pdf of noise, continuous-valued RDP.

Maximum average power in query sequence.

Maximum average power in noise.

Conditional privacy loss.

Worst-case information.

ML estimate function.

ML estimate of $S_i$.

ML estimate of $S$.

Maximum probability of error.

Alphabet for $X_i$.

Number of possible values of $X$.

Number of queries per bit determined.

Lower bound on $\eta_i \forall i \geq m$.

$\beta$ Small bias of discrete RDP.

Average probability of error.

Entropy.

Query complexity per record.

Lower bound on $\gamma_m \forall i \geq m$.

Number of records.

The author would like to acknowledge the substantial contributions of the anonymous reviewers, including a pointer to [6].

REFERENCES

[1] N. R. Adam and J. C. Worton, “Security-control methods for statistical databases: A comparative study,” ACM Comput. Surv., vol. 21, no. 4, pp. 515–556, Dec. 1989.

[2] D. Agrawal and C. C. Aggarwal, “On the design and quantification of privacy preserving data mining algorithms,” in Proc. 20th ACM SIGACT-SIGMOD-SIGART Symp. Principles of Database System., 2001.

[3] R. Agrawal and R. Srikant, “Privacy-preserving data mining,” in Proc. ACM SIGMOD Conf. Manage. Data, 2000.

[4] M. K. C. Clifton, “Privacy-preserving distributed mining of association rules on horizontally partitioned data,” IEEE Trans. Knowl. Data Eng., vol. 16, no. 9, pp. 1026–1037, Sep. 2004.

[5] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley, 1991.

[6] A. Evfimievski, J. Gehrke, and R. Srikant, “Limiting privacy breaches in privacy preserving data mining,” in Proc. 22nd ACM SIGACT-SIGMOD-SIGART Symp. Principles of Database System., 2003.

[7] C. Farkas and S. Jajodia, “The inference problem: A survey,” ACM SIGKDD Explorat. Newsl., vol. 4, no. 2, pp. 6–11, Dec. 2003.

[8] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. 1st Int. Conf. Mobile Syst., Appl. Services (MobiSys’03), 2003, pp. 31–42.

[9] M. Kantarcioglu, J. Jin, and C. Clifton, “When do mining results violate privacy?”, in Proc. 10th ACM SIGKDD Int. Conf. Knowl. Disc. Data Mining, 2004, pp. 599–604.

[10] H. Kargupta, H. Dutta, S. Datta, and K. Sivakumar, “Privacy preserving data mining and random perturbation,” in Proc. Workshop on Privacy in the Electron. Soc. (WPES’03), 2003.

[11] D. Lambert, “Measures of disclosure risk and harm,” J. Official Stat., vol. 9, pp. 313–331, 1993.

[12] S. Merugu and J. Ghosh, “Privacy-preserving distributed clustering using generative models,” in Proc. 3rd IEEE Int. Conf. Data Mining (ICDM), 2003.

[13] K. Muralidhar and R. Sarathy, “Security of random data perturbation methods,” ACM Trans. Database Syst. (TODS), vol. 24, no. 4, pp. 487–493, Dec. 1999.

[14] S. Rizvi and J. Haritsa, “Maintaining data privacy in association rule mining,” in Proc. 28th Conf. Very Large Data Base (VLDB’02), 2002.

[15] G. Soroossi, Personal Communication 2002.

[16] C. Shannon, “A mathematical theory of communication,” Bell Syst. Tech. J., vol. 27, pp. 379–423, Jul. 1948.

[17] V. S. Verykios, A. K. Elmagarmid, E. Bertino, Y. Saygin, and E. Dassenti, “Association rule hiding,” IEEE Trans. Knowl. Data Eng., vol. 16, no. 4, pp. 434–447, 2004.

[18] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis, “State-of-the-art in privacy preserving data mining,” ACM SIGMOD Rec., vol. 33, no. 1, Mar. 2004.

[19] P. L. Vora, “The channel coding theorem and the security of binary randomization,” in Proc. 2003 IEEE Int. Symp. Inf. Theory, Yokohama, Japan, Jun. 30–Jul. 4 2003, p. 306.

[20] P. L. Vora, A. Canteaut and K. Viswanathan, Eds., “Information theory and the security of binary data perturbation,” in Progress in Cryptol. —INDOCRYPT 2004: 5th Int. Conf. Cryptol. India, Chennai, India, Dec. 20–22, 2004, pp. 136–147.

Single-Symbol ML Decodable Distributed STBCs for Cooperative Networks

Zhihang Yi and Il-Min Kim, Senior Member, IEEE

Abstract—In this correspondence, the distributed orthogonal space–time block codes (DOSTBCs), which achieve the single-symbol maximum likelihood (ML) decodability and full diversity order, are first considered. However, systematic construction of the DOSTBCs is very hard, since the noise covariance matrix is not diagonal in general. Thus, some special DOSTBCs, which have diagonal noise covariance matrices at the destination terminal, are investigated. These codes are referred to as the row-monomial DOSTBCs. An upper bound of the data-rate of the row-monomial DOSTBC is derived and it is approximately twice higher than that of the repetition-based cooperative strategy. Furthermore, systematic construction methods of the row-monomial DOSTBCs achieving the upper bound of the data-rate are developed when the number of relays and/or the number of information-bearing symbols are even.

Index Terms—Cooperative networks, distributed space–time block codes, diversity, single-symbol maximum likelihood (ML) decoding.

I. INTRODUCTION

It is well known that relay terminal cooperation can improve the performance of a wireless network considerably [1]–[4]. A source terminal, several relay terminals, and a destination terminal constitute a cooperative network, where the relay terminals relay the signals from
the source terminal to the destination terminal. Because the destination terminal may receive different signals from several relay terminals simultaneously, some mechanism is needed to prevent or cancel the interference among these signals.

A simple solution is the so-called repetition-based cooperative strategy, which was proposed in [3]. In this strategy, only one relay terminal is allowed to transmit the signals at every time slot. Consequently, no interference exists at the destination terminal, and hence, the decoding process is single-symbol maximum likelihood (ML) decodable. Furthermore, it has been shown that the repetition-based cooperative strategy could achieve the full diversity order $K$, where $K$ is the number of relay terminals. Due to its single-symbol ML decodability and full diversity order, the repetition-based cooperative strategy was used and studied in many papers [4], [6]–[10]. However, the repetition-based cooperative strategy has very poor bandwidth efficiency. It is easy to see that the data-rate of the repetition-based cooperative strategy is $1/K$.

Recently, many researchers noticed that the use of distributed space–time codes could improve the bandwidth efficiency of cooperative networks [11]–[13] and many practical distributed space–time codes were proposed [14]–[17]. However, none of those codes were single-symbol ML decodable in general. In [18], Hua et al. investigated the use of the generalized orthogonal designs in cooperative networks. It is well-known that the generalized orthogonal designs can achieve the single-symbol ML decodability and full diversity [19], [20]. However, when the generalized orthogonal designs were directly used in cooperative networks, the orthogonality of the codes was lost, and hence, the codes were not single-symbol ML decodable any more. Very recently, Jing et al. used the existing orthogonal and quasi-orthogonal designs in cooperative networks [21]. But, the codes proposed in [21] were not single-symbol ML decodable in general. To the best of our knowledge, distributed space–time codes which achieve both the single-symbol ML decodability and the full diversity order have never been designed. This motivated our work.

