

# On the Feasibility of Precoding-Based Network Alignment for Three Unicast Sessions

Chun Meng, Abinеш Ramakrishnan, Athina Markopoulou, Syed Ali Jafar

Department of Electrical Engineering and Computer Science

University of California, Irvine

Email: {cmengl, abinеш.r, athina, syed}@uci.edu

**Abstract**—We consider the problem of network coding across three unicast sessions over a directed acyclic graph, when each session has min-cut one. Previous work by Das et al. adapted a precoding-based interference alignment technique, originally developed for the wireless interference channel, specifically to this problem. We refer to this approach as precoding-based network alignment (PBNA). Similar to the wireless setting, PBNA asymptotically achieves half the minimum cut; different from the wireless setting, its feasibility depends on the graph structure. Das et al. provided a set of feasibility conditions for PBNA with respect to a particular precoding matrix. However, the set consisted of an infinite number of conditions, which is impossible to check in practice. Furthermore, the conditions were purely algebraic, without interpretation with regards to the graph structure. In this paper, we first prove that the set of conditions provided by Das et al. are also necessary for the feasibility of PBNA with respect to *any* precoding matrix. Then, using two graph-related properties and a degree-counting technique, we reduce the set to just four conditions. This reduction enables an efficient algorithm for checking the feasibility of PBNA on a given graph.

## I. INTRODUCTION

Network coding was originally introduced to maximize the rate of a single multicast session over a network [1] [2] [3]. However, network coding across different sessions, which includes *multiple unicasts* as a special case, is a well-known open problem. For example, finding linear network codes for multiple unicasts is NP-hard [4]. Thus, suboptimal, heuristic approaches, such as linear programming [5] and evolutionary approaches [6], are typically used. Moreover, while it has been shown that scalar or vector linear network codes might be insufficient to achieve the optimal rate [7], only approximation methods [8] exist to characterize the rate region for this setting.

In this paper, we consider the simplest inter-session linear network coding scenario: three unicast sessions over a directed acyclic graph, each session with minimum cut one. Das et al. [9] applied a precoding-based interference alignment technique, originally developed by Cadambe and Jafar [10] for wireless interference channel, to this problem; we refer to this technique as *precoding-based network alignment (PBNA)*. In a nutshell, PBNA (i) simulates a wireless channel through random network coding [3] in the middle of the network and (ii) applies interference alignment at the edge, i.e., via precoding at the sources and decoding at the receivers. This way, it greatly simplifies the network code design, while it

guarantees that each unicast session asymptotically achieves a rate equal to half of its minimum cut [9].

An important difference from the wireless interference channel is that, in our problem, there may be dependencies between elements of the transfer matrix introduced by the graph structure, which make PBNA infeasible in some networks [11]. As a first step, Das et al. [9] provided a set of feasibility conditions for PBNA, and proved they are sufficient for the feasibility of PBNA with respect to a particular precoding matrix. One important limitation is that the set consists of an infinite number of conditions, which makes it impossible to check in practice. Another limitation is the lack of consideration of graph structure, which turns out to be the reason for the significant redundancy in the set of conditions. Ramakrishnan et al. [11] conjectured that the infinite set of conditions can be reduced to just two conditions. Han et al. [12] proved that the conjecture holds for three symbol extensions; however, this result cannot be generalized beyond three symbol extensions.

In this paper, we make the following contributions. First, we prove that the set of conditions provided in [9] are also necessary for the feasibility of PBNA with respect to *any* valid precoding matrix. Then, using a simple degree-counting technique and two graph-related properties, we greatly reduce the set to just three conditions; two of them turn out to have an intuitive interpretation in terms of graph structure. Finally, we present an efficient algorithm for checking the three conditions.

The rest of this paper is organized as follows. In Section II, we present the problem formulation. In Section III, we summarize our main results. In Section IV, we discuss the graph-related properties that are key to the simplification of the conditions. In Section V, we prove and discuss our main results regarding the feasibility condition of PBNA. In Section VI, we present an algorithm for checking the condition. In Section VII, we conclude the paper. The Appendices provide details on the proofs that were outlined or omitted from the main part of the paper.

## II. PROBLEM FORMULATION

The network is a delay-free directed acyclic graph, denoted by  $G = (V, E)$ , where  $V$  is the set of nodes and  $E$  the set of edges. Without loss of generality, each edge has capacity one, i.e., can transmit one symbol of finite field  $\mathbb{F}_{2^m}$  in a unit time. For the  $i$ th unicast session ( $i \in \{1, 2, 3\}$ ), let  $s_i$  and  $d_i$  be its sender and receiver respectively, and  $R_i$  its transmission rate. Every edge  $e \in E$  represents an error free channel. We assume

that the minimum cut between  $s_i$  and  $d_i$  is one. Let  $X_i$  be the source symbol transmitted at  $s_i$  and  $Z_i$  be the symbol received at  $d_i$ . We further extend  $G$  as follows: For the  $i$ th unicast session ( $i \in \{1, 2, 3\}$ ), we add a virtual sender  $s'_i$  and a virtual receiver  $d'_i$  and two edges  $\sigma_i = (s'_i, s_i)$  and  $\tau_i = (d_i, d'_i)$ . The extended graph is denoted by  $G' = (V', E')$ . For  $e \in E'$ , let  $head(e)$  and  $tail(e)$  denote its head and tail respectively.

In the middle of the network, we employ random network coding [3] to mimic wireless channel. The symbol transmitted along  $e \in E'$ , denoted by  $Y_e$ , is a linear combination of incoming symbols at  $tail(e)$ .

$$Y_e = \begin{cases} X_i & \text{If } e = \sigma_i; \\ \sum_{head(e')=tail(e)} x_{e'e} Y_{e'} & \text{Otherwise.} \end{cases}$$

where  $x_{e'e}$  is a variable, which takes values from  $\mathbb{F}_{2^m}$  and represents the coding coefficient used to combine the incoming symbol along  $e'$  into the symbol along  $e$ . We group all coding coefficients  $x_{e'e}$ 's into a vector  $\mathbf{x}$ , called the coding vector of  $G'$ . The network acts as a linear system: the output at  $d'_i$  is a mixture of source symbols,  $Z_i = \sum_{j=1}^3 m_{ij}(\mathbf{x}) X_j$ , where  $m_{ij}(\mathbf{x}) \in \mathbb{F}_{2^m}[\mathbf{x}]$  is the *transfer function* from  $s'_j$  to  $d'_i$  and can be written as follows [2]:

$$m_{ij}(\mathbf{x}) = \sum_{P \in \mathcal{P}_{ij}} t(P)$$

where  $\mathcal{P}_{ij}$  is the set of paths from  $s'_j$  to  $d'_i$ , and  $t(P)$  is the product of coding coefficients along path  $P$ . We assume that all  $m_{ij}(\mathbf{x})$ 's are non-zeros, which is the most challenging case. Indeed, as shown in Section V, when some  $m_{ij}(\mathbf{x})$  ( $i \neq j$ ) is zero, the feasibility condition of PBNA is significantly simplified due to reduced number of interferences.

At the edge of the network, we apply interference alignment [9] [10] via precoding at senders and decoding at receivers. Let  $\mathbf{X}_i = (X_i^1, \dots, X_i^{k_i})^T$  denote the input vector at sender  $s'_i$ , where  $k_i$  is a two-phase function of some integers  $n$ , depending on whether  $i$  equals one:

$$k_i = \begin{cases} L_1(n) & \text{if } i = 1 \\ L_2(n) & \text{otherwise.} \end{cases}$$

where  $L_1 : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  and  $L_2 : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  are two functions defined on  $\mathbb{Z}^+$ . We will determine  $L_1(n)$  and  $L_2(n)$  later in this section. In order for PBNA to work properly, we require  $L_1(n)$  and  $L_2(n)$  satisfy the following condition:

$$L_1(n) \geq L_2(n) \quad (1)$$

$$\lim_{n \rightarrow \infty} \frac{L_1(n)}{L_2(n)} = 1 \quad (2)$$

Define  $L(n) = L_1(n) + L_2(n)$ . As we will see later, the above two conditions are essential in the construction of a valid solution to PBNA. We use *precoding matrix*  $\mathbf{V}_i$  to encode  $\mathbf{X}_i$  into  $L(n)$  symbols, which are then transmitted via  $L(n)$  uses of the network (time slots). The output vector at  $d'_i$  is

$$\mathbf{Z}_i = (Z_i^1, \dots, Z_i^{L(n)})^T = \sum_{j=1}^3 \mathbf{M}_{ij} \mathbf{V}_j \mathbf{X}_j$$

where  $\mathbf{M}_{ij}$  is a  $L(n) \times L(n)$  diagonal matrix with the  $(k, k)$  element being  $m_{ij}(\mathbf{x}^k)$ , where  $\mathbf{x}^k$  represents the coding vector

for the  $k$ th use of the network.  $\mathbf{V}_1$  is a  $L(n) \times L_1(n)$  matrix, and  $\mathbf{V}_2, \mathbf{V}_3$  are both  $L(n) \times L_2(n)$  matrices.  $\mathbf{V}_i$  can still contain indeterminate variables. Let  $\xi$  denote the vector of all variables in  $\mathbf{x}^1, \dots, \mathbf{x}^{L(n)}$  and  $\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3$ . We require the following conditions are satisfied for some values of  $\xi$  [10]:

$$\begin{aligned} \mathcal{A}_1 &: \text{span}(\mathbf{M}_{12} \mathbf{V}_2) = \text{span}(\mathbf{M}_{13} \mathbf{V}_3) \\ \mathcal{A}_2 &: \text{span}(\mathbf{M}_{23} \mathbf{V}_3) \subseteq \text{span}(\mathbf{M}_{21} \mathbf{V}_1) \\ \mathcal{A}_3 &: \text{span}(\mathbf{M}_{32} \mathbf{V}_2) \subseteq \text{span}(\mathbf{M}_{31} \mathbf{V}_1) \\ \mathcal{B}_1 &: \text{rank}(\mathbf{M}_{11} \mathbf{V}_1 \quad \mathbf{M}_{12} \mathbf{V}_2) = L(n) \\ \mathcal{B}_2 &: \text{rank}(\mathbf{M}_{21} \mathbf{V}_1 \quad \mathbf{M}_{22} \mathbf{V}_2) = L(n) \\ \mathcal{B}_3 &: \text{rank}(\mathbf{M}_{31} \mathbf{V}_1 \quad \mathbf{M}_{33} \mathbf{V}_3) = L(n) \end{aligned}$$

Condition  $\mathcal{A}_i$  guarantees that all the interferences at  $d'_i$  are aligned, i.e., mapped into the same linear space, while condition  $\mathcal{B}_i$  ensures that all source symbols for the  $i$ th unicast session can be decoded. These conditions ensure that we can achieve a rate tuple  $(R_1, R_2, R_3) = \mathbf{R}_n \triangleq (\frac{L_1(n)}{L(n)}, \frac{L_2(n)}{L(n)}, \frac{L_2(n)}{L(n)})$ , which approaches  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  as  $n \rightarrow \infty$ . In this case, we say that  $\mathbf{R}_n$  is *feasible through PBNA*.<sup>1</sup>

Previous work [9] [11] [12] only considered the feasibility of PBNA under a particular precoding matrix, i.e.,  $\mathbf{V}_1^*$  in Eq. (6), which was first introduced in [10]. To address this limitation and characterize the feasibility of PBNA for any precoding matrix, we reformulate  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$  and  $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$  without any assumption about the structure of precoding matrix. First, we reformulate  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$  as:

$$\begin{aligned} \mathcal{A}'_1 &: \mathbf{M}_{12} \mathbf{V}_2 = \mathbf{M}_{13} \mathbf{V}_3 \mathbf{A} \\ \mathcal{A}'_2 &: \mathbf{M}_{23} \mathbf{V}_3 = \mathbf{M}_{21} \mathbf{V}_1 \mathbf{B} \\ \mathcal{A}'_3 &: \mathbf{M}_{32} \mathbf{V}_2 = \mathbf{M}_{31} \mathbf{V}_1 \mathbf{C} \end{aligned}$$

where  $\mathbf{A}$  is an  $L_2(n) \times L_2(n)$  invertible matrix, and  $\mathbf{B}$  and  $\mathbf{C}$  are both  $L_1(n) \times L_2(n)$  matrices with rank  $L_2(n)$ .  $\mathcal{A}'_1, \mathcal{A}'_2, \mathcal{A}'_3$  can be further condensed into a single condition:

$$\mathbf{T} \mathbf{V}_1 \mathbf{C} = \mathbf{V}_1 \mathbf{B} \mathbf{A} \quad (3)$$

where  $\mathbf{T} = \mathbf{M}_{12} \mathbf{M}_{21}^{-1} \mathbf{M}_{23} \mathbf{M}_{32}^{-1} \mathbf{M}_{31} \mathbf{M}_{13}^{-1}$ . Finally, conditions  $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$  are reformulated as:

$$\begin{aligned} \mathcal{B}'_1 &: \psi_1(\xi) = \det(\mathbf{V}_1 \quad \mathbf{P}_1 \mathbf{V}_1 \mathbf{C}) \neq 0 \\ \mathcal{B}'_2 &: \psi_2(\xi) = \det(\mathbf{V}_1 \quad \mathbf{P}_2 \mathbf{V}_1 \mathbf{C}) \neq 0 \\ \mathcal{B}'_3 &: \psi_3(\xi) = \det(\mathbf{V}_1 \quad \mathbf{P}_3 \mathbf{V}_1 \mathbf{C} \mathbf{A}^{-1}) \neq 0 \end{aligned}$$

where  $\mathbf{P}_1 = \mathbf{M}_{31} \mathbf{M}_{11}^{-1} \mathbf{M}_{12} \mathbf{M}_{32}^{-1}$ ,  $\mathbf{P}_2 = \mathbf{M}_{31} \mathbf{M}_{21}^{-1} \mathbf{M}_{22} \mathbf{M}_{32}^{-1}$ , and  $\mathbf{P}_3 = \mathbf{M}_{12} \mathbf{M}_{32}^{-1} \mathbf{M}_{33} \mathbf{M}_{13}^{-1}$ , and  $\psi_1(\xi), \psi_2(\xi), \psi_3(\xi)$  are rational functions in the field  $\mathbb{F}_{2^m}(\xi)$ . Define  $\psi(\xi) = \prod_{i=1}^3 \psi_i(\xi)$ . We assume that  $\mathbb{F}_{2^m}$  is sufficiently large such that if  $\psi(\xi)$  is a non-zero rational function, there are values to  $\xi$ , denoted by  $\xi_0$ , such that  $\psi(\xi_0) \neq 0$ .

