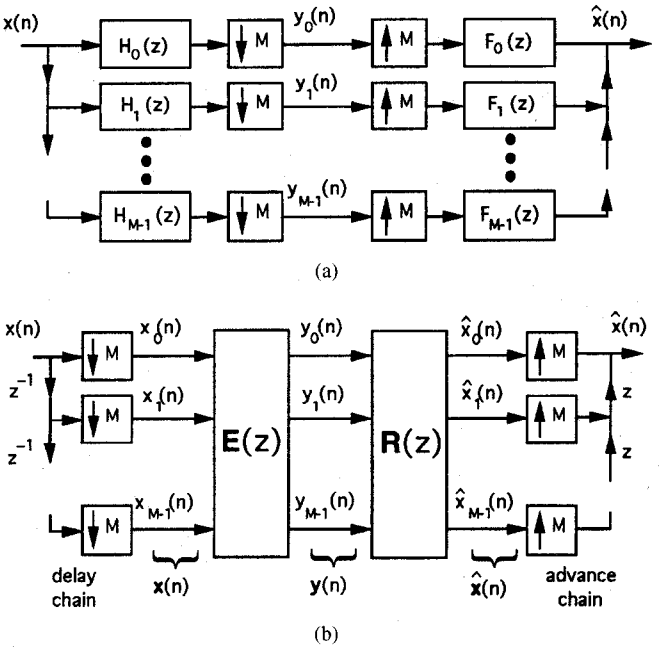


Fig. 1. (a) M-channel maximally decimated FB. (b) Its polyphase representation.

Despite the success of real or complex FB's in various applications, little attention has been paid to the case of finite fields. Even though in most of the applications the input is a digital signal that has a finite number of quantization levels, FB's from real or complex field have been used. FB's over finite fields have the advantage that all the round-off error and the coefficient quantization error can be eliminated completely. In addition, FB's in finite fields have potential applications in cryptography, in the theory of error-correcting codes, and in the coding or analysis of halftone images [9]–[11]. While these applications still remain to be explored, the immediate purpose of this paper is to study the theory of PU FB's in finite fields.

It should be noted that the finite field methods developed in our paper are not meant to be alternate implementations of traditional real-field subband coders. Such real-field subband coders have lossy quantizers in the subband. Such lossy quantization is not allowed in the finite field case because errors cannot be quantified as being small or large. It is, however, conceivable that finite field FB's can employ lossless quantization in the subbands; some applications of this kind have indeed been considered in the past [11].

A. Previous Work

The generalization of PU FB's to the case of $GF(2)$ was first done in [9]. The author showed that even though many properties of PU FB's in complex field continue to hold in the

Manuscript received September 23, 1995; revised February 3, 1997. This work was supported by Office of Naval Research Grant N00014-93-1-0231, funds from Tektronix, Inc., and Rockwell International. The associate editor coordinating the review of this paper and approving it for publication was Dr. Bruce W. Suter.

S.-M. Phoong was with the Department of Electrical Engineering, California Institute of Technology, Pasadena CA 91125 USA. He is now with Nanyang Technical University, Republic of Singapore.

P. P. Vaidyanathan is with the Department of Electrical Engineering, California Institute of Technology, Pasadena CA 91125 USA.

Publisher Item Identifier S 1053-587X(97)04208-6.

case of $GF(2)$, there were some unexpected properties. Unlike the conventional PU FB's, it was shown that there are PU FB's over $GF(2)$ that cannot be decomposed into degree-one building blocks. In [10], the authors used the alias cancellation (AC) matrix approach to study the theory of FB's over finite fields. In order to obtain PR FB's in finite fields using the AC matrix approach, the authors needed the existence of Mth root of unity in $GF(q)$ for a M-channel FB over $GF(q)$ (which is not always possible). Because of this limitation, the authors in [10] are unable to obtain M-channel PR FB's over $GF(q)$ when $M \geq q$. In [11], the authors proposed a new binary field transform as an alternative to the DFT over $GF(2)$. Using the new transform, the authors were able to define bandwidth, vanishing moments and spectral content in the filters over $GF(2)$. The application of FB's in $GF(2)$ to the analysis of binary images was also demonstrated. In [12], the author studies the connection between the theory of finite field FB's and the theory of convolutional codes and applies the finite field FB's to the problem of partial response channel. In [13] and [14], the authors consider the wavelet construction for the class of finite length signals (the length is a prime number) with real or complex value. The domain (i.e., time argument) of the input signal is therefore drawn from a finite field. In this paper, we consider the case where the signals have infinite length and amplitudes drawn from a finite field.

B. A Note on Jargon in $GF(q)$

In finite fields, since a nonzero vector $\boldsymbol{v}$ can have $\boldsymbol{v}^T\boldsymbol{v} = 0$, the vector space of all M-dimentional vectors is not an inner-product space. Hence, orthogonality is not well defined. However, for simplicity, in this paper, we will borrow the jargon from the theory of convolutional codes [15], [16]. Two vectors that satisfy $\boldsymbol{u}^T\boldsymbol{v} = 0$ are said to be *orthogonal*, and matrices that satisfy $\boldsymbol{A}^T\boldsymbol{A} = \boldsymbol{I}$ will be called *unitary* matrices. Similarly, in finite fields, we call a rational matrix that satisfies $\boldsymbol{E}^T(z^{-1})\boldsymbol{E}(z) = \boldsymbol{I}$ a PU matrix. Since we do not have an inner product space, many properties of unitary matrices in finite fields are different from those of unitary matrices in the complex field.

C. Main Results of the Paper

Our aim in this paper is to study theoretical aspects of FB's in finite fields. We will focus on the class of unitary and PU matrices. In Sections II–VII, we will consider the $GF(2)$ case, and in Section VIII, we will consider the $GF(q)$ case for any prime number $q > 2$. The following are the main results and outline of the paper:

1) In Section II, we will discuss some basic properties of unitary matrices in $GF(2)$. Even though unitary matrices in $GF(2)$ have many properties similar to those of the unitary matrices in complex field, there are some exceptions. For example, in $GF(2)$ case, the fact that $\boldsymbol{u}^T\boldsymbol{A}^T\boldsymbol{A}\boldsymbol{u} = \boldsymbol{u}^T\boldsymbol{u}$ for all vectors $\boldsymbol{u}$ does not imply the unitariness of the matrix $\boldsymbol{A}$, and none of the columns (or rows) of a unitary matrix can have all elements equal to 1. Despite all these unusual properties, we can prove that all unitary matrices can be expressed as a product of permutation matrices and Householder-like matrices.
2) PU matrices in $GF(2)$ are studied in Section III. As in the complex case, we will show that the synthesis filters of a PR PU FB are the mirror images of the analysis filters.
3) In Section IV, we will present a degree-one building block for PU matrices in $GF(2)$ and derive the conditions under which arbitrary PU matrices in $GF(2)$ can be factorized into these building blocks. A degree-one reduction algorithm will be given. Even though the building block is the most general degree-one PU system, as we will show, there are PU systems in $GF(2)$ that cannot be expressed in terms of these building blocks. In fact, in the 2×2 case, all PU matrices that are factorizable in terms of degree-one PU systems are diagonal.
4) We will establish new factorization theorems for PU matrices in Section V. The new theorems involve a building block of degree two. Using these degree-two building blocks, we are able to factorize some PU systems that are unfactorizable in terms of degree-one building blocks. However, there are PU systems that cannot be decomposed into any combination of these degree-one and degree-two building blocks.
5) In real or complex fields, the lapped orthogonal transform (LOT) has been studied in detail [3]. In Section VI, we will study the LOT in $GF(2)$. A LOT of degree ρ in $GF(2)$ can be completely characterized by a set of ρ independent vectors. Moreover, the class of LOT's in $GF(2)$ can always be factorized in terms of the degree-one and degree-two building blocks. We also find the constraints on the degree-one and degree-two building blocks, which will guarantee the LOT property structurally.
6) State-space representation of PU systems in $GF(2)$ will be considered in Section VII. We will show that the implementations based on the factorization given in previous sections are minimal in terms of delay elements. In real or complex fields, it is known [4] that a system is PU if and only if there is a unitary *realization matrix*. In $GF(2)$, we will show that a system is PU if its realization matrix is unitary. However, unlike the conventional PU systems, PU systems in finite fields may not have a unitary realization matrix. Thus, the well-known LBR lemma [4] cannot be extended to the $GF(2)$ case.
7) In the last section, the theory of PU systems in $GF(2)$ will be extended to the case of $GF(q)$ for prime $q > 2$. Even though they share many similarities, there are many differences between these two cases. In particular, the factorization theorems are very different. In $GF(q)$ with $q > 2$, all LOT's are factorizable in terms of degree-one building blocks. No degree-two building block is needed.

D. Notations and Definitions

1) *Notations:* Boldfaced lowercase and uppercase letters (such as $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{U}, \boldsymbol{V}$) represent vectors and matrices, respectively. The transpose of a matrix $\boldsymbol{A}$ is denoted as

A^T. The dimension of the matrices are $M \times M$ unless it is mentioned otherwise. The symbol I is reserved for the identity matrix, and the vector e_i is used to denote the ith column vector of the identity matrix I. The symbol J denotes the reversal matrix. For example, the 4×4 reversal matrix is

$$J_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{1.2}$$

2) *Finite Fields:* In this paper, we will consider finite fields of the form $GF(q)$ with prime q only. All the computations (addition and multiplication for scalars and matrices) are defined modulo q. The multiplicative inverse of a nonzero scalar c in $GF(q)$ is denoted by c^{-1}.
3) *Dot Product and Orthogonality:* The dot product of two vectors u and v is defined as $u^T v = \Sigma_i u_i v_i$. Note that the defined dot product is not a valid inner product because it is possible that $u^T u = 0$ even if $u \neq 0$. The scalar quantity $u^T u$ is represented by l_u. There are nonzero vectors u in finite fields with $l_u = 0$. Two vectors u and v are said to be *orthogonal* if $u^T v = 0$.
4) *Unitary Matrices:* A matrix A in $GF(q)$ is said to be unitary if $A^T A = I$.
5) *Paraunitary (PU) Matrices:* A rational matrix $E(z)$ in $GF(q)$ is called a PU matrix if $E^T(z^{-1})E(z) = I$. In this paper, we will only study polynomial PU matrices.
6) *Order versus Degree:* The order of a causal FIR transfer matrix $E(z)$ is the largest power of z^{-1} in its expression, whereas the McMillan degree (which is often just called degree) is the smallest number of delays with which we can implement the system. For example, if $E(z) = e(0) + z^{-1}e(1)$ with $e(1) \neq 0$, then its order $= 1$, whereas its degree is equal to the rank of the matrix $e(1)$ [4].
7) *Lapped Orthogonal Transforms (LOT):* In $GF(q)$, a first-order PU system, i.e., a PU system of the form $E(z) = e(0) + z^{-1}e(1)$, is said to be a LOT in $GF(q)$.

II. Unitary Matrices Over $GF(2)$

For simplicity, we assume that all the matrices in this section are $M \times M$ square matrices. The result for rectangular matrices can be obtained in a similar manner. In the first part of this section, we will study some basic properties of unitary matrices over $GF(2)$, which we are going to use throughout the paper. In the second part, we will show that all unitary matrices can be factorized by using some basic building blocks similar to the Householder transformation.

A. Basic Properties of Unitary Matrices

As defined in Section I, the matrix A over $GF(2)$ is said to be unitary if

$$A^T A = I. \tag{2.1}$$

One important property of unitary matrices that we are going to use repeatedly later is the following:

Fact 2.1: None of the column (or row) vectors of a unitary matrix in $GF(2)$ can have an even number of 1. ■

It is not difficult to see that if A_1 and A_2 are unitary, so is the product $A_1 A_2$. Post-multiplying (2.1) by A^{-1}, we obtain that $A^{-1} = A^T$. Thus, if A is unitary, its inverse is simply its own transpose. Pre-multiplying $A^{-1} = A^T$ by A, we get $AA^T = I$. Summarizing the results, we have shown that the following are equivalent:

i) A is unitary.
ii) $A^T A = I$.
iii) $AA^T = I$.
iv) $A^{-1} = A^T$.

From the above discussion, we see that unitary matrices over $GF(2)$ enjoy many properties similar to unitary matrices over the real or complex field. However, there are some differences. For example, it is well known that in real or complex field, a matrix is unitary if and only if it has the property of energy conservation [4]. This means that A is unitary if and only if $u^\dagger A^\dagger A u = u^\dagger u$ for all u. In $GF(2)$, there are nonunitary matrices that satisfy $u^T A^T A u = u^T u$ for all u. To explain this, note that

$$u^T B u = \sum_l u_l u_l b_{ll} + \sum_{i>j} u_i u_j (b_{ij} + b_{ji}). \tag{2.2}$$

For any symmetric matrix B over $GF(2)$, the above equation reduces to $u^T B u = \Sigma_l u_l b_{ll}$. Thus, any symmetric matrix with $b_{ii} = 1$ will satisfy $u^T B u = u^T u$. If A is such that all columns have odd number of nonzero elements, then $A^T A$ is symmetric with diagonal elements $= 1$. Thus, even though A is not unitary, we have $u^T A^T A u = u^T u$ for all vectors u. For unitariness of matrices in $GF(2)$, we need a stronger condition as follows:

Fact 2.2: If $u^T A^T A v = u^T v$ for all possible vectors u and v, then A is unitary. ■

Proof: Let u and v be, respectively, the unit vectors e_i and e_j defined in Section I. If $e_i^T A^T A e_j = e_i^T e_j$ for all i, j, then we have

$$\begin{bmatrix} e_0^T \\ e_1^T \\ \vdots \\ e_{M-1}^T \end{bmatrix} A^T A [e_0 \quad e_1 \quad \cdots \quad e_{M-1}] = \begin{bmatrix} e_0^T \\ e_1^T \\ \vdots \\ e_{M-1}^T \end{bmatrix} [e_0 \quad e_1 \quad \cdots \quad e_{M-1}]. \tag{2.3}$$

Since $[e_0 \quad e_1 \quad \cdots \quad e_{M-1}] = I$, it immediately follows from the above equation that $A^T A = I$. ■

Fact 2.3: If A is a unitary matrix over $GF(2)$, then none of the columns (or rows) can have all elements equal to unity.

Proof: Let $A = [a_0 \quad a_1 \quad \cdots \quad a_{M-1}]$. Suppose a_0 is a column vector with all elements equal to unity. Since $a_i^T a_0 = 0$ for $i \neq 0$, we conclude that a_i must have an even number of unit elements, which is a contradiction to Fact 2.1. ■

Combining Facts 2.1 and 2.3, we conclude that for any $M \times M$ unitary matrix with $M \leq 3$, the column has only one nonzero element. Therefore, any $M \times M$ unitary matrix

with $M \leq 3$ must be a permutation of the identity matrix. As we will see later in this section, Fact 2.3 is very useful in the factorization of unitary matrices. Before we derive the factorization theorem for unitary matrices, we would like to introduce the following building block:

Fact 2.4: In $GF(2)$, the matrix $\boldsymbol{U} = \boldsymbol{I} + \boldsymbol{u}\boldsymbol{u}^T$ with $\boldsymbol{u}^T\boldsymbol{u} = 0$ is unitary. ■

The above fact can be proven by direct computation of $\boldsymbol{U}^T\boldsymbol{U}$. Moreover, it can be verified that $\boldsymbol{U}$ is its own inverse. As we will see next, the building block in Fact 2.4 has a similar function as the Householder transformation.