In this correspondence, we first consider the distributed orthogonal space–time block codes (DOSTBCs) in the amplify-and-forward cooperative networks. The DOSTBCs achieve the single-symbol ML decodability and the full diversity order. However, systematic construction of the DOSTBCs is very hard due to the fact that the covariance matrix of the noise at the destination terminal is non-diagonal in general. Therefore, we restrict our interests to a subset of the DOSTBCs, which result in a diagonal noise covariance matrix at the destination terminal. We refer to the codes in this subset as the row-monomial DOSTBCs and derive an upper bound of the data-rate of the row-monomial DOSTBCs. Compared to the repetition-based cooperative strategy, the row-monomial DOSTBCs achieve approximately twice higher data-rate, while having the same decoding complexity and diversity order. Furthermore, systematic construction methods of the row-monomial DOSTBCs are developed. We prove that the codes generated by the systematic construction methods achieve the upper bound of the data-rate when the number of relays and/or the number $N$ of information-bearing symbols are even.

The rest of this correspondence is organized as follows. Section II describes the cooperative network considered in this correspondence. In Section III, we define the DOSTBCs and show that they achieve the single-symbol ML decodability and the full diversity order. In Section IV, the row-monomial DOSTBCs are first defined and an upper bound of the data-rate of the row-monomial DOSTBC is then derived. Section V presents the systematic construction methods of the row-monomial DOSTBCs. We present some numerical results in Section VI and then conclude this correspondence in Section VII.

Notations: Bold upper and lower letters denote matrices and row vectors, respectively. Also, $\text{diag}[x_1, \ldots, x_K]$ denotes the $K \times K$ diagonal matrix with $x_1, \ldots, x_K$ on its main diagonal; $\Omega_{k_1 k_2}$ the $k_1 \times k_2$ all-zero matrix; $\mathbf{I}_T \times T$ the $T \times T$ identity matrix; $[\cdot]_k$ the $k$th entry of a vector; $[\cdot]_{k_1 k_2}$ the $(k_1, k_2)$th entry of a matrix; $(\cdot)^*$ the complex conjugate; $(\cdot)^H$ the Hermitian; $(\cdot)^T$ the transpose. For two real numbers $a$ and $b$, $[a]$ denotes the ceiling function of $a$; $[a]$ the floor function of $a$; $\text{tr} \{a, b\}$ the modulo operation. For two sets $S_1$ and $S_2$, $S_1 \setminus S_2$ denotes the set whose elements are in $S_1$ but not in $S_2$.

II. SYSTEM MODEL

Consider a cooperative network with one source terminal, $K$ relay terminals, and one destination terminal. Every terminal has only one antenna and is half-duplex. Denote the channel from the source terminal to the $k$th relay terminal by $h_k$, and the channel from the $k$th relay terminal to the destination terminal by $f_k$. $h_k$ and $f_k$ are spatially uncorrelated complex Gaussian random variables with zero mean and unit variance. We assume that the destination terminal knows the instantaneous values of the channel coefficients $h_k$ and $f_k$ by using training sequences; while the source and relay terminals have no knowledge of the instantaneous channel coefficients.

At the beginning, the source terminal transmits $N$ complex-valued symbols over $N$ consecutive time slots. Let $\mathbf{s} = [s_1, \ldots, s_N]$ denote the symbol vector transmitted from the source terminal, where the power of $s_n$ is $E_s$. Assume the coherence time of $h_k$ is larger than $N$; then the received signal vector $\mathbf{y}_k$ at the $k$th relay terminal is $\mathbf{y}_k = h_k \mathbf{s} + \mathbf{n}_k$, where $\mathbf{n}_k = [n_{1_k}, \ldots, n_{K_k}]$ is the additive noise at the $k$th relay terminal and it is uncorrelated complex Gaussian with zero mean and identity covariance matrix. All the relay terminals are working in the amplify-and-forward mode and the amplifying coefficient $\rho$ is $\sqrt{E_s/(1 + E_s)}$ for every relay terminal, where $E_s$ is the transmission power at every relay terminal.

In order to construct a distributed space–time code, every relay terminal multiplies $\mathbf{y}_k$ and $\mathbf{y}_k'$ by $\mathbf{A}_k$ and $\mathbf{B}_k$, respectively, and then sum up these two products. The dimension of $\mathbf{A}_k$ and $\mathbf{B}_k$ is $N \times T$. Thus, the transmitted signal vector $\mathbf{x}_k$ from the $k$th relay terminal is

$$
\mathbf{x}_k = \rho \left( \mathbf{y}_k \mathbf{A}_k + \mathbf{y}_k' \mathbf{B}_k \right) = \rho h_k \mathbf{s}_k \mathbf{A}_k + \rho h_k' \mathbf{s}_k' \mathbf{B}_k + \rho \mathbf{n}_k \mathbf{A}_k + \rho \mathbf{n}_k' \mathbf{B}_k.
$$

This construction method originates from the construction of a space–time code for co-located multiple-antenna systems, where the transmitted signal vector from the $k$th antenna is $\mathbf{u} \mathbf{A}_k + \mathbf{s} \mathbf{B}_k$ [22]. Since we consider the amplify-and-forward cooperative networks, the relay terminals do not have the knowledge of $\mathbf{s}$. Therefore, they use $\mathbf{y}_k$ and $\mathbf{y}_k'$, which contain the information of $\mathbf{s}$, to construct the transmitted signal vector.

If the transmitted symbols are real-valued, it is easy to show that the rate-one generalized real orthogonal design proposed in [20] can be used in cooperative networks without any changes, while achieving the single-symbol ML decodability and full diversity order [18]. Therefore, we focus on the complex-valued symbols in this correspondence.

In many previous papers such as [12] and [17], the same choice of $\rho = \sqrt{E_s/(1 + E_s)}$ has been made.
Assume the coherence time of $f_k$ is larger than $T$; then the received signal vector $y_D$ at the destination terminal is given by:

$$y_D = \sum_{k=1}^{K} f_k x_k + n_D$$

$$= \sum_{k=1}^{K} (\rho f_k h_k s A_k + \rho f_k h_k^* B_k) + \sum_{k=1}^{K} (\rho f_k n_k A_k + \rho f_k n_k^* B_k) + n_D$$

(2)

where $n_D = [n_{D,1}, \ldots, n_{D,T}]$ is the additive noise at the destination terminal and is uncorrelated complex Gaussian with zero mean and identity covariance matrix.\(^6\) Define $w$, $X$ and $n$ as follows:

$$w = [\rho f_1, \ldots, \rho f_K]$$

(3)

$$X = [h_1 s A_1 + h_1^* s^* B_1; \ldots; h_K s A_K + h_K^* s^* B_K]$$

(4)

$$n = \sum_{k=1}^{K} (\rho f_k n_k A_k + \rho f_k n_k^* B_k) + n_D$$

(5)

then we can rewrite (2) in the following way:

$$y_D = w X + n.$$  

(6)

Because the matrix $X$ contains $N$ information-bearing symbols $s_1, \ldots, s_N$ and it lasts for $T$ time slots, the data-rate of $X$ is equal to $N/T$. From (5), it is easy to see that the mean of $n$ is zero and the covariance matrix $R$ of $n$ is given by

$$R = \sum_{k=1}^{K} (\rho f_k^2 (A_k^H B_k + B_k^H A_k)) + I_{T \times T}.$$  

(7)

III. DISTRIBUTED ORTHOGONAL SPACE–TIME BLOCK CODES

In this section, we will first define the DOSTBCs. Then, in order to evaluate the diversity order of the DOSTBCs, some properties of $A_k$ and $B_k$ are presented. Lastly, we show that the DOSTBCs can achieve the full diversity order.

