Shift-Full-Rank Matrices and Applications in Space–Time Trellis Codes for Relay Networks With Asynchronous Cooperative Diversity

Yue Shang and Xiang-Gen Xia, *Senior Member, IEEE*

***Abstract*—To achieve full cooperative diversity in a relay network, most of the existing space–time coding schemes require the synchronization between terminals. A family of space–time trellis codes that achieve full cooperative diversity order without the assumption of synchronization has been recently proposed. The family is based on the stack construction by Hammons and El Gamal and its generalizations by Lu and Kumar. It has been shown that the construction of such a family is equivalent to the construction of binary matrices that have full row rank no matter how their rows are shifted, where a row corresponds to a terminal (or transmit antenna) and its length corresponds to the memory size of the trellis code on that terminal. We call such matrices as shift-full-rank (SFR) matrices. A family of SFR matrices has been also constructed, but the memory sizes of the corresponding space–time trellis codes (the number of columns of SFR matrices) grow exponentially in terms of the number of terminals (the number of rows of SFR matrices), which may cause a high decoding complexity when the number of terminals is not small. In this paper, we systematically study and construct SFR matrices of any sizes for any number of terminals. Furthermore, we construct shortest (square) SFR (SSFR) matrices that correspond to space–time trellis codes with the smallest memory sizes and asynchronous full cooperative diversity. We also present some simulation results to illustrate the performances of the space–time trellis codes associated with SFR matrices in asynchronous cooperative communications.**

***Index Terms*—Asynchronous cooperative diversity, relay networks, shift equivalence, shift-full-rank (SFR) matrices, space–time coding.**

I. Introduction

RELAY networks have attracted much attention lately for combating fading, which have applications in both cellular networks and sensor networks where it is not easy to equip multiple antennas for a mobile station or sensor terminal due to size and cost limitations. For relay networks, the idea of arranging different relay terminals to communicate cooperatively to achieve spatial diversity called *cooperative diversity* has been proposed in, for example, [1]–[4]. In most of the existing protocols and space–time coding schemes for relay networks, for example, [3]–[10], in order to achieve the full cooperative diversity, the synchronization between relay terminals is assumed. However, different from a conventional multiple antenna system where multiple antennas are located at the same place and only one local oscillator is used, the individual terminals in relay networks can be geographically dispersed and respective local oscillators are used, so the cooperative diversity is asynchronous in nature. With this consideration, asynchronous cooperative diversity has been studied in, for example, [11], [12], [26], [27], [13]–[17].

Recently, in [12], [26], [27] a family of space–time trellis codes achieving full cooperative diversity without the synchronization assumption between relay terminals has been proposed. This family is based on the algebraic stack construction of space–time codes by Hammons and El Gamal [18] and its generalizations by Lu and Kumar in [19], [20]. In [12], [26], [27] it has been shown that the construction of such a family is equivalent to the construction of binary matrices that have full row rank no matter how their rows are shifted, where a row corresponds to a terminal (or transmit antenna) and its length corresponds to the memory size of the trellis code on that terminal. We call such matrices as *shift-full-rank* (SFR) matrices. A family of SFR matrices has been also constructed in [12], [26], [27] but the memory sizes of the corresponding space–time trellis codes (the number of columns of SFR matrices) grow exponentially in terms of the number of terminals (the number of rows of SFR matrices), which may cause a high decoding complexity when the number of terminals is not small.

In this paper, we systematically study and construct SFR matrices of any sizes for any number of relay terminals. Furthermore, we construct shortest (square) SFR (SSFR) matrices that correspond to space–time trellis codes with the smallest memory sizes and asynchronous full cooperative diversity. We also obtain numerous properties of SSFR matrices. We emphasize that, although our study is carried out for binary matrices (over the binary field), we shall see that most of the constructions hold over any commutative integral domain [25] (including any field). We further present some simulation results to illustrate the performances of the space–time trellis codes associated with SFR matrices in asynchronous cooperative communications.

This paper is organized as follows. In Section II, the system model is described and the results obtained in [12], [26], [27] are briefly reviewed. In Section III, some notations and symbols are first introduced and the concept of SFR matrices is then

Manuscript received March 11, 2005; revised March 1, 2006. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-05-1-0161 and the National Science Foundation under Grants CCR-0097240 and CCR-0325180.The material in this paper was presented in part at the UCSD Information Theory and Application—Inaugural Workshop, University of California at San Diego, La Jolla, CA, February 2006.

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: shang@ee.udel.edu; xxia@ee.udel.edu).

Communicated by Ø. Ytrehus, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2006.876222

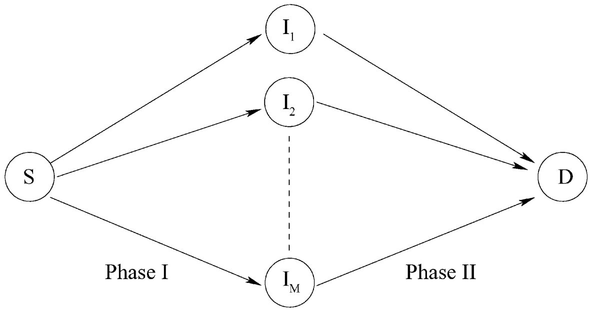

Fig. 1. System architecture.

formally defined. Some basic properties that will be used in the subsequent constructions of SFR matrices are also provided. In Sections IV and V, systematic constructions and properties of SFR matrices and SSFR matrices are presented, respectively. In Section VI, some simulation results are provided. Finally, in Section VII, this paper is concluded.

II. System Model and Problem Formulation

In this section, we first describe the system model by recalling some of the descriptions in [12], [26], [27] for this paper to be self-contained, and then briefly review the main results obtained in [12], [26], [27] which reveal the problem we are interested in. In what follows, we adopt the notations used in [12], [26], [27].

A. System Model and Asynchronous Cooperative Communications

Consider a relay network shown in Fig. 1 with $M+2$ terminals that communicate cooperatively, where S is the source terminal, D is the destination terminal, and $I_i, i=1,2,\ldots,M$, are the potential relays (intermediate terminals). The same as [3][4], we assume that there are two phases during the cooperative communication. In Phase I, S broadcasts its information to potential relays I_i, $i=1,2,\ldots,M$. In Phase II, S stops transmission, and potential relays start to transmit. In this paper, we are interested in the *decode-and-forward* approach, where the potential relay detects the source information first, and if it can successfully detect the source information, then it is enrolled in Phase II transmission.

During Phase II, relay terminal I_i first demodulates the received signal and does CRC check to see whether the detected information is correct. Assume the ones that can pass the CRC check do not have any errors in their detected information. We use $\mathcal{R}_s$ to denote the set of potential relays that can successfully detect the source information during a packet/frame from S, and use M_s to denote the cardinality of the set $\mathcal{R}_s$, i.e., $M_s=|\mathcal{R}_s|$. Then, the terminals $I_i \in \mathcal{R}_s$ will be enrolled in the transmission of Phase II. It is clear that the terminals and the number M_s of the terminals in set $\mathcal{R}_s$ depend on the channel quality between the source and the potential relays. It is usually assumed that M_s is a random variable [4]. As analyzed in [4], the protocol that relays transmit space–time coded signals on the overlapped channels performs better than the protocol that relays just repeat their detected information on the orthogonal channels. Therefore, in what follows, we assume that a space–time coded transmission is used during Phase II. In Phase II, if the enrolled relays are synchronized upto a symbol duration, the destination receives

$$y_d(n) = \sum_{\substack{I_i\in\mathcal{R}_s \\ 1\le i\le M}} h_{I_i,d}(n)x_{I_i}(n) + w_d(n), \qquad (1)$$

where $h_{I_i,d}(n)$ is the channel coefficient between I_i and the destination D, Rayleigh distributed with unit power, and assumed known at the receiver, $w_d(n)$ is the AWGN at D and has zero mean and variance σ^2 per real dimension, and $x_{I_i}(n)$ is the transmitted information symbol by I_i that is encoded based on the information $x_s(n)$ the relay terminal I_i correctly received and detected from the source S. Note that $x_s(n)$ is the same for all I_i. To achieve a spatial diversity, a channel is typically assumed to be quasi-static, i.e., $h_{I_i,d}$ keeps constant during the transmission of one packet/frame, and then changes independently in the next packet/frame. Assuming the packet/frame length is L, (1) can be written in matrix form as

$$\mathbf{y}_d = \mathbf{h}_{I,d}X_I + \mathbf{w}_d \qquad (2)$$

where $\mathbf{y}_d \in \mathbb{C}^{1\times L}$, $\mathbf{h}_{I,d} \in \mathbb{C}^{1\times M_s}$, $\mathbf{w}_d \in \mathbb{C}^{1\times L}$, and $X_I \in \mathbb{C}^{M_s\times L}$ is the space–time coded signal matrix of dimension $M_s \times L$:

$$X_I = \begin{pmatrix} x_{I_1}(1) & x_{I_1}(2) & \cdots & x_{I_1}(L) \\ x_{I_2}(1) & x_{I_2}(2) & \cdots & x_{I_2}(L) \\ \vdots & \vdots & \ddots & \vdots \\ x_{I_{M_s}}(1) & x_{I_{M_s}}(2) & \cdots & x_{I_{M_s}}(L) \end{pmatrix},$$

and different rows in X_I are transmitted by different relay terminals, and $\mathbb{C}$ is the set of all the complex numbers. There are two major differences between the conventional space–time codes [21], [28], [22] and the space–time codes in cooperative communications. One is that the number M_s of rows in X_I is a random variable instead of a constant in the conventional space–time codes which equals to the number of transmit antennas in the co-located antenna array. The other is that each row in matrix X_I may not be symbol aligned, and the relative timing errors between different relays may be random. For example, X_I can be equal to (3) shown at the top of the following page. In the following, we call X_I^a as an asynchronous version of X_I. This is due to the asynchronous nature of cooperative communications, where the transceivers are distributed in different terminals and a central local oscillator is lacking. In the above *asynchronous cooperative communication*, although the symbol synchronization is not required, we assume that each relay terminal is packet/frame synchronized, i.e., the start and the end of each packet/frame in different enrolled relays are aligned, which can be implemented by using network signaling. When a relay terminal is waiting for a packet/frame synchronizing flag, the dumb signal $\star$ is transmitted. We also assume that the relative timing errors between different relays are integer multiples of the symbol duration and a fractional timing error can be absorbed in the channel dispersion. We further assume that these relative timing errors are known at the receiver but not at the transmitter. The maximum relative timing error is assumed to be L_e. So, the actual transmitted space–time code matrix is of dimension $M_s \times L'$, where $L \le L' \le L+L_e$. In each row, totally

$$X_I^a = \begin{pmatrix} \star & x_{I_1}(1) & x_{I_1}(2) & \cdots & x_{I_1}(L) & \star & \star \\ \star & \star & x_{I_2}(1) & x_{I_2}(2) & \cdots & x_{I_2}(L) & \star \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{I_{M_s}}(1) & x_{I_{M_s}}(2) & \cdots & x_{I_{M_s}}(L) & \star & \star & \star \end{pmatrix}. \quad (3)$$

$L' - L$ dumb symbols $\star$ are padded to the beginning and/or the ending of a packet/frame transmission. Similar to the conventional space–time code design, to achieve good performance, we need to have the full *diversity order* and a good *diversity product* as shown in [21], [28], [22], while the following two differences must be considered as we mentioned previously: 1) the number of rows in the space–time code matrix is random; 2) the rows in the space–time code matrix are not symbol-aligned. The first one is, in fact, not too difficult to deal with since every space–time code of dimension $M \times L$ designed to have full diversity order, M, also has full diversity order, M_s, if any $M - M_s$ rows in X_I^a are deleted, where it is assumed that the frame/packet length $L \geq M$. However, the second difference is not easy to handle. For example, the delay diversity codes [22], [23] that are designed to ensure full diversity order in the conventional space–time codes [22] do not have the full diversity property in asynchronous cooperative communications. Also, the existing space–time block codes, for example, orthogonal space–time codes and lattice based space–time block codes, do not have the full diversity order property when the transmission is not synchronized.

B. Some of the Main Results Obtained in [12], [26], [27] and Problem Formulation

We next briefly review some of the main results obtained in [12], [26], [27], i.e., a family of space–time trellis codes that can achieve full diversity order in the asynchronous cooperative communication for any symbol-wise timing errors within a maximal range L_e. We first design the space–time trellis codes where each element in X_I is a BPSK signal based on the algebraic stack construction by Hammons and El Gamal [18], and then generalize the construction to QAM, PSK, and PAM signals by using the unified construction by Lu and Kumar [20].