B. Factorization of Unitary Matrices over $GF(2)$

In this section, we will show how to parameterize all $M \times M$ unitary matrices. In the real field, all unitary matrices can be written as a product of planar rotations. Since the planar rotations involve sines and cosines, we cannot attempt the same approach in the finite field. Instead, we will use an approach similar to the Householder factorization. In real or complex field, the Householder transformation is a matrix of the form $(\boldsymbol{I} - 2\boldsymbol{v}\boldsymbol{v}^T/\boldsymbol{v}^T\boldsymbol{v})$ [17]. In $GF(2)$, since all the computations are performed modulo 2, there is no such Householder transformation in $GF(2)$. However, we will show that we can capture all unitary matrices using the building block $\boldsymbol{U}$ introduced in Fact 2.4. As we have pointed out above, all $M \times M$ unitary matrix with $M \leq 3$ must be a permutation of the identity matrix so that only $M > 3$ is of interest in the discussion of this section. Before we derive the factorization theorem for $M > 3$, we will show two lemmas that are crucial in this context.

Lemma 2.1: Let $\boldsymbol{v}$ be a vector over $GF(2)$ such that $\boldsymbol{v}^T\boldsymbol{v} = 1$, and $v_0 = 0$. Then

$$(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)\boldsymbol{v} = \boldsymbol{e}_0, \quad \text{and} \quad \boldsymbol{v}^T(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T) = \boldsymbol{e}_0^T \tag{2.4}$$

where $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}_0$, and $\boldsymbol{e}_0 = [1 \quad 0 \quad \cdots \quad 0]^T$. ■

The above lemma can be proved by direct substitution. Note that the vector $\boldsymbol{w}$ has $\boldsymbol{w}^T\boldsymbol{w} = 0$ so that $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ is unitary (by Fact 2.4). The function of $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ is similar to the Householder matrix in the real or complex case. The matrix $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ will transform the vector $\boldsymbol{v}$ into the vector $\boldsymbol{e}_0$. It is not difficult to generalize the result of Lemma 2.1 as follows: If $\boldsymbol{v}$ is a vector such that $\boldsymbol{v}^T\boldsymbol{v} = 1$ and $v_i = 0$, then it can be shown that the matrix $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ with $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}_i$ transforms the vector $\boldsymbol{v}$ into $\boldsymbol{e}_i$. As a consequence of Lemma 2.1, we have the following:

Lemma 2.2: Let $\boldsymbol{A}$ be $M \times M$ unitary over $GF(2)$ with $A_{00} = 0$. Define the vector $\boldsymbol{w} = \boldsymbol{a}_0 + \boldsymbol{e}_0$, where $\boldsymbol{a}_0$ is the zeroth column of $\boldsymbol{A}$. Then, $\boldsymbol{w}^T\boldsymbol{w} = 0$, and

$$\boldsymbol{A} = (\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)\begin{bmatrix} 1 & 0 \\ 0 & \boldsymbol{B} \end{bmatrix} \tag{2.5}$$

where $\boldsymbol{B}$ is $(M-1) \times (M-1)$ unitary. ■

Proof: Since $\boldsymbol{A}$ is unitary with $A_{00} = 0$, the vector $\boldsymbol{a}_0$ satisfies the conditions in Lemma 2.1. Applying the result of Lemma 2.1, we have $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)\boldsymbol{a}_0 = \boldsymbol{e}_0$. Thus

$$(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)\boldsymbol{A} = [\boldsymbol{e}_0 \quad \boldsymbol{C}] \tag{2.6}$$

where $\boldsymbol{C}$ is $M \times (M-1)$. Since both $\boldsymbol{A}$ and $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ are unitary, the right-hand side of (2.6) is also unitary. Thus, the first row of $\boldsymbol{C}$ contains only zeros. Inverting $(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T)$ in (2.6), we immediately get (2.5). ■

With the above two lemmas, we are now ready to prove the main factorization for unitary matrices in $GF(2)$.

Theorem 2.1: An $M \times M$ matrix $\boldsymbol{A}$ over $GF(2)$ (with $M > 3$) is unitary if and only if it can be factorized as

$$\boldsymbol{A} = \boldsymbol{U}_M \cdots \boldsymbol{U}_4\boldsymbol{P} \tag{2.7}$$

where $\boldsymbol{U}_i = \boldsymbol{I} + \boldsymbol{u}_i\boldsymbol{u}_i^T$ with $\boldsymbol{u}_i^T\boldsymbol{u}_i = 0$, and $\boldsymbol{P}$ is a permutation of the identity matrix. ■

Proof: The "if" part is self evident. To prove the "only if" part, assume that $\boldsymbol{A}$ is unitary. If $A_{00} \neq 0$, we can apply a row permutation such that the (0, 0)th element is zero. This is always possible because of Fact 2.3. Then, the factorization in Lemma 2.2 can be applied. Repeat the permutation and factorization operations on the smaller unitary matrix $\boldsymbol{B}$. Continuing the process, we can successively generate unitary matrices of increasingly smaller size until we get a 3×3 unitary matrix, which itself is a permutation of the identity matrix. Thus, we have the following factorization:

$$\boldsymbol{A} = \boldsymbol{P}_M\boldsymbol{V}_M\boldsymbol{P}_{M-1}\cdots\boldsymbol{P}_4\boldsymbol{V}_4\boldsymbol{P}_3 \tag{2.8}$$

where $\boldsymbol{V}_i = \boldsymbol{I} + \boldsymbol{v}_i\boldsymbol{v}_i^T$ with $\boldsymbol{v}_i^T\boldsymbol{v}_i = 0$, and $\boldsymbol{P}_i$ are permutations of the identity matrix. By using the fact that $\boldsymbol{P}_i\boldsymbol{V}_i = \boldsymbol{U}_i\boldsymbol{P}_i$ for some unitary matrix of the form $\boldsymbol{U}_i = \boldsymbol{I} + \boldsymbol{u}_i\boldsymbol{u}_i^T$, we can shift all the permutations to the right and obtain (2.7). ■

Remark: In (2.5) we have extracted a left factor from $\boldsymbol{A}$. If we take the zeroth row of $\boldsymbol{A}$, $\hat{\boldsymbol{a}}_0^T$ to form the vector $\hat{\boldsymbol{w}} = \hat{\boldsymbol{a}}_0 + \boldsymbol{e}_0$, then we can rewrite (2.5) as

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 \\ 0 & \hat{\boldsymbol{B}} \end{bmatrix}(\boldsymbol{I} + \hat{\boldsymbol{w}}\hat{\boldsymbol{w}}^T).$$

In this case, we can extract a factor from the right of $\boldsymbol{A}$.

III. Paraunitary Matrices and Filter Banks Over $GF(2)$

Let $\boldsymbol{E}(z)$ be a matrix whose entries are rational with coefficients from $GF(2)$. As defined in Section I, the matrix $\boldsymbol{E}(z)$ is said to be PU if

$$\boldsymbol{E}^T(z^{-1})\boldsymbol{E}(z) = \boldsymbol{I}. \tag{3.1}$$

In this section, we will restrict our attention to the FIR case when $\boldsymbol{E}(z) = \Sigma_{k=0}^{N} \boldsymbol{e}(k)z^{-k}$. As we mentioned in the introduction, the number N is called the order of the system. In the case of real or complex field, the first-order PU matrix is called the lapped orthogonal transform (LOT) [3]. The class of LOT in $GF(2)$ can be similarly defined. We will see that this class allows a minimal factorization in terms of smaller PU building blocks. However, unlike the complex case, we need both degree-one and degree-two building blocks in the factorization of LOT in $GF(2)$.

A. Some Basic Properties of PU Matrices

Equation (3.1) gives a z-domain characterization of PU matrices. In the time domain, it can be shown that the impulse response satisfies

$$\sum_n \boldsymbol{e}^T(n)\boldsymbol{e}(n+k) = \begin{cases} \boldsymbol{I}, & k=0; \\ \boldsymbol{0}, & \text{otherwise.} \end{cases} \tag{3.2}$$

The conditions in (3.2) are very similar to those for PU matrices in real or complex field. Equation (3.2) gives one time-domain condition for PU matrices. Using the fact that (3.1) implies $\boldsymbol{E}(z)\boldsymbol{E}^T(z^{-1}) = \boldsymbol{I}$, we obtain another time-domain condition as

$$\sum_n \boldsymbol{e}(n)\boldsymbol{e}^T(n+k) = \begin{cases} \boldsymbol{I}, & k=0; \\ \boldsymbol{0}, & \text{otherwise.} \end{cases} \tag{3.3}$$

Even though some properties of the real or complex case continue to hold in the case of $GF(2)$, there are some exceptions. For example, in the real or complex field, if the system $\boldsymbol{E}(z)$ has the input–output energy preservation property, then it is PU. In general, this is not true for the $GF(2)$ case. A counterexample is given by

$$\boldsymbol{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}. \tag{3.4}$$

In this case, $\boldsymbol{u}^T\boldsymbol{A}^T\boldsymbol{A}\boldsymbol{u} = \boldsymbol{u}^T\boldsymbol{u}$ for all $\boldsymbol{u}$, but $\boldsymbol{A}^T\boldsymbol{A} \neq \boldsymbol{I}$. The precise relation between PU property and input–output mapping is given by the following result:

Lemma 3.1: Let $\boldsymbol{y}_0(n)$ and $\boldsymbol{y}_1(n)$ be, respectively, the outputs of $\boldsymbol{E}(z)$ in response to $\boldsymbol{u}_0(n)$ and $\boldsymbol{u}_1(n)$. Then, $\boldsymbol{E}(z)$ [over $GF(2)$] is paraunitary if and only if

$$\sum_n \boldsymbol{y}_0^T(n)\boldsymbol{y}_1(n) = \sum_n \boldsymbol{u}_0^T(n)\boldsymbol{u}_1(n) \tag{3.5}$$

for all possible inputs pairs $\boldsymbol{u}_0(n)$ and $\boldsymbol{u}_1(n)$. ■

Proof: The outputs can be written as $\boldsymbol{y}_i(n) = \Sigma_k \boldsymbol{e}(k)\boldsymbol{u}_i(n-k)$ for $i = 0, 1$. Substituting this into the left-hand side of (3.5) and rearranging the result, we get

$$\sum_n \boldsymbol{y}_0^T(n)\boldsymbol{y}_1(n) = \sum_{k,l} \boldsymbol{u}_0^T(l) \underbrace{\left(\sum_n \boldsymbol{e}^T(n)\boldsymbol{e}(n+k)\right)}_{\boldsymbol{A}(k)} \boldsymbol{u}_1(l-k). \tag{3.6}$$

If we choose $\boldsymbol{u}_0(n) = \boldsymbol{e}_i\delta(n)$ and $\boldsymbol{u}_1(n) = \boldsymbol{e}_j\delta(n)$, then the right-hand side of (3.6) reduces to $a_{ij}(0)$, which is the (i,j)th element of $\boldsymbol{A}(0)$. Using (3.5), we conclude that $\boldsymbol{A}(0) = \boldsymbol{I}$. Similarly, by choosing $\boldsymbol{u}_0(n) = \boldsymbol{e}_i\delta(n)$ and $\boldsymbol{u}_1(n) = \boldsymbol{e}_j\delta(n+k)$, we can prove that $\boldsymbol{A}(k) = \boldsymbol{0}$ for $k \neq 0$. ■

1) McMillan Degree and Determinant of PU Systems: In the FIR case, the PU property puts a strong constraint on the determinant of $\boldsymbol{E}(z)$. Taking the determinant of (3.1), we get $[\det \boldsymbol{E}(z)] = z^{-\rho}$ for some integer ρ. In [18], it is proved for the real and complex fields that the McMillan degree of causal systems with anticausal inverses is equal to the degree of the determinant. One can verify that the same proof carries through for systems in the finite fields. In particular, the PU system in $GF(2)$ has an anticausal inverse; therefore, the degree of the determinant is equal to McMillan degree. The McMillan degree of systems in finite fields has been investigated by researchers in coding theory [15], [16]. For a detailed study on the topic of McMillan degree, refer to [4], [15], [16], [18], and [19].

B. PU FB's in $GF(2)$

Consider Fig. 1. The analysis and synthesis filters are related to the polyphase matrices as

$$H_k(z) = \sum_{i=0}^{M-1} E_{ki}(z^M)z^{-i}, \quad F_k(z) = \sum_{i=0}^{M-1} R_{ik}(z^M)z^i \tag{3.7}$$

where $E_{ki}(z)$ and $R_{ik}(z)$ are, respectively, the (k,i)th and (i,k)th elements of $\boldsymbol{E}(z)$ and $\boldsymbol{R}(z)$. If the analysis polyphase matrix $\boldsymbol{E}(z)$ is PU, then the polyphase components of the analysis filters satisfy the relation

$$\sum_i E_{ki}(z)E_{li}(z^{-1}) = \delta(k-l) \tag{3.8}$$

which is very similar to the orthogonality condition in the case of real or complex field. Equation (3.8) can be rewritten as $[H_l(z^{-1})H_k(z)]_{\downarrow M} = \delta(k-l)$, where $X(z)|_{\downarrow M}$ denotes the z transform of $x(Mn)$. If we take the synthesis polyphase matrix as

$$\boldsymbol{R}(z) = \boldsymbol{E}^T(z^{-1}) \tag{3.9}$$

then we have a perfect reconstruction (PR) FB in $GF(2)$. Using (3.7) and (3.9), we find that the synthesis filters $F_k(z)$ are time-reversed versions of the analysis filters $H_k(z)$

$$F_k(z) = H_k(z^{-1}). \tag{3.10}$$

In the special case of two-channel FIR PU FB's, all the analysis and synthesis filters are determined by one filter. To be more specific, we have

$$\begin{aligned} H_1(z) &= z^{-N}H_0(z^{-1}), \quad F_0(z) = H_0(z^{-1}) \\ F_1(z) &= z^N H_0(z) \end{aligned} \tag{3.11}$$

where N is the order of the filter $H_0(z)$. The other filters are simply either time-reversed or delayed versions of $H_0(z)$.

IV. Degree-One PU Systems and Factorizations

In this section, we introduce the following degree-one causal FIR system over $GF(2)$

$$\boldsymbol{D}(z) = \boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z^{-1}\boldsymbol{v}\boldsymbol{v}^T, \quad \boldsymbol{v}^T\boldsymbol{v} = 1. \tag{4.1}$$

By direct computation, we can verify that $\boldsymbol{D}^T(z^{-1})\boldsymbol{D}(z) = \boldsymbol{I}$. Therefore, this is a PU system. The system in (4.1) has degree one, and Fig. 2 shows an implementation using one delay. We will study its properties and show that it can be used for the synthesis of more general PU systems.