From (6), the ML estimate $\hat{s}$ of $s$ is given by

$$\hat{s} = \arg \min_{s \in C} |y_D - w X R^{-1} y_D - w X|^H$$

$$= \arg \min_{s \in C} (2 R (w X R^{-1} y_D^H w^H) + w X R^{-1} X^H w^H)$$

(8)

where $C$ is the set containing all the possible symbol vectors $s$. Inspired by the definition of the generalized orthogonal designs [20], [22], we define the DOSTBCs in the following way.

**Definition 1:** A $K \times T$ matrix $X$ is called a Distributed Orthogonal Space–Time Block Code (DOSTBC) in variables $s_1, \ldots, s_N$ if the following two conditions are satisfied:

D1.1) The entries of $X$ are 0, $\pm h_{k,s}$, or multiples of these indeterminates by $j$, where $j = \sqrt{-1}$.

D1.2) The matrix $X$ satisfies the following equality:

$$X R^{-1} X^H = \sum_{n=1}^{N} [s_n D_n + \cdots + s_N D_N]$$

(9)

\(^6\)Note that we assume that there is no direct link between the source and destination terminals. The same assumption has been made in many previous publications [14]–[17]. Furthermore, we assume perfect synchronization among the relays as in [4], [14]–[18]. Synchronization is a critical issue for the practical implementation of cooperative networks; but it is beyond the scope of this correspondence.

\(^3\)Considering the $N$ time slots used by the source terminal to transmit the symbol vector $s$, the overall data-rate of the entire transmission scheme is $N/(N + T)$. In this correspondence, because we focus on the design of $X$, we will use the data-rate $N/T$ of $X$ as the metric to evaluate the bandwidth efficiency, as we have mentioned in Section I.

where $D_n = \text{diag}[[h_{1,n}]^2 D_{n,1}, \ldots, [h_{K,n}]^2 D_{n,K}],$ and $D_{n,k}$ are nonzero for $k = 1, \ldots, K$.

Substituting (9) into (8), it is easy to show that the DOSTBCs are single-symbol ML decodable.\(^8\) Furthermore, the DOSTBCs can also achieve the full diversity order $K$. Before presenting the proof, we first derive some fundamental properties on $A_k$ and $B_k$, which will be used throughout this correspondence. For convenience, we define that a matrix is column-monomial (row-monomial) if there is at most one nonzero entry on every column (row) of it.

**Lemma 1:** If a DOSTBC $X$ in variables $s_1, \ldots, s_N$ exists, its associated matrices $A_k$ and $B_k$; $1 \leq k \leq K$, have the following properties.

1) $A_k$ and $B_k$ cannot have nonzero entries at the same position.

2) $A_k$, $B_k$ are column-monomial.

3) $A_k R^{-1} A_k^H = h_k R^{-1} B_k^H = 0_{N \times N}$, for $1 \leq k \neq k_2 \leq K$.

4) $A_k R^{-1} A_k^H + B_k R^{-1} B_k^H = \text{diag}[D_{1,k}, \ldots, D_{N,k}], \quad$ for $1 \leq k \leq K$.

Proof: The proof of the first two properties is similar with the proof of Property 3.2 in [23]. The proof of the fourth property is similar with the proof of [22, Prop. 1]. The proof of the third property is given in the following lemma. When $k_1 \neq k_2$, according to (9), $[X R^{-1} X^H]_{k_1,k_2}$ is given by

$$[X R^{-1} X^H]_{k_1,k_2} = h_{k_1} h_{k_2}^* A_k R^{-1} A_k^H s_i^H$$

$$+ h_{k_1} h_{k_2}^* B_k R^{-1} B_k^H s_i^H$$

$$+ h_{k_2} h_{k_1}^* A_k R^{-1} B_k^H s_i^H$$

$$+ h_{k_1} h_{k_2}^* B_k R^{-1} B_k^H s_i^H$$

$$= 0.$$  

(10)

Note that $h_{k_1}$ and $h_{k_2}$ can be any complex numbers. Thus, in order to make (10) hold for every possible value of $h_{k_1}$ and $h_{k_2}$, the following equalities must hold:

$$s A_k R^{-1} A_k^H s_i^H = s_i^H B_k R^{-1} B_k^H s_i^H = 0.$$  

(11)

By using Lemma 1 of [24], we have the third property.

**Lemma 2:** Assume $T \geq K$, $E_r = c_r E$, and $E_s = c_s E$, where $c_r$ and $c_s$ are positive constants. The DOSTBCs can achieve the full diversity order $K$.

Proof: See Appendix A.

After evaluating the diversity order of the DOSTBCs, a natural question is how to systematically construct the DOSTBCs. Unfortunately, the systematic construction method has not been found yet. We note that the major hindrance comes from the fact that the noise covariance matrix $R$ in (7) is not diagonal in general. In the next section, thus, we will consider a subset of the DOSTBCs, whose codes result in a diagonal $R$.

IV. ROW-MONOMIAL DISTRIBUTED ORTHOGONAL SPACE–TIME BLOCK CODES

In this section, we first show that, if $A_k$ and $B_k$ are row-monomial, the covariance matrix $R$ becomes diagonal. Then we define a subset of the DOSTBCs, whose associated matrices $A_k$ and $B_k$ are row-monomial, and hence, we refer to the codes in this subset as the row-mono-
mial DOSTBCs. Last, an upper bound of the data-rate of the row-monomial DOSTBC is derived.

As we stated in Section III, the nondiagonality of \( R \) makes the systematic construction of the DOSTBCs very hard. Thus, we restrict our interests to a special subset of the DOSTBCs, where \( R \) is diagonal. In the following, we show that the diagonality of \( R \) is equivalent with the row-monomial condition of \( A_k \) and \( B_k \).

Theorem 1: The matrix \( R \) in (7) is a diagonal matrix if and only if \( A_k \) and \( B_k \) are row-monomial.

Proof: See Appendix B.

Based on Theorem 1, we define the row-monomial DOSTBCs in the following way.

Definition 2: A \( K \times T \) matrix \( X \) is called a row-monomial DOSTBC in variables \( s_1, \ldots, s_N \) if it satisfies D1.1 and D1.2 in Definition 1 and its associated matrices \( A_k \) and \( B_k \), \( 1 \leq k \leq K \), are all row-monomial.

Obviously, the row-monomial DOSTBCs are single-symbol ML decodable and they achieve the full diversity order \( K \), because they are in a subset of the DOSTBCs. For the same reason, all the results in Section III are still valid for the row-monomial DOSTBCs. In order to evaluate the bandwidth efficiency, we drive an upper bound of the data-rate of the row-monomial DOSTBC. To this end, we present several conditions on \( A_k \) and \( B_k \) at first. In this correspondence, two matrices \( A \) and \( B \) are said to be column-disjoint, if \( A \) and \( B \) cannot contain nonzero entries on the same column simultaneously, i.e., if a column in \( A \) contains a nonzero entry at any row, then all the entries of the same column in \( B \) must be zero; conversely, if a column in \( B \) contains a nonzero entry at any row, then all the entries of the same column in \( A \) must be zero.