When the source information bits are detected in a relay I_i, $i = 1, 2, \ldots, M$, if they are correct during a packet/frame, they are passed through a tapped delay line (or a linear shift register) with tapped coefficients $(g_{i,0}, g_{i,1}, \ldots, g_{i,\nu})$, where $g_{i,d} \in \mathbb{F}_2 \triangleq \{0, 1\}$ for $d = 1, 2, \ldots, \nu$, and ν is the maximal delay. We denote $g_i(D) \triangleq g_{i,0} + g_{i,1}D + \cdots + g_{i,\nu}D^\nu$ and $G_M(D) = (g_1(D), g_2(D), \ldots, g_M(D))$, where and in what follows D denotes the delay symbol. The coefficient matrix of $G_M(D)$ is defined as

$$G_M = \begin{pmatrix} g_{1,0} & g_{1,1} & \cdots & g_{1,\nu} \\ g_{2,0} & g_{2,1} & \cdots & g_{2,\nu} \\ \vdots & \vdots & \vdots & \vdots \\ g_{M,0} & g_{M,1} & \cdots & g_{M,\nu} \end{pmatrix}. \quad (4)$$

If the binary source information bits detected in the relays in one packet/frame is $\bar{u} \in \mathbb{F}_2^{L_u}$, then the binary output of the tapped delay lines is the set $\mathcal{C} = \{C(\bar{u}) \in \mathbb{F}_2^{M \times (\nu + L_u)} \mid C(\bar{u}) = (c_1(\bar{u}), c_2(\bar{u}), \ldots, c_M(\bar{u}))^T, \bar{u} \in \mathbb{F}_2^{L_u}\}$, where $c_i(\bar{u})$ for $i = 1, 2, \ldots, M$ is (5) shown at the bottom of the page.

Space–time code generated by $G_M(D)$ (or G_M) is defined as the set

$$\mathcal{X} = \{X_I(\bar{u}) \in \mathbb{C}^{M \times (\nu + L_u)} | (X_I(\bar{u}))_{m,n} = (-1)^{(C(\bar{u}))_{m,n}}, C(\bar{u}) \in \mathcal{C}\}.$$

In this construction, if the maximum timing error range in one packet/frame is L_e and BPSK modulation scheme is used, when the information bits in one packet/frame is L_u, the rate of the space–time code $\mathcal{X}$ generated from $G_M(D)$ is $L_u/(L_u + \nu + L_e)$ bits/s/Hz. For long packet/frame, the rate approaches 1 bit/sec/Hz. The above construction in general is the same as the one obtained by Hammons and El Gamal [18]. In [12], [26], [27], further conditions described below have been obtained on the generator matrix G_M for achieving the full diversity order in asynchronous cooperative communications.

Assuming that the relative timing error of relay I_i is k_i, i.e., k_i dumb symbols $\star$ are padded to the left of the ith row of the matrix X_I in $\mathcal{X}$ to obtain X_I^a of $\mathcal{X}^a$, the asynchronous version of $\mathcal{X}$, in (3). If dumb symbol $\star = 1 = (-1)^0$, then it is equivalent to that k_i many 0's are padded to the left of the ith row of binary matrix C in $\mathcal{C}$. These matrices can be generated by $G^a(D) = (g_1^a(D), g_2^a(D), \ldots, g_M^a(D))$, where $g_i^a(D) = D^{k_i} g_i(D)$. Correspondingly, to ensure the full diversity order

$$c_i(\bar{u}) = (u_1, u_2, \ldots, u_{L_u}) \times \begin{pmatrix} g_{i,0} & g_{i,1} & \cdots & g_{i,\nu} & 0 & \cdots & 0 \\ 0 & g_{i,0} & g_{i,1} & \cdots & g_{i,\nu} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_{i,0} & g_{i,1} & \cdots & g_{i,\nu} \end{pmatrix}_{L_u \times (\nu + L_u)}. \quad (5)$$

in the asynchronous cooperative communication, there are requirements for the tapped coefficients $g_{i,d}$, $i = 1, 2, \ldots, M$, $d = 1, 2, \ldots, \nu$, which are stated in the following theorem and the proof is given in [12], [26], [27].

Theorem 1: [12], [26], [27]: The space–time code generated by $G_M(D) = (g_1(D), g_2(D), \ldots, g_M(D))$ has full diversity order in the asynchronous cooperative communication if and only if the coefficient matrix G_M^a of any asynchronous version $G_M^a(D) = (g_1^a(D), g_2^a(D), \ldots, g_M^a(D)) = (D^{k_1} g_1(D), D^{k_2} g_2(D), \ldots, D^{k_M} g_M(D))$ of $G_M(D)$

$$G_M^a = \begin{pmatrix} \bar{g}_1^a \\ \bar{g}_2^a \\ \vdots \\ \bar{g}_M^a \end{pmatrix} = \begin{pmatrix} g_{1,0}^a & g_{1,1}^a & \cdots & g_{1,\nu+L_e}^a \\ g_{2,0}^a & g_{2,1}^a & \cdots & g_{2,\nu+L_e}^a \\ \vdots & \vdots & \vdots & \vdots \\ g_{M,0}^a & g_{M,1}^a & \cdots & g_{M,\nu+L_e}^a \end{pmatrix}$$

has full rank, M, in the binary field $\mathbb{F}_2$ for arbitrary $k_1, k_2, \ldots, k_M$, where $L_e = \max_{1 \le i \le M} k_i$.

The above result is for BPSK signals. For higher QAM, PSK and PAM signals, based on the results by Lu and Kumar in [19], [20], a general result is also obtained in [12], [26], [27].

Theorem 2: [12], [26], [27]: Let K, U be integers with $K > 0$, $U > 0$. Let

$$\{\mathcal{C}_{i,j} \,|\, 0 \le i \le U-1, 0 \le j \le K-1\}$$

be a collection of UK sets of $M \times (\nu + L_u)$ binary matrices generated by $G_M(D)$ using (5) with UK independent binary vectors $\bar{u}^{(i,j)}$ of dimension L_u. Let θ be a primitive 2^K-th root of unity. Let $\eta \in \mathbb{Z}[\theta]$, $\eta \ne 0$, such that η belongs to the ideal $2\mathbb{Z}[\theta]$ generated by 2 in $\mathbb{Z}[\theta]$. Let

$$f : \mathcal{C}_{0,0} \times \mathcal{C}_{0,1} \times \cdots \times \mathcal{C}_{U-1,K-1} \to \mathcal{X} \subset \mathbb{C}^{M \times (L_u + \nu)}$$

be the map defined by

$$(C_{0,0}, C_{0,1}, \ldots, C_{U-1,K-1}) \to \kappa \sum_{i=0}^{U-1} \eta^i \theta^{\sum_{j=0}^{K-1} 2^j C_{i,j}},$$

where κ is a nonzero complex number, $C_{i,j}$ is a matrix in the binary matrix set $\mathcal{C}_{i,j}$, and the multiplication and exponential of $C_{i,j}$ to θ are carried out entry by entry. Then, if $G_M(D)$ satisfies the condition of full diversity order in asynchronous cooperative communications in Theorem 1, then the space–time code $\mathcal{X}$ generated by the above map f also has full diversity order in asynchronous cooperative communications.

From the above results in Theorem 1 and Theorem 2, in order to construct a space–time code $\mathcal{X}$ generated by G_M in (4) with full diversity order in asynchronous cooperative communications, it suffices for us to construct a generator matrix G_M such that its any row-shifted version G_M^a has full rank. As pointed out in [12], [26], [27], to construct such matrices G_M might not be an easy task. The difficulty comes from the fact that for a flat matrix G_M such that its all row-shifted versions have full row rank, adding an additional column to G_M may not maintain the property, which is different from the conventional matrix full rankness. Despite this difficulty, in [12], [26], [27], a family of such binary matrices G_M has been constructed, where the number of columns of G_M, however, grows exponentially in terms of the number M of rows, i.e., the number of relays, of G_M, while some shorter ones for small $M = 2, 3, 4$, have been also constructed. Note that the number of columns in the generator matrix G_M determines the memory size and hence the decoding complexity of the trellis code generated by it. Therefore, the decoding complexity of the family of space–time trellis codes presented in [12], [26], [27] may be high when the number of terminals is not too small.

The main goal of this paper is to systematically study and construct matrices G_M for any sizes such that they have full row rank no matter how their rows are shifted. We also construct such shortest, i.e., square, matrices G_M that correspond to space–time trellis codes with the smallest memory sizes when M is fixed. In the following, we consider the binary case and will see that the binary case can be easily generalized to the general case of commutative integral domain. To do so, we first introduce some notations, concepts and properties of binary vectors and matrices.

III. SFR Matrices: Notations, Definitions, and Properties

Since the shifts of binary row vectors are considered here, it is necessary and convenient to use a horizontal coordinate system to characterize the shifts of binary vectors in which the position of the component with a dot underneath denotes the origin and the right to the origin is the positive direction, such as $\mathbf{v} = \ldots a\underset{\cdot}{b}cde\ldots$. In what follows, we use small case bold font letters to denote vectors over the binary field $\mathbb{F}_2$ and small case letters to denote scalars and components of a vector, such as, $\mathbf{v} = (\ldots, v_{-1}, v_0, v_1, \ldots)$, where v_i is the component of $\mathbf{v}$ at coordinate i. For example, if $\mathbf{v} = 1\underset{\cdot}{1}001$, then its components corresponding to coordinates from -1 to 3 are $v_{-1} = 1, v_0 = 1, v_1 = 0, v_2 = 0, v_3 = 1$, respectively. Furthermore, we use $\mathbf{0}$ to denote the all-zero binary vector and $\mathbf{1}$ to denote the single-component vector $\underset{\cdot}{1}$.

Definition 1: The length $l(\mathbf{v})$ of a binary row vector $\mathbf{v}$ is defined as the number of components between the most left and the most right 1's in $\mathbf{v}$, including the two 1's themselves. In particular, let $l(\mathbf{0}) = 0$ and the length of a vector with only one nonzero component is defined as 1. We define $\mathcal{S}$ to be the set of all binary row vectors with finite lengths. The weight $w(\mathbf{v})$ of $\mathbf{v}$ is defined as the number of 1's in $\mathbf{v}$ as usual.

So, $l(\mathbf{1}) = 1$ and we have $l(\mathbf{v}) = 5$ and $w(\mathbf{v}) = 3$ for the previous $\mathbf{v} = 1\underset{\cdot}{1}001$. Since padding any number of 0's to the two ends of a vector in $\mathcal{S}$ does not affect its properties in the following discussions, we do not differentiate them. For example, we treat vector $1\underset{\cdot}{1}001$ and vector $001\underset{\cdot}{1}001000$ the same.

Definition 2: For any vector $\mathbf{v} \in \mathcal{S}$, $\mathbf{v}^{R_j}$ denotes the row vector resulted from the j bits (coordinate positions) right shift of every component of $\mathbf{v}$ and simultaneously padding 0's to its two ends if needed, where, when j is negative, it means the $|j|$ bits left shift of $\mathbf{v}$.

Obviously, we have $(\mathbf{u} + \mathbf{v})^{R_i} = \mathbf{u}^{R_i} + \mathbf{v}^{R_i}$, $(a \cdot \mathbf{v})^{R_i} = a \cdot \mathbf{v}^{R_i}$, $(\mathbf{v}^{R_i})^{R_j} = \mathbf{v}^{R_{i+j}}$, $\mathbf{v} = \mathbf{u}^{R_{-i}}$ if $\mathbf{u} = \mathbf{v}^{R_i}$, and $l(\mathbf{v}) = l(\mathbf{v}^{R_i})$ for any $\mathbf{u}, \mathbf{v} \in \mathcal{S}$, $i, j \in \mathbb{Z}$ and $a \in \mathbb{F}_2$, where and herein $\cdot$ is the conventional scalar multiplication over $\mathbb{F}_2$, $+$ between two vectors in $\mathcal{S}$ is the conventional vector addition over $\mathbb{F}_2$, i.e., the component-wise addition over $\mathbb{F}_2$, and $\mathbb{Z}$ is the set of all integers. For example, the 3 bits right shift of the previous vector $\mathbf{v} = 1\underset{\cdot}{1}001$ is $\mathbf{v}^{R_3} = \underset{\cdot}{0}011001$, its -2 bits right shift is $\mathbf{v}^{R_{-2}} = 110\underset{\cdot}{0}1$, $(\mathbf{v}^{R_{-2}})^{R_3} = (\mathbf{v}^{R_3})^{R_{-2}} = \underset{\cdot}{1}1001 = \mathbf{v}^{R_1}$ and $l(\mathbf{v}^{R_3}) = l(\mathbf{v}^{R_{-2}}) = l(\mathbf{v}) = 5$.

Definition 3: For two vectors $\mathbf{u}, \mathbf{v} \in \mathcal{S}$, their vector multiplication $\circ$ is defined as their convolution, i.e., the component of $\mathbf{u} \circ \mathbf{v}$ at coordinate k is

$$\sum_i u_i \cdot v_{k-i},$$

where u_i (or v_i) denotes the component of $\mathbf{u}$ (or $\mathbf{v}$) at coordinate i. Furthermore, the ith power of the vector $\mathbf{v}$ is defined as

$$\mathbf{v}^i = \underbrace{\mathbf{v} \circ \mathbf{v} \circ \cdots \circ \mathbf{v}}_{i}$$

for $i > 0$ and we also define $\mathbf{v}^0 = \mathbf{1}$.

As a remark, an alternative expression

$$\mathbf{u} \circ \mathbf{v} = \sum_i u_i \cdot \mathbf{v}^{R_i}$$

for convolution between two vectors in $\mathcal{S}$ is sometimes helpful to understand the following constructions. There are many useful properties on convolution and some of them are listed here, which will be used in this paper.