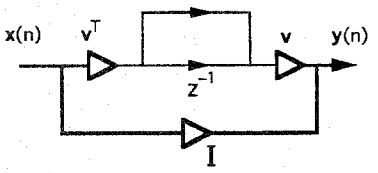


Fig. 2. Degree-one PU building block. Here, $\boldsymbol{v}^T\boldsymbol{v} = 1$.

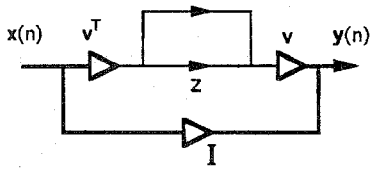


Fig. 3. Inverse of the degree-one PU system in Fig. 2.

A. Basic Properties of the Degree-one Building Block

1) The inverse system is obtained by replacing z^{-1} with z. That is

$$\boldsymbol{D}^{-1}(z) = \boldsymbol{D}(z^{-1}) = \boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z\boldsymbol{v}\boldsymbol{v}^T, \quad \boldsymbol{v}^T\boldsymbol{v} = 1. \tag{4.2}$$

Fig. 3 shows an implementation of the inverse $\boldsymbol{D}^{-1}(z)$.

2) A cascade of k such systems gives $\Pi_{k \text{ times}}\boldsymbol{D}(z) = \boldsymbol{D}(z^k)$.

3) Let $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{s-1}\}$ be a set of vectors in $GF(2)$ such that $\boldsymbol{v}_i^T\boldsymbol{v}_j = \delta(i-j)$. Then, the cascade

$$\prod_{i=0}^{s-1}[\boldsymbol{I}+\boldsymbol{v}_i\boldsymbol{v}_i^T+z^{-1}\boldsymbol{v}_i\boldsymbol{v}_i^T] = \boldsymbol{I}+\sum_{i=0}^{s-1}\boldsymbol{v}_i\boldsymbol{v}_i^T+z^{-1}\sum_{i=0}^{s-1}\boldsymbol{v}_i\boldsymbol{v}_i^T. \tag{4.3}$$

It is clear from the right-hand side of (4.3) that if we interchange any $\boldsymbol{v}_i$ with any $\boldsymbol{v}_j$, the system remains the same. Hence, the factors $(\boldsymbol{I}+\boldsymbol{v}_i\boldsymbol{v}_i^T+z^{-1}\boldsymbol{v}_i\boldsymbol{v}_i^T)$ commute. Moreover, it can be shown that a cascade of PU building blocks $\boldsymbol{D}_i(z)$ with vectors $\boldsymbol{v}_i$ will have order-one if and only if the vectors satisfy $\boldsymbol{v}_i^T\boldsymbol{v}_j = \delta(i-j)$. If we let $\boldsymbol{V} = [\boldsymbol{v}_0 \cdots \boldsymbol{v}_{s-1}]$, then the system in (4.3) can be rewritten as $\boldsymbol{I} + \boldsymbol{V}\boldsymbol{V}^T + z^{-1}\boldsymbol{V}\boldsymbol{V}^T$.

Lemma 4.1—Most General Degree-One PU System: The most general $M \times M$ causal FIR degree-one PU system over $GF(2)$ can be written as

$$\boldsymbol{E}(z) = (\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z^{-1}\boldsymbol{v}\boldsymbol{v}^T)\boldsymbol{E}(1) \tag{4.4}$$

where $\boldsymbol{v}$ is a column vector with $\boldsymbol{v}^T\boldsymbol{v} = 1$, and $\boldsymbol{E}(1)$ is a $M \times M$ unitary matrix. ■

The proof of Lemma 4.1 is very similar to the case of real or complex field [4]. Note that the PU system $\boldsymbol{E}(z)$ in (4.4) can be rewritten as $\boldsymbol{E}(z) = \boldsymbol{E}(1)(\boldsymbol{I} + \boldsymbol{u}\boldsymbol{u}^T + z^{-1}\boldsymbol{u}\boldsymbol{u}^T)$ with $\boldsymbol{u} = \boldsymbol{E}^T(1)\boldsymbol{v}$ (hence, $\boldsymbol{u}^T\boldsymbol{u} = \boldsymbol{v}^T\boldsymbol{v} = 1$).

B. Degree-One Reduction Using $D(z)$

To show how we can extract $\boldsymbol{D}(z)$ from a PU system, we consider the general $M \times M$ PU system of the form $\boldsymbol{E}(z) = \Sigma_{k=0}^{N}\boldsymbol{e}(k)z^{-k}$ with degree ρ. To avoid trivial cases, let $\boldsymbol{e}(0) \neq \boldsymbol{0}$, and $\boldsymbol{e}(N) \neq \boldsymbol{0}$. Therefore, the system $\boldsymbol{E}(z)$ has order N. From the PU conditions in (3.2), we get $\boldsymbol{e}^T(0)\boldsymbol{e}(N) = \boldsymbol{0}$, which implies that both the matrices $\boldsymbol{e}(0)$ and $\boldsymbol{e}(N)$ are singular. Let $\boldsymbol{v}$ be a vector in the null space of $\boldsymbol{e}(0)$ such that $\boldsymbol{v}^T\boldsymbol{v} = 1$. Form the new system

$$\boldsymbol{E}'(z) = \boldsymbol{E}(z)(\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z\boldsymbol{v}\boldsymbol{v}^T). \tag{4.5}$$

We say that the degree-one reduction is *successful* if the new system $\boldsymbol{E}'(z)$ satisfies the following three conditions:

i) It is causal.
ii) It is PU.
iii) It has degree $\rho - 1$, where ρ is the degree of $\boldsymbol{E}(z)$.

The new system $\boldsymbol{E}'(z)$ in (4.5) is causal because $\boldsymbol{e}(0)\boldsymbol{v} = 0$. Since both $\boldsymbol{E}(z)$ and $(\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z\boldsymbol{v}\boldsymbol{v}^T)$ are PU, so is $\boldsymbol{E}'(z)$. Taking the determinant of (4.5), we see that the degree of $\boldsymbol{E}'(z)$ is $\rho' = [\det \boldsymbol{E}'(z)] = \rho - 1$. Hence, $\boldsymbol{E}'(z)$ satisfies the three conditions mentioned above. We have sucessfully extracted a degree-one building block from $\boldsymbol{E}(z)$. Inverting $(\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z\boldsymbol{v}\boldsymbol{v}^T)$, we conclude that $\boldsymbol{E}(z)$ can be written as $\boldsymbol{E}(z) = \boldsymbol{E}'(z)(\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z^{-1}\boldsymbol{v}\boldsymbol{v}^T)$. If we can successfully repeat the above degree reduction process ρ times, then $\boldsymbol{E}(z)$ can be written as

$$\begin{aligned}\boldsymbol{E}(z) = \boldsymbol{E}(1)&(\boldsymbol{I} + \boldsymbol{v}_{\rho-1}\boldsymbol{v}_{\rho-1}^T + z^{-1}\boldsymbol{v}_{\rho-1}\boldsymbol{v}_{\rho-1}^T)\cdots \\ &(\boldsymbol{I} + \boldsymbol{v}_0\boldsymbol{v}_0^T + z^{-1}\boldsymbol{v}_0\boldsymbol{v}_0^T)\end{aligned} \tag{4.6}$$

where $\boldsymbol{v}_i^T\boldsymbol{v}_i = 1$, and $\boldsymbol{E}(1)$ is a constant unitary matrix. Similarly, one can show that if the null space of $\boldsymbol{e}^T(0)$ contains a vector $\boldsymbol{u}$ with $\boldsymbol{u}^T\boldsymbol{u} = 1$, then we can write $\boldsymbol{E}(z)$ as $(\boldsymbol{I}+\boldsymbol{u}\boldsymbol{u}^T+z^{-1}\boldsymbol{u}\boldsymbol{u}^T)\boldsymbol{E}'(z)$ for some causal PU system $\boldsymbol{E}'(z)$. If $\boldsymbol{E}(z)$ is completely factorizable into ρ terms, using this degree reduction process from the left, we can write $\boldsymbol{E}(z)$ as

$$\begin{aligned}\boldsymbol{E}(z) = (\boldsymbol{I} + \boldsymbol{u}_0\boldsymbol{u}_0^T + z^{-1}\boldsymbol{u}_0\boldsymbol{u}_0^T)\cdots(\boldsymbol{I} + \boldsymbol{u}_{\rho-1}\boldsymbol{u}_{\rho-1}^T \\ + z^{-1}\boldsymbol{u}_{\rho-1}\boldsymbol{u}_{\rho-1}^T)\boldsymbol{E}(1).\end{aligned} \tag{4.7}$$

1) The Equivalence of (4.6) and (4.7): If $\boldsymbol{E}(z)$ can be written as the factorized form in (4.6), then it can also be expressed as (4.7). To prove this, we consider (4.6). Starting from the left, we can move the constant matrix $\boldsymbol{E}(1)$ to the right by letting $\boldsymbol{u}_i = \boldsymbol{E}(1)\boldsymbol{v}_i$.

In the real or complex field, it is well known that all FIR causal PU matrices of degree ρ can always be factorized into a product of ρ degree-one PU systems of the form $\boldsymbol{D}(z)$. A similar property is not true in $GF(2)$. To see this, consider the following example:

Example 4.1—A PU System that Is Unfactorizable in Terms of $D(z)$: Let $\boldsymbol{G}(z)$ be the following $M \times M$ system with M odd:

$$\boldsymbol{G}(z) = \boldsymbol{w}\boldsymbol{w}^T + z^{-1}(\boldsymbol{I} + \boldsymbol{w}\boldsymbol{w}^T) \tag{4.8}$$

where $\boldsymbol{w} = [1 \quad 1 \quad \cdots \quad 1]^T$ so that $\boldsymbol{w}^T\boldsymbol{w} = 1$. It can be verified that $\boldsymbol{G}^T(z^{-1})\boldsymbol{G}(z) = \boldsymbol{I}$. Therefore, $\boldsymbol{G}(z)$ is PU. Let $\{\boldsymbol{u}_0, \cdots, \boldsymbol{u}_{M-2}\}$ be a set of independent vectors such that $\boldsymbol{w}^T\boldsymbol{u}_k = 0$. Then, we get $\boldsymbol{g}(1)\boldsymbol{w} = \boldsymbol{0}$ and $\boldsymbol{g}(1)\boldsymbol{u}_k = \boldsymbol{u}_k$ for $0 \leq k \leq M-2$. Therefore, $\boldsymbol{g}(1)$ has rank $M-1$, and the degree of $\boldsymbol{G}(z)$ is $M-1$. Suppose that degree reduction from the left is possible. This means that $\boldsymbol{G}(z) = (\boldsymbol{I}+\boldsymbol{v}\boldsymbol{v}^T+z^{-1}\boldsymbol{v}\boldsymbol{v}^T)\boldsymbol{G}'(z)$, where $\boldsymbol{v}^T\boldsymbol{v} = 1$, and $\boldsymbol{G}'(z)$ is a causal FIR PU system of degree $\rho' = M - 2$. Inverting the degree-one system, we have

$$\boldsymbol{G}'(z) = (\boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T + z\boldsymbol{v}\boldsymbol{v}^T)\boldsymbol{G}(z). \tag{4.9}$$

Therefore, $G'(z)$ is causal only if $v^T w = 0$, which implies that v has an even number of ones, violating the requirement of $v^T v = 1$. Thus, degree reduction from the left is impossible. Similarly, we can show that degree reduction from the right is also impossible. Therefore, we conclude that the system $G(z)$ in (4.8) cannot be factorized in terms of degree-one PU system $D(z)$. From the above discussion, it is clear that the degree reduction fails because neither the null space of $e(0)$ nor $e^T(0)$ contains a vector with an odd number of ones. In the complex field, this can never happen because nonzero vectors always have nonzero norm. ■

Lemma 4.2: Let $E(z) = \sum_{k=0}^{N} e(k) z^{-k}$ be a causal PU system. The degree-one reduction for $E(z)$ fails if and only if the null spaces of $e(0)$ and $e^T(0)$ contain only vectors with an *even* number of ones. ■

The above lemma can be proved in a straightforward manner. Note that it is not necessary to exhaust the whole null space for the test. We need only to look at any basis that spans the null space. If none of the vectors in this basis has an odd weight, then any linear combination of vectors in the null space has an even weight because in $GF(2)$

$$\left(\sum_i v_i\right)^T \left(\sum_i v_i\right) = \sum_i v_i^T v_i. \tag{4.10}$$

V. Degree-Two PU Building Blocks and Factorizations

As we have seen in Example 4.1, there are PU systems that cannot be factorized by using the degree-one building blocks. In this section, we will include a degree-two building block in the factorization so that some PU systems that cannot be factorized before can now be factorized. To establish new factorization theorems for PU systems, we introduce the following degree-one system:

$$G(z) = I + uv^T + z^{-1}uv^T \tag{5.1}$$

where u and v are nonzero vectors over $GF(2)$. The above system is not PU unless $u = v$, and $v^T v = 1$. To see this, suppose $G^T(z^{-1})G(z) = I$. Computing the coefficient of z^{-1}, we get $u^T(I + uv^T) = 0$, which implies that $u^T = v^T$ and that $u^T u = 1$. The non-PU system $G(z)$ is useful because it can generate degree-two PU building blocks for the new factorization theorem.

Lemma 5.1: The system $G(z)$ over $GF(2)$ in (5.1) *always* has a FIR inverse. Its inverse is

$$G^{-1}(z) = \begin{cases} G(z^{-1}), & \text{if } v^T u = 1; \\ G(z), & \text{if } v^T u = 0. \end{cases} \tag{5.2}$$

■

The above lemma can be proved by direct substitution. It shows that in $GF(2)$, we can have a nontrivial system that is its own inverse, i.e., $G(z)G(z) = I$.

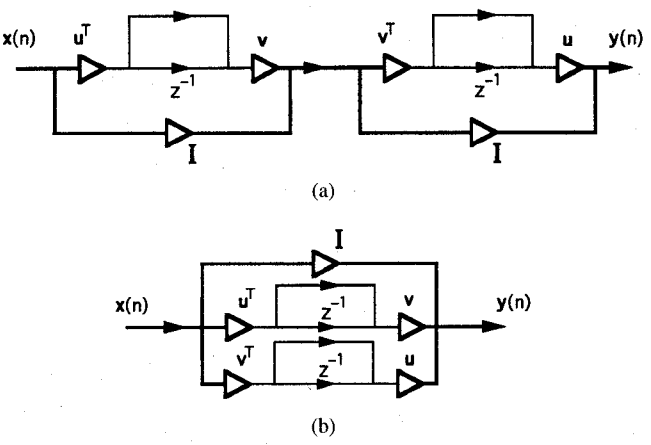


Fig. 4. (a) Cascade implementation of the degree-two PU system $K(z)$. (b) Parallel implementation of the degree-two PU system $K(z)$. Here, $u^T u = v^T v = 0$, and $v^T u = 1$.