We also define the following rational functions:

$$\begin{aligned} p_1(\mathbf{x}) &= \frac{m_{31}(\mathbf{x}) m_{12}(\mathbf{x})}{m_{11}(\mathbf{x}) m_{32}(\mathbf{x})} & p_2(\mathbf{x}) &= \frac{m_{31}(\mathbf{x}) m_{22}(\mathbf{x})}{m_{21}(\mathbf{x}) m_{32}(\mathbf{x})} \\ p_3(\mathbf{x}) &= \frac{m_{12}(\mathbf{x}) m_{33}(\mathbf{x})}{m_{32}(\mathbf{x}) m_{13}(\mathbf{x})} & \eta(\mathbf{x}) &= \frac{m_{31}(\mathbf{x}) m_{12}(\mathbf{x}) m_{23}(\mathbf{x})}{m_{21}(\mathbf{x}) m_{32}(\mathbf{x}) m_{13}(\mathbf{x})} \end{aligned} \quad (4)$$

<sup>1</sup>In this paper, we first consider the feasibility conditions of PBNA for a fixed value of  $n$ . Then, in the Main Theorem, we prove that the feasibility conditions of PBNA are actually irrelevant to  $n$  for  $n > 1$ .

Clearly,  $p_i(\mathbf{x})$  and  $\eta(\mathbf{x})$  form the elements along the diagonals of  $\mathbf{P}_i$  and  $\mathbf{T}$  respectively. Hence, the following lemma holds:

**Lemma 1:**  $\mathbf{R}_n^*$  is feasible through PBNA if and only if 1) Eq. (3) is satisfied, and 2)  $\mathcal{B}'_1, \mathcal{B}'_2, \mathcal{B}'_3$  are satisfied.

Form Lemma 1, we see that a solution to PBNA consists of four matrices, i.e.,  $\mathbf{V}_1, \mathbf{A}, \mathbf{B}$  and  $\mathbf{C}$ . We use vector  $\mathbf{\Gamma}$  to represent such a solution:

$$\mathbf{\Gamma} = (\mathbf{V}_1, \mathbf{A}, \mathbf{B}, \mathbf{C}) \quad (5)$$

The fundamental design problem in PBNA is to find  $\mathbf{\Gamma}$  such that all the conditions in Lemma 1 are satisfied. Indeed, the major restriction comes from Eq. (3). As shown in [9], the construction of  $\mathbf{\Gamma}$  depends on whether  $\eta(\mathbf{x})$  is constant. When  $\eta(\mathbf{x})$  is constant, and thus  $\mathbf{T}$  is an identity matrix, we set  $\mathbf{C} = \mathbf{B}\mathbf{A}$ . Therefore, any arbitrary  $\mathbf{V}_1$  can satisfy Eq. (3). In fact, for this case, as we will see in Section V-A that all the interferences can be perfectly aligned such that the we can achieve one half rate for each unicast session in exactly two time slots.

In contrast, when  $\eta(\mathbf{x})$  is not constant, we can no longer choose  $\mathbf{V}_1$  freely. [10] proposed the following solution, which has also been used by most of recent work [9] [11] [12]. Let  $L_1(n) = n + 1$  and  $L_2(n) = n$ , and define the precoding matrix

$$\mathbf{V}_1^* = (\mathbf{w} \quad \mathbf{T}\mathbf{w} \quad \cdots \quad \mathbf{T}^n\mathbf{w}) \quad (6)$$

where  $\mathbf{w}$  is a column vector of  $2n + 1$  ones. Meanwhile, we set  $\mathbf{A} = \mathbf{I}_n$ ,  $\mathbf{C}$  consists of the left  $n$  columns of  $\mathbf{I}_{n+1}$ , and  $\mathbf{B}$  the right  $n$  columns of  $\mathbf{I}_{n+1}$ ; this construction satisfies Eq. (3). Note that the form of  $\mathbf{V}_1$  is determined by  $\mathbf{A}, \mathbf{B}$  and  $\mathbf{C}$ . With different  $\mathbf{A}, \mathbf{B}$  and  $\mathbf{C}$ , we can derive different  $\mathbf{V}_1$ ; therefore the choice of  $\mathbf{V}_1$  is not limited to just  $\mathbf{V}_1^*$ . Using this solution, we can achieve the following rate tuple through PBNA:

$$\mathbf{R}_n^* = \left( \frac{n+1}{2n+1}, \frac{n}{2n+1}, \frac{n}{2n+1} \right) \quad (7)$$

As observed in [11], graphs can introduce dependence between transfer functions<sup>2</sup> so that PBNA may be infeasible. This is a fundamental difference compared to wireless interference channel, where channel gains can change independently and interference alignment is always feasible. Fig. 1 depicts some examples of graphs where PBNA is infeasible. In Fig. 1(a),  $p_i(\mathbf{x}) = \eta(\mathbf{x}) = 1$  for  $i \in \{1, 2, 3\}$ , thus  $\mathbf{P}_i = \mathbf{I}_{2n+1}$ , implying  $\mathcal{B}'_1, \mathcal{B}'_2, \mathcal{B}'_3$  are all violated. In Fig. 1(b),  $p_1(\mathbf{x}) = \frac{\eta(\mathbf{x})}{\eta(\mathbf{x})+1}$ , which also violates  $\mathcal{B}'_1$ . This example shows that the conjecture proposed by Ramakrishnan et al. [11] doesn't hold beyond three symbol extensions. Moreover, by exchanging  $s_1 \leftrightarrow s_2$  and  $d_1 \leftrightarrow d_2$ , we obtain another counter example, where  $p_2(\mathbf{x}) = 1 + \eta(\mathbf{x})$ , violating  $\mathcal{B}'_2$ .

As a first step, [9] proposed the following set of conditions

<sup>2</sup>Dependence here means that one transfer function (namely  $m_{ii}(\mathbf{x})$ , corresponding to signal for the  $i$ th unicast flow) can be written as a rational function of other transfer (interference) functions. The exact functional form is dictated by Eq. (9) or Eq. (10)-(12).

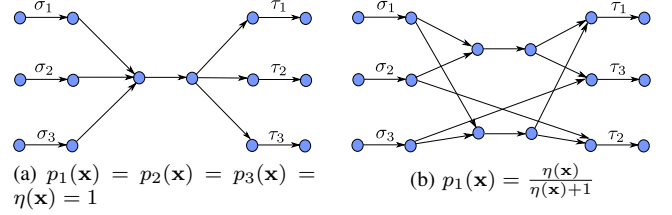


Fig. 1: Examples of graphs where PBNA is infeasible

for PBNA.<sup>3</sup> For  $i \in \{1, 2, 3\}$ ,

$$p_i(\mathbf{x}) \notin \left\{ \frac{f(\eta(\mathbf{x}))}{g(\eta(\mathbf{x}))} : f(z), g(z) \in \mathbb{F}_{2^m}[z], g(z) \neq 0 \right\} \quad (8)$$

In [9], it was proved that if Eq. (8) is satisfied, we can use  $\mathbf{V}_1^*$  to asymptotically achieve half rate in an infinite number of time slots. Unfortunately, since Eq. (8) contains an infinite number of conditions, it is impractical to verify. Moreover, since only one particular matrix was considered in [9], Eq. (8) was only shown to be sufficient for PBNA.

### III. OVERVIEW OF MAIN RESULTS

We now state our main results; proofs are deferred to Section V and to the appendices. Since the construction of  $\mathbf{V}_1$  depends on whether  $\eta(\mathbf{x})$  is constant, we distinguish two cases.

#### A. $\eta(\mathbf{x})$ Is Constant

In this case, we can choose  $\mathbf{V}_1$  freely, and thus the feasibility condition of PBNA can be significantly simplified. Moreover, we can achieve one half rate in exactly two time slots, as stated in the following theorem:

**Theorem 1:** Assume  $\eta(\mathbf{x})$  is constant. The rate tuple  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  is feasible through PBNA if and only if  $p_i(\mathbf{x})$  is not constant for each  $i \in \{1, 2, 3\}$ .

#### B. $\eta(\mathbf{x})$ Is Not Constant

In this case, we cannot choose  $\mathbf{V}_1$  freely. Using similar technique as in [9], we can rewrite Eq. (8) as follows:<sup>4</sup>

$$p_i(\mathbf{x}) \notin \mathcal{S}_n = \left\{ \frac{f(\eta(\mathbf{x}))}{g(\eta(\mathbf{x}))} : f(z), g(z) \in \mathbb{F}_{2^m}[z], \right. \\ \left. f(z)g(z) \neq 0, \gcd(f(z), g(z)) = 1, \right. \\ \left. d_f \leq n, d_g \leq n-1 \right\} \quad \forall i \in \{1, 2, 3\} \quad (9)$$

Note that, in contrast to Eq. (8), the above set of conditions guarantee that  $\mathbf{R}_n^*$  is NA-feasible for a fixed value of  $n$ .

Next, we show that Eq. (9) is also necessary for the feasibility of PBNA with respect to any  $\mathbf{V}_1$  satisfying the conditions of Lemma 1.

**Theorem 2:** Assume  $\eta(\mathbf{x})$  is not constant.  $\mathbf{R}_n^*$  is feasible through PBNA if and only if for each  $i \in \{1, 2, 3\}$ ,  $p_i(\mathbf{x}) \notin \mathcal{S}_n$ .

<sup>3</sup>There is actually a small difference between Eq. (8) and the original formulation in [9], in which  $p_1(\mathbf{x})$  is replaced by  $1/p_1(\mathbf{x})$ . It is easy to see that the two are equivalent.

<sup>4</sup>Notation: For two polynomials  $f(x)$  and  $g(x)$ , let  $\gcd(f(x), g(x))$  denote their greatest common divisor, and  $d_f$  the degree of  $f(x)$ .

Finally, we greatly reduce  $\mathcal{S}_n$  to just four rational functions:

**Theorem 3 (The Main Theorem):** Assume  $\eta(\mathbf{x})$  is not constant. For  $n > 1$ ,  $\mathbf{R}_n^*$  is feasible through PBNA if and only if the following conditions are satisfied:

$$m_{11}(\mathbf{x}) \neq a_1 \frac{m_{21}(\mathbf{x})m_{13}(\mathbf{x})}{m_{23}(\mathbf{x})} + b_1 \frac{m_{31}(\mathbf{x})m_{12}(\mathbf{x})}{m_{32}(\mathbf{x})} \quad (10)$$

$$m_{22}(\mathbf{x}) \neq a_2 \frac{m_{32}(\mathbf{x})m_{21}(\mathbf{x})}{m_{31}(\mathbf{x})} + b_2 \frac{m_{12}(\mathbf{x})m_{23}(\mathbf{x})}{m_{13}(\mathbf{x})} \quad (11)$$

$$m_{33}(\mathbf{x}) \neq a_3 \frac{m_{13}(\mathbf{x})m_{32}(\mathbf{x})}{m_{12}(\mathbf{x})} + b_3 \frac{m_{23}(\mathbf{x})m_{31}(\mathbf{x})}{m_{21}(\mathbf{x})} \quad (12)$$

where for  $i \in \{1, 2, 3\}$ ,  $a_i, b_i$  are constants in  $\{0, 1\}$  and cannot be zeros at the same time.

Note that Eq. (10)-(12) correspond to the following conditions respectively:

$$p_1(\mathbf{x}) \notin \left\{1, \eta(\mathbf{x}), \frac{\eta(\mathbf{x})}{1 + \eta(\mathbf{x})}\right\} \quad (13)$$

$$p_2(\mathbf{x}) \notin \{1, \eta(\mathbf{x}), 1 + \eta(\mathbf{x})\} \quad (14)$$

$$p_3(\mathbf{x}) \notin \{1, \eta(\mathbf{x}), 1 + \eta(\mathbf{x})\} \quad (15)$$

As shown in the Main Theorem, the feasibility conditions for PBNA are irrelevant to  $n$  for  $n > 1$ . This indicates that if PBNA is feasible for  $n = 2$ , then it is feasible for any arbitrary  $n > 1$ , and thus we can use PBNA to achieve half rate asymptotically. Otherwise, if PBNA is not feasible for some  $n > 1$ , PBNA doesn't even allow us to achieve any rate greater than  $(\frac{2}{3}, \frac{1}{3}, \frac{1}{3})$ .