Some Useful Properties on Multiplication (or Convolution) $\circ$

For any $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{S}$, $i, j \in \mathbb{Z}$ and $a \in \mathbb{F}_2$, we have the following.

a) Identity, commutative law, associative law, and distributive law

$$\begin{aligned} \mathbf{v}^{R_i} &= \mathbf{1}^{R_i} \circ \mathbf{v} = \mathbf{v} \circ \mathbf{1}^{R_i}, \\ \mathbf{u} \circ \mathbf{v} &= \mathbf{v} \circ \mathbf{u}, \\ (\mathbf{u} \circ \mathbf{v}) \circ \mathbf{w} &= \mathbf{u} \circ (\mathbf{v} \circ \mathbf{w}), \\ \mathbf{u} \circ (\mathbf{v} + \mathbf{w}) &= \mathbf{u} \circ \mathbf{v} + \mathbf{u} \circ \mathbf{w}, && (6) \\ (a \cdot \mathbf{u}) \circ \mathbf{v} &= \mathbf{u} \circ (a \cdot \mathbf{v}) = a \cdot (\mathbf{u} \circ \mathbf{v}). && (7) \end{aligned}$$

b) If $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{v} \neq \mathbf{0}$, then

$$l(\mathbf{u} \circ \mathbf{v}) = l(\mathbf{u}) + l(\mathbf{v}) - 1. \tag{8}$$

Hence,

$$\begin{aligned} &\mathbf{u} \circ \mathbf{v} \neq \mathbf{0} \quad \text{if } \mathbf{u} \neq \mathbf{0} \quad \text{and} \quad \mathbf{v} \neq \mathbf{0}, && (9) \\ &\mathbf{u} \circ \mathbf{w} = \mathbf{v} \circ \mathbf{w}, \quad \mathbf{w} \neq \mathbf{0} \quad \text{imply } \mathbf{u} = \mathbf{v}. && (10) \end{aligned}$$

c) For two shifted vectors

$$\mathbf{u}^{R_i} \circ \mathbf{v}^{R_j} = (\mathbf{u} \circ \mathbf{v})^{R_{i+j}}. \tag{11}$$

d) If either $\mathbf{u}$ or $\mathbf{v}$ is of even weight, $\mathbf{u} \circ \mathbf{v}$ is of even weight. If both $\mathbf{u}$ and $\mathbf{v}$ are of odd weight, $\mathbf{u} \circ \mathbf{v}$ is of odd weight. Furthermore, $\mathbf{v}^i$ is of odd weight (or even weight) if $\mathbf{v}$ is of odd weight (or even weight) for $i \geq 1$.

The above property c) follows from

$$\begin{aligned} \mathbf{u}^{R_i} \circ \mathbf{v}^{R_j} &= \mathbf{u} \circ \mathbf{1}^{R_i} \circ \mathbf{v} \circ \mathbf{1}^{R_j} \\ &= (\mathbf{u} \circ \mathbf{v}) \circ \mathbf{1}^{R_{i+j}} = (\mathbf{u} \circ \mathbf{v})^{R_{i+j}} \end{aligned}$$

and the property d) is because there is always an even difference between $w(\mathbf{u} \circ \mathbf{v})$ and $w(\mathbf{u})w(\mathbf{v})$. The above properties imply that the set $\mathcal{S}$ with the vector addition $(+)$ and the vector multiplication $(\circ)$ is a commutative integral domain [25] with the additive identity $\mathbf{0}$ and the multiplicative identity $\mathbf{1}$. As we know, convolution of two vectors in $\mathcal{S}$ is equivalent to product of their corresponding polynomials, so $(\mathcal{S}, +, \circ)$ is equivalent to the polynomial ring[1] over $\mathbb{F}_2$. In fact, our general constructions of SFR matrices to be presented later can also be illustrated by the polynomials over the polynomial ring, but since the expression of vectors in $(\mathcal{S}, +, \circ)$ is more intuitive and explicit in forming a matrix, we adopt the latter in the following discussions.

Similar to some concepts of polynomials, we define divisions and factorizations over $(\mathcal{S}, +, \circ)$ as follows. Let $\mathbf{u}, \mathbf{v} \in \mathcal{S}$. If there is an $\mathbf{x} \in \mathcal{S}$ such that $\mathbf{v} = \mathbf{u} \circ \mathbf{x}$, $\mathbf{v}$ is said to be a multiple of $\mathbf{u}$, and $\mathbf{u}$ is said to be a divisor of $\mathbf{v}$ or to divide $\mathbf{v}$. We write $\mathbf{u}|\mathbf{v}$ when $\mathbf{u}$ divides $\mathbf{v}$, otherwise $\mathbf{u} \nmid \mathbf{v}$, and $\frac{\mathbf{v}}{\mathbf{u}} = \mathbf{x}$ when $\mathbf{u} \,|\, \mathbf{v}$. Obviously, we have $\mathbf{1} \,|\, \mathbf{v}$, $\mathbf{v} \,|\, \mathbf{v}$ for all $\mathbf{v} \in \mathcal{S}$, and $\mathbf{u} \,|\, \mathbf{v}^{R_j}$ if $\mathbf{u} \,|\, \mathbf{v}$ for any $j \in \mathbb{Z}$. For given vectors $\mathbf{u}, \mathbf{v} \in \mathcal{S}$, we can directly check whether $\mathbf{u} \,|\, \mathbf{v}$ or $\mathbf{u} \nmid \mathbf{v}$ by using their corresponding polynomials.

Definition 4: A *shift linear combination* of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathcal{S}$ is defined as

$$a_1 \cdot \mathbf{v}_1^{R_{j_1}} + a_2 \cdot \mathbf{v}_2^{R_{j_2}} + \cdots + a_n \cdot \mathbf{v}_n^{R_{j_n}},$$

where $a_i \in \mathbb{F}_2$ and $j_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$. Furthermore, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ are called *shift linearly independent* if

$$a_1 \cdot \mathbf{v}_1^{R_{j_1}} + a_2 \cdot \mathbf{v}_2^{R_{j_2}} + \cdots + a_n \cdot \mathbf{v}_n^{R_{j_n}} \neq \mathbf{0}$$

for any $a_1, a_2, \ldots, a_n \in \mathbb{F}_2$, not all zero, and any $j_1, j_2, \ldots, j_n \in \mathbb{Z}$; otherwise, they are called *shift linearly dependent*.

Definition 5: A matrix formed as $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \ldots, \mathbf{r}_n^T]^T$ with $\mathbf{r}_i \in \mathcal{S}$ as its ith row is called shift-full-rank (SFR) if all of its row vectors are shift linearly independent.

Since we treat vectors from adding zeros to the two ends the same, we also treat their corresponding matrices the same. For example, we do not differentiate the following matrices

$$G_1 = \begin{pmatrix} \underset{\cdot}{1} & 0 & 0 & 0 \\ \underset{\cdot}{1} & 1 & 0 & 0 \\ \underset{\cdot}{1} & 1 & 1 & 1 \end{pmatrix} \quad \text{and}$$

$$G_2 = \begin{pmatrix} 0 & \underset{\cdot}{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \underset{\cdot}{1} & 1 & 0 & 0 & 0 & 0 \\ 0 & \underset{\cdot}{1} & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

which certainly have the same SFR property, i.e., either both are SFR or neither is. Furthermore, since the shift linear independence/dependence of n vectors belonging to $\mathcal{S}$ implies the same

[1] This polynomial ring is slightly different from the conventional polynomial ring over the binary field, since negative exponent terms are allowed in its elements, i.e., polynomials. For example, the corresponding polynomial of vector $\mathbf{v} = 1\underset{\cdot}{1}001$ is $f_{\mathbf{v}}(x) = x^{-1} + 1 + x^3$. However, the set of such polynomials corresponding to the vectors of finite lengths is still a ring (furthermore, a commutative integral domain) under the polynomial addition and the polynomial multiplication.

property for their shifted versions and a permutation of rows in a matrix does not affect its SFR, matrices

$$G_1 = \begin{pmatrix} \underset{\cdot}{1} & 0 & 0 & 0 \\ \underset{\cdot}{1} & 1 & 0 & 0 \\ \underset{\cdot}{1} & 1 & 1 & 1 \end{pmatrix} \quad \text{and}$$

$$G_3 = \begin{pmatrix} \underset{\cdot}{0} & 0 & 1 & 1 & 1 & 1 \\ \underset{\cdot}{1} & 0 & 0 & 0 & 0 & 0 \\ \underset{\cdot}{0} & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

have the same SFR property too. With this observation, we give the definition of shift equivalence.

Definition 6: Two matrices $A = [\mathbf{a}_1^T, \mathbf{a}_2^T, \ldots, \mathbf{a}_n^T]^T$ and $B = [\mathbf{b}_1^T, \mathbf{b}_2^T, \ldots, \mathbf{b}_n^T]^T$ of the same number of rows are called *shift equivalent* if there exist integers $j_1, j_2, \ldots, j_n$ such that

$$\mathbf{b}_{\sigma(i)} = \mathbf{a}_i^{R_{j_i}}, \quad i = 1, 2, \ldots, n,$$

where σ is a permutation on the set $\{1, 2, \ldots, n\}$. We denote this relationship by $A \backsim B$. Furthermore, a *class* of shift equivalent matrices (or a *shift equivalent class*) means a collection of matrices in which every pair of matrices is shift equivalent.

As an example, the above G_1 and G_3 are shift equivalent, i.e., $G_1 \backsim G_3$. It is not hard to see that, for a class of shift equivalent matrices, it is sufficient for us to only consider the SFR property of any one matrix representative in it. Therefore, for convenience, we next define matrix representatives which have the most compact forms with respect to the number of columns and, without loss of generality, we only consider them in the following discussions. To do so, we first define a subset of $\mathcal{S}$, which will be useful by itself alone later.

Definition 7: We define $\mathcal{T}$ to be the set of all the vectors in $\mathcal{S}$ with their most left 1's located at the origin, i.e., $\mathcal{T} = \{\ldots 0\underset{\cdot}{1}abc \ldots \,|\, a, b, c, \ldots \in \mathbb{F}_2\}$.

So, $\mathbf{0} \notin \mathcal{T}$ and $(\mathcal{T}, \circ)$ is a commutative semi-group with the identity $\mathbf{1}$ because it is closed under the vector multiplication. Moreover, if $\mathbf{u}, \mathbf{v} \in \mathcal{T}$, we have $\frac{\mathbf{v}}{\mathbf{u}} \in \mathcal{T}$ if $\mathbf{u} \,|\, \mathbf{v}$, and $\mathbf{u} \circ \mathbf{v} \neq \mathbf{1}$ unless $\mathbf{u} = \mathbf{v} = \mathbf{1}$. However, we can easily find an example such that $\mathbf{u} \circ \mathbf{v} \in \mathcal{T}$ with $\mathbf{u}, \mathbf{v} \notin \mathcal{T}$, such as, $\mathbf{u} = 1\underset{\cdot}{1}1$ and $\mathbf{v} = \underset{\cdot}{0}11$. Constrained in $(\mathcal{T}, \circ)$, we let $\mathbf{d} = \gcd(\mathbf{u}, \mathbf{v}) \in \mathcal{T}$ denote the greatest common divisor of $\mathbf{u}, \mathbf{v} \in \mathcal{T}$. A useful property is that, for $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{T}$, $\mathbf{u} | \mathbf{v} \circ \mathbf{w}$ and $\gcd(\mathbf{u}, \mathbf{w}) = \mathbf{1}$ imply $\mathbf{u} | \mathbf{v}$.

Definition 8: We call a matrix G as of *standard form* if all of its row vectors belong to $\mathcal{T}$ and there is no all-zero columns at its two ends.

In the above example, G_1 is of standard form but G_2 and G_3 are not. Notice that the shift equivalence between two matrices of standard form only means that there is a row permutation between them, i.e., $\mathbf{b}_{\sigma(i)} = \mathbf{a}_i$ in Definition 6. In what follows, for convenience, the dots denoting the coordinate origin at the first column of a matrix of standard form will be omitted. With the above discussions, the following lemma is straightforward.

Lemma 1: Any binary matrix without all-zero rows must be shift equivalent to a binary matrix of standard form.

With this result, for the shift-full rankness, we only need to study matrices of standard form.

Definition 9: Given a vector $\mathbf{v} \in \mathcal{S}$ and a matrix $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \ldots, \mathbf{r}_n^T]^T$, their multiplication (or convolution) $\circ$ is defined as $\mathbf{v} \circ G = [(\mathbf{v} \circ \mathbf{r}_1)^T, (\mathbf{v} \circ \mathbf{r}_2)^T, \ldots, (\mathbf{v} \circ \mathbf{r}_n)^T]^T$.

For any two vectors $\mathbf{v}, \mathbf{v}' \in \mathcal{S}$ such that $\mathbf{v} = (\mathbf{v}')^{R_j}$ for some integer j and any two matrices G and G' such that $G \backsim G'$, from (11), we have

$$\mathbf{v} \circ G \backsim \mathbf{v}' \circ G'. \tag{12}$$

We now present a lemma that plays an important role for the constructions of SFR matrices later in this paper.