A. Degree-Two PU Building Blocks

One useful special case of the system $G(z)$ in (5.1) is when the vectors u and v satisfy

$$[u \quad v]^T [u \quad v] = J_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5.3}$$

In this case, if we form the following cascade system:

$$\begin{aligned} K(z) &= (I + uv^T + z^{-1}uv^T)(I + vu^T + z^{-1}vu^T) \\ &= \underbrace{I + uv^T + vu^T}_{k(0)} + z^{-1}\underbrace{(uv^T + vu^T)}_{k(1)} \end{aligned} \tag{5.4}$$

then it can be verified that $K^T(z^{-1})K(z) = I$. Therefore, $K(z)$ is PU even though each individual factor is not PU. From the second equality of (5.4), it is clear that $K(z)$ remains the same if we interchange the vectors u and v. Therefore, we can also write $K(z)$ as $(I + vu^T + z^{-1}vu^T)(I + uv^T + z^{-1}uv^T)$. Using (5.4), we have the cascade and parallel implementations of $K(z)$ as shown in Fig. 4(a) and (b), respectively.

B. Basic Properties of $K(z)$

1) It is symmetric, i.e., $K^T(z) = K(z)$. The inverse system is given by $K^{-1}(z) = K(z^{-1})$.
2) Note that $k(1)u = u$ and $k(1)v = v$; therefore, the range of $k(1)$ has rank = 2, which implies the system $K(z)$ has degree two. Hence, we have $[\det K(z)] = z^{-2}$.
3) $K(z)$ cannot be factorized into building blocks of the form $D(z)$ in (4.1). This can be seen by investigating the null space of the zeroth coefficient $k(0) = I + uv^T + vu^T$. If w is a vector in the null space of $k(0)$, then it must satisfy $w = (v^T w)u + (u^T w)v$. This implies that w has an even weight since it is a linear combination of two even weight vectors [see (4.10)]. Using Lemma 4.2, we can conclude that $K(z)$ cannot be written in terms of degree-one PU system $D(z)$.
4) Let $K_i(z) = [I + u_i v_i^T + v_i u_i^T + z^{-1}(u_i v_i^T + v_i u_i^T)]$ for $0 \le i \le s-1$ be degree-two PU systems. Then, it can be verified that the product $K(z) = K_0(z) \cdots K_{s-1}(z)$ remains order-one if and only if the vectors u_i and v_i are

such that the matrix $\boldsymbol{W} = [\boldsymbol{u}_0\boldsymbol{v}_0 \cdots \boldsymbol{u}_{s-1}\boldsymbol{v}_{s-1}]$ satisfies

$$\boldsymbol{W}^T\boldsymbol{W} = \mathcal{J}_{2s} = \begin{bmatrix} \boldsymbol{J}_2 & & & \\ & \boldsymbol{J}_2 & & \boldsymbol{0} \\ & & \boldsymbol{J}_2 & \\ & \boldsymbol{0} & & \ddots \\ & & & \boldsymbol{J}_2 \end{bmatrix} \tag{5.5}$$

where

$$\boldsymbol{J}_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Furthermore, if (5.5) is true, then the factors $\boldsymbol{K}_i(z)$ commute so that we can write the product as

$$\prod_{i=0}^{s-1} \boldsymbol{K}_i(z) = \boldsymbol{I} + \sum_{i=0}^{s-1} (\boldsymbol{u}_i\boldsymbol{v}_i^T + \boldsymbol{v}_i\boldsymbol{u}_i^T) + z^{-1}$$

$$\sum_{i=0}^{s-1} (\boldsymbol{u}_i\boldsymbol{v}_i^T + \boldsymbol{v}_i\boldsymbol{u}_i^T) = \boldsymbol{I} + \boldsymbol{W}\mathcal{J}_{2s}\boldsymbol{W}^T + z^{-1}\boldsymbol{W}\mathcal{J}_{2s}\boldsymbol{W}^T \tag{5.6}$$

where the $2s \times 2s$ matrix $\mathcal{J}_{2s}$ is as defined in (5.5).

C. Degree-Two Reduction Using $\boldsymbol{K}(z)$

In Section IV-B, we have given a procedure for the extraction of degree-one building block $\boldsymbol{D}(z)$. Suppose that we have factored out all the extractable degree-one building blocks of the form $\boldsymbol{D}(z)$, and $\boldsymbol{E}(z)$ is the remaining system that is unfactorizable in terms of $\boldsymbol{D}(z)$. Hence, the null spaces of $\boldsymbol{e}(0)$ and $\boldsymbol{e}^T(0)$ do not contain any vector with an odd weight. Next, we will provide an algorithm to extract the degree-two PU building block $\boldsymbol{K}(z)$ whenever it is possible.

Let $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_{s-1}\}$ be a set of independent vectors that span the null space of $\boldsymbol{e}(0)$. Since there is no degree-one building block, we have $\boldsymbol{v}_i^T\boldsymbol{v}_i = 0$ for all i. Suppose there is a pair of vectors $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ such that $\boldsymbol{v}_i^T\boldsymbol{v}_j = 1$. Then, the following system

$$\boldsymbol{E}'(z) = \boldsymbol{E}(z)(\boldsymbol{I} + \boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T + z(\boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T)) \tag{5.7}$$

is a causal PU system with degree $\rho' = \rho - 2$, where ρ is the degree of the original system $\boldsymbol{E}(z)$. The causality of $\boldsymbol{E}'(z)$ follows from the fact that both $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ are in the null space of $\boldsymbol{e}(0)$. Since the vectors $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ satisfy the condition (5.3), the anticausal system $(\boldsymbol{I} + \boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T + z(\boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T))$ is the inverse of a degree-two PU system $\boldsymbol{K}(z)$. Therefore, $\boldsymbol{E}'(z)$ is PU. Taking the determinant of (5.7), we get $[\det \boldsymbol{E}'(z)] = z^2 \cdot [\det \boldsymbol{E}(z)] = z^{-(\rho-2)}$. Since $\boldsymbol{E}'(z)$ is PU, its degree is equal to $\rho - 2$ (see Section III-A). After rearranging (5.7), we get

$$\boldsymbol{E}(z) = \boldsymbol{E}'(z)(\boldsymbol{I} + \boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T + z^{-1}(\boldsymbol{v}_i\boldsymbol{v}_j^T + \boldsymbol{v}_j\boldsymbol{v}_i^T)). \tag{5.8}$$

We have sucessfully extracted a degree-two PU building block from the right of $\boldsymbol{E}(z)$. Note that it is possible that we can extract the degree-one PU building block $\boldsymbol{D}(z)$ from the right-hand side of the reduced PU system $\boldsymbol{E}'(z)$ (degree-one reduction from the left of $\boldsymbol{E}'(z)$ is impossible because degree-one reduction from the left of $\boldsymbol{E}(z)$ fails). Therefore, after every degree-two reduction from the right, we must test if there is any degree-one building block. Similarly, if we can find a pair of vectors in the null space of $\boldsymbol{e}^T(0)$ that satisfies (5.3), then we can extract a degree-two factor $\boldsymbol{K}(z)$ from the left of $\boldsymbol{E}(z)$.

Example 5.1—A PU System that Is Factorizable in Terms of $\boldsymbol{K}(z)$ but Not in Terms of $\boldsymbol{D}(z)$: Consider the PU system $\boldsymbol{G}(z)$ in (4.8) in Example 4.1. Let $M = 5$ so that $\boldsymbol{G}(z)$ can be written as:

$$\boldsymbol{G}(z) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} + z^{-1} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}. \tag{5.9}$$

The PU system $\boldsymbol{G}(z)$ has degree equal to 4 as the rank of $\boldsymbol{g}(1) = 4$. Since the null space of $\boldsymbol{g}(0)$ consists of vectors with even weight only, degree-one reduction fails (by Lemma 4.2). However, one can verify that $\boldsymbol{G}(z)$ can be written as a product of two degree-two PU factors $\boldsymbol{K}(z)$. One of such representations is given as

$$\boldsymbol{G}(z) = [\boldsymbol{I} + \boldsymbol{u}_0\boldsymbol{v}_0^T + \boldsymbol{v}_0\boldsymbol{u}_0^T + z^{-1}(\boldsymbol{u}_0\boldsymbol{v}_0^T + \boldsymbol{v}_0\boldsymbol{u}_0^T)] \cdot [\boldsymbol{I} + \boldsymbol{u}_1\boldsymbol{v}_1^T + \boldsymbol{v}_1\boldsymbol{u}_1^T + z^{-1}(\boldsymbol{u}_1\boldsymbol{v}_1^T + \boldsymbol{v}_1\boldsymbol{u}_1^T)] \tag{5.10}$$

where the vectors are

$$\boldsymbol{u}_0 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \boldsymbol{v}_0 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad \boldsymbol{u}_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \quad \boldsymbol{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \tag{5.11}$$

Note that the vectors $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ in (5.11) satisfy (5.3). Moreover, one can show that the ordering of $\boldsymbol{K}(z)$ in (5.10) is irrelevant because the two factors commute (see Property 4 of Section V-A). Later, we will see that in general, it is true that all the factors (degree-one or degree-two) commute for the class of LOT's over $GF(2)$. ■

D. Noncompleteness of $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$

As we have seen in Example 5.1, PU systems that cannot be factorized in terms of $\boldsymbol{D}(z)$ can sometimes be expressed as a product of $\boldsymbol{K}(z)$. It is natural to ask if all PU systems can be represented as a product of $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$. The answer is *no* in general. However, we will see in the next section that the class of LOT over $GF(2)$ can always be factorized in terms of $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$.

E. Most General Unfactorizable Degree-Two 2×2 PU Systems

It is shown in Appendix A that the most general 2×2 PU system over $GF(2)$ that cannot be factored in terms of the degree-one building block $\boldsymbol{D}(z)$ has the following form:

$$\boldsymbol{G}(z) = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + z^{-1}\boldsymbol{g}(1) + z^{-2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{5.12}$$

where $\boldsymbol{g}(1) = \boldsymbol{G}(1)$, which equals to either the identity matrix $\boldsymbol{I}_2$ or the reversal matrix $\boldsymbol{J}_2$. It can be verified that the

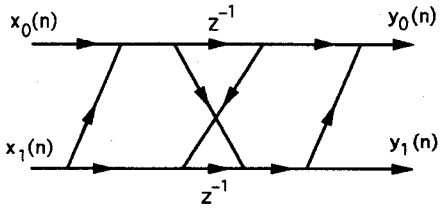


Fig. 5. Unfactorizable degree-two PU system in $GF(2)$.

coefficients $\boldsymbol{g}(k)$ satisfy (3.2) so that $\boldsymbol{G}(z)$ is PU. The system $\boldsymbol{G}(z)$ has degree two because $[\det \boldsymbol{G}(z)] = z^{-2}$. Fig. 5 shows a minimal realization of $\boldsymbol{G}(z)$ when $\boldsymbol{g}(1) = \boldsymbol{I}_2$. Using Lemma 4.2, we know that $\boldsymbol{G}(z)$ cannot be factorized in terms of $\boldsymbol{D}(z)$ because the null spaces of $\boldsymbol{g}(0)$ and $\boldsymbol{g}^T(0)$ contain only one vector, namely, $\begin{bmatrix}1\\1\end{bmatrix}$, which has an even weight. Moreover, the system $\boldsymbol{G}(z)$ cannot be re-expressed in the form $\boldsymbol{K}(z)$. If it could, there would exist two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in the null space of $\boldsymbol{g}(0)$ or $\boldsymbol{g}^T(0)$ such that $\boldsymbol{u}^T\boldsymbol{v} = 1$ (which is impossible as the null spaces contain only $\begin{bmatrix}1\\1\end{bmatrix}$). Therefore, we conclude that $\boldsymbol{G}(z)$ is a PU system that cannot be written as a product of $\boldsymbol{D}(z)$ or $\boldsymbol{K}(z)$.

1) A Degree-Four Unfactorizable PU System: Consider the following 2×2 PU system:

$$\boldsymbol{G}'(z) = \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + z^{-2}\boldsymbol{I} + z^{-4}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}. \tag{5.13}$$

The system $\boldsymbol{G}'(z)$ has degree 4. Both the degree-one reduction by $\boldsymbol{D}(z)$ and the degree-two reduction by $\boldsymbol{K}(z)$ are impossible because the null spaces of $\boldsymbol{g}(0)$ and $\boldsymbol{g}^T(0)$ contain only the vector $[1 \quad 1]^T$, which has an even weight. Moreover, $\boldsymbol{G}'(z)$ cannot be written as a product of the system $\boldsymbol{G}(z)$ in (5.12), even though $\boldsymbol{G}(z)$ is the most general unfactorizable 2×2 PU system. To see this, assume that $\boldsymbol{G}'(z) = \boldsymbol{G}_1(z)\boldsymbol{G}_2(z)$, where $\boldsymbol{G}_i(z)$ are of the form as in (5.12). Comparing the zeroth coefficient, we have

$$\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} = \boldsymbol{0} \tag{5.14}$$

which is a contradiction. Therefore, $\boldsymbol{G}'(z)$ cannot be expressed in terms of $\boldsymbol{D}(z), \boldsymbol{K}(z)$ and $\boldsymbol{G}(z)$.

From the examples given in (5.12) and (5.13), we know that the PU building blocks $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$ are *not complete*. For a general PU system $\boldsymbol{E}(z)$, we have the following test for unfactorizability:

Lemma 5.2: Let $\boldsymbol{E}(z) = \sum_{k=0}^{N} \boldsymbol{e}(k)z^{-k}$ be a causal PU system. Let $\{\boldsymbol{v}_0, \cdots, \boldsymbol{v}_{s-1}\}$ be *any* basis that spans the null space of $\boldsymbol{e}(0)$ and $\{\boldsymbol{u}_0, \cdots, \boldsymbol{u}_{s-1}\}$ be *any* basis that spans the null space of $\boldsymbol{e}^T(0)$. Then, both the degree-one and degree-two reductions fail if and only if $\boldsymbol{v}_i^T\boldsymbol{v}_j = 0$ and $\boldsymbol{u}_i^T\boldsymbol{u}_j = 0$ for all i, j. ■

Note that the number of independent vectors $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ are the same because the null spaces of $\boldsymbol{e}(0)$ and $\boldsymbol{e}^T(0)$ have the same dimension. In addition, note that if there is a basis for the null space of $\boldsymbol{e}(0)$ that satisfies the condition in the above lemma, so are all the other bases because of (4.10). Therefore, it is sufficient to check one basis. Letting the matrices $\boldsymbol{V} = [\boldsymbol{v}_0, \cdots, \boldsymbol{v}_{s-1}]$ and $\boldsymbol{U} = [\boldsymbol{u}_0, \cdots, \boldsymbol{u}_{s-1}]$, then the condition in Lemma 5.2 can be restated as $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{0}$.