The basic idea behind the Main Theorem is that we can compare the degree of a variable in  $p_i(\mathbf{x})$  with that of a rational function in  $\mathcal{S}_n$ . This technique enables us to reduce  $\mathcal{S}_n$  to the form  $\{\frac{a_0 + a_1 \eta(\mathbf{x})}{b_0 + b_1 \eta(\mathbf{x})}\}$ . Thus, we only need to consider a finite number of rational functions, namely Eq. (10)-(12). This enables an efficient algorithm for checking the feasibility of PBNA. The key for enabling this reduction lies in two graph-related properties, which we refer to as Linearization Property and Square-Term Property, as described in the next section.

#### IV. GRAPH-RELATED PROPERTIES

Our key intuition is that  $p_i(\mathbf{x})$  is not an arbitrary function but depends on transfer functions, as specified in Eq. (4). Therefore,  $p_i(\mathbf{x})$  has special algebraic properties, which can be exploited to simplify Eq. (9).

First note that all  $p_i(\mathbf{x})$ 's are of the following general form:

$$h(\mathbf{x}) = \frac{m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})}{m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})}, \quad a, b, p, q \in \{1, 2, 3\}, a \neq p, b \neq q$$

Furthermore, each path pair in  $\mathcal{P}_{ab} \times \mathcal{P}_{pq}$  contributes a term in  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})$ , and each path pair in  $\mathcal{P}_{aq} \times \mathcal{P}_{pb}$  contributes a term in  $m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$ :

$$m_{ab}(\mathbf{x})m_{pq}(\mathbf{x}) = \sum_{(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}} t(P_1)t(P_2)$$

$$m_{aq}(\mathbf{x})m_{pb}(\mathbf{x}) = \sum_{(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}} t(P_3)t(P_4)$$

##### A. Linearization Property

First, consider the following lemma, which provides an easy way to check whether  $p_i(\mathbf{x}) \notin \{1, \eta(\mathbf{x})\}$  (as in Section VI).

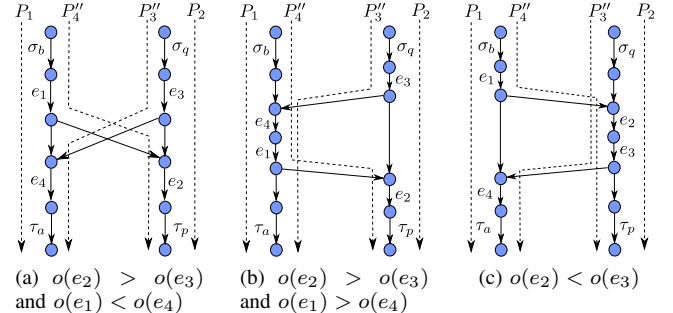


Fig. 2: The construction of  $H$  (in the proof of the Linearization Property) enabled by Lemma 2 ( $P_1$  is disjoint with  $P_2$ )

The intuition is that we can multicast two symbols from  $s'_b, s'_q$  to  $d'_a, d'_p$  by network coding if and only if the minimum cut separating  $s'_b, s'_q$  from  $d'_a, d'_p$  is greater than one [2].

**Lemma 2:**  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x}) \neq m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$  if and only if there is disjoint path pair  $(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}$  or  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$ .

*Proof:* See Appendix A. ■

The first graph-related property states that  $p_i(\mathbf{x})$  can be transformed into its simplest non-trivial form (i.e., a linear function or the inverse of a linear function). The key to Lemma 3 is to find a subgraph  $H$  and consider  $h(\mathbf{x})$  restricted to  $H$ , i.e.,  $h(\mathbf{x}_H) = \frac{m_{ab}(\mathbf{x}_H)m_{pq}(\mathbf{x}_H)}{m_{aq}(\mathbf{x}_H)m_{pb}(\mathbf{x}_H)}$ , where  $\mathbf{x}_H$  represents the coding vector of  $H$ . Due to the graph structure induced by Lemma 2, we can always find  $H$  such that some variable  $x_{ee'}$  appears exclusively in the numerator or the denominator of  $h(\mathbf{x}_H)$ . Thus, by assigning values to  $\mathbf{x}_H$  other than  $x_{ee'}$ , we can transform  $h(\mathbf{x}_H)$  into a linear function or the inverse of a linear function in terms of  $x_{ee'}$ . Since  $h(\mathbf{x}_H)$  can be acquired through a partial assignment to  $\mathbf{x}$ , this transformation also holds for the complete graph  $G$ .

**Lemma 3 (Linearization Property):** Let  $h(\mathbf{x}) = \frac{m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})}{m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})} = \frac{u(\mathbf{x})}{v(\mathbf{x})}$  such that  $\gcd(u(\mathbf{x}), v(\mathbf{x})) = 1$ . Assume  $h(\mathbf{x})$  is not constant. Then, for sufficiently large  $m$ , we can assign values to  $\mathbf{x}$  other than a variable  $x_{ee'}$  such that  $u(\mathbf{x})$  and  $v(\mathbf{x})$  are transformed into either  $u(x_{ee'}) = c_1 x_{ee'} + c_0$ ,  $v(x_{ee'}) = c_2$  or  $u(x_{ee'}) = c_2, v(x_{ee'}) = c_1 x_{ee'} + c_0$ , where  $c_0, c_1, c_2$  are constants in  $\mathbb{F}_{2^m}$ , and  $c_1 c_2 \neq 0$ .

*Proof:* In this proof, given a path  $P$  and  $e, e' \in P$ , let  $P[e : e']$  denote the path segment along  $P$  between  $e$  and  $e'$ , including  $e, e'$ . We arrange the edges of  $G'$  in topological order, and for  $e \in E'$ , let  $o(e)$  denote  $e$ 's position in this ordering. Moreover, denote  $h_1(\mathbf{x}) = m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})$ ,  $h_2(\mathbf{x}) = m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$  and  $d(\mathbf{x}) = \gcd(h_1(\mathbf{x}), h_2(\mathbf{x}))$ . Let  $s_1(\mathbf{x}) = \frac{h_1(\mathbf{x})}{d(\mathbf{x})}$  and  $s_2(\mathbf{x}) = \frac{h_2(\mathbf{x})}{d(\mathbf{x})}$ . Hence  $\gcd(s_1(\mathbf{x}), s_2(\mathbf{x})) = 1$ . It follows  $u(\mathbf{x}) = c s_1(\mathbf{x})$  and  $v(\mathbf{x}) = c s_2(\mathbf{x})$ , where  $c$  is a non-zero constant in  $\mathbb{F}_{2^m}$ . By Lemma 2, there exists disjoint path pair  $(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}$  or  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$ . Now we consider the first case.

Let  $(P'_3, P'_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$ . Since  $P_1, P'_4$  both originate at  $\sigma_b$ , and  $P_2, P'_4$  both terminate at  $\tau_p$ , there exist  $e_1 \in P_1 \cap P'_4$  and  $e_2 \in P_2 \cap P'_4$  such that the path segment along  $P'_4$  between  $e_1$  and  $e_2$  is disjoint with  $P_1 \cup P_2$ . Similarly, there exist  $e_3 \in P_2 \cap$

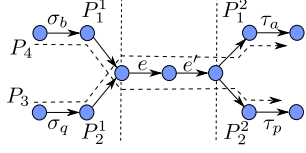


Fig. 3: Illustration of Square-Term Property. A term with  $x_{ee'}^2$  introduced by  $(P_1, P_2)$  in the numerator of  $h(\mathbf{x})$  equals another term introduced by  $(P_3, P_4)$  in the denominator of  $h(\mathbf{x})$ .

$P'_3$  and  $e_4 \in P_1 \cap P'_3$  such that the path segment between  $e_3$  and  $e_4$  along  $P'_3$  is disjoint with  $P_1 \cup P_2$ . Construct the following two paths:  $P''_4 = P_1[\sigma_b : e_1] \cup P'_4[e_1 : e_2] \cup P_2[e_2 : \tau_p]$  and  $P''_3 = P_2[\sigma_q : e_3] \cup P'_3[e_3 : e_4] \cup P_1[e_4 : \tau_a]$  (see Fig. 2). Let  $H$  denote the subgraph of  $G'$  induced by  $P_1 \cup P_2 \cup P''_3 \cup P''_4$ , and  $\mathbf{x}_H$  the coding vector of  $H$ . We will prove that the theorem holds for  $H$ . Note that since  $h_1(\mathbf{x}_H)$  and  $h_2(\mathbf{x}_H)$  are both non-zeros,  $d(\mathbf{x}_H) \neq 0$ .

If  $o(e_2) > o(e_3)$  (Fig. 2(a)-(b)), the variables in  $t(P_2[e_3 : e_2])$  are absent in  $h_2(\mathbf{x}_H)$ . We then arbitrarily select a variable  $x_{ee'}$  from  $t(P_2[e_3 : e_2])$ , and write  $h_1(\mathbf{x}_H)$  as  $f(\mathbf{x}'_H)x_{ee'} + g(\mathbf{x}'_H)$ , where  $\mathbf{x}'_H$  includes all the variables in  $\mathbf{x}_H$  other than  $x_{ee'}$ , and  $f(\mathbf{x}'_H), g(\mathbf{x}'_H) \in \mathbb{F}_{2^m}[\mathbf{x}'_H]$ . Meanwhile,  $h_2(\mathbf{x}_H)$  can be written as  $h_2(\mathbf{x}'_H) \in \mathbb{F}_{2^m}[\mathbf{x}'_H]$ . Clearly,  $x_{ee'}$  will not show up in  $d(\mathbf{x}_H)$  and thus it can also be written as  $d(\mathbf{x}'_H) \in \mathbb{F}_{2^m}[\mathbf{x}'_H]$ . We then find values for  $\mathbf{x}'_H$ , denoted by  $\mathbf{r}$ , such that  $f(\mathbf{r})h_2(\mathbf{r})d(\mathbf{r}) \neq 0$ . Finally, denote  $c_0 = cg(\mathbf{r})d^{-1}(\mathbf{r})$ ,  $c_1 = cf(\mathbf{r})d^{-1}(\mathbf{r})$  and  $c_2 = ch_2(\mathbf{r})d^{-1}(\mathbf{r})$  and the theorem holds.

On the other hand, if  $o(e_2) < o(e_3)$  (see Fig. 2(c)), the variables in  $t(P_1[e_1 : e_4])$  are absent in  $h_2(\mathbf{x}_H)$ . We then select a variable  $x_{ee'}$  from  $t(P_1[e_1 : e_4])$ . Similar to above, it's easy to see that  $u(\mathbf{x})$  and  $v(\mathbf{x})$  can be transformed into  $c_1x_{ee'} + c_0$  and  $c_2$  respectively.

For the case where there exists disjoint path pair  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$ , we can show that  $u(\mathbf{x})$  and  $v(\mathbf{x})$  can be transformed into  $c_2$  and  $c_1x_{ee'} + c_0$  respectively. ■

### B. Square-Term Property

The second graph-related property is stated in Lemma 4: the coefficient of  $x_{ee'}^2$  in the numerator of  $h(\mathbf{x})$  equals its counterpart in the denominator of  $h(\mathbf{x})$ . Thus, if  $x_{ee'}^2$  appears in the numerator of  $h(\mathbf{x})$  under some assignment to  $\mathbf{x}$ , it must also appear in the denominator of  $h(\mathbf{x})$ , and vice versa.

**Lemma 4 (Square-Term Property):** Given a coding variable  $x_{ee'}$ , let  $f_1(\mathbf{x})$  and  $f_2(\mathbf{x})$  be the coefficients of  $x_{ee'}^2$  in  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})$  and  $m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$  respectively. Then  $f_1(\mathbf{x}) = f_2(\mathbf{x})$ .

*Proof:* For any  $x_{ee'}$ , define  $\mathcal{Q}_1 = \{(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq} : x_{ee'}^2 \mid t(P_1)t(P_2)\}$  and  $\mathcal{Q}_2 = \{(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb} : x_{ee'}^2 \mid t(P_3)t(P_4)\}$ . Consider a path pair  $(P_1, P_2) \in \mathcal{Q}_1$ . Since the degree of  $x_{ee'}$  in  $t(P_1)$  and  $t(P_2)$  is at most one, we must have  $x_{ee'} \mid t(P_1)$  and  $x_{ee'} \mid t(P_2)$ . Thus  $e, e' \in P_1 \cap P_2$ . Let  $P_1^1, P_1^2$  be the parts of  $P_1$  before  $e$  and after  $e'$  respectively. Similarly, define  $P_2^1$  and  $P_2^2$ . Then construct two new paths:  $P_3 = P_2^1 \cup \{e, e'\} \cup P_1^1$  and  $P_4 = P_1^2 \cup \{e, e'\} \cup P_2^2$  (see Fig. 3). Clearly,  $t(P_1)t(P_2) = t(P_3)t(P_4)$ , and thus  $(P_3, P_4) \in \mathcal{Q}_2$ . The above method establishes a one-to-one mapping  $\phi : \mathcal{Q}_1 \rightarrow \mathcal{Q}_2$ , such that for  $\phi((P_1, P_2)) = (P_3, P_4)$ ,  $t(P_1)t(P_2) =$

$t(P_3)t(P_4)$ . Hence,  $f_1(\mathbf{x}) = \frac{1}{x_{ee'}^2} \sum_{(P_1, P_2) \in \mathcal{Q}_1} t(P_1)t(P_2) = \frac{1}{x_{ee'}^2} \sum_{(P_3, P_4) \in \mathcal{Q}_2} t(P_3)t(P_4) = f_2(\mathbf{x})$ . ■

## V. FEASIBILITY CONDITION OF PBNA

In this section, we provide the proofs of Theorems 1, 2 and 3 (Main Theorem).