Lemma 2: Let $\mathbf{0} \neq \mathbf{v} \in \mathcal{S}$ and $\tilde{G} = \mathbf{v} \circ G$. Then, $\tilde{G}$ is an SFR matrix if and only if G is an SFR matrix.

Proof: Let us prove the "if" part first. Assume $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \ldots, \mathbf{r}_n^T]^T$, then $\tilde{G} = [\tilde{\mathbf{r}}_1^T, \tilde{\mathbf{r}}_2^T, \ldots, \tilde{\mathbf{r}}_n^T]^T$ with $\tilde{\mathbf{r}}_i = \mathbf{v} \circ \mathbf{r}_i$. For any nonzero shift linear combination $\sum_{i=1}^n a_i \cdot \tilde{\mathbf{r}}_i^{R_{j_i}}$ of $\tilde{\mathbf{r}}_i$ with any $j_i \in \mathbb{Z}$ and $a_i \in \mathbb{F}_2$, not all zero, $i = 1, 2, \ldots, n$, we have

$$\begin{aligned} \sum_{i=1}^n a_i \cdot \tilde{\mathbf{r}}_i^{R_{j_i}} &= \sum_{i=1}^n a_i \cdot (\mathbf{v} \circ \mathbf{r}_i)^{R_{j_i}} \\ &= \sum_{i=1}^n a_i \cdot \left(\mathbf{v} \circ \mathbf{r}_i^{R_{j_i}}\right) && (13) \\ &= \sum_{i=1}^n \mathbf{v} \circ \left(a_i \cdot \mathbf{r}_i^{R_{j_i}}\right) && (14) \\ &= \mathbf{v} \circ \left(\sum_{i=1}^n a_i \cdot \mathbf{r}_i^{R_{j_i}}\right) && (15) \end{aligned}$$

where (13) follows from (11), (14) follows from (7) and (15) follows from (6). Since G is SFR, we know $\sum_{i=1}^n a_i \cdot \mathbf{r}_i^{R_{j_i}} \neq \mathbf{0}$. From (9) and $\mathbf{v} \neq \mathbf{0}$, we have

$$\sum_{i=1}^n a_i \cdot \tilde{\mathbf{r}}_i^{R_{j_i}} = \mathbf{v} \circ \left(\sum_{i=1}^n a_i \cdot \mathbf{r}_i^{R_{j_i}}\right) \neq \mathbf{0}.$$

Hence $\tilde{G}$ is an SFR matrix. The "only if" part holds obviously from the above proof. □

As a remark, although this lemma is mainly for the proof of the constructions for SFR matrices in next sections, it is also an important method by itself to generate new SFR matrices based on all the SFR matrices to be constructed later.

IV. SFR Matrices: General Construction

In this section, a general construction of binary SFR matrices based on known SFR matrices is first presented. Then, two special and simplified constructions are provided, which are partially used to illustrate the repetitions in the general construction. Finally, an important result that SFR matrix exists for any desired size (the number of columns is, of course, no less than the number of rows) is constructively proved.

It is clear that any nonzero vector $\mathbf{v} \in \mathcal{S}$ is an SFR matrix by itself. Matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is also an SFR matrix. Now, given any initial SFR matrix G_0 with n_0 rows, we construct a matrix with n_0+n-1 rows by

$$G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i} = \begin{pmatrix} \bar{\mathbf{v}}_{n-1} \\ \mathbf{v}_{n-1}\circ\bar{\mathbf{v}}_{n-2} \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\bar{\mathbf{v}}_{n-3} \\ \vdots \qquad \ddots \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\bar{\mathbf{v}}_2 \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\bar{\mathbf{v}}_1 \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\mathbf{v}_1\circ G_0 \end{pmatrix} \tag{16}$$

for $\forall n \geq 1$, where $\mathbf{v}_i, \bar{\mathbf{v}}_i$ can be any nonzero vectors in $\mathcal{S}$ such that $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$, $i=1,2,\ldots,n-1$. In particular, when $G_0=\mathbf{v}_0\neq\mathbf{0}\in\mathcal{S}$ and then $n_0=1$, we write $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}=G_n^{\mathbf{v}_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$. The requirement of $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$ to ensure the SFR property of $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ will be clear in the Proof of Theorem 3.

Therefore, we need at most $2n-2$ nonzero vectors, not necessarily different, and an known SFR matrix to construct such a general matrix in (16). Obviously, $\mathbf{v}_i \neq \mathbf{1}$ since $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$. If we use $\mathbf{r}_i$ to denote the ith row vector of $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}=[\mathbf{r}_1^T,\mathbf{r}_2^T,\ldots,\mathbf{r}_{n_0+n-1}^T]^T$, we have

$$\mathbf{r}_i=\mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\cdots\circ\mathbf{v}_{n-i+1}\circ\bar{\mathbf{v}}_{n-i}$$

for $1\leq i\leq n-1$ and

$$\mathbf{r}_i=\mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\cdots\circ\mathbf{v}_1\circ\mathbf{r}_{i-n+1}^{G_0}$$

for $n\leq i\leq n_0+n-1$, where $\mathbf{r}_j^{G_0}$ is the jth row of G_0 and $\mathbf{r}_1^{G_0}=\mathbf{v}_0$ if $G_0=\mathbf{v}_0\neq\mathbf{0}\in\mathcal{S}$.

Lemma 3: If $G_0' \backsim G_0$ and $\mathbf{v}_i'$ and $\bar{\mathbf{v}}_i'$ are the shifted versions of $\mathbf{v}_i$ and $\bar{\mathbf{v}}_i$, $i=1,2,\ldots,n-1$, respectively, then $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i} \backsim G_{n_0+n-1}^{G_0',\mathbf{v}_i',\bar{\mathbf{v}}_i'}$.

Proof: This follows easily from (11) and (12). □

This lemma tells us that we only need to consider the case that $\mathbf{v}_i,\bar{\mathbf{v}}_i\in\mathcal{T}$ and G_0 is of standard form in the following discussions and hence the shift equivalence is only limited to a row permutation. We next prove that $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ in (16) is an SFR matrix.

Theorem 3: Any matrix $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ constructed in (16) with an initial SFR matrix G_0 of standard form and $\mathbf{v}_i,\bar{\mathbf{v}}_i\in\mathcal{T}$ such that $\mathbf{v}_i\nmid\bar{\mathbf{v}}_i$, $i=1,2,\ldots,n-1$, is an SFR matrix of standard form.

Proof: We prove this theorem by induction on n. It is obvious that the result holds for $n=1$.

Assume the result holds for $G_{n_0+n-2}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$, i.e.,

$$\begin{pmatrix} \bar{\mathbf{v}}_{n-2} \\ \mathbf{v}_{n-2}\circ\bar{\mathbf{v}}_{n-3} \\ \vdots \\ \mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\bar{\mathbf{v}}_2 \\ \mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\bar{\mathbf{v}}_1 \\ \mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\mathbf{v}_1\circ G_0 \end{pmatrix}$$

is an SFR matrix for any $\mathbf{v}_i,\bar{\mathbf{v}}_i\in\mathcal{T}$ such that $\mathbf{v}_i\nmid\bar{\mathbf{v}}_i$, $i=1,2,\ldots,n-2$. Consider matrix $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$.

For the last n_0+n-2 rows $\mathbf{r}_2,\mathbf{r}_3,\ldots,\mathbf{r}_{n_0+n-1}$ of $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$, we have

$$\begin{pmatrix} \mathbf{r}_2 \\ \mathbf{r}_3 \\ \vdots \\ \mathbf{r}_{n_0+n-3} \\ \mathbf{r}_{n_0+n-2} \\ \mathbf{r}_{n_0+n-1} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_{n-1}\circ\bar{\mathbf{v}}_{n-2} \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\bar{\mathbf{v}}_{n-3} \\ \vdots \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\bar{\mathbf{v}}_2 \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\bar{\mathbf{v}}_1 \\ \mathbf{v}_{n-1}\circ\mathbf{v}_{n-2}\circ\mathbf{v}_{n-3}\circ\cdots\circ\mathbf{v}_2\circ\mathbf{v}_1\circ G_0 \end{pmatrix} = \mathbf{v}_{n-1}\circ G_{n_0+n-2}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}.$$

From the assumption that $G_{n_0+n-2}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ is an SFR matrix and Lemma 2, matrix $[\mathbf{r}_2^T,\mathbf{r}_3^T,\ldots,\mathbf{r}_{n_0+n-1}^T]^T$ is also an SFR matrix, i.e., $\mathbf{r}_2,\mathbf{r}_3,\ldots,\mathbf{r}_{n_0+n-1}$ are shift linearly independent. Furthermore, since every $\mathbf{r}_i$ contains a divisor $\mathbf{v}_{n-1}$ for $i=2,3,\ldots,n_0+n-1$, their shift linear combination has the form of $\mathbf{v}_{n-1}\circ\mathbf{v}'$ by (15), where $\mathbf{0}\neq\mathbf{v}'\in\mathcal{S}$ is the corresponding shift linear combination of the row vectors in $G_{n_0+n-2}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$. If $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ is not SFR, i.e., $\mathbf{r}_1,\mathbf{r}_2,\ldots,\mathbf{r}_{n_0+n-1}$ are shift linearly dependent, then there exist $a_i\in\mathbb{F}_2$, not all zero, and $j_i\in\mathbb{Z}$ such that $a_1\cdot\mathbf{r}_1^{R_{j_1}}+a_2\cdot\mathbf{r}_2^{R_{j_2}}+\cdots+a_{n_0+n-1}\cdot\mathbf{r}_{n_0+n-1}^{R_{j_{n_0+n-1}}}=\mathbf{0}$. Since $\mathbf{r}_2,\ldots,\mathbf{r}_{n_0+n-1}$ are shift linearly independent as we have proved, we have $a_1=1$. Thus, by the above argument, we have $\mathbf{r}_1=\mathbf{v}_{n-1}\circ\mathbf{v}'$ or $\bar{\mathbf{v}}_{n-1}=\mathbf{v}_{n-1}\circ\mathbf{v}'$ for some $\mathbf{0}\neq\mathbf{v}'\in\mathcal{S}$, which contradicts with construction condition $\mathbf{v}_{n-1}\nmid\bar{\mathbf{v}}_{n-1}$. Consequently, all the n_0+n-1 rows of $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ are shift linearly independent, i.e., $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ is an SFR matrix.

Thus, we have completed the proof by induction. □

The basic idea underlying this construction is that from one known SFR matrix G_0, we can generate a new SFR matrix with one more row by first convoluting G_0 by a nonzero vector $\mathbf{v}\in\mathcal{S}$ and then adding a nonzero row vector $\bar{\mathbf{v}}\in\mathcal{S}$ such that $\mathbf{v}\nmid\bar{\mathbf{v}}$ into the matrix, i.e., the basic building block has the form[2]

$$\begin{pmatrix} \bar{\mathbf{v}} \\ \mathbf{v}\circ G_0 \end{pmatrix}.$$

Then we can repeat this process to obtain more new SFR matrices with higher dimensions.

The selection of $\mathbf{v}_i$ and $\bar{\mathbf{v}}_i$ in the construction (16) is arbitrary. We can choose them such that $l(\bar{\mathbf{v}}_i)<l(\mathbf{v}_i)$ for large $l(\mathbf{v}_i)$ or choose odd weight $\bar{\mathbf{v}}_i$ while $\mathbf{v}_i$ is of even weight by Property d). By (8), it is not difficult for us to calculate the number of possible

[2] For its generalization to a commutative integral domain $\mathcal{D}$, the condition $\mathbf{v}\nmid\bar{\mathbf{v}}$ is changed to $\mathbf{v}\nmid a\cdot\bar{\mathbf{v}}$ for any $0\neq a\in\mathcal{D}$, when $\mathcal{D}$ is not a field. If $\mathcal{D}$ is a field, the condition $\mathbf{v}\nmid\bar{\mathbf{v}}$ does not need to be changed.

$\bar{\mathbf{v}}_i \in \mathcal{T}$ of length l such that $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$ for a given $\mathbf{v}_i \in \mathcal{T}$, which is

$$N_l^{\bar{\mathbf{v}}_i:\mathbf{v}_i} = \begin{cases} 1, & l = 1 \\ 2^{l-2}, & 1 < l < l(\mathbf{v}_i) \\ 2^{l-2} - 1, & l = l(\mathbf{v}_i) \\ 2^{l-2} - 2^{l-l(\mathbf{v}_i)-1}, & l > l(\mathbf{v}_i) \end{cases}$$

for $l(\mathbf{v}_i) \geq 2$. Therefore, $\mathbf{v}_i$ and $\bar{\mathbf{v}}_i$ can be of any lengths unless $l(\mathbf{v}_i) = l(\bar{\mathbf{v}}_i) = 2$ and we can get infinite SFR matrices of standard form for any given number of rows. However, there also exist a lot of repetitions for this construction which we will illustrate by two examples later.