VI. Lapped Orthogonal Transforms Over $GF(2)$

In this section, we consider the following $M \times M$ first-order system over $GF(2)$

$$\boldsymbol{E}(z) = \boldsymbol{e}(0) + \boldsymbol{e}(1)z^{-1}. \tag{6.1}$$

The rank ρ of the matrix $\boldsymbol{e}(1)$ is the degree of the system, and $\rho \leq M$. If $\boldsymbol{E}(z)$ is a PU system, then we call the system $\boldsymbol{E}(z)$ a lapped orthogonal transform (LOT) over $GF(2)$. The coefficients of the LOT in (6.1) should satisfy the PU condition in (3.2), which we restate as follows:

$$\boldsymbol{e}^T(0)\boldsymbol{e}(1) = \boldsymbol{0} \tag{6.2a}$$

$$\boldsymbol{e}^T(0)\boldsymbol{e}(0) + \boldsymbol{e}^T(1)\boldsymbol{e}(1) = \boldsymbol{I}. \tag{6.2b}$$

In the following, we will first give a minimal parameterization of LOT's over $GF(2)$ and then show the factorization theorem.

A. Minimal Characterization of LOT

In the case of real or complex field, it is well-known [3], [4] that all LOT's of degree ρ can be parameterized by a set of ρ orthonormal vectors and a unitary matrix. We can capture all LOT's by varying the ρ orthonormal vectors and the unitary matrix. There is an implementation associated with this minimal parameterization that will structurally guarantee the LOT properties [4], [3]. In this section, we will derive a similar result for the $GF(2)$ case.

Theorem 6.1: In $GF(2)$, the $M \times M$ system $\boldsymbol{E}(z) = \boldsymbol{e}(0) + \boldsymbol{e}(1)z^{-1}$ is a LOT with degree ρ if and only if there is a $M \times \rho$ matrix $\boldsymbol{U}_\rho = [\boldsymbol{u}_0 \quad \boldsymbol{u}_1 \quad \cdots \quad \boldsymbol{u}_{\rho-1}]$ such that $\boldsymbol{U}_\rho^T\boldsymbol{U}_\rho$ is invertible, and

$$\boldsymbol{E}(z) = \boldsymbol{E}(1)[\boldsymbol{I} + \boldsymbol{U}_\rho\boldsymbol{L}^{-1}\boldsymbol{U}_\rho^T + z^{-1}\boldsymbol{U}_\rho\boldsymbol{L}^{-1}\boldsymbol{U}_\rho^T] \tag{6.3}$$

where $\boldsymbol{L} = \boldsymbol{U}_\rho^T\boldsymbol{U}_\rho$, and $\boldsymbol{E}(1)$ is unitary. ■

Proof: The "if" part can be proved by directly substituting the expression in (6.3) into the product $\boldsymbol{E}^T(z^{-1})\boldsymbol{E}(z)$. One can verify that $\boldsymbol{E}^T(z^{-1})\boldsymbol{E}(z) = \boldsymbol{I}$. To show the "only if" part, assume $\boldsymbol{E}(z)$ is LOT with degree ρ. As $\boldsymbol{E}(z)$ is PU, it can always be rewritten as

$$\boldsymbol{E}(z) = \boldsymbol{E}(1)[\boldsymbol{I} + \boldsymbol{W} + z^{-1}\boldsymbol{W}] \tag{6.4}$$

where $\boldsymbol{E}(1)$ is unitary, and $\boldsymbol{I} + \boldsymbol{W} + z^{-1}\boldsymbol{W}$ is PU. Since $\boldsymbol{E}(z)$ has degree ρ, the matrix $\boldsymbol{e}(1) = \boldsymbol{E}(1)\boldsymbol{W}$ has rank ρ. Thus, there are independent vectors $\boldsymbol{u}_i$ and independent vectors $\boldsymbol{v}_i$ for $i = 0, 1, \cdots, \rho - 1$ such that

$$\boldsymbol{W} = [\boldsymbol{u}_0 \quad \boldsymbol{u}_1 \quad \cdots \quad \boldsymbol{u}_{\rho-1}][\boldsymbol{v}_0 \quad \boldsymbol{v}_1 \quad \cdots \quad \boldsymbol{v}_{\rho-1}]^T.$$

Letting

$$\boldsymbol{U}_\rho = [\boldsymbol{u}_0 \quad \boldsymbol{u}_1 \quad \cdots \quad \boldsymbol{u}_{\rho-1}] \quad \text{and}$$
$$\boldsymbol{V}_\rho = [\boldsymbol{v}_0 \quad \boldsymbol{v}_1 \quad \cdots \quad \boldsymbol{v}_{\rho-1}]$$

we can rewrite (6.4) as

$$\boldsymbol{E}(z) = \boldsymbol{E}(1)[\boldsymbol{I} + \boldsymbol{U}_\rho\boldsymbol{V}_\rho^T + z^{-1}\boldsymbol{U}_\rho\boldsymbol{V}_\rho^T]. \tag{6.5}$$

Substituting the coefficients into (6.2a) and simplifying the result, we get

$$(\boldsymbol{I} + \boldsymbol{V}_\rho\boldsymbol{U}_\rho^T)\boldsymbol{U}_\rho\boldsymbol{V}_\rho^T = \boldsymbol{0}. \tag{6.6}$$

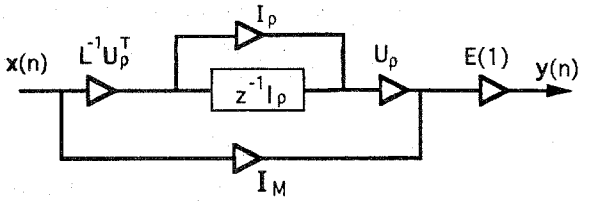


Fig. 6. Minimal characterization of a LOT with degree ρ. Here, $E(1)$ is a unitary matrix, and $L = U_\rho^T U_\rho$.

As the vectors v_i are independent, we can conclude from (6.6) that

$$U_\rho = V_\rho U_\rho^T U_\rho. \tag{6.7}$$

The above equation has two implications: i) The vector u_i is a linear combination of v_i, and ii) the $\rho \times \rho$ matrix $U_\rho^T U_\rho$ is invertible as both U_ρ and V_ρ have rank equal to ρ. Hence, we can write $V_\rho = U_\rho L^{-1}$, where $L = U_\rho^T U_\rho$. Substituting $V_\rho = U_\rho L^{-1}$ into (6.5), we immediately get (6.3). ■

Note that in the proof of the "only if" part, we have not used the second PU condition of (6.2b). One can verify that the choice of $V = UL^{-1}$ will automatically satisfy (6.2b). From Theorem 6.1, we have the implementation of LOT as in Fig. 6. Note that the matrix L in Theorem 6.1 functions like a "normalization" matrix. In the special case of $L = I_\rho$, we can write $E(z)$ as

$$E(z) = E(1)[I + UU^T + z^{-1}UU^T] \tag{6.8}$$

where the matrix $U^T U = I_\rho$. Using Property 3 of $D(z)$ in Section IV-A, we conclude that in the special case of $L = I$, the LOT in (6.3) can be written as a product of $D(z)$

$$E(z) = E(1)\prod_{i=0}^{\rho-1}[I + u_i u_i^T + z^{-1}u_i u_i^T]. \tag{6.9}$$

Remarks:

1) In Theorem 6.1, the vectors u_i cannot be arbitrary independent vectors. They should be chosen such that the matrix $U_\rho^T U_\rho$ is invertible. The subtlety is that in finite fields, the independence of u_i does not always guarantee the invertibility of $U_\rho^T U_\rho$. Unlike the real or complex field, the matrices U_ρ and $U_\rho^T U_\rho$ may not have the same rank in finite fields. One such counter example is the matrix
$$U_2^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$
in $GF(2)$.
2) In the real or complex field, the matrix L in (6.3) can always be decomposed as $Q^T Q$ for some positive definite $\rho \times \rho$ matrix Q. This is the same as saying that the vectors u_i can always be orthonormalized in the cases of real or complex field.

B. Complete Factorization of LOT

Consider the first-order system $E(z)$ in (6.1). Assume that $E(z)$ is a LOT with degree ρ so that the conditions in (6.2) are met. To avoid trivial cases, we assume $1 \le \rho \le M-1$. From (6.2a), we know that the column vectors in the matrix $e(1)$ is in the null space of $e^T(0)$. Suppose that we cannot extract either a degree-one or a degree-two building block from $E(z)$. By Lemma 5.2, it is necessary that $e^T(1)e(1) = 0$, which implies $e^T(0)e(0) = I$ from (6.2b). Hence, $e(0)$ is unitary and invertible. Inverting $e^T(0)$ of (6.2a), we have $e(1) = 0$, which implies that $E(z)$ is a constant unitary matrix. Therefore, we conclude that $e^T(1)e(1) \neq 0$ if $\rho > 0$. Using Lemma 5.2, we know that we can always extract either the factor $D(z)$ or the factor $K(z)$ from $E(z)$ if its degree $\rho > 0$. After the degree reduction, we will have a new LOT system $E'(z)$ with degree $\rho' < \rho$. We can further reduce the degree of $E'(z)$ by extracting a degree-one or degree-two building blocks. Continuing the degree-reduction process, we will finally arrive at a constant unitary matrix. Summarizing the result, we have proved Theorem 6.2.

Theorem 6.2: All LOT's over $GF(2)$ are factorizable in terms of $D(z)$ and $K(z)$. ■

Since the LOT's have order one, the vectors in the factors of $D(z)$ and $K(z)$ have to satisfy some constraints so that the product of these first-order building blocks remains a first-order system. Let w_i be the vectors in $D_i(z)$ and (u_j, v_j) be the vectors in $K_j(z)$. Then, we have the following:

1) The product of $D_0(z)$ and $D_1(z)$ has order one if and only if the vectors w_0 and w_1 are such that the matrix $W = [w_0 \quad w_1]$ satisfies (see Section IV-A)
$$W^T W = I_2 \tag{6.10}$$
where I_2 is a 2×2 identity matrix. Moreover, $D_0(z)D_1(z) = D_1(z)D_0(z)$ in this case.
2) The product of $K_0(z)$ and $K_1(z)$ has order one if and only if the vectors u_i and v_i are such that the matrix $C = [u_0\ v_0\ u_1\ v_1]$ satisfies (see Section V-A)
$$C^T C = \begin{bmatrix} J_2 & 0 \\ 0 & J_2 \end{bmatrix} \tag{6.11}$$
where the matrix
$$J_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$
Moreover, $K_0(z)K_1(z) = K_1(z)K_0(z)$ in this case.
3) The product of $D_0(z)$ and $K_0(z)$ has order one if and only if the vector w_0 is such that $w_0^T u_0 = 0$ and $w_0^T v_0 = 0$. Moreover, $D_0(z)K_0(z) = K_0(z)D_0(z)$ in this case.

Combining the above results with Theorem 6.2, we have Theorem 6.3.

Theorem 6.3: The system $E(z)$ in (6.1) is a LOT with degree ρ if and only if it can be written as

$$E(z) = E(1)\prod_{i=0}^{\rho_1-1}[I + w_i w_i^T + z^{-1}w_i w_i^T] \cdot \prod_{j=0}^{\rho_2-1}[I + u_j v_j^T + v_j u_j^T + z^{-1}(u_j v_j^T + v_j u_j^T)] \tag{6.12}$$

where $\rho = \rho_1 + 2\rho_2$, $E(1)$ is a unitary matrix, and the vectors are such that the $M \times \rho$ matrix

$$C = [w_0 \quad \cdots \quad w_{\rho_1-1} \quad u_0 \quad v_0 \quad \cdots \quad u_{\rho_2-1} \quad v_{\rho_2-1}]$$

satisfies

$$\boldsymbol{C}^T\boldsymbol{C} = \begin{bmatrix} \boldsymbol{I}_{\rho_1} & & & \\ & \boldsymbol{J}_2 & & \boldsymbol{0} \\ & & \boldsymbol{J}_2 & \\ & \boldsymbol{0} & & \ddots \\ & & & & \boldsymbol{J}_2 \end{bmatrix}. \quad (6.13)$$

■

Remark: Recall the "normalization" matrix $\boldsymbol{L}$ in Theorem 6.2. Using the result in Theorem 6.3, we conclude that there is always a $\boldsymbol{L}$ of the form (6.13).

VII. State-Space Manifestation of PU Systems

Consider the $M \times M$ causal FIR system $\boldsymbol{E}(z) = \Sigma_{i=0}^{N} \boldsymbol{e}(i)z^{-i}$ in $GF(2)$. Let $\boldsymbol{x}(n)$ and $\boldsymbol{y}(n)$ be the input and the output of $\boldsymbol{E}(z)$, respectively. Then, given any structure for $\boldsymbol{E}(z)$, we can write down two equations of the form

$$\begin{aligned} \boldsymbol{s}(n+1) &= \boldsymbol{A}\boldsymbol{s}(n) + \boldsymbol{B}\boldsymbol{x}(n), \quad \text{(state eqn.)} \\ \boldsymbol{y}(n) &= \boldsymbol{C}\boldsymbol{s}(n) + \boldsymbol{D}\boldsymbol{x}(n), \quad \text{(output eqn.)} \end{aligned} \quad (7.1)$$

where $\boldsymbol{A}$ is $\rho \times \rho$, $\boldsymbol{B}$ is $\rho \times M$, $\boldsymbol{C}$ is $M \times \rho$, and $\boldsymbol{D}$ is $M \times M$. The vector $\boldsymbol{s}(n)$ is called the state vector, which consists of the output of delay elements. If the dimension of the matrix $\boldsymbol{A}$ is the smallest possible, then the structure is said to be *minimal*, and ρ is called the McMillan degree of the system. As shown in [4] and [18], the McMillan degree of a PU system is equal to the degree of its determinant. Given $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$ for a structure, the $(M+\rho) \times (M+\rho)$ matrix

$$\mathcal{R} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{bmatrix} \quad (7.2)$$

is called the *realization matrix* of the structure. The state-space description (7.1) of MIMO systems in the real or complex case has been studied extensively in the past [4], [19]. In finite fields, the concept of minimality has been introduced and studied in the area of coding theory [15], [16]. Analogous to the complex case, we can define the concepts of complete reachability (cr), complete observability (co), and minimality in finite fields. It can be verified that the following properties continue to hold:

1) A structure is cr if and only if the following matrix $\mathcal{S}_{\boldsymbol{A},\boldsymbol{B}}$ has rank ρ in $GF(q)$:

$$\mathcal{S}_{\boldsymbol{A},\boldsymbol{B}} = [\boldsymbol{B} \quad \boldsymbol{A}\boldsymbol{B} \quad \cdots \quad \boldsymbol{A}^{\rho-1}\boldsymbol{B}]. \quad (7.3)$$

2) A structure is co if and only if the following matrix $\mathcal{O}_{\boldsymbol{A},\boldsymbol{C}}$ has rank ρ in $GF(q)$:

$$\mathcal{O}_{\boldsymbol{A},\boldsymbol{C}} = \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{C}\boldsymbol{A} \\ \vdots \\ \boldsymbol{C}\boldsymbol{A}^{\rho-1} \end{bmatrix}. \quad (7.4)$$

3) A structure is minimal if and only if it is both cr and co.
4) The impulse responses $\boldsymbol{e}(i)$ are related to $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$ as

$$\boldsymbol{e}(0) = \boldsymbol{D}, \quad \boldsymbol{e}(i) = \boldsymbol{C}\boldsymbol{A}^{i-1}\boldsymbol{B}, \quad \text{for} \quad 1 \le i \le N. \quad (7.5)$$

Note that in $GF(q)$, the Cayley–Hamilton theorem continues to hold [17]. For any $\rho \times \rho$ matrix $\boldsymbol{A}$, its power $\boldsymbol{A}^{\rho}$ is a linear combination of $\boldsymbol{A}^i$ for $0 \le i \le \rho - 1$. That means if the matrix $\mathcal{S}_{\boldsymbol{A},\boldsymbol{B}}$ in (7.3) does not have rank ρ, then adding more columns of the form $\boldsymbol{A}^j\boldsymbol{B}$ for $j \ge \rho$ will not increase the rank. Therefore, providing more inputs will not help the reachability of the state. The situation is similar for the observability.