### A. $\eta(\mathbf{x})$ Is Constant

*Proof of Theorem 1:* In this case,  $\mathbf{T}$  is identity matrix. We set  $L_1(n) = L_2(n) = 1$  and  $\mathbf{V}_1 = (\theta_1 \ \theta_2)^T$ , where  $\theta_1, \theta_2$  are arbitrary variables, and  $\mathbf{A}, \mathbf{B}, \mathbf{C}$  are all scalar ones. It is easy to see that Eq. (3) is satisfied. Moreover, if  $p_i(\mathbf{x})$  is not constant, we have

$$\psi_i(\xi) = \det \begin{pmatrix} \theta_1 & p_i(\mathbf{x}^1)\theta_1 \\ \theta_2 & p_i(\mathbf{x}^2)\theta_2 \end{pmatrix} = \theta_1\theta_2(p_i(\mathbf{x}^1) - p_i(\mathbf{x}^2)) \neq 0$$

and  $\mathcal{B}'_i$  is satisfied. Thus  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  is feasible through PBNA. Conversely, if  $p_i(\mathbf{x})$  is constant,  $\mathcal{B}'_i$  is violated, and thus  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  is not feasible through PBNA. ■

### B. $\eta(\mathbf{x})$ Is Not Constant

Due to the importance of  $\mathbf{V}_1$ , we first consider how to construct  $\mathbf{V}_1$  which satisfies (3). The construction of  $\mathbf{V}_1$  involves solving a system of linear equations:

$$\mathbf{r}(z)(z\mathbf{C} - \mathbf{BA}) = 0 \quad (16)$$

where  $\mathbf{r}(z) = (r_1(z), \dots, r_{n+1}(z)) \in \mathbb{F}_{2^m}^{n+1}(z)$ . It is easy to see that  $z\mathbf{C} - \mathbf{BA}$  is a matrix on  $\mathbb{F}_{2^m}(z)$ . Assume  $\mathbf{r}_0(z)$  is a non-zero solution to (16). Substitute  $z$  with  $\eta(\mathbf{x}^i)$ , and we have

$$\eta(\mathbf{x}^i)\mathbf{r}_0(\eta(\mathbf{x}^i))\mathbf{C} = \mathbf{r}_0(\eta(\mathbf{x}^i))\mathbf{BA}$$

Finally, construct the following precoding matrix

$$\mathbf{V}_1^T = (\mathbf{r}_0^T(\eta(\mathbf{x}^1)) \ \mathbf{r}_0^T(\eta(\mathbf{x}^2)) \ \dots \ \mathbf{r}_0^T(\eta(\mathbf{x}^{2^{n+1}})))$$

Apparently,  $\mathbf{V}_1$  satisfies (3). Hence, each non-zero solution to (16) corresponds to a row of  $\mathbf{V}_1$  satisfying (3). Conversely, it is straightforward to see that each row of  $\mathbf{V}_1$  satisfying (3) corresponds to a solution to (16).

*Example 1:* As an example, consider the case where  $n = 2$  and  $m = 2$ . Let  $\alpha$  be the primitive element of  $\mathbb{F}_4$  such that  $\alpha^3 = 1$  and  $\alpha^2 + \alpha + 1 = 0$ . Moreover, let  $\mathbf{A} = \mathbf{I}_2$  and

$$\mathbf{C} = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \\ \alpha^2 & 1 \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} \alpha^2 & \alpha \\ 1 & 1 \\ 1 & \alpha \end{pmatrix}$$

Apparently,  $\text{rank}(\mathbf{C}) = \text{rank}(\mathbf{B}) = 2$ . It's easy to verify that  $\mathbf{r}(z) = (\alpha^2 z^2 + \alpha, z + \alpha, z^2 + \alpha z + \alpha^2)$  satisfies equation (16). Thus, we substitute  $z$  with  $\eta(\mathbf{x}^j)$  and construct  $\mathbf{V}_1^T = (\mathbf{r}_0^T(\eta(\mathbf{x}^1)) \ \mathbf{r}_0^T(\eta(\mathbf{x}^2)) \ \dots \ \mathbf{r}_0^T(\eta(\mathbf{x}^5)))$ . According to the above discussion, equation (3) is satisfied. ■

Using (16), we can derive the general form of  $\mathbf{V}_1$  which satisfies  $\mathbf{V}_1$ .

**Lemma 5:** Any  $\mathbf{V}_1$  satisfying (3) has the form  $\mathbf{V}_1 = \mathbf{G}\mathbf{V}_1^*\mathbf{F}$ , where  $\mathbf{V}_1^*$  is defined in (6),  $\mathbf{F}$  is an  $(n+1) \times (n+1)$  matrix, and  $\mathbf{G}$  is a  $(2n+1) \times (2n+1)$  diagonal matrix, with the  $(i, i)$  element being  $f_i(\eta(\mathbf{x}^i))$ , where  $f_i(z)$  is a non-zero



rational function in  $\mathbb{F}_{2^m}(z)$ . Moreover, the  $(n+1)$ th row of **FC** and the 1st row of **FBA** are both zero vectors.

*Proof:* See Appendix B. ■

Lemma 5 indicates that there is a direct relation between  $\mathbf{V}_1^*$  and the general form of  $\mathbf{V}_1$ , which we use to prove that Eq. (9) is also necessary for the feasibility of PBNA.

*Proof of Theorem 2:* The sufficiency of (9) was proved in [9]. Now assume  $p_i(\mathbf{x}) = \frac{f(\eta(\mathbf{x}))}{g(\eta(\mathbf{x}))} \in \mathcal{S}_n$ , where  $f(z) = \sum_{k=0}^n a_k z^k$  and  $g(z) = \sum_{k=0}^{n-1} b_k z^k$ . We will prove that for any  $\mathbf{V}_1$  satisfying (3),  $\mathcal{B}_i$  cannot be satisfied, thus  $\mathbf{R}_n^*$  is not NA-feasible. Apparently, if  $\text{rank}(\mathbf{V}_1) < n+1$ ,  $\mathcal{B}_i$  is violated. Thus, in the rest of this proof, we assume  $\text{rank}(\mathbf{V}_1) = n+1$ .

By Lemma 5,  $\mathbf{V}_1 = \mathbf{G}\mathbf{V}_1^*\mathbf{F}$ , where  $\mathbf{F}$  is an  $(n+1) \times (n+1)$  invertible matrix. The  $j$ th row of  $\mathbf{V}_1$  is  $\mathbf{r}_j = f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^n(\mathbf{x}^j))\mathbf{F}$ . Since the  $(n+1)$ th row of **FC** is zero, we have

$$\mathbf{r}_j \mathbf{C} = f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^{n-1}(\mathbf{x}^j))\mathbf{H}$$

where  $\mathbf{H}$  consists of the top  $n$  rows of **FC** and  $\text{rank}(\mathbf{H}) = n$ . Let  $\mathbf{a} = (a_0, a_1, \dots, a_n)^T$  and  $\mathbf{b} = (b_0, b_1, \dots, b_{n-1})^T$ . For  $i = 1, 2$ , we define  $\mathbf{a}' = \mathbf{F}^{-1}\mathbf{a}$  and  $\mathbf{b}' = \mathbf{H}^{-1}\mathbf{b}$ . It follows

$$\begin{aligned} \mathbf{r}_j \mathbf{a}' &= f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^n(\mathbf{x}^j))\mathbf{F}\mathbf{a}' \\ &= f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^n(\mathbf{x}^j))\mathbf{a} \\ &= f_j(\eta(\mathbf{x}^j))f(\eta(\mathbf{x}^j)) \\ &= f_j(\eta(\mathbf{x}^j))p_i(\mathbf{x}^j)g(\eta(\mathbf{x}^j)) \\ &= p_i(\mathbf{x}^j)f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^{n-1}(\mathbf{x}^j))\mathbf{b} \\ &= p_i(\mathbf{x}^j)f_j(\eta(\mathbf{x}^j))(1, \eta(\mathbf{x}^j), \dots, \eta^{n-1}(\mathbf{x}^j))\mathbf{H}\mathbf{b}' \\ &= p_i(\mathbf{x}^j)\mathbf{r}_j \mathbf{C}\mathbf{b}' \end{aligned}$$

Hence, the columns of  $(\mathbf{V}_1 \ \mathbf{P}_i \mathbf{V}_1 \mathbf{C})$  are linearly dependent, violating  $\mathcal{B}_i$ . Similarly, we can prove the case of  $i = 3$ . ■

For the proof of the Main Theorem, we need to rearrange the ratio of rational functions  $\frac{f(\eta(\mathbf{x}))}{g(\eta(\mathbf{x}))}$  in Eq. (9) to a ratio of coprime polynomials with variables  $\mathbf{x}$ . To this end, we use a property of polynomials stated in the following lemma.

*Lemma 6:* Let  $\mathbb{F}$  be a field.  $z$  is a variable and  $\mathbf{y} = (y_1, y_2, \dots, y_k)$  is a vector of variables. Consider four non-zero polynomials  $f(z), g(z) \in \mathbb{F}[z]$  and  $s(\mathbf{y}), t(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ , such that  $\gcd(f(z), g(z)) = 1$  and  $\gcd(s(\mathbf{y}), t(\mathbf{y})) = 1$ . Denote  $d = \max\{d_f, d_g\}$ . Define two polynomials in  $\mathbb{F}[\mathbf{y}]$ :  $\alpha(\mathbf{y}) = f(\frac{s(\mathbf{y})}{t(\mathbf{y})})t^d(\mathbf{y})$  and  $\beta(\mathbf{y}) = g(\frac{s(\mathbf{y})}{t(\mathbf{y})})t^d(\mathbf{y})$ . Then  $\gcd(\alpha(\mathbf{y}), \beta(\mathbf{y})) = 1$ .

*Proof:* See Appendix C. ■

The proof of the Main Theorem consists of three steps. In the first step, we use degree-counting technique and Linearization Property to reduce  $\mathcal{S}_n$  to the form  $\{\frac{a_0 + a_1 \eta(\mathbf{x})}{b_0 + b_1 \eta(\mathbf{x})}\}$ . In the second step, we use Linearization Property and Square Term Property to further reduce  $\mathcal{S}_n$  to the four rational functions in  $\mathcal{S}' = \{1, \eta(\mathbf{x}), 1 + \eta(\mathbf{x}), \frac{\eta(\mathbf{x})}{1 + \eta(\mathbf{x})}\}$ . Finally, we use the results from [12] to rule out the remaining redundant conditions.

*Proof of the Main Theorem:* Clearly, the necessity of (10)-(12) (or Eq. (13)-(15)) follows directly from Theorem 2. Now assume for  $i \in \{1, 2, 3\}$ ,  $p_i(\mathbf{x}) \notin \mathcal{S}'$ . We will prove that  $p_i(\mathbf{x}) \notin \mathcal{S}_n$  and thus  $\mathbf{R}_n^*$  is NA-feasible by Theorem 2. We only prove  $p_1(\mathbf{x}) \notin \mathcal{S}_n$ . The other cases follow similar lines.

By contradiction, assume there exists  $p_1(\mathbf{x}) = \frac{f(\eta(\mathbf{x}))}{g(\eta(\mathbf{x}))} \in \mathcal{S}_n$ , where  $f(z) = \sum_{i=0}^k a_i z^i$  and  $g(z) = \sum_{i=0}^l b_i z^i$  such that  $a_l b_k \neq 0$  and  $\gcd(f(z), g(z)) = 1$ . Moreover, let  $p_1(\mathbf{x}) = \frac{u(\mathbf{x})}{v(\mathbf{x})}$  and  $\eta(\mathbf{x}) = \frac{s(\mathbf{x})}{t(\mathbf{x})}$ , where  $\gcd(u(\mathbf{x}), v(\mathbf{x})) = \gcd(s(\mathbf{x}), t(\mathbf{x})) = 1$ . Let  $d = \max\{k, l\}$ . Define the following two polynomials  $\alpha(\mathbf{x}) = f(\eta(\mathbf{x}))t^d(\mathbf{x})$  and  $\beta(\mathbf{x}) = g(\eta(\mathbf{x}))t^d(\mathbf{x})$ . According to Lemma 6,  $\gcd(\alpha(\mathbf{x}), \beta(\mathbf{x})) = 1$ . Thus, we have  $\alpha(\mathbf{x}) = cu(\mathbf{x})$ , and  $\beta(\mathbf{x}) = cv(\mathbf{x})$ , where  $c \in \mathbb{F}_{2^m}$  and  $c \neq 0$ .

According to Lemma 3, there exists an assignment to  $\mathbf{x}$  under which  $u(\mathbf{x})$  and  $v(\mathbf{x})$  are transformed into either  $u(x_{ee'}) = c_1 x_{ee'} + c_0$ ,  $v(x_{ee'}) = c_2$  or  $u(x_{ee'}) = c_2$ ,  $v(x_{ee'}) = c_1 x_{ee'} + c_0$ . We only consider the first case. The proof for the other case is similar. In this case,  $\alpha(\mathbf{x})$  and  $\beta(\mathbf{x})$  are transformed into  $\alpha(x_{ee'}) = cc_1 x_{ee'} + cc_0$  and  $\beta(x_{ee'}) = cc_2$  respectively.

First, we prove that both  $t(x_{ee'})$  and  $s(x_{ee'})$  are non-zeros. Assume  $t(x_{ee'}) = 0$ . If  $k \neq l$ , at least one of  $\alpha(x_{ee'})$  and  $\beta(x_{ee'})$  equals zero, which is impossible. On the other hand, if  $k = l$ , we have  $\alpha(x_{ee'}) = a_k s^k(x_{ee'})$  and  $\beta(x_{ee'}) = b_k s^k(x_{ee'})$ . It follows that  $cc_1 x_{ee'} + cc_0 = a_k b_k^{-1} cc_2$ , which is impossible. Thus we have proved that  $t(x_{ee'}) \neq 0$ . Similarly, we can also prove that  $s(x_{ee'}) \neq 0$ .