Since an initial SFR matrix and $2n - 2$ nonzero vectors are needed to construct a $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$, which is somewhat complex, we give the following two special cases to simplify the construction. First, let $G_0 = \mathbf{v}_0 \in \mathcal{T}$, $\mathbf{v}_1 = \mathbf{v}_2 = \cdots = \mathbf{v}_{n-1} = \mathbf{v} \in \mathcal{T}$ and then choose $\bar{\mathbf{v}}_i \in \mathcal{T}$ such that $\mathbf{v} \nmid \bar{\mathbf{v}}_i$ in (16) for $i = 1, 2, \ldots, n-1$. The number of vectors needed in this construction is now reduced to $n + 1$ and we denote the resulted matrices of this form by $G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i}$, i.e.,

$$G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i} = \begin{pmatrix} \mathbf{v}^0 \circ \bar{\mathbf{v}}_{n-1} \\ \mathbf{v}^1 \circ \bar{\mathbf{v}}_{n-2} \\ \vdots \\ \mathbf{v}^{n-2} \circ \bar{\mathbf{v}}_1 \\ \mathbf{v}^{n-1} \circ \mathbf{v}_0 \end{pmatrix} \tag{17}$$

which will be discussed in details in next section for more properties. Furthermore, let $\mathbf{v}_0 = \bar{\mathbf{v}}_i = \mathbf{1}$ in $G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i}$ for $i = 1, 2, \ldots, n-1$ and we denote such matrices, which only need one vector, by $G_n^{\mathbf{v}}$ and the corresponding matrix system for a given $\mathbf{v}$ and different n by $\{G_n^{\mathbf{v}}\}_{n\geq 1}$ or $\{G_n^{\mathbf{v}}\}$, i.e.,

$$G_n^{\mathbf{v}} = \begin{pmatrix} \mathbf{v}^0 \\ \mathbf{v}^1 \\ \mathbf{v}^2 \\ \vdots \\ \mathbf{v}^{n-1} \end{pmatrix} \tag{18}$$

where $\mathbf{1} \neq \mathbf{v} \in \mathcal{T}$ and $\mathbf{v}^i$ is the ith power of $\mathbf{v}$. From Theorem 3, we have the following corollary.

Corollary 1: For any vector $\mathbf{v} \in \mathcal{S}$, if its length is above 1, i.e., $l(\mathbf{v}) > 1$, then matrix $G_n^{\mathbf{v}}$ defined in (18) is an SFR matrix.

Proof: For any vector $\mathbf{v} \in \mathcal{S}$ with $l(\mathbf{v}) > 1$, we know $\mathbf{v} \nmid \mathbf{1}$. Then, this corollary follows from the above discussions and Theorem 3. □

From the above corollary, we can see that one vector in $\mathcal{S}$ is enough to construct SFR matrices for any number of rows. On the other hand, if $\mathbf{v}, \mathbf{v}' \in \mathcal{S}$ such that $\mathbf{v}' = \mathbf{v}^m$ for some $m > 1$, then $G_n^{\mathbf{v}'}$ is a submatrix of $G_{(n-1)m+1}^{\mathbf{v}}$ and its rows are the rows $\mathbf{r}_1, \mathbf{r}_{m+1}, \mathbf{r}_{2m+1}, \ldots, \mathbf{r}_{(n-1)m+1}$ of $G_{(n-1)m+1}^{\mathbf{v}}$ for any $n \geq 1$ because of the form in (18). Besides this repetition, other repetitions also exist in the general construction (16). Let us see two examples.

Example 1: This is an example in which we obtain the same $G_n^{\mathbf{v}_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ from different $\mathbf{v}_0, \mathbf{v}_i$, and $\bar{\mathbf{v}}_i$. If $\mathbf{u}_i = \mathbf{u}, \mathbf{v}_i = \mathbf{v} \in \mathcal{T}$ such that $\mathbf{v} \nmid \mathbf{u}^i$ and $\mathbf{u} \nmid \mathbf{v}^i$ for $\forall i \geq 1$, let $\mathbf{u}_0 = \mathbf{v}^{n-1}$, $\mathbf{v}_0 = \mathbf{u}^{n-1}$, $\bar{\mathbf{u}}_i = \mathbf{v}^{n-1-i}$, $\bar{\mathbf{v}}_i = \mathbf{u}^{n-1-i}$ and $\mathbf{w} = \mathbf{u} \circ \mathbf{v}$, then the following SFR matrices:

$$G_n^{\mathbf{u}_0,\mathbf{u},\bar{\mathbf{u}}_i} = \begin{pmatrix} \mathbf{u}^0 \circ \mathbf{v}^0 \\ \mathbf{u}^1 \circ \mathbf{v}^1 \\ \mathbf{u}^2 \circ \mathbf{v}^2 \\ \vdots \\ \mathbf{u}^{n-1} \circ \mathbf{v}^{n-1} \end{pmatrix}$$

$$G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i} = \begin{pmatrix} \mathbf{v}^0 \circ \mathbf{u}^0 \\ \mathbf{v}^1 \circ \mathbf{u}^1 \\ \mathbf{v}^2 \circ \mathbf{u}^2 \\ \vdots \\ \mathbf{v}^{n-1} \circ \mathbf{u}^{n-1} \end{pmatrix}$$

$$G_n^{\mathbf{w}} = \begin{pmatrix} \mathbf{w}^0 \\ \mathbf{w}^1 \\ \mathbf{w}^2 \\ \vdots \\ \mathbf{w}^{n-1} \end{pmatrix}$$

with the forms in (17) or (18) are the same. An example of such a pair of vectors is $\mathbf{1} \neq \mathbf{u}, \mathbf{v} \in \mathcal{T}$ such that $\mathbf{u} = \mathbf{v} + \mathbf{1}^{R_j}$ for some integer $j > 0$. A simple proof is as follows. Expanding $\mathbf{u}^i$ in terms of $\mathbf{v}$ and $\mathbf{1}^{R_j}$, we have

$$\begin{aligned} \mathbf{u}^i = (\mathbf{v} + \mathbf{1}^{R_j})^i &= \sum_{k=1}^{i} \binom{i}{k} \mathbf{v}^{i-k} \circ (\mathbf{1}^{R_j})^k \\ &= \sum_{k=1}^{i-1} \binom{i}{k} \mathbf{v}^{i-k} \circ \mathbf{1}^{R_{jk}} + \mathbf{1}^{R_{ji}} \end{aligned}$$

for $i \geq 1$. All terms except the last one in the above expression are the multiples of $\mathbf{v}$ and hence $\mathbf{v} \nmid \mathbf{u}^i$; Similarly, $\mathbf{u} \nmid \mathbf{v}^i$ since $\mathbf{v} = \mathbf{u} + \mathbf{1}^{R_j}$.

Notice that another fact we can obtain from this example is that $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$ in Theorem 3 is just a sufficient, but not necessary, condition for the matrix in (16) to be SFR, i.e., $\mathbf{v}_i | \bar{\mathbf{v}}_i$ doesn't imply that $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ is not an SFR matrix. For example, if we let $\mathbf{u} = \mathbf{v}$ instead of $\mathbf{v} \nmid \mathbf{u}^i$ in the above example, then, $G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i} = G_n^{\mathbf{v}^2}$ that is an SFR matrix by Corollary 1.

Example 2: In Example 1, the same matrix is obtained from totally different $(G_0, \mathbf{v}_i, \bar{\mathbf{v}}_i)$'s. We now illustrate that we can also get the same matrix from the same initial SFR matrix G_0 but different $(\mathbf{v}_i, \bar{\mathbf{v}}_i)$'s. Let $\mathbf{v}_1, \mathbf{v}_2, \bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2 \in \mathcal{T}$ such that $\gcd(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{1}$, $\mathbf{v}_1 | \bar{\mathbf{v}}_2$, and $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$, $i = 1, 2$. Assume $\bar{\mathbf{v}}_2 = \mathbf{v}_1 \circ \bar{\mathbf{v}}_2'$ with $\bar{\mathbf{v}}_2' \in \mathcal{T}$. Then, $\mathbf{v}_2 \nmid \bar{\mathbf{v}}_2'$ since $\mathbf{v}_2 \nmid \bar{\mathbf{v}}_2$, and $\mathbf{v}_1 \nmid \bar{\mathbf{v}}_1 \circ \mathbf{v}_2$ since $\mathbf{v}_1 \nmid \bar{\mathbf{v}}_1$ and $\gcd(\mathbf{v}_1, \mathbf{v}_2) = \mathbf{1}$. Thus, a pair of shift equivalent matrices in the sense of a row permutation can be obtained from G_0 by $(\mathbf{v}_1, \mathbf{v}_2, \bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2)$ and $(\mathbf{v}_2, \mathbf{v}_1, \bar{\mathbf{v}}_2', \bar{\mathbf{v}}_1 \circ \mathbf{v}_2)$, respectively, i.e.,

$$\begin{pmatrix} \bar{\mathbf{v}}_2 \\ \mathbf{v}_2 \circ \bar{\mathbf{v}}_1 \\ \mathbf{v}_2 \circ \mathbf{v}_1 \circ G_0 \end{pmatrix} \backsim \begin{pmatrix} \bar{\mathbf{v}}_1 \circ \mathbf{v}_2 & \\ \mathbf{v}_1 & \circ \bar{\mathbf{v}}_2' \\ \mathbf{v}_1 & \circ \mathbf{v}_2 \circ G_0 \end{pmatrix}.$$

We can easily find a lot of such 4-tuples and an example is $(\mathbf{v}_1, \mathbf{v}_2, \bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2) = (\underset{\cdot}{1}1, \underset{\cdot}{1}11, \underset{\cdot}{1}, \underset{\cdot}{1}01)$.

Let us now derive the existence of SFR matrices by construction.

Lemma 4: Let $\mathbf{v}_0, \mathbf{v}, \bar{\mathbf{v}}_i \in \mathcal{T}$ for $i = 1, 2, \ldots, n-1$. Then matrix $G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i}$ in (17) (also $G_n^{\mathbf{v}}$ in (18)) is of standard form and $G_n^{\mathbf{v}}$ has size $n \times (1 + (n-1)(l(\mathbf{v}) - 1))$.

Proof: The first part that $G_n^{\mathbf{v}_0,\mathbf{v},\bar{\mathbf{v}}_i}$ and $G_n^{\mathbf{v}}$ are of standard form follows from the fact that $\mathcal{T}$ is closed under the vector multiplication. From (8), we know the length of the ith row of $G_n^{\mathbf{v}}$ is $l(\mathbf{v}^{i-1}) = l(\mathbf{v}^{i-2}) + l(\mathbf{v}) - 1 = l(\mathbf{v}^{i-3}) + 2(l(\mathbf{v}) - 1) = \cdots = l(\mathbf{v}^0) + (i-1)(l(\mathbf{v}) - 1) = 1 + (i-1)(l(\mathbf{v}) - 1)$ for $i \geq 1$. Since the length of every row is increasing, the number of columns of $G_n^{\mathbf{v}}$ is $l(\mathbf{v}^{n-1}) = 1 + (n-1)(l(\mathbf{v}) - 1)$. □

The following lemma is obvious from the definitions of shift linear combination and shift linear independence.

Lemma 5: If G is an SFR matrix, the matrix obtained by replacing any number of rows in G by their nonzero shift linear combination is also an SFR matrix.

A special case for Lemma 5 is that we can construct a new SFR matrix by arbitrarily selecting or deleting some rows from one known SFR matrix. This method to construct new SFR matrices is sometimes useful because shift linear combinations may help to reduce the size including the number of columns of a matrix. For conventional full-rank matrices, it is trivial that there exist full row rank matrices of size $n \times m$ for any $m \geq n$. This is because adding any additional columns to a full row rank matrix still results in a full row rank matrix. As mentioned in Section II and pointed out in [12], [26], [27], this is no longer true for SFR matrices. Although it is the case, the following result holds for SFR matrices.

Corollary 2: There exists at least one binary SFR matrix of standard form with size $n \times m$ if and only if $m \geq n$.

Proof: Since any SFR matrix has full row rank, the "only if" part is obvious.

For any n and m with $m \geq n$, let $\mathbf{v} = \underset{\cdot}{1}1$ and hence $l(\mathbf{v}) = 2 > 1$. From Corollary 1 and Lemma 4, matrix $G_m^{\mathbf{v}}$ is an SFR matrix of standard form with size $m \times m$. From Lemma 5, an SFR matrix of standard form with size $n \times m$ can be obtained by deleting any $m - n$ rows from the first $m - 1$ rows of $G_m^{\mathbf{v}}$. This proves the "if" part. □

As a remark, the above constructions and the results in Theorem 3 and subsequent corollaries on SFR matrices hold not only over $\mathbb{F}_2$ but also over any commutative integral domain (including any field), while the counting of the number of SFR matrices to be presented in the following section holds only for the binary field $\mathbb{F}_2$.

V. Shortest Shift-Full-Rank (SSFR) Matrices

Since the number of columns in an SFR matrix determines the memory size of the space–time trellis codes in Section II, we are interested in SFR matrices with the smallest number of columns. From Corollary 2, for any fixed number of rows, smallest SFR matrices are square matrices, i.e., the number of columns is the same as the number of rows, which are certainly shortest SFR (SSFR) matrices. Furthermore, from Corollary 2, for any fixed number of rows, SSFR matrices must include at least one of standard form. Therefore, in what follows, without loss of generality, we only consider SSFR matrices of standard form, and an SSFR matrix is always of standard form in case it is not explicitly stated. The goal of this section is to study such SSFR matrices with as many constructions as possible.