Example 7.1—Realization Matrices of $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$:

1) Consider Fig. 2. The realization matrix of the structure for $\boldsymbol{D}(z)$ in Fig. 2 is

$$\mathcal{R} = \begin{bmatrix} 0 & \boldsymbol{v}^T \\ \boldsymbol{v} & \boldsymbol{I} + \boldsymbol{v}\boldsymbol{v}^T \end{bmatrix}. \quad (7.6)$$

One can verify that $\mathcal{R}^T\mathcal{R} = \boldsymbol{I}$ so that $\mathcal{R}$ is unitary. It can be shown that the realization matrix for a cascade of $\boldsymbol{D}(z)$ is also unitary.

2) Consider Fig. 4(b). The realization matrix of the structure for $\boldsymbol{K}(z)$ in Fig. 4(b) is

$$\mathcal{R} = \begin{bmatrix} \boldsymbol{0} & \begin{bmatrix} \boldsymbol{v}^T \\ \boldsymbol{u}^T \end{bmatrix} \\ \begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \end{bmatrix} & \boldsymbol{I} + \boldsymbol{u}\boldsymbol{v}^T + \boldsymbol{v}\boldsymbol{u}^T \end{bmatrix}. \quad (7.7)$$

One can verify that $\mathcal{R}^T\mathcal{R} \neq \boldsymbol{I}$ so that the realization matrix is not unitary. In this case

$$\mathcal{S}_{\boldsymbol{A},\boldsymbol{B}} = [\boldsymbol{B} \quad \boldsymbol{A}\boldsymbol{B}] = \begin{bmatrix} \boldsymbol{v}^T & \boldsymbol{0}^T \\ \boldsymbol{u}^T & \boldsymbol{0}^T \end{bmatrix} \quad \text{and}$$

$$\mathcal{O}_{\boldsymbol{A},\boldsymbol{C}} = \begin{bmatrix} \boldsymbol{C} \\ \boldsymbol{C}\boldsymbol{A} \end{bmatrix} = \begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}.$$

Since $\boldsymbol{u}$ and $\boldsymbol{v}$ are independent, both $\mathcal{S}_{\boldsymbol{A},\boldsymbol{B}}$ and $\mathcal{O}_{\boldsymbol{A},\boldsymbol{C}}$ have rank two. Thus, the structure in Fig. 4(b) is minimal. ■

Since a cascade of minimal structures is also minimal [19], we conclude that the implementation based on cascade of $\boldsymbol{D}(z)$ and $\boldsymbol{K}(z)$ is minimal. In particular, the factorization of LOT given in Theorem 6.3 is minimal. Moreover, the realization matrix $\mathcal{R}$ of $\boldsymbol{D}(z)$ given in (7.6) is unitary. Therefore, a cascade of $\boldsymbol{D}(z)$ also has a unitary realization matrix. On the other hand, the realization matrix for $\boldsymbol{K}(z)$ given in (7.7) is not unitary. In fact, later, we will show that there does not exist any unitary realization matrix for $\boldsymbol{K}(z)$. Even though PU systems in $GF(2)$ may not have a unitary realization matrix, the following is true:

Lemma 7.1: Consider the causal FIR system $\boldsymbol{E}(z) = \Sigma_{i=0}^{N} \boldsymbol{e}(i)z^{-i}$ in $GF(2)$. If there is a minimal implementation with a unitary realization matrix $\mathcal{R}$, then $\boldsymbol{E}(z)$ is PU. ■

Proof: Assume that the initial state $\boldsymbol{s}(n_0) = \boldsymbol{0}$. Let $\boldsymbol{x}_0(n)$ and $\boldsymbol{x}_1(n)$ be two arbitrary finite-length inputs such that the corresponding outputs $\boldsymbol{y}_0(n), \boldsymbol{y}_1(n)$, and the state vector $\boldsymbol{s}(n)$ are zero for $n > K$ for some finite K. Using the unitariness of $\mathcal{R}$, one can show that

$$\sum_{n=n_0}^{K} \boldsymbol{y}_0^T(n)\boldsymbol{y}_1(n) = \sum_{n=n_0}^{K} \boldsymbol{x}_0^T(n)\boldsymbol{x}_1(n). \quad (7.8)$$

Since (7.8) holds for arbitrary choice of $\boldsymbol{x}_0(n)$ and $\boldsymbol{x}_1(n)$, we conclude from Lemma 3.1 that $\boldsymbol{E}(z)$ is PU. ■

One natural question is to ask if the converse of Lemma 7.1 is true. The answer is yes when we are dealing with real or complex case [4]. It is shown that in the real or complex case, a system is PU if and only if there is an implementation with unitary realization matrix. In $GF(2)$, the converse of Lemma 7.1 is not necessarily true as we will see in the following.

1) Realization Matrices of $\boldsymbol{K}(z)$: One minimal realization matrix $\mathcal{R}$ of $\boldsymbol{K}(z)$ is given in (7.7). Since the realization $(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})$ is minimal, any other minimal realization $(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{D})$ is related to $(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})$ as follows [4], [19]:

$$\boldsymbol{a}=\boldsymbol{T}^{-1}\boldsymbol{A}\boldsymbol{T},\quad \boldsymbol{b}=\boldsymbol{T}^{-1}\boldsymbol{B},\quad \boldsymbol{c}=\boldsymbol{C}\boldsymbol{T} \tag{7.9}$$

for some nonsingular matrix $\boldsymbol{T}$ in $GF(2)$. If there is a unitary realization for $\boldsymbol{K}(z)$, there will exist a 2×2 nonsingular matrix $\boldsymbol{T}$ such that

$$\mathcal{R}'=\begin{bmatrix}\boldsymbol{0} & \mathcal{T}^{-1}\begin{bmatrix}\boldsymbol{v}^T\\ \boldsymbol{u}^T\end{bmatrix}\\ [\boldsymbol{u}\quad \boldsymbol{v}]\boldsymbol{T} & \boldsymbol{I}+\boldsymbol{u}\boldsymbol{v}^T+\boldsymbol{v}\boldsymbol{u}^T\end{bmatrix} \tag{7.10}$$

is unitary. Computing the product $\mathcal{R}'^T\mathcal{R}'$ and equating to the identity, we get

$$\boldsymbol{T}^T\boldsymbol{J}_2\boldsymbol{T}=\boldsymbol{I}_2 \tag{7.11}$$

where

$$\boldsymbol{J}_2=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

Equation (7.11) implies $\boldsymbol{J}_2=(\boldsymbol{T}^{-1})^T\boldsymbol{T}^{-1}$, which is not possible (see Appendix B). Therefore, we conclude that the PU system $\boldsymbol{K}(z)$ does not have a unitary realization matrix.

VIII. Unitary Matrices and PU Systems Over $GF(q)$

In this section, we will generalize the theory developed earlier to the case of $GF(q)$ for any prime number $q>2$. While many results in the $GF(2)$ case can be easily extended to the case of $GF(q)$, there are some exceptions, which we first point out.

A. Unitary Matrices Over $GF(q)$

Let $\boldsymbol{A}$ be a matrix with elements in $GF(q)$ for some prime $q>2$. In $GF(q)$, there are a number of properties that are different from those in $GF(2)$. In particular, the condition that $\boldsymbol{u}^T\boldsymbol{A}^T\boldsymbol{A}\boldsymbol{u}=\boldsymbol{u}^T\boldsymbol{u}$ for all $\boldsymbol{u}$ is sufficient to ensure the unitariness of $\boldsymbol{A}$ in $GF(q)$ for $q>2$. To be more precise, we have Fact 8.1.

Fact 8.1: In $GF(q)$ for some prime $q>2$, $\boldsymbol{A}$ is unitary if and only if $\boldsymbol{u}^T\boldsymbol{A}^T\boldsymbol{A}\boldsymbol{u}=\boldsymbol{u}^T\boldsymbol{u}$ for all possible vectors $\boldsymbol{u}$ in $GF(q)$. ■

Proof: The "only if" part is clear. To show the "if" part, assume that $\boldsymbol{u}^T\boldsymbol{u}=\boldsymbol{u}^T\boldsymbol{A}^T\boldsymbol{A}\boldsymbol{u}$. Substituting $\boldsymbol{B}=\boldsymbol{A}^T\boldsymbol{A}$ into (2.2), we get

$$\sum_l u_l^2=\sum_l u_l^2 b_{ll}+2\sum_{i>j}u_iu_jb_{ij} \tag{8.1}$$

where we have used the fact that $\boldsymbol{B}=\boldsymbol{A}^T\boldsymbol{A}$ is symmetric. Letting $\boldsymbol{u}$ to be the unit vector $\boldsymbol{e}_i$, we get $b_{ll}=1$ from (8.1). Using $b_{ll}=1$, (8.1) can be rewritten as $2\sum_{i>j}u_iu_jb_{ij}=0$. Now, if we choose $\boldsymbol{u}=\boldsymbol{e}_{i_0}+\boldsymbol{e}_{j_0}$ for some $i_0>j_0$, we get $2b_{i_0j_0}=0$, which implies $b_{i_0j_0}=0$ (as 2 is coprime to q). Therefore, $\boldsymbol{B}=\boldsymbol{A}^T\boldsymbol{A}=\boldsymbol{I}$. ■

Recall from Fact 2.3 that in $GF(2)$, none of the columns or rows of a unitary matrix can have all elements equal to 1. The same is not true for unitary matrices in $GF(q)$ for $q>2$. For example, the following matrix is unitary in $GF(5)$.

$$\boldsymbol{A}=\begin{bmatrix}1&1&2&2&4&0\\1&1&3&3&4&0\\1&1&0&0&2&0\\1&4&2&3&0&4\\1&4&3&2&0&4\\1&4&0&0&0&2\end{bmatrix}. \tag{8.2}$$

In Section II-B, we have seen that the factorizability of unitary matrices in $GF(2)$ depends on Fact 2.3. In $GF(q)$, even though a result similar to Fact 2.3 is no longer true, we will see later that all unitary matrices in $GF(q)$ are still factorizable.

Householder-like Transformation in $GF(q)$: Recall from Section II-B that for the factorization of unitary matrices in $GF(2)$, we have used the building blocks of the form $[\boldsymbol{I}+\boldsymbol{u}\boldsymbol{u}^T]$, where $\boldsymbol{u}^T\boldsymbol{u}=0$. In the $GF(q)$ case, we will make use of the following building block:

$$\boldsymbol{U}=\boldsymbol{I}-2l_{\boldsymbol{u}}^{-1}\boldsymbol{u}\boldsymbol{u}^T \tag{8.3}$$

where $\boldsymbol{u}$ is any vector with $l_{\boldsymbol{u}}=\boldsymbol{u}^T\boldsymbol{u}\neq 0$ so that $\boldsymbol{u}^{-1}$ exists. One can verify that $\boldsymbol{U}$ is unitary and that it is its own inverse. Note that unlike the complex field, $l_{\boldsymbol{u}}$ may not be the square of some number in $GF(q)$. Hence, it is not always possible to "normalize" a nonzero vector $\boldsymbol{u}$ in $GF(q)$ such that $l_{\boldsymbol{u}}=1$. One such example is the vector $\begin{bmatrix}1\\1\end{bmatrix}$ in $GF(3)$. The Householder matrix in (8.3) has a very useful property. Given any two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ such that $\boldsymbol{x}^T\boldsymbol{x}=\boldsymbol{y}^T\boldsymbol{y}$ and $(\boldsymbol{x}-\boldsymbol{y})^T(\boldsymbol{x}-\boldsymbol{y})\neq 0$, the Householder matrix in (8.3) with $\boldsymbol{u}=\boldsymbol{x}-\boldsymbol{y}$ transforms the vector $\boldsymbol{x}$ into the vector $\boldsymbol{y}$. More precisely, we have $\boldsymbol{U}\boldsymbol{x}=\boldsymbol{y}$, where $\boldsymbol{u}=\boldsymbol{x}-\boldsymbol{y}$. Using this transformation property of Householder matrix, we can prove the following lemma:

Lemma 8.1: Let $\boldsymbol{A}$ be $M\times M$ unitary over $GF(q)$ for some prime $q>2$, and let $A_{00}\neq 1$. Define the vector $\boldsymbol{u}=\boldsymbol{e}_0-\boldsymbol{a}_0$, where $\boldsymbol{a}_0$ is the zeroth column of $\boldsymbol{A}$. Then, $l_{\boldsymbol{u}}=\boldsymbol{u}^T\boldsymbol{u}\neq 0$, and

$$\boldsymbol{A}=(\boldsymbol{I}-2l_{\boldsymbol{u}}^{-1}\boldsymbol{u}\boldsymbol{u}^T)\begin{bmatrix}1&0\\0&\boldsymbol{B}\end{bmatrix} \tag{8.4}$$

where $\boldsymbol{B}$ is $(M-1)\times(M-1)$ unitary. ■

Proof: As $A_{00}\neq 1$, we have $l_{\boldsymbol{u}}=(\boldsymbol{e}_0-\boldsymbol{a}_0)^T(\boldsymbol{e}_0-\boldsymbol{a}_0)=2-2A_{00}\neq 0$. Therefore, we can form the unitary matrix $\boldsymbol{U}$ given in (8.3). As we mentioned before, the matrix $\boldsymbol{U}$ has the property that $\boldsymbol{U}\boldsymbol{a}_0=\boldsymbol{e}_0$. Therefore, we have

$$\boldsymbol{U}\boldsymbol{A}=\begin{bmatrix}1&\boldsymbol{v}^T\\0&\boldsymbol{B}\end{bmatrix}. \tag{8.5}$$

The matrix on the right-hand side of (8.5) is unitary as $\boldsymbol{A}$ and $\boldsymbol{U}$ are unitary. Thus, $\boldsymbol{v}=\boldsymbol{0}$ and $\boldsymbol{B}$ is unitary. ■

With Lemma 8.1, we are ready to prove the factorization theorem for the unitary matrix $\boldsymbol{A}$ in $GF(q)$. The problem to be solved is, given any unitary matrix $\boldsymbol{A}$, how to avoid the

case where $A_{00} = 1$. This can be avoided by using both column permutation $\boldsymbol{P}_{\text{col}}$ and row permutation $\boldsymbol{P}_{\text{row}}$. Given any $M \times M$ unitary matrix $\boldsymbol{A}$ with $M > 1$, there is always an element $A_{ij} \neq 1$. Therefore, we can find $\boldsymbol{P}_{\text{col}}$ and $\boldsymbol{P}_{\text{row}}$ such that $\boldsymbol{A}' = \boldsymbol{P}_{\text{row}}\boldsymbol{A}\boldsymbol{P}_{\text{col}}$ with $A'_{00} = A_{ij} \neq 1$. Then, Lemma 8.1 can be applied to $\boldsymbol{A}'$, and we can write $\boldsymbol{A}$ as

$$\boldsymbol{A} = \boldsymbol{P}_{\text{row}}(\boldsymbol{I} - 2l_{\boldsymbol{u}}^{-1}\boldsymbol{u}\boldsymbol{u}^T)\begin{bmatrix}1 & 0\\ 0 & \boldsymbol{B}\end{bmatrix}\boldsymbol{P}_{\text{col}} \tag{8.6}$$

for some vector $\boldsymbol{u}$ with $l_{\boldsymbol{u}} \neq 0$. We can continue the above process and arrive at the following result:

Theorem 8.1: An $M \times M$ matrix $\boldsymbol{A}$ over $GF(q)$ (where q is a prime >2) is unitary if and only if it can be factorized as

$$\boldsymbol{A} = \boldsymbol{U}_M \cdots \boldsymbol{U}_3\boldsymbol{U}_2\boldsymbol{P} \tag{8.7}$$

where $\boldsymbol{U}_k$ are as in (8.3), and $\boldsymbol{P}$ is a permutation of the identity matrix. ■

B. Paraunitary Matrices Over $GF(q)$

As we have seen in the previous discussion, many properties of unitary matrices in $GF(q)$ are different from those in $GF(2)$. In this section, we will extend the results of PU matrices in $GF(2)$ derived in Sections III–VII to the $GF(q)$ case and point out the differences between these two cases.