We then prove that  $d = 1$ . By contradiction, assume  $d \geq 2$ . We first consider the case where  $l \leq k$  and thus  $d = k$ . In this case, we have

$$\begin{aligned} \alpha(x_{ee'}) &= \sum_{j=0}^k a_j t^{k-j}(x_{ee'}) s^j(x_{ee'}) = cc_1 x_{ee'} + cc_0 \\ \beta(x_{ee'}) &= \sum_{j=0}^l b_j t^{k-j}(x_{ee'}) s^j(x_{ee'}) = cc_2 \end{aligned}$$

Assume  $s(x_{ee'}) = \sum_{j=0}^r s_j x_{ee'}^j$  and  $t(x_{ee'}) = \sum_{j=0}^{r'} t_j x_{ee'}^j$ , where  $s_r, t_{r'} \neq 0$ . Thus  $r = d_s$  and  $r' = d_t$  and  $\max\{r, r'\} \geq 1$ . Note that the degree of  $x_{ee'}^j$  in  $t^{k-j}(x_{ee'}) s^j(x_{ee'})$  is  $kr' + j(r - r')$ . We consider the following two cases:

Case I:  $r \neq r'$ . If  $r > r'$ ,  $d_\alpha = kr \geq 2$ , contradicting that  $d_\alpha = 1$ . Now assume  $r < r'$ . Let  $l_1$  and  $l_2$  be the minimum exponents of  $z$  in  $f(z)$  and  $g(z)$  respectively. It follows that  $d_\alpha = kr' - l_1(r' - r) = 1$  and  $d_\beta = kr' - l_2(r' - r) = 0$ . Clearly,  $l_2 > 0$  due to  $d_\beta = 0$ . If  $r > 0$ ,  $kr' - l_2(r' - r) > kr' - l_2 r' \geq 0$ , contradicting  $d_\beta = 0$ . Hence,  $r = 0$ , and  $l_2 = k$  due to  $d_\beta = 0$ . Meanwhile,  $d_\alpha = (k - l_1)r' = 1$ , which implies that  $l_1 = k - 1$  and  $r' = 1$ . Thus,  $z^{k-1}$  is a common divisor of  $f(z)$  and  $g(z)$ , contradicting  $\gcd(f(z), g(z)) = 1$ .

Case II:  $r = r'$ . Since  $d_\alpha = 1$  and  $d_\beta(x_{ee'}) = 0$ , all the terms in  $\alpha(x_{ee'})$  and  $\beta(x_{ee'})$  containing  $x_{ee'}^{kr}$  must be cancelled out, implying that

$$\begin{aligned} \sum_{j=0}^k a_j t_r^{k-j} s_r^j &= t_r^k \sum_{j=0}^k a_j \left(\frac{s_r}{t_r}\right)^j = t_r^k f\left(\frac{s_r}{t_r}\right) = 0 \\ \sum_{j=0}^l b_j t_r^{k-j} s_r^j &= t_r^k \sum_{j=0}^l b_j \left(\frac{s_r}{t_r}\right)^j = t_r^k g\left(\frac{s_r}{t_r}\right) = 0 \end{aligned}$$

Hence  $z - \frac{s_r}{t_r}$  is a common divisor of  $f(z)$  and  $g(z)$ , contradicting  $\gcd(f(z), g(z)) = 1$ .

Therefore, we have proved  $d = 1$  when  $l \leq k$ . Using similar technique, we can prove that  $d = 1$  when  $l \geq k$ .

Define  $q_1(\mathbf{x}) = \frac{\eta(\mathbf{x})}{p_1(\mathbf{x})} = \frac{m_{11}(\mathbf{x})m_{23}(\mathbf{x})}{m_{13}(\mathbf{x})m_{21}(\mathbf{x})}$ . For  $d = 1$ , we consider the following cases.

Case I:  $\frac{f(z)}{g(z)} = \frac{a_0 + a_1 z}{b_0 + b_1 z}$ , where  $a_1 a_0 b_1 b_0 \neq 0$ , and  $a_0 b_1 \neq a_1 b_0$ . For this case, we have  $p_1(x_{ee'}) = \frac{a_0 + a_1 p_1(x_{ee'}) q_1(x_{ee'})}{b_0 + b_1 p_1(x_{ee'}) q_1(x_{ee'})}$ . It immediately follows

$$q_1(x_{ee'}) = \frac{a_0 c_2^2 - b_0 c_0 c_2 - b_0 c_1 c_2 x_{ee'}}{b_1 c_1^2 x_{ee'}^2 - a_1 c_1 c_2 x_{ee'} + b_1 c_0^2 - a_1 c_0 c_2}$$

Denote  $u_1(x_{ee'}) = a_0 c_2^2 - b_0 c_0 c_2 - b_0 c_1 c_2 x_{ee'}$  and  $v_1(x_{ee'}) = b_1 c_1^2 x_{ee'}^2 - a_1 c_1 c_2 x_{ee'} + b_1 c_0^2 - a_1 c_0 c_2$ . Assume  $u_1(x_{ee'}) \mid v_1(x_{ee'})$  and thus  $x_{ee'} = \frac{a_0 c_2 - b_0 c_0}{b_0 c_1}$  is a solution to  $v_1(x_{ee'}) = 0$ . However,  $v_1(\frac{a_0 c_2 - b_0 c_0}{b_0 c_1}) = \frac{a_0^2 c_2^2}{b_0^2} (a_0 b_1 + a_1 b_0) \neq 0$ . Hence,  $u_1(x_{ee'}) \nmid v_1(x_{ee'})$ . Thus, by the definition of  $q_1(\mathbf{x})$  and Lemma 4,  $x_{ee'}^2$  must appear in  $u_1(x_{ee'})$ , which contradicts the formulation of  $u_1(x_{ee'})$ .

Case II:  $\frac{f(z)}{g(z)} = \frac{a_0 + a_1 z}{b_1 z}$ , where  $a_0 a_1 b_0 \neq 0$ . Similar to Case I, we can derive

$$q_1(x_{ee'}) = \frac{a_0 c_2^2}{b_1 c_1^2 x_{ee'}^2 - a_1 c_1 c_2 x_{ee'} + b_1 c_0^2 - a_1 c_0 c_2}$$

which contradicts Lemma 4.

Case III:  $\frac{f(z)}{g(z)} = \frac{a_1 z}{b_0 + b_1 z}$ , where  $a_1 b_0 b_1 \neq 0$ . Thus

$$q_1(\mathbf{x}) = \frac{a_1}{b_1} - \frac{b_0}{b_1} \frac{m_{13}(\mathbf{x})m_{21}(\mathbf{x})}{m_{11}(\mathbf{x})m_{23}(\mathbf{x})}$$

Since the coefficient of each monomial in  $m_{11}(\mathbf{x})m_{23}(\mathbf{x})$  and  $m_{13}(\mathbf{x})m_{21}(\mathbf{x})$  equals one, it directly follows  $\frac{a_1}{b_1} = -\frac{b_0}{b_1} = \frac{b_0}{b_1} = 1$ . This indicates that  $p_1(\mathbf{x}) = \frac{\eta(\mathbf{x})}{\eta(\mathbf{x})+1}$ , contradicting  $p_1(\mathbf{x}) \notin \mathcal{S}'$ .

Case IV:  $\frac{f(z)}{g(z)} = \frac{a_0}{b_0 + b_1 z}$ , where  $a_0 b_0 b_1 \neq 0$ . It follows that

$$q_1(x_{ee'}) = \frac{a_0 c_2^2 - b_0 c_0 c_2 - b_0 c_1 c_2 x_{ee'}}{b_1 c_0^2 + b_1 c_1^2 x_{ee'}^2}$$

Similar to Case I, this also contradicts Lemma 4.

Case V:  $\frac{f(z)}{g(z)} = \frac{a_0}{z}$ , where  $a_0 \neq 0$ . Hence,  $q_1(x_{ee'}) = \frac{a_0 c_2^2}{c_1^2 x_{ee'}^2 + c_0^2}$ , contradicting Lemma 4.

Case VI:  $\frac{f(z)}{g(z)} = a_0 + a_1 z$ , where  $a_0 a_1 \neq 0$ . Thus, it follows

$$p_1(\mathbf{x}) = a_0 + a_1 \frac{m_{31}(\mathbf{x})m_{12}(\mathbf{x})m_{23}(\mathbf{x})}{m_{21}(\mathbf{x})m_{32}(\mathbf{x})m_{13}(\mathbf{x})}$$

Similar to Case III,  $a_1 = a_0 = 1$ , contradicting  $p_1(\mathbf{x}) \notin \mathcal{S}'$ .

Case VII:  $\frac{f(z)}{g(z)} = a_1 z$ , where  $a_1 \neq 0$ . Similar to Case III,  $p_1(\mathbf{x}) = \eta(\mathbf{x})$ , contradicting  $p_1(\mathbf{x}) \notin \mathcal{S}'$ .

Thus, we have proved that if  $p_i(\mathbf{x}) \notin \mathcal{S}'$ ,  $p_i(\mathbf{x}) \notin \mathcal{S}_n$  and hence  $\mathbf{R}_n^*$  is NA-feasible by Theorem 2. We note that in [12] the authors proved that  $p_1(\mathbf{x}) \neq 1 + \eta(\mathbf{x})$ ,  $p_2(\mathbf{x}) \neq \frac{\eta(\mathbf{x})}{1+\eta(\mathbf{x})}$  and  $p_3(\mathbf{x}) \neq \frac{\eta(\mathbf{x})}{1+\eta(\mathbf{x})}$ . Combined with the above results, we have proved that if Eq. (10)-(12) are satisfied,  $\mathbf{R}_n^*$  is feasible through PBNA. ■

C. Some  $m_{ij}(\mathbf{x}) = 0$  ( $i \neq j$ )

In this case, since the number of interference terms is reduced, at least one of  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$  is removed, and thus the restriction on  $\mathbf{V}_1$  imposed by Eq. (3) vanishes. Therefore,

we can choose  $\mathbf{V}_1$  freely, and the feasibility condition of PBNA is greatly simplified. For example, assume  $m_{23}(\mathbf{x}) = 0$  and all other transfer functions are non-zeros. Hence  $\mathcal{A}_2$  is removed. Meanwhile,  $\mathcal{B}_1', \mathcal{B}_2', \mathcal{B}_3'$  remain the same. Similarly to Theorem 1, we can set  $\mathbf{V}_1 = (\theta_{ij})_{(2n+1) \times (n+1)}$ , where  $\theta_{ij}$  is an arbitrary variable. It is easy to see that  $\mathbf{R}_n^*$  is feasible through PBNA if and only if  $p_i(\mathbf{x})$  is not constant for every  $i \in \{1, 2, 3\}$ . Using similar arguments, we can discuss other cases.

## VI. CHECKING THE FEASIBILITY OF PBNA

For a given graph, checking the feasibility of PBNA is now reduced to checking whether Eq. (13)-(15). This is a multivariate polynomial identity testing problem. To check whether  $p_i(\mathbf{x}) \neq 1$ , we use Ford-Fulkerson Algorithm, as per Lemma 2. To check whether  $p_i(\mathbf{x}) \neq \eta(\mathbf{x})$ , we define  $q_i(\mathbf{x}) = \frac{\eta(\mathbf{x})}{p_i(\mathbf{x})}$  and consider  $q_i(\mathbf{x}) \neq 1$ . Therefore, Ford-Fulkerson Algorithm can be used to check this condition as well. For the other conditions ( $p_1(\mathbf{x}) \neq \frac{\eta(\mathbf{x})}{1+\eta(\mathbf{x})}$  and  $p_2(\mathbf{x}), p_3(\mathbf{x}) \neq 1 + \eta(\mathbf{x})$ ), it is still not clear what is their interpretation in terms of graph structure. A counter example is shown in Fig. 1(b). Nevertheless, we can still check the conditions by evaluating the rational functions through  $T$  random tests:

---

```

for  $k = 1$  to  $T$  do
  Assign random values to  $\mathbf{x}$ , denoted by  $\mathbf{x}_0$ 
  If  $p_1(\mathbf{x}_0) \neq \frac{\eta(\mathbf{x}_0)}{1+\eta(\mathbf{x}_0)}$ , return success
end for
Return failure (i.e.,  $\mathcal{B}_i'$  is violated)

```

---

Let  $L$  denote the maximum distance from any sender to any receiver in the network. Using Lemma 4 of [3], we can upper-bound the probability of error as follows. We consider the case of  $i = 1$ . Other cases follow along similar lines. Note that Eq. (10) is equivalent to the following equation:

$$f(\mathbf{x}) = m_{11}(\mathbf{x})m_{32}(\mathbf{x})m_{23}(\mathbf{x}) + m_{21}(\mathbf{x})m_{32}(\mathbf{x})m_{12}(\mathbf{x}) + m_{31}(\mathbf{x})m_{12}(\mathbf{x})m_{23}(\mathbf{x}) = 0$$

Since the maximum degree of any variable  $x_{ee'}$  in a transfer function is at most one, the total degree of each term in  $f(\mathbf{x})$  is at most  $3L$ . For each random test, the probability of error in checking if Eq. (10), denoted by  $\delta_1$ , can be upper bounded by using Lemma 4 of [3]:  $\delta_1 = \Pr(f(\mathbf{x}_0) = 0 \mid f(\mathbf{x}) \neq 0) \leq 1 - (1 - \frac{3}{2^m})^L$ . Hence, the total probability of error in checking if  $p_1(\mathbf{x}) \neq 1 + \eta(\mathbf{x})$  is  $P_1(\text{Error}) = \delta_1^T \leq [1 - (1 - \frac{3}{2^m})^L]^T$ . Thus, the error can be made arbitrarily small for sufficiently large  $m$  and  $T$ . The running time of the algorithm is  $O(T|E|D_{in})$ , where  $D_{in}$  is the maximum in-degree of any node in the network.