For a general construction $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ in (16) from an initial SFR matrix G_0 of standard form of size $n_0 \times m_0$ and $\mathbf{v}_i, \bar{\mathbf{v}}_i \in \mathcal{T}$ such that $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$ for $i = 1, 2, \ldots, n-1$, let $\mathbf{r}_i$ be the ith row of $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$, then we have

$$\begin{aligned} &\max\{l(\mathbf{r}_1), l(\mathbf{r}_2), \ldots, l(\mathbf{r}_{n_0+n-1})\} \\ &\geq l(\mathbf{v}_{n-1} \circ \mathbf{v}_{n-2} \circ \cdots \circ \mathbf{v}_1) + m_0 - 1 \geq n + m_0 - 1 \end{aligned} \tag{19}$$

since $l(\mathbf{v}_i) > 1$ that is from condition $\mathbf{v}_i \nmid \bar{\mathbf{v}}_i$. On the other hand, the number of rows equals to the number of columns means that

$$\max\{l(\mathbf{r}_1), l(\mathbf{r}_2), \ldots, l(\mathbf{r}_{n_0+n-1})\} = n + n_0 - 1 \leq n + m_0 - 1.$$

Hence, $n_0 = m_0$ and $\mathbf{v}_1 = \mathbf{v}_2 = \cdots = \mathbf{v}_{n-1} = \underset{\cdot}{1}1$. Since the vector $\underset{\cdot}{1}1$ is often used in this section, we denote it by $\mathbf{e}$, i.e., $\mathbf{e} \triangleq \underset{\cdot}{1}1$. This proves the following lemma.

Lemma 6: For a matrix $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ in (16) to be shortest, it must have the following form: $\mathbf{v}_i = \mathbf{e}$ and

$$G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i} = G_{n_0+n-1}^{G_0,\mathbf{e},\bar{\mathbf{v}}_i} = \begin{pmatrix} \mathbf{e}^0 \circ \bar{\mathbf{v}}_{n-1} \\ \mathbf{e}^1 \circ \bar{\mathbf{v}}_{n-2} \\ \vdots \\ \mathbf{e}^{n-2} \circ \bar{\mathbf{v}}_1 \\ \mathbf{e}^{n-1} \circ G_0 \end{pmatrix} \tag{20}$$

where G_0 is an SSFR matrix of standard form and $\bar{\mathbf{v}}_i \in \mathcal{T}$ such that $\mathbf{e} \nmid \bar{\mathbf{v}}_i$ for $i = 1, 2, \ldots, n-1$.

We can see that (17) is a special case of (20) when $G_0 = \mathbf{v}_0 \in \mathcal{T}$. Based on this lemma, we next study when $\mathbf{e} \nmid \bar{\mathbf{v}}_i$.

Lemma 7: Let $\mathbf{v} \in \mathcal{S}$. Then, $\mathbf{e} \mid \mathbf{v}$ if and only if $w(\mathbf{v})$ is even.

Proof: This lemma follows easily if a binary vector $\mathbf{v}$ of finite length is associated with a polynomial. □

With the above two lemmas, we have the following theorem.

Theorem 4: For a matrix $G_{n_0+n-1}^{G_0,\mathbf{v}_i,\bar{\mathbf{v}}_i}$ in (16) to be shortest if and only if $\mathbf{v}_i = \mathbf{e}$ for $i = 1, 2, \ldots, n-1$ and it has the form in (20) where G_0 is an SSFR matrix of standard form of size $n_0 \times n_0$, and $\bar{\mathbf{v}}_i \in \mathcal{T}$ with odd weight $w(\bar{\mathbf{v}}_i)$ such that its length satisfies $l(\bar{\mathbf{v}}_i) \leq n_0 + i$ for $i = 1, 2, \ldots, n-1$.

Proof: By Lemmas 6 and 7, it is necessary and sufficient to prove the length of every row $\mathbf{r}_i$ of $G_{n_0+n-1}^{G_0,\mathbf{e},\bar{\mathbf{v}}_i} \leq n + n_0 - 1$. This holds obviously for the last n_0 rows. For $1 \leq i \leq n-1$, we have

$$\begin{aligned} l(\mathbf{r}_i) &= l(\mathbf{e}^{i-1} \circ \bar{\mathbf{v}}_{n-i}) \\ &= 1 + (i-1)(l(\mathbf{e}) - 1) + l(\bar{\mathbf{v}}_{n-i}) - 1 \\ &\leq n_0 + n - 1, \end{aligned}$$

which holds if and only if $l(\bar{\mathbf{v}}_i) \leq n_0 + i$ for $1 \leq i \leq n-1$. This completes the proof. □

With this theorem and Property d), we can see that any SSFR matrix with the form in (20) contains and only contains an odd weight row vector for $n > 1$. We next list some design examples.

Example 3: Let initial SSFR matrix $G_0 = (1) = \mathbf{1}$ in this example. First, also let $\bar{\mathbf{v}}_i = \mathbf{1}$ in $G_n^{G_0,\mathbf{e},\bar{\mathbf{v}}_i}$ which is then equal to $G_n^{\mathbf{e}}$. We list $G_n^{\mathbf{e}}$ for $1 \leq n \leq 8$ as follows:

$$G_1^{\mathbf{e}} = (1), \quad G_2^{\mathbf{e}} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$G_3^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$G_4^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G_5^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_6^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$G_7^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$G_8^{\mathbf{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We can easily verify that the matrix system $\{G_n^{\mathrm{LX}}\}_{n\geq 1}$ given in [12], [26], [27] with

$$G_n^{\mathrm{LX}} = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \mathbf{r}_3 \\ \vdots \\ \mathbf{r}_n \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ \mathbf{r}_1 + \mathbf{r}_1^{R_{l(\mathbf{r}_1)}} \\ \mathbf{r}_2 + \mathbf{r}_2^{R_{l(\mathbf{r}_2)}} \\ \vdots \\ \mathbf{r}_{n-1} + \mathbf{r}_{n-1}^{R_{l(\mathbf{r}_{n-1})}} \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,0 \cdots 0\,0\,0 \\ 1\,1\,0\,0\,0 \cdots 0\,0\,0 \\ 1\,1\,1\,1\,0 \cdots 0\,0\,0 \\ \vdots \\ 1\,1\,1\,1\,1 \cdots 1\,1\,1 \end{pmatrix}_{n\times 2^{n-1}} \tag{21}$$

is just a submatrix system of $\{G_n^{\mathbf{e}}\}_{n\geq 1}$ since the ith row in $\{G_n^{\mathrm{LX}}\}$ is equal to the 2^{i-1}th row in $\{G_n^{\mathbf{e}}\}$ for $i \geq 1$. One can see that the number of columns of this submatrix system grows exponentially with the number of rows.

It is not hard to see that $G_1^{\mathbf{e}}$ and $G_2^{\mathbf{e}}$ are the only SSFR matrices of standard form of sizes 1×1 and 2×2, respectively. For other designs different from $G_3^{\mathbf{e}}$ and $G_4^{\mathbf{e}}$, we list various choices of $\bar{\mathbf{v}}_i$ in Table I. The corresponding SSFR matrix of size 3×3 is

TABLE I
CHOICES OF $\bar{\mathbf{v}}_i$

Matrix	$\bar{\mathrm{v}}_1$	$\bar{\mathrm{v}}_2$	$\bar{\mathrm{v}}_3$
G_3^{sh}	$\mathbf{1}$	$\underset{\cdot}{1}11$	/
$G_4^{\mathrm{sh}_1}$	$\mathbf{1}$	$\mathbf{1}$	$\underset{\cdot}{1}11$
$G_4^{\mathrm{sh}_2}$	$\mathbf{1}$	$\mathbf{1}$	$\underset{\cdot}{1}101$
$G_4^{\mathrm{sh}_3}$	$\mathbf{1}$	$\mathbf{1}$	$\underset{\cdot}{1}011$
$G_4^{\mathrm{sh}_4}$	$\mathbf{1}$	$\underset{\cdot}{1}11$	$\mathbf{1}$
$G_4^{\mathrm{sh}_5}$	$\mathbf{1}$	$\underset{\cdot}{1}11$	$\underset{\cdot}{1}11$
$G_4^{\mathrm{sh}_6}$	$\mathbf{1}$	$\underset{\cdot}{1}11$	$\underset{\cdot}{1}101$
$G_4^{\mathrm{sh}_7}$	$\mathbf{1}$	$\underset{\cdot}{1}11$	$\underset{\cdot}{1}011$

$$G_3^{\mathrm{sh}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{22}$$

and the corresponding seven SSFR matrices of size 4×4 are

$$G_4^{\mathrm{sh}_1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad G_4^{\mathrm{sh}_2} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G_4^{\mathrm{sh}_3} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad G_4^{\mathrm{sh}_4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G_4^{\mathrm{sh}_5} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad G_4^{\mathrm{sh}_6} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$G_4^{\mathrm{sh}_7} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}. \tag{23}$$

A property for the above SSFR matrix construction is that there are no repetitions in the designs, i.e., any two designs from different $(G_0, \bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-1})$'s are not shift equivalent or one is a submatrix of another as we shall see later. The next question we are interested in is how many SSFR matrices there are for a given size. To do so, let us first see more properties of SFR and SSFR matrices.

Theorem 5: There does not exist any binary $n \times n$ full-rank matrix with all even weight row vectors. There does not exist any binary SSFR matrix except for $G_1^{\mathbf{e}}$ with all odd weight row vectors.

Proof: Let us first prove the first part. Assume $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \ldots, \mathbf{r}_n^T]^T$ is a binary $n \times n$ full-rank matrix with row vectors $\mathbf{r}_i \in \mathcal{S}$, $1 \leq i \leq n$, of all even weights. By Lemma 7, for every $\mathbf{r}_i$, there exists $\hat{\mathbf{r}}_i \in \mathcal{S}$ such that $\mathbf{r}_i = \mathbf{e} \circ \hat{\mathbf{r}}_i$.

Therefore, we can get a matrix $\hat{G} = [\hat{\mathbf{r}}_1^T, \hat{\mathbf{r}}_2^T, \ldots, \hat{\mathbf{r}}_n^T]^T$ of size $n \times (n-1)$ such that $G = \mathbf{e} \circ \hat{G}$. Similar to the Proof of Lemma 2, we know that the rank of $\hat{G}$ is also n, which is impossible for an $n \times (n-1)$ matrix. This completes the proof of the first part.

We next prove the second part. Assume there exists such a binary SSFR matrix $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \ldots, \mathbf{r}_n^T]^T$ of size $n \times n$ with its row vectors $\mathbf{r}_i \in \mathcal{T}$, $1 \le i \le n$. Since G is of standard form and has full rank, the following matrix:

$$\begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 - \mathbf{r}_1 \\ \mathbf{r}_3 - \mathbf{r}_1 \\ \vdots \\ \mathbf{r}_n - \mathbf{r}_1 \end{pmatrix} = \left(\begin{array}{c|c} \multicolumn{2}{c}{\mathbf{r}_1} \\ \hline 0 & \\ 0 & \\ \vdots & \hat{G} \\ 0 & \end{array} \right)$$

also has full rank. Now, by deleting the first row and the first column of the above matrix, we get a full-rank matrix $\hat{G}$ of size $(n-1) \times (n-1)$ with all even weight row vectors. This contradicts with the first part of this theorem and hence the second part is proved. □

From this theorem, the following corollary is immediate.

Corollary 3: It is necessary for an SSFR matrix of size $n \times n$ with $n > 1$ to contain at least one even weight row vector and one odd weight row vector.

While an SSFR matrix with all odd weight row vectors does not exist except $G_1^{\mathbf{e}} = (1)$, we can easily find a full-rank square matrix with all odd weight row vectors. For example, the matrix $[\mathbf{r}_1^T, (\mathbf{r}_2 - \mathbf{r}_1)^T, (\mathbf{r}_3 - \mathbf{r}_1)^T, \ldots, (\mathbf{r}_n - \mathbf{r}_1)^T]^T$ is such a matrix, where $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n$ are the row vectors of $G_n^{\mathbf{e}}$.

We next study the number of SSFR matrices of standard form, which are not shift equivalent with each other, i.e., the number of different shift equivalent classes. To do so, let us see a definition for simplicity.

Definition 10: An SSFR matrix of standard form is called *basic* if it either equals to $G_1^{\mathbf{e}} = (1)$ or contains more than one odd weight row vector.

Thus, all SSFR matrices of standard form other than basic ones contain and only contain one odd weight row from Corollary 3, such as the matrices in (20) for $n > 1$. In the following, two matrices are different means they are in different shift equivalent classes, i.e., they are not shift equivalent.

Theorem 6: From a basic SSFR matrix G_0 of size $n_0 \times n_0$, based on the construction (20) there are only

$$2^{(n-n_0)(\frac{n+n_0-3}{2})}$$

different SSFR matrices of standard form of size $n \times n$ for $n \ge n_0$. Conversely, for every given SSFR matrix G of standard form, we can trace it back to a unique basic SSFR matrix.