Lemma 3: If a row-monomial DOSTBC \( X \) in variables \( s_1, \ldots, s_N \) exists, its associated matrices \( A_k \) and \( B_k \), \( 1 \leq k \leq K \), satisfy the following two conditions:

1) \( A_{k_1} \) and \( A_{k_2} \) are column-disjoint for \( k_1 \neq k_2 \);
2) \( B_{k_1} \) and \( B_{k_2} \) are column-disjoint for \( k_1 \neq k_2 \).

Proof: See Appendix C.

Lemma 3 is crucial to find the upper bound of the data-rate of the row-monomial DOSTBC. According to Definition 2, if \( X \) is a row-monomial DOSTBC, there are two types of nonzero entries in it: 1) the entries containing \( \pm h_k s_n \) or the multiples of it by \( j \); 2) the entries containing \( \pm h_k^* s_n^* \) or the multiples of it by \( j \). In the following, we will refer to the first type of entries as the nonconjugate entries and refer to the second type of entries as the conjugate entries. Lemma 3 implies that any column in \( X \) cannot contain more than one nonconjugate entry or more than one conjugate entry. However, one column in \( X \) can contain one nonconjugate entry and one conjugate entry at the same time. Therefore, the columns in \( X \) can be partitioned into two types: 1) the columns containing one nonconjugate entry or one conjugate entry; 2) the columns containing one nonconjugate entry and one conjugate entry. In the following, we will refer to the first type of columns as the Type-I columns and refer to the second type of columns as the Type-II columns. For the Type-II columns, we have the following lemma.

Lemma 4: If a row-monomial DOSTBC \( X \) in variables \( s_1, \ldots, s_N \) exists, the Type-II columns in \( X \) have the following properties:

1) The total number of the Type-II columns in \( X \) is even.
2) In all the Type-II columns of \( X \), the total number of the entries containing \( s_n \) or \( s_n^* \), \( 1 \leq n \leq N \), is even.

Proof: See Appendix D.

Since the data-rate of \( X \) is defined as \( N/T \), improving the data-rate of \( X \) is equivalent to reducing the length \( T \) of \( X \), when \( N \) is fixed. Furthermore, we note that a Type-II column contains two nonzero entries; while a Type-I column contains only one nonzero entry. Therefore, if all the nonzero entries in \( X \) are contained in the Type-II columns, the data-rate of \( X \) achieves the maximum value. Unfortunately, in some circumstances, not all the nonzero entries in \( X \) can be contained in the Type-II columns. In those circumstances, in order to reduce \( T \), we need to make \( X \) contain nonzero entries in the Type-II columns as many as possible. Based on this and Lemmas 3 and 4, we derive an upper bound of the data-rate of the row-monomial DOSTBC and the result is given in the following theorem.

Theorem 2: If a row-monomial DOSTBC \( X \) in variables \( s_1, \ldots, s_N \) exists, its data-rate \( \mathcal{R}_r \), satisfies (12) shown at the top of the page, where \( N \geq 1 \) and \( K \geq 1 \).

Proof: See Appendix E.

Because the data-rate of the repetition-based cooperative strategy is just \( 1/K \), the data-rate of the row-monomial DOSTBC is approximately twice higher than that of the repetition-based cooperative strategy according to (12). As we stated before, these are the data-rates of the transmission from the relays to the destination. On the other hand, we can also consider the overall data-rate of the cooperative network, i.e., the data-rate of the entire transmission from the source terminal to the destination terminal. For example, when \( N \) and \( K \) are both even, it is not hard to see that the overall data-rate of the cooperative networks using the row-monomial DOSTBCs is \( 2/(2+K) \). On the other hand, the overall data-rate of the repetition-based cooperative strategy is \( 1/(1+K) \), which is always smaller than \( 2/(2+K) \) for nonnegative \( K \). Thus, we can conclude that the row-monomial DOSTBCs always have better bandwidth efficiency than the repetition-based cooperative strategy. Note that the better bandwidth efficiency of the row-monomial DOSTBCs is achieved without losing the single-symbol ML decodability or the full diversity order.

But we notice that the upper bounds of the data-rates of the row-monomial DOSTBCs decrease when \( K \) increases. For a large cooperative network, the row-monomial DOSTBCs will not have good bandwidth efficiency. Therefore, although the row-monomial DOSTBCs are designed for a cooperative network with an arbitrary \( K \), it may be preferable to implement them only for a cooperative network with a small \( K \). When \( K \) is large, we may improve the bandwidth efficiency by relaxing the constraint of single-symbol ML decodability. Furthermore, when \( K \) is larger, it is harder to achieve good synchronization among the relay terminals.

V. SYSTEMATIC CONSTRUCTION OF THE ROW-MONOMIAL DOSTBCS

ACHIEVING THE UPPER BOUND OF THE DATA-RATE

In this section, we present the systematic construction methods of the row-monomial DOSTBCs. For given \( N \) and \( K \), we use \( X(N, K) \) to denote the code generated by the systematic construction method. There are four different cases depending on the values of \( N \) and \( K \).
A. \( N = 2l \) and \( K = 2m \)

For convenience, we will use \( \mathbf{A}_k(:, t_1 : t_2) \) to denote the submatrix consisting of the \( t_1 \) th, \( t_1 + 1 \) th, \( \ldots \), \( t_2 \) th columns of \( \mathbf{A}_k \). Similarly, \( \mathbf{B}_k(:, t_1 : t_2) \) denotes the submatrix consisting of the \( t_1 \) th, \( t_1 + 1 \) th, \( \ldots \), \( t_2 \) th columns of \( \mathbf{B}_k \). Furthermore, define \( \mathbf{G}_s \) as follows:

\[
\mathbf{G}_s = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{13}
\]

Based on \( \mathbf{G}_s \), two matrices \( \mathbf{G}_\lambda \) and \( \mathbf{G}_H \) with dimension \( N \times N \) are defined:

\[
\mathbf{G}_\lambda = \text{diag}[1, -1, 1, -1, \ldots, 1, -1] \tag{14}
\]

\[
\mathbf{G}_H = \text{diag}[\mathbf{G}_s, \ldots, \mathbf{G}_s]. \tag{15}
\]

The proposed systematic construction method of the row-monomial DOSTBCs achieving the upper bound of (12) is as follows.

Construction I:

**Initialization:** Set \( p = 1 \). Set \( \mathbf{A}_k = \mathbf{B}_k = 0_{N \times \infty}, 1 \leq k \leq K \), where \( \infty \) means that the length of the matrices is not decided.

**Step 1:** Set \( \mathbf{A}_{p-1}(:, (p-1)N + 1 : pN) = \mathbf{G}_\lambda \) and \( \mathbf{B}_{p-1}(:, (p-1)N + 1 : pN) = \mathbf{G}_H \).

**Step 2:** Set \( p = p + 1 \). If \( p \leq m \), go to Step 1; otherwise, go to Step 3.

**Step 3:** Discard the all-zero columns at the tail of \( \mathbf{A}_{K-1} \) and \( \mathbf{B}_K \). Set the length of \( \mathbf{A}_K \) and \( \mathbf{B}_K, 1 \leq k \leq K \) equal to that of \( \mathbf{A}_{K-1} \) and \( \mathbf{B}_K \).