## VII. CONCLUSION

In this paper, we study the feasibility of PBNA for three unicast sessions. We first prove that the set of conditions proposed by [9] are also necessary for the feasibility of PBNA with respect to any valid precoding matrix. Then, we reduce this set of conditions to just four conditions, using two graph-related properties along with a simple degree-counting technique. This reduction enables an efficient algorithm for checking the feasibility of PBNA.

APPENDIX A  
PROOFS OF GRAPH PROPERTIES

The following lemma is used in the proof of Lemma 2.

*Lemma 7:* Let  $(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}$ . Then, there exists  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$  such that  $t(P_1)t(P_2) = t(P_3)t(P_4)$  if and only if  $P_1 \cap P_2 \neq \emptyset$ .

*Proof:* First, Assume  $P_1 \cap P_2 \neq \emptyset$ . Pick an arbitrary edge  $e \in P_1 \cap P_2$ . Let  $P_1^1$  and  $P_1^2$  be the path segments along  $P_1$  before and after  $e$  respectively. Similarly, we can define  $P_2^1$  and  $P_2^2$ . Construct  $P_3 = P_1^1 \cup \{e\} \cup P_2^1$  and  $P_4 = P_1^2 \cup \{e\} \cup P_2^2$ . Hence, it is easy to see that  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$  and  $t(P_1)t(P_2) = t(P_3)t(P_4)$ .

Now assume  $P_1 \cap P_2 = \emptyset$ . By contradiction, assume there exists  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$  such that  $t(P_1)t(P_2) = t(P_3)t(P_4)$ . Clearly,  $P_1 \cup P_2 = P_3 \cup P_4$ . Then, there exist  $e, e' \in P_4$  such that  $\text{head}(e) = \text{tail}(e')$  and  $e \in P_1, e' \in P_2$ . Hence,  $x_{ee'} \mid t(P_3)t(P_4)$  but  $x_{ee'} \nmid t(P_1)t(P_2)$ , contradicting our assumption. ■

*Proof of Lemma 2:* Assume  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x}) \neq m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$ . Thus there exists  $(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}$  such that for any  $(P_3, P_4) \in \mathcal{P}_{aq} \times \mathcal{P}_{pb}$ ,  $t(P_1)t(P_2) \neq t(P_3)t(P_4)$ , or vice versa. By Lemma 7,  $P_1 \cap P_2 = \emptyset$  ( $P_3 \cap P_4 = \emptyset$  for the other case). On the other hand, if there exists disjoint path pair  $(P_1, P_2) \in \mathcal{P}_{ab} \times \mathcal{P}_{pq}$ ,  $t(P_1)t(P_2)$  is absent from  $m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$ . Moreover, there is only one term in  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})$  which equals  $t(P_1)t(P_2)$ . Thus  $t(P_1)t(P_2)$  doesn't vanish from  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x})$ . Hence  $m_{ab}(\mathbf{x})m_{pq}(\mathbf{x}) \neq m_{aq}(\mathbf{x})m_{pb}(\mathbf{x})$ . Similarly, the theorem holds for the other case. ■

APPENDIX B  
GENERAL FORM OF  $\mathbf{V}_1$

The following lemma shows that given any full-rank matrices  $\mathbf{A}$ ,  $\mathbf{B}$  and  $\mathbf{C}$  as defined in  $\mathcal{A}'_1, \mathcal{A}'_2, \mathcal{A}'_3$ , we can always find a non-zero solution to (16), and thus construct a precoding matrix  $\mathbf{B}_1$  which satisfies (16).

*Lemma 8:* Equation (16) has a non-zero solution in  $\mathbb{F}_{2^m}^{n+1}[z]$  in the form of  $\mathbf{r}(z) = (1, z, z^2, \dots, z^n)\mathbf{F}$ , where  $\mathbf{F}$  is an  $(n+1) \times (n+1)$  matrix in  $\mathbb{F}_{2^m}$ . Moreover, any solution to (16) is linearly dependent on  $(1, z, \dots, z^n)\mathbf{F}$ .

*Proof:* Denote  $\mathbf{D} = \mathbf{B}\mathbf{A}$ . First, we will prove that  $\text{rank}(z\mathbf{C} - \mathbf{D}) = n$ . Let  $\mathbf{c}_i$  and  $\mathbf{d}_i$  denote the  $i$ th column of  $\mathbf{C}$  and  $\mathbf{D}$  respectively. Hence,  $\mathbf{c}_1, \dots, \mathbf{c}_n$  are linearly independent and so are  $\mathbf{d}_1, \dots, \mathbf{d}_n$ . Assume there exist  $f_1(z), \dots, f_n(z) \in \mathbb{F}_{2^m}(z)$  such that  $\sum_{i=1}^n f_i(z)(z\mathbf{c}_i - \mathbf{d}_i) = 0$ . Without loss of generality, assume  $f_i(z) = \frac{g_i(z)}{h(z)}$  for  $i \in \{1, 2, \dots, n\}$ , where  $g_i(z), h(z) \in \mathbb{F}_{2^m}[z]$ . Thus,  $\sum_{i=1}^n g_i(z)(z\mathbf{c}_i - \mathbf{d}_i) = 0$ . Let  $k = \max_{i \in \{1, 2, \dots, n\}} \{d_{g_i}\}$  and assume  $g_i(z) = \sum_{l=0}^k a_{l,i}z^l$ . Then, it follows

$$\begin{aligned} \sum_{i=1}^n g_i(z)(z\mathbf{c}_i - \mathbf{d}_i) &= \sum_{l=0}^k \sum_{i=1}^n (a_{l,i}z^{l+1}\mathbf{c}_i - a_{l,i}z^l\mathbf{d}_i) \\ &= z^{k+1} \sum_{i=1}^n a_{k,i}\mathbf{c}_i + \sum_{l=0}^{k-1} z^{l+1} \sum_{i=1}^n (a_{l,i}\mathbf{c}_i - a_{l+1,i}\mathbf{d}_i) \\ &\quad - \sum_{i=1}^n a_{0,i}\mathbf{d}_i = 0 \end{aligned}$$

Therefore, the following equations must hold:

$$\begin{aligned} \sum_{i=1}^n a_{k,i}\mathbf{c}_i &= 0 \quad \sum_{i=1}^n a_{0,i}\mathbf{d}_i = 0 \\ \sum_{i=1}^n (a_{l,i}\mathbf{c}_i - a_{l+1,i}\mathbf{d}_i) &= 0 \quad \forall l \in \{0, \dots, k-1\} \end{aligned}$$

Thus  $a_{l,i} = 0$  for any  $i \in \{1, \dots, n\}, l \in \{0, \dots, k\}$ , implying  $f_i(z) = 0$ . Hence,  $\text{rank}(z\mathbf{C} - \mathbf{D}) = n$ .

Then, there must be an  $n \times n$  invertible submatrix in  $z\mathbf{C} - \mathbf{D}$ . Without loss of generality, assume this submatrix consists of the top  $n$  rows of  $z\mathbf{C} - \mathbf{D}$  and denote this submatrix by  $\mathbf{E}_{n+1}$ . Let  $\mathbf{b}$  denote the  $(n+1)$ th row of  $z\mathbf{C} - \mathbf{D}$ . In order to get a non-zero solution to equation (16), we first fix  $r_{n+1}(z) = -1$ . Therefore, equation (16) is transformed into  $(r_1(z), \dots, r_n(z))\mathbf{E}_{n+1} = \mathbf{b}$ . For  $i \in \{1, 2, \dots, n\}$ , let  $\mathbf{E}_i$  denote the submatrix acquired by replacing the  $i$ th row of  $\mathbf{E}_{n+1}$  with  $\mathbf{b}$ . Hence, we get a non-zero solution to (16):

$$\mathbf{r}(z) = \left( \frac{\det \mathbf{E}_1}{\det \mathbf{E}_{n+1}}, \dots, \frac{\det \mathbf{E}_n}{\det \mathbf{E}_{n+1}}, -1 \right)$$

Moreover,  $\bar{\mathbf{r}}(z) = (\det \mathbf{E}_1, \dots, \det \mathbf{E}_n, -\det \mathbf{E}_{n+1})$  is also a solution. Also note that the degree of  $z$  in each  $\det \mathbf{E}_i$  ( $i \in \{1, 2, \dots, n+1\}$ ) is at most  $n$ . Thus,  $\bar{\mathbf{r}}(z)$  can be formulated as  $(1, z, z^2, \dots, z^n)\mathbf{F}$ , where  $\mathbf{F}$  is an  $(n+1) \times (n+1)$  matrix in  $\mathbb{F}_{2^m}$ . Since  $\text{rank}(z\mathbf{C} - \mathbf{D}) = n$ , all the solutions to equation (16) form a one-dimensional linear space. Thus, all solutions must be linearly dependent on  $\bar{\mathbf{r}}(z)$ . ■

*Proof of Lemma 5:* Let  $\mathbf{r}_i$  be the  $i$ th row of  $\mathbf{V}_1$ , which satisfies equation (3). According to Lemma 8,  $\mathbf{r}_i$  must have the form  $f_i(\eta(\mathbf{x}^i))(1, \eta(\mathbf{x}^i), \dots, \eta^n(\mathbf{x}^i))\mathbf{F}$ , where  $f_i(z)$  is a non-zero rational function in  $\mathbb{F}_{2^m}(z)$ . Hence,  $\mathbf{V}_1$  can be written as  $\mathbf{G}\mathbf{V}_1^*\mathbf{F}$ .

According to Lemma 8, equation (16) can be rewritten as follows:

$$(z, z^2, \dots, z^{n+1})\mathbf{F}\mathbf{C} = (1, z, \dots, z^n)\mathbf{F}\mathbf{B}\mathbf{A}$$

The right side of the above equation contains no  $z^{n+1}$ , and thus the  $(n+1)$ th row of  $\mathbf{F}\mathbf{C}$  must be zero. Similarly, there is no constant term on the left side of the above equation, implying that the 1st row of  $\mathbf{F}\mathbf{B}\mathbf{A}$  is zero. ■

APPENDIX C  
RESULTS ON MULTIVARIATE POLYNOMIAL

Let  $\mathbf{y} = (y_1, y_2, \dots, y_k)$  be a vector of variables. For any  $i \in \{1, 2, \dots, k\}$ , define  $\mathbf{y}_i = (y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_k)$ , i.e., the vector consisting of all variables in  $\mathbf{y}$  other than  $y_i$ . Note that any polynomial  $f(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  can be formulated as

$$f(\mathbf{y}) = f_0(\mathbf{y}_i) + f_1(\mathbf{y}_i)y_i + \dots + f_p(\mathbf{y}_i)y_i^p$$

where  $f_j(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$  for  $j \in \{0, 1, \dots, p\}$  and  $f_p(\mathbf{y}_i) \neq 0$ . Let  $\mathbb{F}(\mathbf{y}_i)$  denote the field consisting of all rational functions in the form of  $\frac{u(\mathbf{y}_i)}{v(\mathbf{y}_i)}$ , where  $u(\mathbf{y}_i), v(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ . Because  $\mathbb{F}[\mathbf{y}_i]$  is a subset of  $\mathbb{F}(\mathbf{y}_i)$ ,  $f(\mathbf{y})$  can also be viewed as a univariate polynomial in the ring  $\mathbb{F}(\mathbf{y}_i)[y_i]$ . For any  $h(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ , we use  $h(y_i)$  to denote its equivalent counterpart in  $\mathbb{F}(\mathbf{y}_i)[y_i]$ . To differentiate these two concepts, we reserve the notations,



such as “|”, “gcd” and “lcm”<sup>5</sup>, for field  $\mathbb{F}$ , and append “1” as a subscript to these notations to suggest they are specific to field  $\mathbb{F}(\mathbf{y}_i)$ . For example, for  $f(\mathbf{y}), g(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  and  $u(y_i), v(y_i) \in \mathbb{F}(\mathbf{y}_i)[y_i]$ ,  $g(\mathbf{y}) \mid f(\mathbf{y})$  means that there exists  $h(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  such that  $f(\mathbf{y}) = h(\mathbf{y})g(\mathbf{y})$ , and  $u(y_i) \mid_1 v(y_i)$  means that there exists  $w(y_i) \in \mathbb{F}[\mathbf{y}_i][y_i]$  such that  $v(y_i) = w(y_i)u(y_i)$ . Similarly,  $\gcd(f(\mathbf{y}), g(\mathbf{y}))$  is the greatest common divisor of  $f(\mathbf{y})$  and  $g(\mathbf{y})$  within  $\mathbb{F}[\mathbf{y}]$ , and  $\gcd_1(u(y_i), v(y_i))$  is the greatest common divisor of  $u(y_i)$  and  $v(y_i)$  in  $\mathbb{F}(\mathbf{y}_i)[y_i]$ .