Proof: We first prove that two SSFR matrices of the same size derived from the same basic SSFR matrix G_0 and different $(\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-n_0})$'s are different. From the form of $G_n^{G_0, \mathbf{e}, \bar{\mathbf{v}}_i}$ in (20), we know that the last n_0 rows are always the same and at least one row in the first $n - n_0$ rows is different for different $(\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-n_0})$'s. Now we consider the shift equivalence in the sense of a row permutation. For the ith row $\mathbf{r}_i$ of a matrix, we have $\mathbf{e}^{i-1} | \mathbf{r}_i$, but $\mathbf{e}^i \nmid \mathbf{r}_i$ since $\mathbf{e} \nmid \bar{\mathbf{v}}_{n-i}$ (from Lemma 7 and Theorem 4) for $1 \le i \le n - n_0$, and $\mathbf{e}^{n-n_0} \mid \mathbf{r}_i$ for $n - n_0 + 1 \le i \le n$. Obviously, there does not exist any permutation for the last n_0 rows of any two matrices. Assume the ith row $\mathbf{r}_i$ of one matrix is equal to the jth row $\mathbf{r}'_j$ of the other matrix with $i < j$, we have $\mathbf{e}^{j-1} | \mathbf{r}'_j \Rightarrow \mathbf{e}^{j-1} | \mathbf{r}_i \Rightarrow \mathbf{e}^i | \mathbf{r}_i$ for $j \le n - n_0$ and $\mathbf{e}^{n-n_0} | \mathbf{r}'_j \Rightarrow \mathbf{e}^{n-n_0} | \mathbf{r}_i \Rightarrow \mathbf{e}^i | \mathbf{r}_i$ for $i \le n - n_0 < j$. This is a contradiction and hence every SSFR matrix derived from G_0 with the form (20) corresponds to a unique $(\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-n_0})$.

TABLE II
THE NUMBERS OF SSFR MATRICES DERIVED FROM $G_1^{\mathbf{e}}$

n	1	2	3	4	5	6	7	8	9	10
N_n^1	1	1	2	2^3	2^6	2^{10}	2^{15}	2^{21}	2^{28}	2^{36}

By the above derivations and Theorem 4, the number of different SSFR matrices of size $n \times n$ derived from G_0 is equal to the number of possible $(\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-n_0})$ such that $w(\bar{\mathbf{v}}_i)$ are odd and $l(\bar{\mathbf{v}}_i) \le n_0 + i$. For any given integer $l > 0$, the number of odd weight vectors $\mathbf{v} \in \mathcal{T}$ such that $l(\mathbf{v}) \le l$ is

$$\binom{l-1}{0} + \binom{l-1}{2} + \cdots + \binom{l-1}{k} = \begin{cases} 1, & l = 1 \\ 2^{l-2}, & l > 1 \end{cases}$$

where $k = l - 1$ for l odd and $k = l - 2$ for l even. Therefore, the number of possible $\bar{\mathbf{v}}_i$ is 2^{n_0+i-2} and the number of possible $(\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2, \ldots, \bar{\mathbf{v}}_{n-n_0})$ is

$$\begin{aligned} \prod_{i=1}^{n-n_0} 2^{n_0+i-2} &= 2^{(n_0-2)(n-n_0)+\frac{1}{2}(n-n_0)(n-n_0+1)} \\ &= 2^{(n-n_0)(\frac{n+n_0-3}{2})}. \end{aligned} \qquad (24)$$

Conversely, if G is basic, the conclusion is obvious. Otherwise, assume G of size $n \times n$ is not basic, then it must have a unique odd weight row vector because of Corollary 3 and the definition of basic SSFR matrices, and an even weight row vector of length n because, otherwise, it contradicts with Theorem 5. Thus, we can get another SSFR matrix of size $(n-1) \times (n-1)$ from G by first deleting the unique odd weight row vector and then dividing all the remaining $n-1$ rows by $\mathbf{e}$. If the resulted matrix is basic, the conclusion holds. Otherwise, this process continues until we find a basic one. The uniqueness of the resulted basic SSFR matrix, which G is traced back to, is from the uniqueness of every step in this process. □

Obviously, the single-entry matrix $G_1^{\mathbf{e}} = (1)$ is the simplest basic SSFR matrix. Then, the number of different SSFR matrices of size $n \times n$ derived from $G_1^{\mathbf{e}}$ is $N_n^1 \triangleq 2^{\frac{1}{2}(n-2)(n-1)}$ by (24). We list the values of N_n^1 for $n = 1, 2, \ldots, 10$ in Table II. Moreover, from this theorem, we can see that any nonbasic SSFR matrix must have the form (20) with G_0 being a basic SSFR matrix and $n > 1$, i.e., it can be derived from a basic SSFR matrix with the form (20).

Corollary 4: Any two SSFR matrices of standard form with the same size but derived from two different basic SSFR matrices are different.

Proof: If they are the same, we can trace them back to the same basic SSFR matrix due to the uniqueness of the inverse process in the Proof of Theorem 6. Therefore, we get a contradiction. □

With the above results, the following corollary is immediate.

Corollary 5: Let N_n^{BS} denote the number of different basic SSFR matrices of size $n \times n$ for $n \geq 1$. Then, the number N_n of different SSFR matrices of standard form of size $n \times n$ is

$$N_n = \sum_{i=1}^{n} N_i^{\mathrm{BS}} \cdot 2^{(n-i)(\frac{n+i-3}{2})}.$$

Obviously, $N_1^{\mathrm{BS}} = 1$ and $N_2^{\mathrm{BS}} = N_3^{\mathrm{BS}} = 0$. A further problem is if there exist basic SSFR matrices other than $G_1^{\mathbf{e}}$. We claim there are other such matrices by presenting the following theorem.

Theorem 7: The following two matrices

$$\begin{aligned} G_4^{\mathrm{BS}_1} &= G_4^{\mathbf{e}} + \begin{pmatrix} \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{e}^0 + \mathbf{1}^{R_3} \\ \mathbf{e}^1 + \mathbf{1}^{R_3} \\ \mathbf{e}^2 + \mathbf{1}^{R_3} \\ \mathbf{e}^3 + \mathbf{1}^{R_3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} G_4^{\mathrm{BS}_2} &= G_4^{\mathrm{sh}_1} + \begin{pmatrix} \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \\ \mathbf{1}^{R_3} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{e}^0 \circ \bar{\mathbf{v}} + \mathbf{1}^{R_3} \\ \mathbf{e}^1 + \mathbf{1}^{R_3} \\ \mathbf{e}^2 + \mathbf{1}^{R_3} \\ \mathbf{e}^3 + \mathbf{1}^{R_3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{aligned}$$

are basic SSFR matrices of size 4×4, where $\bar{\mathbf{v}} = \underset{\cdot}{1}11 \in \mathcal{T}$, $G_4^{\mathbf{e}}$ is shown in Example 3 and $G_4^{\mathrm{sh}_1}$ is shown in (23).

Proof: Let $\mathbf{r}_i$ denote the ith row of $G_4^{\mathrm{BS}_1}$, then $\mathbf{r}_i = \mathbf{e}^{i-1} + \mathbf{1}^{R_3}$, $1 \leq i \leq 4$. Consider their nonzero shift linear combination

$$\begin{aligned} \mathbf{c} &= a_1 \cdot \mathbf{r}_1^{R_{j_1}} + a_2 \cdot \mathbf{r}_2^{R_{j_2}} + a_3 \cdot \mathbf{r}_3^{R_{j_3}} + a_4 \cdot \mathbf{r}_4^{R_{j_4}} \\ &= [a_1 \cdot (\mathbf{e}^0)^{R_{j_1}} + a_2 \cdot (\mathbf{e}^1)^{R_{j_2}} \\ &\quad + a_3 \cdot (\mathbf{e}^2)^{R_{j_3}} + a_4 \cdot (\mathbf{e}^3)^{R_{j_4}}] \\ &\quad + [a_1 \cdot \mathbf{1}^{R_{j_1}} + a_2 \cdot \mathbf{1}^{R_{j_2}} + a_3 \cdot \mathbf{1}^{R_{j_3}} + a_4 \cdot \mathbf{1}^{R_{j_4}}]^{R_3} \\ &= \mathbf{c}_1 + \mathbf{c}_2 \end{aligned}$$

with any $a_i \in \mathbb{F}_2$, not all zero, and $j_i \in \mathbb{Z}$. We now discuss all the possible cases for the values of j_1, j_2, j_3, j_4.

a) When they are different with each other, it is obvious that $\mathbf{c} \neq \mathbf{0}$ regardless of the values of a_i as $\mathbf{c}_1$ and $\mathbf{c}_2$ are nonzero because $G_4^{\mathbf{e}}$ is an SFR matrix by Corollary 1 and there is a 4 bits position difference between the most left 1's of $\mathbf{c}_1$ and $\mathbf{c}_2$.

b) When $j_1 = j_2 = j_3 = j_4$ and $a_i = 1$, obviously $\mathbf{c} \neq \mathbf{0}$.

c) When three row vectors have the same shift j and corresponding coefficients 1, their shift linear combination must have 1 at the coordinate j. Thus, for shift linear dependence, the fourth row vector must have the same shift as the others, which is reduced to b).

d) When two of j_1, j_2, j_3, j_4 are equal and both have the coefficients 1, we can verify by enumerating all the possibilities that their shift linear combination has length less than the lengths of the other two vectors. Therefore, the remaining two row vectors must have the same shift and also the coefficients 1. Certainly, $\mathbf{c} \neq \mathbf{0}$ in this case due to the SFR property of $G_4^{\mathbf{e}}$.

Therefore, $G_4^{\mathrm{BS}_1}$ is a basic SSFR matrix. Using the same procedure, we know $G_4^{\mathrm{BS}_2}$ is also a basic SSFR matrix. □

The construction method in Theorem 7 cannot be applied to any nonbasic SSFR matrices of size 4×4 to construct basic ones other than $G_4^{\mathbf{e}}$ and $G_4^{\mathrm{sh}_1}$. However, we can easily generalize it to more general cases in the following theorem, while the resulted SFR matrices are not the shortest ones.

Theorem 8: Given any SFR matrix $G = [\mathbf{r}_1^T, \mathbf{r}_2^T, \mathbf{r}_3^T, \mathbf{r}_4^T]^T$ of standard form of size $4 \times m$ with $m \geq 4$, the following matrix:

$$\tilde{G} = \begin{pmatrix} \mathbf{r}_1 + \mathbf{1}^{R_j} \\ \mathbf{r}_2 + \mathbf{1}^{R_j} \\ \mathbf{r}_3 + \mathbf{1}^{R_j} \\ \mathbf{r}_4 + \mathbf{1}^{R_j} \end{pmatrix}$$

is an SFR matrix of standard form of size $4 \times (j + 1)$ for any $j \geq m$.

Notice that Theorem 7 is not contained in Theorem 8 because $j = m - 1$ in Theorem 7 that does not satisfy $j \geq m$ in Theorem 8. But their proofs are similar. Moreover, the converse of Theorem 8 does not hold, i.e., $\tilde{G}$ is an SFR matrix does not imply G is also an SFR matrix. For example

$$\tilde{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{and}$$

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

are such a pair of matrices. It is not difficult to notice that Theorem 8 is similar to Theorem 2 (iii) in [12], where all row vectors of a matrix have the same length, i.e., the first and the last column vectors are all-one vectors, but the construction here is more intuitive. Also, the method used in Theorem 8 can be applied to any SFR matrix of standard form with the number of rows less than 4, but unfortunately can not be applied to those with more rows. For example, matrix

$$\begin{pmatrix} \mathbf{e}^0 + \mathbf{1}^{R_5} \\ \mathbf{e}^1 + \mathbf{1}^{R_5} \\ \mathbf{e}^2 + \mathbf{1}^{R_5} \\ \mathbf{e}^3 + \mathbf{1}^{R_5} \\ \mathbf{e}^4 + \mathbf{1}^{R_5} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

is not an SFR matrix because $(\mathbf{e}^0 + \mathbf{1}^{R_5}) + (\mathbf{e}^1 + \mathbf{1}^{R_5})^{R_4} + (\mathbf{e}^2 + \mathbf{1}^{R_5}) + (\mathbf{e}^3 + \mathbf{1}^{R_5})^{R_4} + (\mathbf{e}^4 + \mathbf{1}^{R_5})^{R_2} = \mathbf{0}$, although $G_5^{\mathbf{e}}$ is an SFR matrix.

By searching all binary $n \times n$ matrices of standard form with more than one odd weight row vector for $n = 4, 5, 6$, we find

TABLE III
VALUES OF N_n

n	N_n^{BS}	$\sum_{i=1}^{n-1} N_i^{BS} \cdot 2^{(n-i)(\frac{n+i-3}{2})}$	N_n
1	1	0	1
2	0	1	1
3	0	2	2
4	2	2^3	10
5	1	$2^6 + 2^4$	81
6	0	$2^{10} + 2^8 + 2^4$	1296

that $G_4^{\mathrm{BS}_1}$ and $G_4^{\mathrm{BS}_2}$ are the only basic SSFR matrices of size 4×4,

$$G_5^{\mathrm{BS}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

is the unique basic SSFR matrix of size 5×5, and there is no 6×6 basic SSFR matrices. Hence, we have $N_4^{\mathrm{BS}} = 2$, $N_5^{\mathrm{BS}} = 1$ and $N_6^{\mathrm{BS}} = 0$. By Corollary 5, we list the values of N_n for $1 \leq n \leq 6$ in Table III. From Table III, the following corollary is immediate.