**Step 4:** Calculate \( \mathbf{X}(N, K) \) through (4) by using the matrices \( \mathbf{A}_k \) and \( \mathbf{B}_k \) obtained in Steps 1–3, and end the construction.

The following lemma shows that Construction I generates the row-monomial DOSTBCs achieving the upper bound of (12) for any even \( N \) and \( K \).

**Lemma 5:** For any even \( N = 2l \) and \( K = 2m \), the codes generated by Construction I achieve the data-rate \( 1/m \).

**Proof:** In Construction I, the length of \( \mathbf{A}_k \) and \( \mathbf{B}_k, 1 \leq k \leq K \), is decided by the length of \( \mathbf{A}_{K-1} \) and \( \mathbf{B}_K \). Because \( \mathbf{A}_{K-1}(:, (m-1)N + 1 : mN) \) and \( \mathbf{B}_K(:, (m-1)N + 1 : mN) \) are set to be \( \mathbf{G}_\lambda \) and \( \mathbf{G}_H \), respectively, the length of \( \mathbf{A}_k \) and \( \mathbf{B}_k, 1 \leq k \leq K \) is \( mN \). Consequently, the value of \( T \) and \( mN \), and hence, the data-rate of \( \mathbf{X}(N, K) \) is \( 1/m \).

For example, when \( N = 4 \) and \( K = 4 \), the code constructed by Construction I is given by (16) shown at the bottom of the page and it achieves the upper bound of the data-rate \( 1/2 \).

B. \( N = 2l + 1 \) and \( K = 2m \)

This case is equivalent with the case that \( N = 2l \) and \( K = 2m \) if \( s_N \) is not considered. Based on this, the proposed systematic construction method of the row-monomial DOSTBCs achieving the upper bound of (12) is as follows.

Construction II:

**Step 1:** Neglect \( s_N \) and construct a \( K \times 2lm \) matrix \( \mathbf{X}_1 \) in variables \( s_1, \ldots, s_{N-1} \) by Construction I.

**Step 2:** Form a \( K \times K \) diagonal matrix \( \mathbf{X}_2 = \text{diag}[h_{1}, h_{1}, \ldots, h_{K}, h_{K}] \).

**Step 3:** Let \( \mathbf{X}(N, K) = [\mathbf{X}_1, \mathbf{X}_2] \) and end the construction.

Because the length of \( \mathbf{X}_1 \) and \( \mathbf{X}_2 \) is \( 2lm \) and \( K \), respectively, the length of \( \mathbf{X}(N, K) \) is \( 2lm + K \). Thus, the data-rate of \( \mathbf{X}(N, K) \) is \((2l + 1)/(2lm + K)\), which is exactly the same as the upper-bound of (12).

C. \( N = 2l \) and \( K = 2m + 1 \)

This case is equivalent with the case that \( N = 2l \) and \( K = 2m + 1 \) if the \( K \) th relay terminal is not considered. Based on this, the proposed systematic construction method of the row-monomial DOSTBCs achieving the upper bound of (12) is as follows.

Construction III:

**Step 1:** Neglect the \( K \) th relay terminal and construct a \( 2m \times 2lm \) matrix \( \mathbf{X}_1 \) by Construction I.

**Step 2:** Form a vector \( \mathbf{x}_2 = [h_{K, s_{1}}, \ldots, h_{K, s_{N}}] \).

**Step 3:** Build a block diagonal matrix \( \mathbf{X}(N, K) = \text{diag}[\mathbf{X}_1, \mathbf{x}_2] \) and end the construction.

Because the length of \( \mathbf{X}_1 \) and \( \mathbf{x}_2 \) is \( 2lm \) and \( N \), respectively, the length of \( \mathbf{X}(N, K) \) is \( 2lm + N \). Thus, the data-rate of \( \mathbf{X}(N, K) \) is \((1 + 1)/(1 + m)\), which is exactly the same as the upper-bound of (12).

D. \( N = 2l + 1 \) and \( K = 2m + 1 \)

For this case, the proposed systematic construction method of the row-monomial DOSTBCs is as follows:

Construction IV:

Part I:

**Initialization:** Set \( p = 0 \) and \( S = \{s_1, \ldots, s_N\} \).

**Step 1:** Neglect \( s_{1+\text{mod}(p, N)} \) and construct a \( 2 \times 2lm \) matrix \( \mathbf{X}(p) \) in variables \( S - \{s_{1+\text{mod}(p, N)}\} \) by Construction I.

**Step 2:** Set \( p = p + 1 \). If \( p < m \), go to Step 1; otherwise, go to Step 3.

**Step 3:** Let \( \mathbf{X}_1 = \text{diag}[\mathbf{X}_1^{(0)}, \ldots, \mathbf{X}_1^{(m-1)}] : 0_{1 \times 2lm} \) and proceed to Part II.

Part II:

**Initialization:** Set \( p = 0 \), \( S^{(K)} = S \), and \( c = 1 \). Construct a \( K \times \infty \) matrix \( \mathbf{X}_2 \) with all zero entries, where \( \infty \) means that the length of \( \mathbf{X}_2 \) is not decided yet.

**Step 1:** Set \( [\mathbf{X}_2]_{2p+1, c} = h_2^{p+1} s_{1+\text{mod}(p, N)} \).

**Step 2:** If \( S^{(K)} = \emptyset \), set \( c = c + 1 \) and go to Step 4.

**Step 3:** Choose the element with the largest subscript from \( S^{(K)} \) and denote it by \( s_{\text{max}} \). Let \( [\mathbf{X}_2]_{K, c} = h_{K, s_{\text{max}}} \) and set \( c = c + 1 \). Let \( [\mathbf{X}_2]_{2p+2, c} = h_2^{p+1} s_{1+\text{mod}(p, N)} \).

**Step 4:** If \( S^{(K)} = \emptyset \), set \( c = c + 1 \) and go to Step 8.

**Step 7:** Choose the element with the largest subscript from \( S^{(K)} \) and denote it by \( s_{\text{max}} \). Let \( [\mathbf{X}_2]_{K, c} = h_{K, s_{\text{max}}} \) and set \( c = c + 1 \). Let

\[
\mathbf{X}(4,4) = \begin{bmatrix}
 h_{1, s_1} & -h_{1, s_2} & h_{1, s_3} & -h_{1, s_4} & 0 & 0 & 0 & 0 \\
 h_{2, s_2} & h_{2, s_1} & h_{2, s_4} & h_{2, s_3} & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & h_{3, s_1} & -h_{3, s_2} & h_{3, s_3} & -h_{3, s_4} \\
 0 & 0 & 0 & 0 & h_{4, s_2} & h_{4, s_1} & h_{4, s_3} & h_{4, s_4}
\end{bmatrix} \tag{16}
\]
VII. Numerical Results

In this section, we compare the performance of the proposed code \( X(4, 4) \), the repetition-based cooperative strategy, the distributed linear dispersion codes in [17], and the quasi-orthogonal distributed space–time codes in [21]. \( N = 4, \, K = 4 \).

For any odd \( N \leq 9 \) and \( K \leq 9 \), we have confirmed that the codes generated by Construction IV achieve the upper bound of (12) indeed. In general, however, it is hard to prove that Construction IV can generate the row-monomial DOSTBCs achieving the upper bound of (12) for any odd \( N \) and \( K \).