In general, each polynomial  $h(y_i) \in \mathbb{F}(\mathbf{y}_i)[y_i]$  is of the following form

$$h(y_i) = \frac{a_0(\mathbf{y}_i)}{b_0(\mathbf{y}_i)} + \frac{a_1(\mathbf{y}_i)}{b_1(\mathbf{y}_i)}y_i + \cdots + \frac{a_p(\mathbf{y}_i)}{b_p(\mathbf{y}_i)}y_i^p$$

In the above formula, for any  $j \in \{0, 1, \dots, p\}$ ,  $a_j(\mathbf{y}_i), b_j(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ ,  $b_j(\mathbf{y}_i) \neq 0$ ,  $\gcd(a_j(\mathbf{y}_i), b_j(\mathbf{y}_i)) = 1$ , and  $a_p(\mathbf{y}_i) \neq 0$ . Note that for any  $y_i^j$  which is absent in  $h(y_i)$ , we let  $a_j(\mathbf{y}_i) = 0$  and  $b_j(\mathbf{y}_i) = 1$ . Define the following polynomial

$$\mu_h(\mathbf{y}_i) = \text{lcm}(b_0(\mathbf{y}_i), b_1(\mathbf{y}_i), \dots, b_p(\mathbf{y}_i))$$

Thus,  $\mu_h(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$  and  $\mu_h(\mathbf{y}_i)h(y_i) \in \mathbb{F}[\mathbf{y}]$ .

**Lemma 9:** Assume  $g(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$  and  $f(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  is of the form  $f(\mathbf{y}) = \sum_{j=0}^p f_j(\mathbf{y}_i)y_i^j$ , where  $f_j(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ . Then  $g(\mathbf{y}_i) \mid f(\mathbf{y})$  if and only if  $g(\mathbf{y}_i) \mid f_j(\mathbf{y}_i)$  for any  $j \in \{0, 1, \dots, p\}$ .

*Proof:* Apparently, if  $g(\mathbf{y}_i) \mid f_j(\mathbf{y}_i)$  for any  $j \in \{0, 1, \dots, p\}$ ,  $g(\mathbf{y}_i) \mid f(\mathbf{y})$ . Now assume  $g(\mathbf{y}_i) \mid f(\mathbf{y})$ . Thus there exists  $h(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  such that  $f(\mathbf{y}) = g(\mathbf{y}_i)h(\mathbf{y})$ . Let  $h(\mathbf{y}) = \sum_{j=0}^p h_j(\mathbf{y}_i)y_i^j$ . Hence, it follows that  $f_j(\mathbf{y}_i) = h_j(\mathbf{y}_i)g(\mathbf{y}_i)$  and thus  $g(\mathbf{y}_i) \mid f_j(\mathbf{y}_i)$ . ■

The following result follows immediately from Lemma 9.

**Corollary 1:** Let  $g(\mathbf{y}_i)$  and  $f(\mathbf{y})$  be defined as Lemma 9. Then  $\gcd(g(\mathbf{y}_i), f(\mathbf{y})) = \gcd(g(\mathbf{y}_i), f_0(\mathbf{y}_i), \dots, f_p(\mathbf{y}_i))$ .

*Proof:* Note that any divisor of  $g(\mathbf{y}_i)$  must be a polynomial in  $\mathbb{F}[\mathbf{y}_i]$ . Let  $d(\mathbf{y}_i) = \gcd(g(\mathbf{y}_i), f(\mathbf{y}))$  and  $d'(\mathbf{y}_i) = \gcd(g(\mathbf{y}_i), f_0(\mathbf{y}_i), \dots, f_p(\mathbf{y}_i))$ . By Lemma 9,  $d(\mathbf{y}_i) \mid f_j(\mathbf{y}_i)$  for any  $j \in \{0, 1, \dots, p\}$ , implying that  $d(\mathbf{y}_i) \mid d'(\mathbf{y}_i)$ . On the other hand,  $d'(\mathbf{y}_i) \mid f(\mathbf{y})$ , and thus  $d'(\mathbf{y}_i) \mid d(\mathbf{y}_i)$ . Hence,  $d(\mathbf{y}_i) = d'(\mathbf{y}_i)$ . ■

**Corollary 2:** For  $t \in \{1, 2, \dots, s\}$ , let  $f_t(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  be defined as  $f_t(\mathbf{y}) = \sum_{j=0}^{p_t} f_{tj}(\mathbf{y}_i)y_i^j$ , where  $f_{tj}(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ . Let  $g(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ . It follows

$$\begin{aligned} & \gcd(g(\mathbf{y}_i), f_1(\mathbf{y}), \dots, f_t(\mathbf{y})) \\ &= \gcd(g(\mathbf{y}_i), f_{10}(\mathbf{y}_i), \dots, f_{1p_1}(\mathbf{y}_i), \dots, \\ & \quad f_{s0}(\mathbf{y}_i), \dots, f_{sp_s}(\mathbf{y}_i)) \end{aligned}$$

*Proof:* We have the following equations

$$\begin{aligned} & \gcd(g(\mathbf{y}_i), f_1(\mathbf{y}), \dots, f_t(\mathbf{y})) \\ &= \gcd(g(\mathbf{y}_i), f_1(\mathbf{y}), \dots, g(\mathbf{y}_i), f_t(\mathbf{y})) \\ &= \gcd(\gcd(g(\mathbf{y}_i), f_1(\mathbf{y})), \dots, \gcd(g(\mathbf{y}_i), f_s(\mathbf{y}))) \\ &= \gcd(g(\mathbf{y}_i), f_{10}(\mathbf{y}_i), \dots, f_{1p_1}(\mathbf{y}_i), \dots, \\ & \quad g(\mathbf{y}_i), f_{s0}(\mathbf{y}_i), \dots, f_{sp_s}(\mathbf{y}_i)) \end{aligned}$$

<sup>5</sup>We use  $\text{lcm}(f(x), g(x))$  to denote the least common multiple of two polynomials  $f(x)$  and  $g(x)$ .

$$= \gcd(g(\mathbf{y}_i), f_{10}(\mathbf{y}_i), \dots, f_{1p_1}(\mathbf{y}_i), \dots, f_{s0}(\mathbf{y}_i), \dots, f_{sp_s}(\mathbf{y}_i))$$

**Lemma 10:** For  $t \in \{1, 2, \dots, s\}$ , let  $a_t(\mathbf{y}), b_t(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$  such that  $b_t(\mathbf{y}) \neq 0$  and  $\gcd(a_t(\mathbf{y}), b_t(\mathbf{y})) = 1$ . For  $t \in \{1, 2, \dots, s\}$ , let  $v_t(\mathbf{y}) = \text{lcm}(b_1(\mathbf{y}), \dots, b_t(\mathbf{y}))$ . Then we have

$$\gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_s(\mathbf{y})\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}, v_s(\mathbf{y})\right) = 1$$

*Proof:* We use induction on  $s$  to prove this lemma. Apparently, the lemma holds for  $s = 1$  due to  $\gcd(a_1(\mathbf{y}), b_1(\mathbf{y})) = 1$ . Assume it holds for  $s - 1$ . Thus it follows

$$\begin{aligned} & \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_s(\mathbf{y})\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}, v_s(\mathbf{y})\right) \\ &= \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_s(\mathbf{y})\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}, b_s(\mathbf{y})\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &= \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, \gcd(a_s(\mathbf{y}), b_s(\mathbf{y}))\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &\stackrel{(a)}{=} \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_{s-1}(\mathbf{y})\frac{v_s(\mathbf{y})}{b_{s-1}(\mathbf{y})}, \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &\stackrel{(b)}{=} \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_{s-1}(\mathbf{y})\frac{v_s(\mathbf{y})}{b_{s-1}(\mathbf{y})}, \right. \\ & \quad \left. \gcd\left(v_{s-1}(\mathbf{y}), \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right)\right) \\ &= \gcd\left(a_1(\mathbf{y})\frac{v_s(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_{s-1}(\mathbf{y})\frac{v_s(\mathbf{y})}{b_{s-1}(\mathbf{y})}, v_{s-1}(\mathbf{y}), \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &= \gcd\left(\frac{v_s(\mathbf{y})}{v_{s-1}(\mathbf{y})} \gcd\left(a_1(\mathbf{y})\frac{v_{s-1}(\mathbf{y})}{b_1(\mathbf{y})}, \dots, a_{s-1}(\mathbf{y})\frac{v_{s-1}(\mathbf{y})}{b_{s-1}(\mathbf{y})}\right), \right. \\ & \quad \left. v_{s-1}(\mathbf{y}), \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &\stackrel{(c)}{=} \gcd\left(\frac{v_s(\mathbf{y})}{v_{s-1}(\mathbf{y})}, v_{s-1}(\mathbf{y}), \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})}\right) \\ &\stackrel{(d)}{=} \gcd\left(\frac{b_s(\mathbf{y})}{\gcd(v_{s-1}(\mathbf{y}), b_s(\mathbf{y}))}, v_{s-1}(\mathbf{y}), \frac{v_{s-1}(\mathbf{y})}{\gcd(v_{s-1}(\mathbf{y}), b_s(\mathbf{y}))}\right) \\ &= \gcd(1, v_{s-1}(\mathbf{y})) = 1 \end{aligned}$$

In the above equations, (a) is due to  $\gcd(a_s(\mathbf{y}), b_s(\mathbf{y})) = 1$ ; (b) follows from the fact that  $\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})} \mid v_{s-1}(\mathbf{y})$  and thus  $\frac{v_s(\mathbf{y})}{b_s(\mathbf{y})} = \gcd(v_{s-1}(\mathbf{y}), \frac{v_s(\mathbf{y})}{b_s(\mathbf{y})})$ ; (c) follows from the inductive assumption; (d) is due to the equality:  $v_s(\mathbf{y}) = \text{lcm}(v_{s-1}(\mathbf{y}), b_s(\mathbf{y})) = \frac{v_{s-1}(\mathbf{y})b_s(\mathbf{y})}{\gcd(v_{s-1}(\mathbf{y}), b_s(\mathbf{y}))}$ . ■

**Corollary 3:** For  $j \in \{1, 2, \dots, s\}$ , let  $f_j(y_i) \in \mathbb{F}(\mathbf{y}_i)[y_i]$ . Define  $v(\mathbf{y}_i) = \text{lcm}(\mu_{f_1}(\mathbf{y}_i), \dots, \mu_{f_s}(\mathbf{y}_i))$  and  $\tilde{f}_j(\mathbf{y}) = v(\mathbf{y}_i)f_j(y_i)$ . Thus  $\gcd(v(\mathbf{y}_i), f_1(\mathbf{y}), \dots, f_s(\mathbf{y})) = 1$

*Proof:* Assume  $f_j(y_i)$  has the following form:

$$f_j(y_i) = \frac{a_{j0}(\mathbf{y}_i)}{b_{j0}(\mathbf{y}_i)} + \frac{a_{j1}(\mathbf{y}_i)}{b_{j1}(\mathbf{y}_i)}y_i + \cdots + \frac{a_{jp_j}(\mathbf{y}_i)}{b_{jp_j}(\mathbf{y}_i)}y_i^{p_j}$$

where for any  $j \in \{1, 2, \dots, s\}$  and  $t \in \{0, 1, \dots, p_j\}$ ,  $a_{jt}(\mathbf{y}_i), b_{jt}(\mathbf{y}_i) \in \mathbb{F}[\mathbf{y}_i]$ ,  $b_{jt}(\mathbf{y}_i) \neq 0$  and  $\gcd(a_{jt}(\mathbf{y}_i), b_{jt}(\mathbf{y}_i)) = 1$ . Apparently,  $v(\mathbf{y}_i)$  is the least common multiple of all  $b_{jt}(\mathbf{y}_i)$ 's. Define

$u_{jt}(\mathbf{y}_i) = \frac{v(\mathbf{y}_i)}{b_{jt}(\mathbf{y}_i)} \in \mathbb{F}[\mathbf{y}_i]$ . Hence, we have  $\bar{f}_j(\mathbf{y}) = \sum_{t=0}^{p_j} a_{jt}(\mathbf{y}_i) u_{jt}(\mathbf{y}_i) y_i^t$ . Then it follows

$$\begin{aligned} & \gcd(v(\mathbf{y}_i), \bar{f}_1(\mathbf{y}), \dots, \bar{f}_s(\mathbf{y})) \\ & \stackrel{(a)}{=} \gcd(v(\mathbf{y}_i), a_{10}(\mathbf{y}_i) u_{10}(\mathbf{y}_i), \dots, a_{1p_1}(\mathbf{y}_i) u_{1p_1}(\mathbf{y}_i), \dots, \\ & \quad a_{s0}(\mathbf{y}_i) u_{s0}(\mathbf{y}_i), \dots, a_{sp_s}(\mathbf{y}_i) u_{sp_s}(\mathbf{y}_i)) \\ & \stackrel{(b)}{=} 1 \end{aligned}$$

where (a) is due to Corollary 2 and (b) follows from Lemma 10. ■

Generally, the definitions of division in  $\mathbb{F}[\mathbf{y}]$  and  $\mathbb{F}(\mathbf{y}_i)[y_i]$  are different. However, the following theorem reveals the two definitions are closely related.

**Theorem 4:** Consider two polynomials  $f(\mathbf{y}), g(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ , where  $g(\mathbf{y}) \neq 0$ . Then  $g(\mathbf{y}) \mid f(\mathbf{y})$  if and only if  $g(y_i) \mid_1 f(y_i)$  for every  $i \in \{1, 2, \dots, k\}$ .