Corrolary 6: Matrices G_3^{e} and G_3^{sh} constructed above are the only two different SSFR matrices of standard form of size 3×3, and matrices G_4^{e}, $G_4^{\mathrm{sh}_i}$ for $1 \leq i \leq 7$, and $G_4^{\mathrm{BS}_1}$ and $G_4^{\mathrm{BS}_2}$ constructed above are the only ten different SSFR matrices of standard form of size 4×4.

While the exact values of N_n for $n > 6$ are not given here, we can see that the numbers are surprisingly large even for not large n. For example, when $n = 8$, there exist at least $2^{21} + 2^{19} + 2^{15} = 2\,654\,208$ different binary SSFR matrices. Moreover, for a small n, we find that the number N_n^1 of the SSFR matrices derived from G_1^{e} contributes the most to the value of N_n and the number N_n^{BS} of basic SSFR matrices is not large. We conjecture that N_n^{BS} is always small and therefore N_n^1 contributes the most to the value of N_n for any n.

As a final comment, after having discussed all the above constructions of SFR matrices, for a given matrix, one may be able to also check whether it is SFR in some way by following the converse steps of the above construction methods. For example, for a given matrix of n rows, one may check whether its $n-1$ row vectors can be factorized so that it can be converted to a smaller size matrix. If so, factorize the $n-1$ rows and form a submatrix of $n-1$ rows, and then repeat this procedure until the last one whose rows can not be factorized anymore.

VI. Simulation Results

In all our simulations, we assume that the channel is quasistatic Rayleigh flat fading. Furthermore, we assume that no errors occur in phase I transmission, i.e., what the relays detect is the same as what the source terminal has sent. We also assume that there is only one antenna in the destination terminal and the random delays are uniformly generated from the set $\{0, 1, \ldots, L_e\}$, where L_e is the maximum relative timing error.

In [12], [26], [27], the SFR matrix designed for 3 relays with the smallest number of columns is

$$G_3^{\mathrm{LX}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

which is from the systematic construction (21) introduced in [12], [26], [27]. In Fig. 2, we compare the frame error rate (FER) performances of the space–time trellis code generated from the 3×3 SSFR matrix G_3^{sh} in (22) with delay diversity code [22], [23] and the space–time trellis code generated from G_3^{LX}, where both synchronous (i.e., $L_e = 0$) and asynchronous $(L_e = 3, 5)$ cases are considered. As we have discussed, for the space–time trellis codes associated with G_3^{sh} and G_3^{LX}, full diversity can be achieved for arbitrary delays, while it is not the case for delay diversity code. This can be clearly seen in Fig. 2. In synchronous case, the slopes of the performance curves for the three codes are the same at high SNR, while the code generated from G_3^{LX} has the biggest coding gain among them. However, in asynchronous cases, the performances of the trellis codes with asynchronous full diversity further improve as L_e increases, which is the same as what has been observed in [12], [26], [27], while the performance of delay diversity code degrades and its full diversity property is lost. Furthermore, we can see in Fig. 2 that, compared with the trellis code generated from G_3^{LX}, the code generated from the SSFR matrix G_3^{sh} has not only the smaller memory size and hence the lower decoding complexity but also the better performance in asynchronous cases.

VII. Conclusion

In this paper, we introduced the concept of shift-full-rank (SFR) matrices and systematically studied and constructed SFR matrices for any sizes. Note that it was shown in [12], [26], [27] that SFR matrices can be used to construct space–time trellis codes for relay networks to have full cooperative diversity order without the symbol synchronization requirement. Since the number of columns of SFR matrices determines the memory size of the corresponding space–time trellis codes, we then systematically constructed shortest (square) SFR (SSFR) matrices for any number of rows, i.e., relay terminals. Furthermore, we presented some numbers and properties of SSFR matrices. Although our studies on SFR matrices were carried out over the binary field, the constructions can be generalized to any commutative integral domain. For example, Lemma 2, Theorem 3, Corollary 1, Lemma 4, Lemma 5, Corollary 2, Lemma 6 can be easily generalized from the binary field to any commutative integral domain. Finally, some simulation results were presented to illustrate the performances of the space–time trellis codes generated from SFR (including SSFR) matrices in asynchronous cooperative communications. As a remark, in our recent work [24], it has been shown that the space–time trellis codes generated from SFR matrices, which are descried in [12], [26], [27] and this paper, can also achieve asynchronous full cooperative diversity in a relay network where the delays can be fractional symbol duration and oversampling is used at the destination.

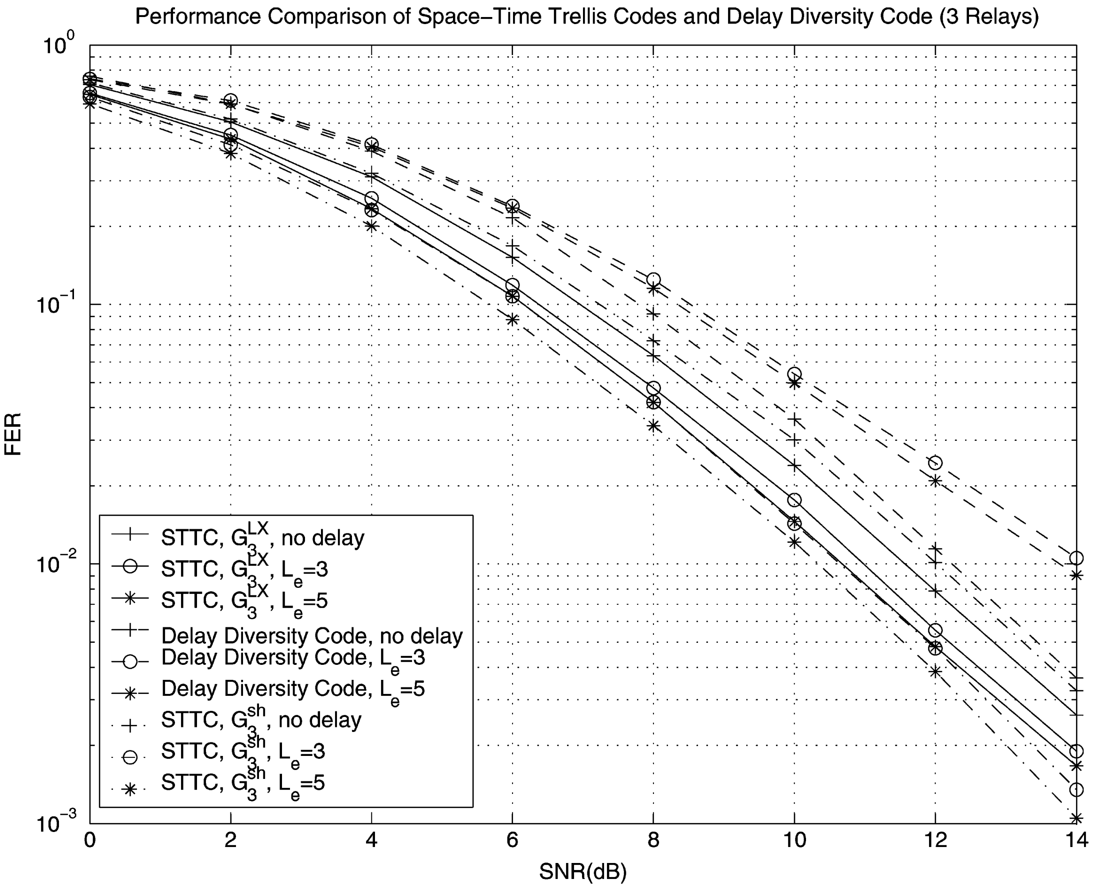

Fig. 2. Comparison of the performances of delay diversity code and the space–time trellis codes generated from G_3^{LX} and G_3^{sh} for different L_e's.

REFERENCES

[1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperative diversity—Part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[2] ——, "User cooperative diversity—Part II: Implementation aspects and performance analysis," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1939–1948, Nov. 2003.

[3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[4] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.

[5] Y. Hua, Y. Mei, and Y. Chang, "Wireless antennas—Making wireless communications line wireline communications," in *Proc. IEEE Top. Conf. Wireless Commun. Technol.*, Honolulu, HI, Oct. 15–17, 2003, pp. 1–27.

[6] M. Janani, A. Hedayat, T. E. Hunter, and A. Nosratinia, "Coded cooperation in wireless communications: Space-time transmission and iterative decoding," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 362–371, Feb. 2004.

[7] A. Stefanov and E. Erkip, "Cooperative coding for wireless networks," *IEEE Trans. Commun.*, vol. 52, no. 9, pp. 1470–1476, Sep. 2004.

[8] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: Performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1099–1109, Aug. 2004.

[9] Y. Jing and B. Hassibi, "Distributed space-time coding in wireless relay networks—Part I: Basic diversity results," *IEEE Trans. Wireless Commun.* submitted, Jul. 2004.

[10] ——, "Distributed space-time coding in wirelesss relay networks—Part II: Tighter bounds and a more general case," *IEEE Trans. Wireless Commun.* submitted, Jul. 2004.

[11] S. Wei, D. Goeckel, and M. Valenti, "Asynchronous cooperative diversity," in *Proc. Conf. Inform. Sci. and Sys*, Princeton, NJ, Mar. 17–19, 2004.

[12] Y. Li and X.-G. Xia, "A family of distributed space-time trellis codes with asynchronous cooperative diversity," *IEEE Trans. Commun.* Nov. 2004, submitted. [Online]. Available: http://www.ece.udel.edu/~xxia/LiXia.pdf

[13] X. Li, "Space-time coded multi-transmission among distributed transmitters without perfect synchronization," *IEEE Signal Process. Lett.*, vol. 11, no. 12, pp. 948–951, Dec. 2004.

[14] F. Ng, J.-H. Hwu, M. Chen, and X. Li, "Asynchronous space-time cooperative communications in sensor and robotic networks," in *Proc. IEEE Int. Conf. Mechatron. Automation (ICMA 2005)*, Niagara Falls, ON, Canada, Jul. 29–Aug. 1, 2005.

[15] Y. Mei, Y. Hua, A. Swami, and B. Daneshrad, "Combating synchronization errors in cooperative relays," in *Proc. IEEE Int. Conf. Acoust., Speech, and Signal Process. (ICASSP 2005)*, Philadelphia, PA, Mar. 18–23, 2005.

[16] Y. Li, W. Zhang, and X.-G. Xia, Distributive high-rate space-frequency codes achieving full cooperative and multipath diversity for asynchronous cooperative communications Oct. 2005, preprint.

[17] A. R. Hammons, "Algebraic space-time codes for quasisynchronous cooperative diversity," in *Proc. IEEE Int. Conf. Wireless Netw., Commun. Mobile Comput. (WirelessCom 2005)*, Maui, HI, USA, June 13–16, 2005.

[18] A. R. Hammons and H. E. Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 524–542, Mar. 2000.

[19] H.-F. Lu and P. V. Kumar, "Rate-diversity trade-off of space-time codes with fixed alphabet and optimal constructions for PSK modulation," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2747–2751, Oct. 2003.

[20] ——, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1709–1730, May 2005.

[21] J.-C. Guey, M. P. Fitz, M. R. Bell, and W.-Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," in *Proc. IEEE VTC'96*, Atlanta, GA, Apr. 28–May 1, 2006, pp. 136–140.

[22] V. Tarokh, N. Seshadri, and A. R. Calderbank, “Space-time codes for high data rate wireless communication: Performance criterion and code construction,” *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, Mar. 1998.

[23] N. Seshadri and J. H. Winters, “Two signaling schemes for improving the error performance of frequency-division-duplex (FDD) transmission systems using transmitter antenna diversity,” *Int. J. Wireless Inf. Netw.*, vol. 1, no. 1, pp. 49–60, Jan. 1994.

[24] Y. Shang and X.-G. Xia, Space-time trellis codes with asynchronous full diversity up to fractional symbol delays Feb. 2006, preprint.

[25] N. Jacobson, *Lectures in Abstract Algebra I: Basic Concepts*. New York: Springer-Verlag, 1951.

[26] Y. Li and X.-G. Xia, “A family of distributed space–time trellis codes with asynchronous cooperative diversity,” in *Proc. 4th Int. Conf. Inf. Proc. Sensor Netw. (IPSN’05)*, Los Angeles, CA, Apr. 25–27, 2005.

[27] Y. Li and X.-G. Xia, “Full diversity distributed space–time trellis codes for asynchronous cooperative communications,” in *Proc. IEEE Int. Symp. Information Theory (ISIT’05)*, Adelaide, Australia, Sep. 2005.

[28] J.-C. Guey, M.-P. Fitz, M.-R. Bell, and W.-Y. Kuo, “Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels,” *IEEE Trans. Commun.*, vol. 47, no. 4, pp. 527–537, Apr. 1999.