VI. Numerical Results

In this section, we compare the performance of the proposed code \( X(4, 4) \), the repetition-based cooperative strategy, the distributed linear dispersion codes in [17], and the quasi-orthogonal distributed space–time codes in [21]. We plot the average Bit Error Rate (BER) against the average Signal to Noise Ratio (SNR) per bit, where the average SNR per bit equals to the ratio of \( E_b \) to the logarithm of the size of the modulation scheme. Furthermore, the optimum power allocation proposed in [17] is adopted, i.e., \( E_b = K E_r \). The comparison results are given in Fig. 1. It can be seen that the performance of the row-monomial DOSTBCs is much better than that of the repetition-based cooperative strategy in the whole SNR range. The performance gain of the row-monomial DOSTBCs is even more impressive when the bandwidth efficiency is 2 b/s/Hz. Furthermore, because the BER curves of the row-monomial DOSTBCs are parallel with those of the repetition-based cooperative strategy, the row-monomial DOSTBCs indeed achieve the full diversity order \( K \). Compared to the distributed linear dispersion codes in [17] and the quasi-orthogonal distributed space–time codes in [21], the row-monomial DOSTBCs have worse performance. However, the row-monomial DOSTBCs have much less decoding complexity, because they are single-symbol ML decodable.

VIII. Conclusion

We have first studied the DOSTBCs and showed that the DOSTBCs are single-symbol ML decodable and have the full diversity order \( K \). Then, further investigation has been given to the row-monomial DOSTBCs and an upper bound of the data-rate of the row-monomial DOSTBC has been derived. Compared to the repetition-based cooperative strategy, the row-monomial DOSTBCs achieve approximately twice higher data-rate without losing the single-symbol ML decodability or the full diversity order. Furthermore, systematic construction methods of the row-monomial DOSTBCs have been developed. When \( N \) and/or \( K \) are both odd, the proof has not been found; but we have confirmed that the codes generated by the systematic construction methods always achieve the upper-bound of the data-rate. When \( N \) and \( K \) are both odd, the proof has not been found; but we have confirmed that the codes generated by the systematic construction method achieve the upper-bound of the data-rate for \( N \) and \( K \) up to 9.

Appendix A

Proof of Lemma 2

In this proof, for a matrix \( H \), we use \( \lambda_{\text{max}}(H) \) to denote its largest eigenvalue; \( d(H) \) is its spectral radius; \( |H| \) the matrix containing the absolute value of the entries in \( H \). As in [25], we use \( \leq \) and \( \geq \) to denote the asymptotic exponential equality and inequality, respectively.

The proof starts by defining \( \tilde{w} \) and \( \tilde{X} \) as follows:

\[
\tilde{w} = [\rho f_1|h_1|, \ldots, \rho f_K|h_K|]
\]
where \( \phi_k \) is the phase of \( h_k \). Consequently, we have \( \mathbf{y}_D = \bar{\mathbf{w}} \mathbf{X} + \mathbf{n} \) from (6). When \( \bar{\mathbf{w}} \) is given, the mutual information between \( \mathbf{y}_D \) and \( \mathbf{X} \) is given by

\[
I(\mathbf{X}; \mathbf{y}_D | \bar{\mathbf{w}}) = \log(1 + \bar{\mathbf{w}}^H \mathbf{X}^H \mathbf{X} \bar{\mathbf{w}}^H) \geq \log \left( 1 + \frac{1}{\lambda_{\text{max}}(\mathbf{R})} \bar{\mathbf{w}}^H \mathbf{X}^H \mathbf{X} \bar{\mathbf{w}}^H \right).
\]

(A3)

In general, \( \mathbf{R} \) is not a diagonal matrix and we can write \( \mathbf{R} = \mathbf{R}_D + \mathbf{R}_O \), where \( \mathbf{R}_D \) and \( \mathbf{R}_O \) contain the main diagonal and the off-diagonal entries of \( \mathbf{R} \), respectively. From [26], the following inequalities hold:

\[
\lambda_{\text{max}}(\mathbf{R}_O) \leq d(\mathbf{R}_O) \leq d(\mathbf{R}_D) \leq \lambda_{\text{max}}(\mathbf{R}_D) \leq \lambda_{\text{max}}(\mathbf{R}_O) \leq \lambda_{\text{max}}(\mathbf{R})
\]

(A4)

The fourth inequality is because \( \sum_{k=1}^{K} |[\mathbf{R}]_{k,k}| \leq [\mathbf{R}]_{k,k,k} \), which can be seen from (7) and the first two properties in Lemma 1. Furthermore, we have [26]

\[
\lambda_{\text{max}}(\mathbf{R}) \leq \lambda_{\text{max}}(\mathbf{R}_O) + \lambda_{\text{max}}(\mathbf{R}_D) \leq 2 \lambda_{\text{max}}(\mathbf{R}_D)
\]

(A5)

where the last inequality is from (7) and the first two properties in Lemma 1.

In [27], it has been shown that \( 1 + \sum_{k=1}^{K} |\rho |f_k|^2 \) is independent of \( E \), i.e., \( 1 + \sum_{k=1}^{K} |\rho |f_k|^2 = E^2 \). Thus, we have

\[
I(\mathbf{X}; \mathbf{y}_D | \bar{\mathbf{w}}) \geq \log \left( 1 + \bar{\mathbf{w}}^H \mathbf{X}^H \mathbf{X} \bar{\mathbf{w}}^H \right)
\]

(A6)

where the last step is because \( T \geq K \) and \( \mathbf{X} \) is full rank. In [27], it has been shown that the average outage probability of (A7) decays with \( E \) as fast as \( 1/E^K \). Therefore, the average outage probability of the cooperative networks using the DOSTBCs decays with \( E \) as fast as \( 1/E^K \), i.e., the full diversity order \( K \) is achieved.

APPENDIX B

PROOF OF THEOREM 1

The sufficient part is easy to verify. We only prove the necessary part here, i.e., if \( \mathbf{R} \) is a diagonal matrix, \( \mathbf{A}_1 \) and \( \mathbf{B}_1 \) are row-monomial. This is done by contradiction. If \( \mathbf{R} \) is a diagonal matrix, the off-diagonal entries \( [\mathbf{R}]_{t_1,t_2}, 1 \leq t_1 \neq t_2 \leq T \), are equal to zero. According to (7), we have

\[
[R]_{t_1,t_2} = \sum_{k=1}^{K} |f_k|^2 \left[ \sum_{n=1}^{N} [A_k]_{n,t_1} [A_k]_{n,t_2} \right] = 0.
\]

(B1)

In order to make the equality hold for every possible \( f_k \), the following equality must hold:

\[
\sum_{n=1}^{N} [A_k]_{n,t_1} [A_k]_{n,t_2} + \sum_{n=1}^{N} [B_k]_{n,t_1} [B_k]_{n,t_2} = 0, \quad 1 \leq k \leq K.
\]

(B2)

Let us assume that the \( n \)th, \( 1 \leq n' \leq N \), row of \( A_k \) contains two nonzero entries: \( [A_k]_{n',t_1} \) and \( [A_k]_{n',t_2} \). Because \( A_k \) is column-monomial according to Lemma 1, \( [A_k]_{n,t_1} = [A_k]_{n,t_2} = 0, 1 \leq n \neq n' \leq N \), and hence

\[
\sum_{n=1}^{N} [A_k]_{n,t_1} [B_k]_{n,t_2} = [A_k]_{n',t_1} [B_k]_{n',t_2} \neq 0.
\]

(B3)