*Proof:* The division equation between  $f(y_i)$  and  $g(y_i)$  is as follows

$$f(y_i) = h_i(y_i)g(y_i) + r_i(y_i) \quad (17)$$

where  $h_i(y_i), r_i(y_i) \in \mathbb{F}(\mathbf{y}_i)[y_i]$ , and either  $r_i(y_i) = 0$  or  $d_{r_i} < d_g$ . Due to the uniqueness of Equation (17),  $f(\mathbf{y}) \mid g(\mathbf{y})$  immediately implies that for any  $i \in \{1, 2, \dots, k\}$ ,  $r_i(y_i) = 0$  and thus  $g(y_i) \mid_1 f(y_i)$ .

Conversely, assume for every  $i \in \{1, \dots, k\}$ ,  $g(y_i) \mid_1 f(y_i)$  and hence  $r_i(y_i) = 0$ . Denote  $\bar{h}_i(\mathbf{y}) = \mu_{h_i}(\mathbf{y}_i) h_i(y_i)$ . Clearly,  $\bar{h}_i(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ . Then, the following equation holds

$$\mu_{h_i}(\mathbf{y}_i) f(\mathbf{y}) = \bar{h}_i(\mathbf{y}) g(\mathbf{y})$$

By Corollary 3,  $\gcd(\mu_{h_i}(\mathbf{y}_i), \bar{h}_i(\mathbf{y})) = 1$ . Thus,  $\mu_{h_i}(\mathbf{y}_i) \mid g(\mathbf{y})$ . Define  $\bar{g}(\mathbf{y}) = \frac{g(\mathbf{y})}{\mu_{h_i}(\mathbf{y}_i)}$ . By Lemma 9,  $\bar{g}(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ . Define  $u(\mathbf{y}) = \frac{g(\mathbf{y})}{\gcd(f(\mathbf{y}), g(\mathbf{y}))} \in \mathbb{F}[\mathbf{y}]$ . It follows that

$$\begin{aligned} u(\mathbf{y}) &= \frac{g(\mathbf{y})}{\gcd(f(\mathbf{y}), g(\mathbf{y}))} \\ &= \frac{\mu_{h_i}(\mathbf{y}_i) \bar{g}(\mathbf{y})}{\gcd(\bar{h}_i(\mathbf{y}) \bar{g}(\mathbf{y}), \mu_{h_i}(\mathbf{y}_i) \bar{g}(\mathbf{y}))} \\ &= \frac{\mu_{h_i}(\mathbf{y}_i) \bar{g}(\mathbf{y})}{\bar{g}(\mathbf{y}) \gcd(\bar{h}_i(\mathbf{y}), \mu_{h_i}(\mathbf{y}_i))} \\ &= \frac{\mu_{h_i}(\mathbf{y}_i) \bar{g}(\mathbf{y})}{\bar{g}(\mathbf{y})} \\ &= \mu_{h_i}(\mathbf{y}_i) \end{aligned}$$

Note that variable  $y_i$  is absent in  $u(\mathbf{y})$ . Because  $y_i$  can be any arbitrary variable in  $\mathbf{y}$ , it immediately follows that all the variables in  $\mathbf{y}$  must be absent in  $u(\mathbf{y})$ , implying that  $u(\mathbf{y})$  is a constant in  $\mathbb{F}$ . Hence  $g(\mathbf{y}) \mid f(\mathbf{y})$ . ■

**Theorem 5:** Let  $f(\mathbf{y}), g(\mathbf{y})$  be two non-zero polynomials in  $\mathbb{F}[\mathbf{y}]$ . Then  $\gcd(f(\mathbf{y}), g(\mathbf{y})) = 1$  if and only if  $\gcd_1(f(y_i), g(y_i)) = 1$  for any  $i \in \{1, 2, \dots, k\}$ .

*Proof:* First, assume for any  $i \in \{1, 2, \dots, k\}$ ,  $\gcd_1(f(y_i), g(y_i)) = 1$ . We use contradiction to prove that  $\gcd(f(\mathbf{y}), g(\mathbf{y})) = 1$ . Assume  $u(\mathbf{y}) = \gcd(f(\mathbf{y}), g(\mathbf{y}))$  is not constant. Let  $y_i$  be a variable which is present in  $u(\mathbf{y})$ . By Theorem 4,  $u(y_i) \mid_1 f(y_i)$  and  $u(y_i) \mid_1 g(y_i)$ , which contradicts that  $\gcd_1(f(y_i), g(y_i)) = 1$ .

Then, assume  $\gcd(f(\mathbf{y}), g(\mathbf{y})) = 1$ . We also use contradiction to prove that for any  $i \in \{1, 2, \dots, k\}$ ,  $\gcd_1(f(y_i), g(y_i)) = 1$ . Assume there exists  $i \in \{1, \dots, k\}$  such that  $v(y_i) = \gcd_1(f(y_i), g(y_i))$  is non-trivial. Define  $w(\mathbf{y}) = \mu_v(\mathbf{y}_i) v(y_i) \in \mathbb{F}[\mathbf{y}]$ . Clearly,  $w(y_i) \mid_1 f(y_i)$  and  $w(y_i) \mid_1 g(y_i)$ . Thus, there exists  $p(y_i), q(y_i) \in \mathbb{F}(\mathbf{y}_i)[y_i]$  such that

$$f(y_i) = w(y_i)p(y_i) \quad g(y_i) = w(y_i)q(y_i)$$

Let  $s(\mathbf{y}_i) = \text{lcm}(\mu_p(\mathbf{y}_i), \mu_q(\mathbf{y}_i))$ . Define  $\bar{p}(\mathbf{y}) = s(\mathbf{y}_i)p(y_i)$  and  $\bar{q}(\mathbf{y}) = s(\mathbf{y}_i)q(y_i)$ . Apparently,  $\bar{p}(\mathbf{y}), \bar{q}(\mathbf{y}) \in \mathbb{F}[\mathbf{y}]$ . It follows that

$$s(\mathbf{y}_i)f(\mathbf{y}) = w(\mathbf{y})\bar{p}(\mathbf{y}) \quad s(\mathbf{y}_i)g(\mathbf{y}) = w(\mathbf{y})\bar{q}(\mathbf{y})$$

Then the following equation holds

$$s(\mathbf{y}_i)\gcd(f(\mathbf{y}), g(\mathbf{y})) = w(\mathbf{y})\gcd(\bar{p}(\mathbf{y}), \bar{q}(\mathbf{y}))$$

Due to Corollary 3,  $\gcd(s(\mathbf{y}_i), \gcd(\bar{p}(\mathbf{y}), \bar{q}(\mathbf{y}))) = \gcd(s(\mathbf{y}_i), \bar{p}(\mathbf{y}), \bar{q}(\mathbf{y})) = 1$ . Hence  $s(\mathbf{y}_i) \mid w(\mathbf{y})$ . Let  $\bar{w}(\mathbf{y}) = \frac{w(\mathbf{y})}{s(\mathbf{y}_i)}$ . According to Lemma 9,  $\bar{w}(\mathbf{y})$  is a non-trivial polynomial in  $\mathbb{F}[\mathbf{y}]$ . Thus,  $\bar{w}(\mathbf{y}) \mid \gcd(f(\mathbf{y}), g(\mathbf{y}))$ , contradicting  $\gcd(f(\mathbf{y}), g(\mathbf{y})) = 1$ . ■

**Lemma 11:** Consider two non-zero polynomials in  $\mathbb{F}[z]$ ,  $f(z) = a_0 + a_1z + \dots + a_pz^p$  and  $g(z) = b_0 + b_1z + \dots + b_qz^q$ , where  $a_i, b_j \in \mathbb{F}$  for  $i \in \{0, 1, \dots, p\}, j \in \{0, 1, \dots, q\}$ ,  $a_pb_q \neq 0$ ,  $p \geq q$  and  $\gcd(f(z), g(z)) = 1$ . Let  $s(x), t(x)$  be two non-zero polynomials in  $\mathbb{F}[x]$  such that  $\gcd(s(x), t(x)) = 1$ . Define the following polynomials in  $\mathbb{F}[x]$ :

$$\begin{aligned} \alpha(x) &= f\left(\frac{s(x)}{t(x)}\right)t^p(x) = \sum_{k=0}^p a_k t^{p-k}(x) s^k(x) \\ \beta(x) &= g\left(\frac{s(x)}{t(x)}\right)t^q(x) = \sum_{k=0}^q b_k t^{q-k}(x) s^k(x) \end{aligned}$$

Then  $\gcd(\alpha(x), \beta(x)) = 1$ .

*Proof:* Assume  $w(x) = \gcd(\alpha(x), \beta(x))$  is non-trivial. Thus we can find an extension field  $\bar{\mathbb{F}}$  of  $\mathbb{F}$  such that there exists  $x_0 \in \bar{\mathbb{F}}$  which satisfies  $w(x_0) = 0$  and hence  $\alpha(x_0) = \beta(x_0) = 0$ . In the rest of this proof, we restrict our discussion in  $\bar{\mathbb{F}}$ . Note that  $\gcd(f(z), g(z)) = 1$  and  $\gcd(s(x), t(x)) = 1$  also hold for  $\bar{\mathbb{F}}$ . Assume  $t(x_0) = 0$  and thus  $x - x_0 \mid t(x)$ . Since  $\gcd(s(x), t(x)) = 1$ , it follows that  $x - x_0 \nmid s(x)$  and thus  $s(x_0) \neq 0$ . Hence,  $\alpha(x_0) = a_p s^p(x_0) \neq 0$ , contradicting that  $\alpha(x_0) = 0$ . Hence, we have proved that  $t(x_0) \neq 0$ . Then we have

$$f\left(\frac{s(x_0)}{t(x_0)}\right) = \frac{\alpha(x_0)}{t^p(x_0)} = 0 \quad g\left(\frac{s(x_0)}{t(x_0)}\right) = \frac{\beta(x_0)}{t^q(x_0)} = 0$$

which implies that  $z - \frac{s(x_0)}{t(x_0)}$  is a common divisor of  $f(z)$  and  $g(z)$ , contradicting  $\gcd(f(z), g(z)) = 1$ . ■

*Proof of Lemma 6:* Note that if we substitute  $\mathbb{F}$  with  $\mathbb{F}(\mathbf{y}_i)$  and  $\gcd$  with  $\gcd_1$  in Lemma 11, the lemma also holds. Apparently,  $f(z), g(z) \in \mathbb{F}(\mathbf{y}_i)[z]$ . We will prove that  $\gcd_1(f(z), g(z)) = 1$ . By contradiction, assume  $r(z) = \gcd_1(f(z), g(z)) \in \mathbb{F}(\mathbf{y}_i)[z]$  is non-trivial. Let  $\bar{f}(z) = \frac{f(z)}{r(z)}$  and  $\bar{g}(z) = \frac{g(z)}{r(z)}$ . Clearly,  $\bar{f}(z)$  and  $\bar{g}(z)$  are both non-zero polynomials in  $\mathbb{F}(\mathbf{y}_i)[z]$ . Then we can find an assignment to

$\mathbf{y}_i$ , denoted by  $\mathbf{y}_i^*$ , such that the coefficients of the maximum powers of  $z$  in  $r(z)$ ,  $\bar{f}(z)$  and  $\bar{g}(z)$  are all non-zeros. Let  $\bar{r}(z)$  denote the univariate polynomial acquired by assigning  $\mathbf{y}_i = \mathbf{y}_i^*$  to  $r(z)$ . Clearly,  $\bar{r}(z)$  is a common divisor of  $f(z)$  and  $g(z)$  in  $\mathbb{F}[z]$ , contradicting  $\gcd(f(z), g(z)) = 1$ . Moreover, due to  $\gcd(s(\mathbf{y}), t(\mathbf{y})) = 1$  and Theorem 5,  $\gcd_1(s(y_i), t(y_i)) = 1$ . Thus, by Lemma 11,  $\gcd_1(\alpha(y_i), \beta(y_i)) = 1$ . Since  $i$  can be any integer in  $\{1, 2, \dots, k\}$ , it follows that  $\gcd(\alpha(\mathbf{y}), \beta(\mathbf{y})) = 1$  by Theorem 5. ■

## REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. Yeung, "Network information flow," *IEEE Trans. on Inf. Th.*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [2] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. on Net.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
- [3] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. on Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.
- [4] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proc. of ACM-SIAM SODA*, 2004.
- [5] D. Traskov, N. Ratnakar, D. S. Lun, R. Koetter, and M. Médard, "Network coding for multiple unicasts: An approach based on linear optimization," in *Proc. of IEEE ISIT*, 2006.
- [6] M. Kim, M. Médard, U.-M. O'Reilly, and D. Traskov, "An evolutionary approach to inter-session network coding," in *Proc. of INFOCOM*, 2009.
- [7] M. Médard, M. Effros, D. Karger, and T. Ho, "On coding for non-multicast networks," in *Proc. of Allerton Conference*, 2003.
- [8] N. J. A. Harvey, R. Kleinberg, and A. R. Lehman, "On the capacity of information networks," *Special of the IEEE ToIT and IEEE/ACM ToN*, vol. 52, no. 6, pp. 2345–2364, June 2006.
- [9] A. Das, S. Vishwanath, S. Jafar, and A. Markopoulou, "Network coding for multiple unicasts: An interference alignment approach," in *Proc. of IEEE ISIT*, 2010.
- [10] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the k-user interference channel," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3425–3441, 2008.
- [11] A. Ramakrishnan, A. Das, H. Maleki, A. Markopoulou, S. Jafar, and S. Vishwanath, "Network coding for three unicast sessions: Interference alignment approaches," in *Allerton Conference*, Sept. 2010.
- [12] J. Han, C. C. Wang, and N. B. Shroff, "Analysis of precoding-based intersession network coding and the corresponding 3-unicast interference alignment scheme," in *Proc. of Allerton Conference*, 2011.