Given any vector $\boldsymbol{v}$ in $GF(q)$ with $l_{\boldsymbol{v}} = \boldsymbol{v}^T\boldsymbol{v} \neq 0$, we form the following degree-one system:

$$\boldsymbol{D}_q(z) = \boldsymbol{I} - l_{\boldsymbol{v}}^{-1}\boldsymbol{v}\boldsymbol{v}^T + z^{-1}l_{\boldsymbol{v}}^{-1}\boldsymbol{v}\boldsymbol{v}^T. \tag{8.8}$$

Note that $\boldsymbol{D}_q(z)$ in (8.8) is slightly different from the $GF(2)$ degree-one building block $\boldsymbol{D}(z)$ in (4.1). It can be verified that $\boldsymbol{D}_q^T(z^{-1})\boldsymbol{D}_q(z) = \boldsymbol{I}$. Theefore, $\boldsymbol{D}_q(z)$ is PU. For the building block $\boldsymbol{D}_q(z)$ in (8.8), it can be shown that all the properties mentioned in Section IV-A continue to hold. In particular, any $M \times M$ causal FIR degree-one PU system over $GF(q)$ can be written as

$$\boldsymbol{E}(z) = (\boldsymbol{I} - l_{\boldsymbol{v}}^{-1}\boldsymbol{v}\boldsymbol{v}^T + z^{-1}l_{\boldsymbol{v}}^{-1}\boldsymbol{v}\boldsymbol{v}^T)\boldsymbol{E}(1) \tag{8.9}$$

for some vector $\boldsymbol{v}$ such that $l_{\boldsymbol{v}} = \boldsymbol{v}^T\boldsymbol{v} \neq 0$ and unitary matrix $\boldsymbol{E}(1)$ in $GF(q)$. Given any causal FIR PU system $\boldsymbol{G}(z)$ in $GF(q)$, the algorithm for degree-one reduction is very similar to that given in Section IV-B for $GF(2)$. The first step is to identify any vector $\boldsymbol{v}$ with $\boldsymbol{v}^T\boldsymbol{v} \neq 0$ in the null space of $\boldsymbol{g}(0)$ or $\boldsymbol{g}^T(0)$. Then, form the building block $\boldsymbol{D}_q(z)$ as in (8.8). It can be verified that such $\boldsymbol{D}_q(z)$ can be used to reduce the degree of $\boldsymbol{G}(z)$. However, the degree-one reduction is not always possible. As in the $GF(2)$ case, the degree-one building block $\boldsymbol{D}_q(z)$ in (8.8) is not complete for the class of PU systems over $GF(q)$. There are PU systems in $GF(q)$ that cannot be written as a product of $\boldsymbol{D}_q(z)$ (see Example 8.1). In $GF(q)$, we can use the following to test if we can extract a degree-one PU building block.

Lemma 8.2: Let $\boldsymbol{E}(z) = \sum_{k=0}^{N}\boldsymbol{e}(k)z^{-k}$ be a causal PU system over $GF(q)$ for some prime $q > 2$. Let $\boldsymbol{U} = [\boldsymbol{u}_0, \cdots, \boldsymbol{u}_s]$ and $\boldsymbol{V} = [\boldsymbol{v}_0, \cdots, \boldsymbol{v}_s]$ be *any* bases that span the null spaces of $\boldsymbol{e}(0)$ and $\boldsymbol{e}^T(0)$, respectively. Then, we cannot extract a degree-one PU building block from $\boldsymbol{E}(z)$ if and only if both $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{0}$ and $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{0}$. ■

Proof: It is not difficult to see that the degree-one reduction fails if and only if neither the null space of $\boldsymbol{e}(0)$ nor $\boldsymbol{e}^T(0)$ contains any vector $\boldsymbol{v}$ with $l_{\boldsymbol{v}} = \boldsymbol{v}^T\boldsymbol{v} \neq 0$. What remains to be shown is that the above condition is equivalent to $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{0}$ and $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{0}$. To show the "if" part, assume that $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{0}$ and that $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{0}$. Then, any vector $\boldsymbol{u}$ in the null space of $\boldsymbol{e}(0)$ is a linear combination of $\boldsymbol{u}_i$, i.e., $\boldsymbol{u} = c_0\boldsymbol{u}_0 + \cdots + c_s\boldsymbol{u}_s$ for some constants $c_i \in GF(q)$. Since $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{0}$, we have $\boldsymbol{u}^T\boldsymbol{u} = 0$. Similarly, we can show that $\boldsymbol{V}^T\boldsymbol{V} = \boldsymbol{0}$ implies that all the vectors in the null space of $\boldsymbol{e}^T(0)$ have $\boldsymbol{v}^T\boldsymbol{v} = 0$. To prove the "only if" part, assume that $\boldsymbol{U}^T\boldsymbol{U} \neq \boldsymbol{0}$ (the proof is similar if $\boldsymbol{V}^T\boldsymbol{V} \neq \boldsymbol{0}$). If there is any $\boldsymbol{u}_i$ with $\boldsymbol{u}_i^T\boldsymbol{u}_i \neq 0$, then we can form $\boldsymbol{D}_q(z)$ with $\boldsymbol{u}_i$, and we are done. Therefore, assume that all $\boldsymbol{u}_i$ have $\boldsymbol{u}_i^T\boldsymbol{u}_i = 0$. As $\boldsymbol{U}^T\boldsymbol{U} \neq \boldsymbol{0}$, there are $\boldsymbol{u}_i$ and $\boldsymbol{u}_j$ such that $\boldsymbol{u}_i^T\boldsymbol{u}_j \neq 0$. With these $\boldsymbol{u}_i$ and $\boldsymbol{u}_j$, we form the new vector $\boldsymbol{u} = \boldsymbol{u}_i + \boldsymbol{u}_j$ so that $\boldsymbol{u}^T\boldsymbol{u} = 2\boldsymbol{u}_i^T\boldsymbol{u}_j \neq 0$ (because 2 is coprime with q). Thus, we can form $\boldsymbol{D}_q(z)$ with the new vector $\boldsymbol{u}$, and the degree-one reduction with $\boldsymbol{D}_q(z)$ will succeed. Therefore, we conclude that if either $\boldsymbol{U}^T\boldsymbol{U} \neq \boldsymbol{0}$ or $\boldsymbol{V}^T\boldsymbol{V} \neq \boldsymbol{0}$, the degree-one reduction will work. The proof is complete. ■

One consequence of Lemma 8.2 is that in $GF(q)$, the degree-two PU system $\boldsymbol{K}(z)$ in (5.4) is factorizable in terms of the degree-one PU building block $\boldsymbol{D}_q(z)$. To see this, recall that

$$\boldsymbol{K}_q(z) = \boldsymbol{I} - \boldsymbol{u}\boldsymbol{v}^T - \boldsymbol{v}\boldsymbol{u}^T + z^{-1}(\boldsymbol{u}\boldsymbol{v}^T + \boldsymbol{v}\boldsymbol{u}^T) \tag{8.10}$$

where the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are such that $\boldsymbol{u}^T\boldsymbol{u} = \boldsymbol{v}^T\boldsymbol{v} = 0$ and $\boldsymbol{u}^T\boldsymbol{v} = 1$ (note that in $GF(2), \boldsymbol{I} - \boldsymbol{u}\boldsymbol{v}^T - \boldsymbol{v}\boldsymbol{u}^T = \boldsymbol{I} + \boldsymbol{u}\boldsymbol{v}^T + \boldsymbol{v}\boldsymbol{u}^T$)). Form $\boldsymbol{v}_+ = \boldsymbol{u} + \boldsymbol{v}$ and $\boldsymbol{v}_- = \boldsymbol{u} - \boldsymbol{v}$ such that $l_{\boldsymbol{v}_+} = \boldsymbol{v}_+^T\boldsymbol{v}_+ = 2 \neq 0$ and $l_{\boldsymbol{v}_-} = \boldsymbol{v}_-^T\boldsymbol{v}_- = q - 2 \neq 0$ (note that $-2 = q - 2$ in $GF(q)$). With $\boldsymbol{v}_+$ and $\boldsymbol{v}_-$, we can factorize the $\boldsymbol{K}_q(z)$ in (8.10) as

$$\begin{aligned}\boldsymbol{K}_q(z) = &\underbrace{[\boldsymbol{I} - 2^{-1}\boldsymbol{v}_+\boldsymbol{v}_+^T + z^{-1}2^{-1}\boldsymbol{v}_+\boldsymbol{v}_+^T]}_{\boldsymbol{D}_{q0}(z)}\\ &\cdot\underbrace{[\boldsymbol{I} + 2^{-1}\boldsymbol{v}_-\boldsymbol{v}_-^T - z^{-1}2^{-1}\boldsymbol{v}_-\boldsymbol{v}_-^T]}_{\boldsymbol{D}_{q1}(z)}\end{aligned} \tag{8.11}$$

where both $\boldsymbol{D}_{q0}(z)$ and $\boldsymbol{D}_{q1}(z)$ are degree-one PU systems. In fact, in $GF(q)$, all first-order PU systems (i.e., LOT) are factorizable in terms of the degree-one PU system $\boldsymbol{D}_q(z)$ in (8.8).

Theorem 8.2—Complete Factorization of LOT in $GF(q)$: Consider the first-order system $\boldsymbol{E}(z) = \boldsymbol{e}(0) + \boldsymbol{e}(1)z^{-1}$ in $GF(q)$ for some prime $q > 2$. Then, $\boldsymbol{E}(z)$ is a LOT of degree ρ if and only if it can be written as

$$\boldsymbol{E}(z) = \boldsymbol{E}(1)\prod_{i=0}^{\rho-1}[\boldsymbol{I} - l_{\boldsymbol{v}_i}^{-1}\boldsymbol{v}_i\boldsymbol{v}_i^T + z^{-1}l_{\boldsymbol{v}_i}^{-1}\boldsymbol{v}_i\boldsymbol{v}_i^T] \tag{8.12}$$

where the number $l_{\boldsymbol{v}_i} = \boldsymbol{v}_i^T\boldsymbol{v}_i \neq 0$, the matrix $\boldsymbol{E}(1)$ is unitary, and the vectors $\boldsymbol{v}_i$ satisfy $\boldsymbol{v}_i^T\boldsymbol{v}_j = l_{\boldsymbol{v}_i}\delta(i-j)$. ■

The proof of the above theorem is very similar to that of Theorem 6.3. The LOT in $GF(q)$ also allows a minimal characterization that is similar to that given in Theorem 6.2. Even though in $GF(q)$ all LOT's are factorizable, there are unfactorizable higher order PU systems.

Example 8.1—A 2×2 Unfactorizable PU System in $GF(5)$: Consider the following second-order system:

$$\boldsymbol{G}(z)=\begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix}+z^{-1}\boldsymbol{I}+z^{-2}\begin{bmatrix}4 & 3\\ 3 & 1\end{bmatrix}. \tag{8.13}$$

The system $\boldsymbol{G}(z)$ is not a LOT because its order >1. One can verify that the impulse response $\boldsymbol{g}(i)$ satisfies the condition in (3.2) so that $\boldsymbol{G}(z)$ is PU. Moreover, $\boldsymbol{G}(z)$ has degree two because $[\det \boldsymbol{G}(z)]=z^{-2}$. Since $\boldsymbol{g}(0)$ is symmetric, the null spaces of $\boldsymbol{g}(0)$ and $\boldsymbol{g}^T(0)$ are identical. The null space of $\boldsymbol{g}(0)$ consists of vectors of the form $c[3\quad 1]^T$, where $c\in GF(5)$. As $[3\quad 1][3\quad 1]^T=0$, using Lemma 8.2, we conclude that the PU system $\boldsymbol{G}(z)$ cannot be factorized in terms of $\boldsymbol{D}_q(z)$. ■

Nontrivial 2×2 Building Block $\boldsymbol{D}_q(z)$ in $GF(q)$: In the theory of FB's and wavelets in the complex field, one important class is the two-channel PU FB's. The corresponding polyphase matrix is a 2×2 PU matrix that can always be decomposed into degree-one building blocks in the complex case. In the case of finite fields, we know from previous dicussions that the building block $\boldsymbol{D}_q(z)$ is not complete. In fact, there are not many nontrivial 2×2 PU systems that are factorizable because there are few nontrivial 2×2 degree-one PU systems. (A system $\boldsymbol{E}(z)$ is said to be *trivial* if it is a diagonal matrix.) In particular, all 2×2 degree-one PU systems in $GF(2)$ are diagonal because there is no 2×1 vector $\boldsymbol{v}$ with $v_0\neq 0, v_1\neq 0$ and $\boldsymbol{v}^T\boldsymbol{v}\neq 0$. Therefore, all factorizable 2×2 PU systems in $GF(2)$ are diagonal systems. In the following, we will derive a formula for the number of nontrivial 2×2 degree-one building block $\boldsymbol{D}_q(z)$ in $GF(q)$ for $q>2$.