On the other hand, because \( A_k \) and \( B_k \) can not have nonzero entries at the same place according to Lemma 1, we have \( [B_k]_{n,t_1} = [B_k]_{n,t_2} = 0 \). Furthermore, because \( A_k + B_k \) is column-monomial, \( [B_k]_{n,t_2} = 0, 1 \leq n \neq n' \leq N \). Therefore, \( [B_k]_{n,t_1} = [B_k]_{n,t_2} = 0 \), and consequently, \( \sum_{n=1}^{N} [B_k]_{n,t_1} [B_k]_{n,t_2} = 0 \). It follows from (B2) and (B3)

\[
\sum_{n=1}^{N} [A_k]_{n,t_1} [A_k]_{n,t_2} = 0.
\]

(B4)

Because (B3) and (B4) contradict with each other, we can conclude that any row of \( A_k \) cannot contain two nonzero entries. Furthermore, in the same way, it can be easily shown that any row of \( A_k \) cannot contain more than two nonzero entries, and hence, \( A_k \) is row-monomial. Similarly, we can show that \( B_k \) is row-monomial, which completes the proof of the necessary part.

APPENDIX C

PROOF OF LEMMA 3

The proof is by contradiction. We assume that the \( t \)th column of \( A_{k_1} \) and \( A_{k_2} \), \( 1 \leq k_1 \neq k_2 \leq K \), contains a nonzero entry \([A_{k_1}]_{n,t} \) and a nonzero entry \([A_{k_2}]_{n,t} \), respectively. By Definition 2, \( A_{k_1} \) and \( A_{k_2} \) are both row-monomial, we have \( [A_{k_1}]_{n,t} = [A_{k_2}]_{n,t} = 0, 1 \leq t \neq t' \leq T \), and hence

\[
\sum_{t=1}^{T} [A_{k_1}]_{n,t} [R^{-1}]_{t,t'} [A_{k_2}]_{n,t'} = 0.
\]

(C1)

On the other hand, by the third property in Lemma 1 and the fact that \( \mathbf{R} \) is diagonal, \( [A_{k_1}]_{n,t} [A_{k_2}]_{n,t} = 0 \) is given by

\[
[A_{k_1}]_{n,t} [R^{-1}]_{t,t'} [A_{k_2}]_{n,t'} = 0.
\]

(C2)

Because (C1) and (C2) contradict with each other, we conclude that \( A_{k_1} \) and \( A_{k_2} \), \( 1 \leq k_1 \neq k_2 \leq K \), can not contain nonzero entries on the same column simultaneously. Therefore, \( A_{k_1} \) and \( A_{k_2} \) are column-disjoint when \( k_1 \neq k_2 \). Similarly, we can show that \( B_{k_1} \) and \( B_{k_2} \) are column-disjoint when \( k_1 \neq k_2 \).

APPENDIX D

PROOF OF LEMMA 4

If no Type-II column exists in \( \mathbf{X} \), it is trivial that the number of the Type-II columns in \( \mathbf{X} \) is even. If there is one Type-II column in \( \mathbf{X} \), without loss of generality, we assume that the \( t \)th column in \( \mathbf{X} \) is a Type-II column and it contains \( h_{k_1} s_{n_1} \) and \( h_{k_2} s_{n_2} \) on the \( k_1 \)th and \( k_2 \)th row, respectively. Consequently, \( \mathbf{X} [R^{-1} - \mathbf{X}^H h_{k_1} h_{k_2}] \) will contain the term \( h_{k_1} s_{n_1} h_{k_2} s_{n_2} [R^{-1}]_{t,t'} \). On the other hand, because \( \mathbf{X} \) is a row-monomial DOSTBC, \( \mathbf{X} [R^{-1} - \mathbf{X}^H h_{k_1} h_{k_2}] \) should be null by the definition. Thus, in order to cancel the term \( h_{k_1} s_{n_1} h_{k_2} s_{n_2} [R^{-1}]_{t,t'} \), there must be another Type-II column, for example the \( t_2 \)th column, \( t_1 \neq t_2 \), which contains \( -h_{k_1} s_{n_2} \) and \( h_{k_2} s_{n_1} \) on the \( k_1 \)th and \( k_2 \)th
row, respectively. Therefore, the Type-II columns in $X$ always appear in pairs, and hence, the total number of the Type-II columns in $X$ is even.

For convenience, we will refer to any entry in $X$ that contains $s_l$ or $s_r$ as the $s_l$-entry. If no $s_l$-entry exists in the Type-II columns of $X$, it is trivial that the total number of $s_l$-entries in the Type-II columns of $X$ is even. If there is one $s_l$-entry in a Type-II column of $X$, we assume it contains $s_l$ without loss of generality. From the proof of the first property in Lemma 4, we can see that there must be an $s_r$-entry in another Type-II column and it contains $s_r$. Therefore, in the Type-II columns of $X$, the $s_l$-entries always appear in pairs, and hence, the total number of the $s_l$-entries in the Type-II columns of $X$ is even.

**APPENDIX E**

**PROOF OF THEOREM 2**

For convenience, we will refer to any entry in $X$ that contains $s_l$ or $s_r$ as the $s_l$-entry. Let $U$ denote the total number of nonzero entries in $X$; $V_n$ the total number of $s_l$-entries in $X$; $W_k$, the total number of nonzero entries in the $k$th row of $X$. Obviously, $U = \sum_{n=1}^{N} V_n = \sum_{k=1}^{N} W_k$. According to the fourth property in Lemma 1, at least one $A_{l,m}$ is nonzero, $1 \leq n \leq N$ and $1 \leq k \leq K$. Thus, every row of $X$ has at least one $s_l$-entry, $1 \leq n \leq N$. On the other hand, by the row-monomial condition of $A_{l,k}$ and $B_{l,k}$, every row of $X$ has at most two $s_l$-entries, where one contains $s_l$ and the other contains $s_r$. Therefore, every row of $X$ contains at least $N$ and at most $2N$ nonzero entries, i.e., $N \leq W_k \leq 2N, 1 \leq k \leq K$. For the same reason, we have $K \leq V_n \leq 2K, 1 \leq n \leq N$. Consequently, we have $N^n \leq U \leq 2N^n$. 

**Case I:** $N = 2l$ and $K = 2m$. When $N = 2l$ and $K = 2m$, $U \geq N^n = 4lm$. Because a pair of Type-II columns contains 4 nonzero entries, at least $4lm/4$ pairs of Type-II columns are needed to transmit all the nonzero entries. Since $T$ is the total number of columns in $X$, we have the following inequality:

$$T \geq 2 \left(4lm/4\right) = 2lm$$

and hence

$$R_e \leq \frac{1}{m}.$$  

**(E2)**

**Case II:** $N = 2l + 1$ and $K = 2m$. When $N = 2l + 1$ and $K = 2m$, without loss of generality, we assume $W_1, \ldots, W_n$ are even and $W_{n+1}, \ldots, W_{2m}$ are odd, where $1 \leq w \leq 2m$. We first have $U \geq N^n = 4lm + 2m$. Furthermore, because $W_k$ is even for $1 \leq k \leq w$, $W_k \geq N + 1 = 2l + 2$. Consequently, $U \geq 4lm + 2m + w$. On the other hand, because the Type-II columns always appear in pairs, the $k$th row of $X$, $w + 1 \leq k \leq 2m$, must contain at least one Type-I column; otherwise, $W_k$ will be even, which violates our assumption. Therefore, there are at least $2m - w$ Type-I columns in $X$ and they contain $2m - w$ nonzero entries. Because a pair of Type-II columns contains 4 nonzero entries, the rest nonzero entries need at least $[(4lm + 2m + w - (2m - w))/4]$ pairs of Type-II columns to transmit. Therefore, we have the following inequality:

$$T \geq 2m - w + 2 \left[\frac{4lm + 2m + w - (2m - w)}{4}\right]$$

and hence

$$R_e \leq \frac{2l + 1}{2lm + 2m}.$$  

**(E5)**

**Case III:** $N = 2l$ and $K = 2m + 1$. When $N = 2l$ and $K = 2m + 1$, without loss of generality, we assume $V_1, \ldots, V_n$ are even and $V_{n+1}, \ldots, V_{2m}$ are odd, where $1 \leq v \leq 2m + 1$. We first have $U \geq N^n = 4lm + 2l$. Furthermore, because $V_v$ is even for $1 \leq v \leq n$, $V_v \geq K + 1 = 2m + 2$. Consequently, $U \geq 4lm + 2m + v$. On the other hand, because the total number of $s_l$-entries in the Type-II columns of $X$ is even, at least one $s_r$-entry, $v + 1 \leq n \leq 2m + 1$, is in a Type-I column; otherwise, $V_v$ will be even, which violates our assumption. Thus, there are at least $2l - v$ Type-I columns in $X$ and they contain $2l - v$ nonzero entries. Because a pair of Type-II columns contains 4 nonzero entries, the rest nonzero entries need at least $[(4lm + 2l + v - (2l - v))/4]$ pairs of Type-II columns to transmit. Therefore, we have the following inequality:

$$T \geq 2l - v + 2 \left[\frac{4lm + 2l + v - (2l - v)}{4}\right]$$

and hence

$$R_e \leq \frac{2l + 1}{2lm + 2m + 2}.$$  

**(E6)**

**Case IV:** $N = 2l + 1$ and $K = 2m + 1$. When $N = 2l + 1$ and $K = 2m + 1$, we can assume that $W_1, \ldots, W_n$ are even and $W_{n+1}, \ldots, W_{2m+1}$ are odd, where $1 \leq w \leq 2m + 1$. By following the proof of Case II, we have

$$T \geq 2m + 1 - w + 2 \left[\frac{4lm + 2l + 2m + 1 + w - (2m + 1 - w)}{4}\right]$$

and hence

$$R_e \leq \frac{1}{m + 1}.$$  

**(E10)**

On the other hand, we can assume $V_1, \ldots, V_n$ are even and $V_{n+1}, \ldots, V_{n+1}$ are odd, where $1 \leq v \leq 2l + 1$. By following the proof of Case III, we have

$$T \geq 2l + 1 - v + 2 \left[\frac{4lm + 2l + 2m + 1 + v - (2l + 1 - v)}{4}\right]$$

and hence

$$R_e \leq \frac{2l + 1}{2lm + 2m + 2}.$$  

**(E17)**

From (E13) and (E16), it is immediate that

$$T \geq \max(2lm + 2m + l + 1, 2lm + 2m + l + 1)$$

and hence

$$R_e \leq \min\left(\frac{2l + 1}{2lm + 2m + l + 1}, \frac{2l + 1}{2lm + 2m + l + 1}\right).$$  

**(E18)**

**REFERENCES**

[1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—Part I: System description," IEEE Trans. Commun., vol. 51, pp. 1927–1938, Nov. 2003.
Further Result of Compressing Maps on Primitive Sequences Modulo Odd Prime Powers

Xuan-Yong Zhu and Wen-Feng Qi

Abstract—Let $\mathbb{Z}/(p^n)$ be the integer residue ring with odd prime $p$ and integer $n \geq 2$. For a sequence $\mathbf{a}$ over $\mathbb{Z}/(p^n)$, there is an unique $p$-adic expansion $\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_1 p + \cdots + \mathbf{a}_{n-1} p^{n-1}$, where each $\mathbf{a}_i$ is a sequence over $\{0, 1, \ldots, p-1\}$, and can be regarded as a sequence over the prime field $\mathbb{F}_p$ naturally. Let $f(x)$ be a strongly primitive polynomial over $\mathbb{Z}/(p^n)$, and $G(f(x), p^n)$ the set of all primitive sequences generated by $f(x)$ over $\mathbb{Z}/(p^n)$. Suppose that $f = [g(x_{n-1}) + \eta_1 x_{n-2} + \cdots + \eta_{n-2} x_0] \in \mathbb{F}_p[x]$, $2 \leq \deg(g(x)) \leq n-1$, $\eta \in \mathbb{F}_p$, and $[g(x_{n-1}) \neq 0]$. It is shown that any function in $G$ is an injective map from $G(f(x), p^n)$ to $\mathbb{F}_p^{\infty}$, and the derived sequences of different functions are also different. That is, if $f(x) = g(x) + \eta x_{n-1}$ and $\varphi$ and $\psi$ are in $G$, then $\varphi = \psi$ if and only if $a = b$ for $\varphi, \psi \in G$ and $\mathbf{a} \equiv \mathbf{b} \pmod{p^n}$, where $p$ is an odd prime. These injective functions in $G$ can be considered as good candidates for the keys of a stream cipher.

Index Terms—Compressing map, integer residue ring, linear recurring sequence, primitive sequence.

I. INTRODUCTION

Suppose $p$ is a prime and $R_p = \mathbb{Z}/(p^n)$ is the integer residue ring modulo $p^n$, which can be also represented as $\{0, 1, \ldots, p^n - 1\}$. In this correspondence, given integer $m \geq 2$, we always consider $a \pmod{m}$ as an element in $\{0, 1, \ldots, m-1\}$. Let $f(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_0$ be a monic polynomial with degree $n \geq 1$ over $R_p$. A sequence $a = (a(t))_{t \geq 0}$ over $R_p$, satisfying the recursion $a(i+n) = -[a_0(i) + c_1(i+1) + \cdots + c_{n-1} a(i+1)] \pmod{p^n}$, $i = 0, 1, 2, \ldots$, is called a linear recurring sequence of degree $n$ over $R_p$. Let $G(f(x), p^n)$ denotes the set of all sequences over $R_p$ generated by $f(x)$. Reference [10] is a good introduction on the linear recurring sequence over $R_p$. Let $a = \langle a(t) \rangle_{t \geq 0}$ and $b = \langle b(t) \rangle_{t \geq 0}$ be sequences over $R_p$ and $c \in R_p$. Define

$$a + b = \langle a(t) + b(t) \pmod{p^n} \rangle_{t \geq 0},$$

$$a \cdot b = \langle a(t) \cdot b(t) \pmod{p^n} \rangle_{t \geq 0},$$

and the left shift operator of sequence as

$$x^k \cdot a = \langle a(t+k) \rangle_{t \geq 0}, \quad k = 0, 1, 2, \ldots.$$

So we have

$$G(f(x), p^n) = \{ \mathbf{a} \in R_p^{\infty} | f(x) \cdot \mathbf{a} = \mathbf{0} \}.$$

Especially, we set

$$G'(f(x), p^n) = \{ \mathbf{a} \in G(f(x), p^n) | \mathbf{a} \not\equiv \mathbf{0} \pmod{p^n} \}.$$