From (8.8), we see that $\boldsymbol{D}_q(z)$ is trivial if and only if the vector $\boldsymbol{v}$ is either $[v_0\quad 0]^T$ or $[0\quad v_1]^T$. Therefore, it is sufficient to consider vectors with $v_0\neq 0$ and $v_1\neq 0$. However, the number of nontrivial $\boldsymbol{D}_q(z)$ is less than the number of distinct vectors (with $v_0\neq 0$ and $v_1\neq 0$) because two distinct vectors could generate the same $\boldsymbol{D}_q(z)$. To be more precise, one can show that two building blocks $\boldsymbol{D}_q(z)$ generated from two different vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are equivalent if and only if the vectors are related as $\boldsymbol{u}=k\boldsymbol{v}$ for some $k\in GF(q)$. Define the set

$$\mathcal{U}=\left\{\begin{bmatrix}1\\ 1\end{bmatrix},\begin{bmatrix}1\\ 2\end{bmatrix},\cdots,\begin{bmatrix}1\\ q-1\end{bmatrix}\right\}. \tag{8.14}$$

Then it can be shown that if $\boldsymbol{u}_0,\boldsymbol{u}_1\in\mathcal{U}, \boldsymbol{u}_0=c\boldsymbol{u}_1$ if and only if $\boldsymbol{u}_0=\boldsymbol{u}_1$. Therefore, if $\boldsymbol{u}_0$ and $\boldsymbol{u}_1$ (with $\boldsymbol{u}_i^T\boldsymbol{u}_i\neq 0$) are vectors in $\mathcal{U}$, then they generate two distinct nontrivial $\boldsymbol{D}_q(z)$. Moreover, it is not difficult to show the set $\mathcal{U}$ has the following property: For any $\boldsymbol{v}$ with nonzero elements, there is an $\boldsymbol{u}\in\mathcal{U}$ and a $k\in GF(q)$ such that $\boldsymbol{v}=k\boldsymbol{u}$. Combining the above results, we can conclude that given any nontrivial degree-one PU building block $\mathcal{D}_q(z)$, there is a *unique* vector $\boldsymbol{u}\in\mathcal{U}$ such that $\boldsymbol{D}_q(z)=\boldsymbol{I}-l_{\boldsymbol{u}}^{-1}\boldsymbol{u}\boldsymbol{u}^T+z^{-1}l_{\boldsymbol{u}}^{-1}\boldsymbol{u}\boldsymbol{u}^T$. Therefore, the number of nontrivial 2×2 degree-one PU systems is exactly the number of elements in the following set:

$$\mathcal{U}_1=\{\boldsymbol{u}\in\mathcal{U}|\boldsymbol{u}^T\boldsymbol{u}\neq 0\}. \tag{8.15}$$

Note that in $\mathcal{U}$, the number of vectors with $\boldsymbol{u}^T\boldsymbol{u}=0$ is equal to the number of solutions to the equation

$$u^2=-1 \mod q, \quad \text{for } u\in GF(q). \tag{8.16}$$

Except for the $GF(2)$ case (because in $GF(2)$, $-1=1$)), one can show that u is a solution to (8.16) if and only if the *order* of u is 4, i.e., $u^4=1 \bmod q$ but $u^i\neq 1 \bmod q$ for $i<4$. From number theory [20], we know that there is an element of order 4 in $GF(q)$ if and only if $q-1$ is divisible by 4. Using the Euler function [20], there are exactly two elements of order 4 if they exist. Therefore, we conclude that (8.16) can have either no solution or two solutions, depending on whether $q-1$ is divisible by 4. More precisely, we have

$$\begin{aligned}&(\text{number of vectors in } \mathcal{U} \text{ with } \boldsymbol{u}^T\boldsymbol{u}=0)\\ &\quad=\begin{cases}2, & \text{if } q-1=0 \bmod 4;\\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{8.17}$$

Combining all the results, we have shown that the number of nontrivial 2×2 degree-one PU systems in $GF(q)$ for $q>2$ is

$$(q-1)-2\cdot\delta([q-1]_4) \tag{8.18}$$

where $[q-1]_4$ denotes $(q-1)$ mod 4. From (8.18), we conclude that for $q>2$, there are at most $(q-1)$ nontrivial 2×2 building blocks $\boldsymbol{D}_q(z)$ in $GF(q)$.

IX. Conclusions

In this paper, we gave a detailed study on the theory of unitary and PU systems in finite fields. Explicit degree-one and degree-two reduction algorithms for the $GF(2)$ case are given (Sections IV-B and V-B). Several tests for factorizability of PU systems are also given (Lemmas 4.2, 5.2, and 8.2). We have proved a number of factorization theorems for both unitary matrices (Theorems 2.1 and 8.1) and PU systems (Theorems 6.2, 6.3, and 8.2). In particular, we have shown that all LOT's in $GF(q)$ for any prime number q are factorizable in terms of smaller (degree-one or degree-two) PU building blocks (Theorems 6.3 and 8.2). Even though these degree-one or degree-two building blocks are the most general, there are PU systems that cannot be factorized [see the examples in (5.12) and (8.13)].

All the theories in this paper are developed for finite fields of the form $GF(q)$ with prime q. It would be interesting to extend the results to the fields of the form $GF(q^m)$. In particular, PU systems that cannot be factorized may be factorizable if we use building blocks from extension fields. This is still an open problem. In addition, we have studied the theory of systems with the PU property only [except the example in (5.1)]. It is important to look at other classes such as the unimodular matrices (which are useful in the coding theory [15], [16]) and the class of causal matrices with anticausal inverses [18] (which cover the PU systems as a special case).

Appendix A
Most General 2×2 Degree-Two Unfactorizable PU Systems in $GF(2)$

Consider the 2×2 degree-two PU system $\boldsymbol{G}(z)=\boldsymbol{g}(0)+\boldsymbol{g}(1)z^{-1}+\boldsymbol{g}(2)z^{-2}$. Since $\boldsymbol{G}(z)$ has degree two, the rank of $\boldsymbol{g}(2)\leq 1$. If $\boldsymbol{g}(2)=\boldsymbol{0}$, then $\boldsymbol{g}(1)$ has full rank so that the system reduces to the trivial factorizable system $\boldsymbol{G}(z)=\boldsymbol{g}(1)z^{-1}$, where $\boldsymbol{g}(1)=\boldsymbol{I}_2$ or $\boldsymbol{J}_2$. Therefore, assume rank $\boldsymbol{g}(2)=1$. As $\boldsymbol{G}(z)$ is unfactorizable, the null spaces of $\boldsymbol{g}(0)$ and $\boldsymbol{g}^T(0)$ should not contain any vector with an

odd weight. This implies that $\boldsymbol{g}(0) = \left[\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right]$. Using the PU conditions $\boldsymbol{g}^T(0)\boldsymbol{g}(2) = \boldsymbol{0}$ and $\boldsymbol{g}(0)\boldsymbol{g}^T(2) = \boldsymbol{0}$, we conclude that $\boldsymbol{g}(2) = \left[\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right]$. To find $\boldsymbol{g}(1)$, we use the condition

$$\boldsymbol{g}^T(0)\boldsymbol{g}(0) + \boldsymbol{g}^T(1)\boldsymbol{g}(1) + \boldsymbol{g}^T(2)\boldsymbol{g}(2) = \boldsymbol{I}. \tag{A.1}$$

Substituting $\boldsymbol{g}(0)$ and $\boldsymbol{g}(2)$ into the above equation, we get $\boldsymbol{g}^T(1)\boldsymbol{g}(1) = \boldsymbol{I}$, which implies that $\boldsymbol{g}(1)$ is unitary. The only 2×2 unitary matrices are $\boldsymbol{I}_2$ and $\boldsymbol{J}_2$. One can verify that both the choices of $\boldsymbol{g}(1) = \boldsymbol{I}_2$ and $\boldsymbol{g}(1) = \boldsymbol{J}_2$ give a PU system. Thus, we conclude that the most general 2×2 degree-two unfactorizable PU system has the form

$$\boldsymbol{G}(z) = \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + \boldsymbol{g}(1)z^{-1} + \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}z^{-2} \tag{A.2}$$

where $\boldsymbol{g}(1) = \boldsymbol{I}_2$ or $\boldsymbol{J}_2$.

APPENDIX B
A FACT FOR MATRICES IN $GF(2)$

Lemma B.1: Let $\boldsymbol{A}$ be an $M \times M$ matrix in $GF(2)$ with M even. Then, $\boldsymbol{A}^T\boldsymbol{A} \neq \boldsymbol{J}_M$. ■

Note that Lemma B.1 is always true for all $M \geq 2$ in the real or complex field as $\boldsymbol{A}^T\boldsymbol{A}$ is always semi positive definite while $\boldsymbol{J}_M$ is not. In $GF(2)$, the lemma does not hold for odd M. To see this, consider $M = 3$. Then, it can be verified that the matrix

$$\boldsymbol{A} = \begin{bmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\end{bmatrix} \tag{B.1}$$

satisfies $\boldsymbol{A}^T\boldsymbol{A} = \boldsymbol{J}_3$.

Proof of Lemma B.1: Suppose that there is a matrix $\boldsymbol{A}$ such that $\boldsymbol{A}^T\boldsymbol{A} = \boldsymbol{J}_M$. Let $\boldsymbol{a}_i$ be the ith column vector of $\boldsymbol{A}$. Then, all $\boldsymbol{a}_i$ has an even weight because $\boldsymbol{a}_i^T\boldsymbol{a}_i = 0$ for all i. Therefore, we have $[1 \quad 1 \quad \cdots \quad 1]\boldsymbol{A} = \boldsymbol{0}$, which implies that $\boldsymbol{A}$ is singular. This contradicts the fact that $\boldsymbol{A}$ is nonsingular (because $\boldsymbol{A}^T\boldsymbol{A} = \boldsymbol{J}_M$). Thus, we conclude that there does not exist such $\boldsymbol{A}$. ■

REFERENCES

[1] R. E. Crochiere, and L. R. Rabiner, *Multirate Digital Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1983.

[2] J. W. Woods, *Subband Coding of Images*. Boston, MA: Kluwer, 1991.

[3] H. S. Malvar, *Signal Processing with Lapped Orthogonal Transforms*. Norwood, MA: Artech House, 1992.

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

[5] N. J. Fliege, *Multirate Digital Signal Processing*. Chichester, U.K.: Wiley, 1994.

[6] M. Vetterli, and J. Kovacevic, *Wavelets and Subband Coding*. Englewood Cliffs, NJ: Prentice-Hall, 1995.

[7] M. J. T. Smith, and T. P. Barnwell, "Exact reconstruction techniques for tree-structured subband coders," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-37, pp. 434–441, June 1987.

[8] T. A. Ramstad, "Analysis/synthesis filter banks with critical sampling," in *Proc. Int. Conf. Digital Signal Processing*, Florence, Italy, Sept. 1984.

[9] P. P. Vaidyanathan, "Unitary and paraunitary systems in finite fields," in *Proc. Int. Symp. Circuits Syst.*, New Orleans, LA, 1990, pp. 1189–1192.

[10] T. Cooklev, A. Nishihara, and M. Sablatash, "Theory of filter banks over finite fields," IN *Proc. Asia Pacific Conf. Circuits Syst.*, Taipei, Taiwan, Dec. 1994 pp. 260–265.

[11] M. D. Swanson, and A. H. Tewfik, "A binary wavelet decomposition of binary images," *IEEE Trans. Image Processing*, vol. 5, pp. 1637–1650, Dec. 1996.

[12] X.-G. Xia, "Filterbank approach for error correction codes with applications in partial response channels," preprint, 1995.

[13] G. Caire, R. L. Grossman, and H. V. Poor, "Wavelet transforms associated with finite cyclic groups," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1157–1166, July 1993.

[14] K. Flornes, A. Grossmann, M. Holschneider, and B. Torresani, "Wavelets over discrete fields," *Applied Comput. Harmonic Anal.*, vol. 1, no. 2, pp. 137–146, Mar. 1994.

[15] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.

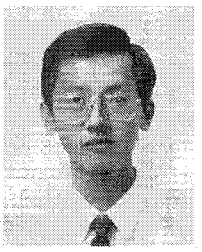
[16] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*. Amsterdam: Elsevier, Aug. 1995.

[17] R. A. Horn, and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.

[18] P. P. Vaidyanathan and T. Chen, "Role of anticausal inverses in multirate filter-banks, Part I: System-theoretic fundamentals," *IEEE Trans. Signal Processing*, vol. 43, pp. 1090–1103, May 1995.

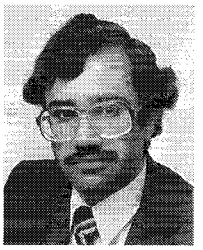
[19] T. Kailath, *Linear Systems*. Englewood Cliffs, NJ: Prentice-Hall, 1980.

[20] J. H. McClellan, and C. M. Rader, *Number Theory in Digital Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1979.



See-May Phoong (M'96) was born in Johor, Malaysia, in 1968. He received the B.S. degree in electrical engineering from the National Taiwan University, Taipei, Taiwan, R.O.C., in 1991 and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, in 1992 and 1996, respectively.

He is now on the faculty of the Department of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His interests include digital signal processing, multirate FB's and wavelet transforms.



P. P. Vaidyanathan (S'80–M'83–SM'88–F'91) was born in Calcutta, India, on October 16, 1954. He received the B.Sc. (Hons.) degree in physics and the B.Tech. and M.Tech. degrees in radiophysics and electronics, all from the University of Calcutta, in 1974, 1977, and 1979, respectively, and the Ph.D. degree in electrical and computer engineering from the University of California, Santa Barbara, in 1982.

He was a post doctoral fellow at the University of California, Santa Barbara, from September 1982 to March 1983. In March 1983, he joined the Electrical Engineering Department, California Institute of Technology, Pasadena, as an Assistant Professor, and since 1993, he has been Professor of Electrical Engineering there. His main research interests are in digital signal processing, multirate systems, wavelet transforms and adaptive filtering.

Dr. Vaidyanathan served as Vice Chairman of the Technical Program Committee for the 1983 IEEE International Symposium on Circuits and Systems and as the Technical Program Chairman for the 1992 IEEE International Symposium on Circuits and Systems. He was an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS from 1985 to 1987 and is currently an associate editor for IEEE SIGNAL PROCESSING LETTERS. He is a consulting editor for the journal *Applied and Computational Harmonic Analysis*. He has authored a number of papers in IEEE journals. He has written several chapters for various signal processing handbooks. He was a recipient of the Award for Excellence in Teaching at the California Institute of Technology for the years 1983–1984, 1992–1993, and 1993–1994. He also received the NSF's Presidential Young Investigator award in 1986. In 1989, he received the IEEE ASSP Senior Award for his paper on multirate perfect-reconstruction FB's. In 1990, he was the recipient of the S. K. Mitra Memorial Award from the Institute of Electronics and Telecommunications Engineers, India, for his joint paper in the IETE journal. He was also the co-author of a paper on linear-phase perfect construction FB's in the IEEE TRANSACTIONS ON SIGNAL PROCESSING, for which the first author (T. Nguyen) received the *Young Outstanding Author* award in 1993. He received the 1995 F. E. Terman Award of the American Society for Engineering Education, which was sponsored by Hewlett Packard Co., for his contributions to engineering education, especially the book *Multirate Systems And Filter Banks* (Englewood Cliffs, NJ: Prentice-Hall, 1993). He has been chosen a distinguished lecturer for the IEEE Signal Processing Society for 1996–1997.