Precoding-Based Network Alignment
For Three Unicast Sessions

Chun Meng, Student Member, IEEE, Abhik Kumar Das, Student Member, IEEE,
Abinesh Ramakrishnan, Student Member, IEEE, Syed Ali Jafar, Senior Member, IEEE,
Athina Markopoulou, Senior Member, IEEE, and Sriram Vishwanath, Senior Member, IEEE.

Abstract—We consider the problem of network coding across three unicast sessions over a directed acyclic graph, where each sender and the receiver is connected to the network via a single edge of unit capacity. We adapt a precoding-based interference alignment technique, originally developed for the wireless interference channel, to find a solution to this scenario, and we refer to our scheme constructed this way as precoding-based network alignment (PBNA). Similarly to the wireless setting, PBNA asymptotically achieves one half rate for each unicast session. A primary difference between this setting and a wireless one is that the network topology can introduce dependencies between elements of the transfer matrix, which we refer to as coupling relations, and can potentially make PBNA infeasible. We characterize the classes of networks for which PBNA is feasible, by identifying the minimal set of (three) coupling relations. We also interpret these coupling relations in terms of network topology and present a polynomial-time algorithm to check the feasibility of PBNA. Finally, we show that, for the class of networks considered, the optimal symmetric rate achieved by precoding-based linear scheme can take only three possible values and, when feasible, PBNA is also optimal.

Index Terms—network coding, multiple unicasts, interference alignment.

I. INTRODUCTION

Ever since the development of network coding and its success in characterizing the achievable throughput for single multicast scenario [1] [2], there has been hope that the framework can be extended to characterize network capacity in other scenarios, namely inter-session network coding. Of particular practical interest is network coding across multiple unicast sessions, as unicast is the dominant type of traffic in today’s networks. There have been some successes in this domain, such as the derivation of a sufficient condition for linear network coding to achieve the maximal throughput, in networks with multiple unicast sessions [3] [4]. However, scalar or even vector linear network coding [5] [6] [7] alone has been shown to be insufficient for achieving the limits of inter-session network coding [8].

In this paper, we consider the problem of linear network coding across three unicast sessions over an arbitrary network represented by a directed acyclic graph (DAG). We further restrict our focus to the scenario where the sender and the receiver of each unicast session are both connected to the network via a single edge of unit capacity, and refer to it as the Single-Input Single-Output scenario or SISO scenario for short (Fig. 1a). From the point of view of each unicast session, the network, whose nodes perform linear network coding, has the effect of a linear transfer function [3] [9]; other unicast sessions cause interference that affect the achievable rate for the unicast session of interest. The algebraic network coding framework [3] provided a sufficient condition for interference-free transmission in a network with multiple unicast sessions, which, however, can prove to be highly restrictive and linear network code design for guaranteeing rates for multiple unicasts is known to be NP-hard [10]. Only sub-optimal and heuristic methods are known today, including methods based on linear optimization [11] [12] and evolutionary approaches [13].

Differently from the interference-free framework [3], we allow the existence of interference at the receivers and we propose an interference-alignment approach. Our approach is motivated by the observation that under the linear network coding framework, a SISO scenario essentially mimics the wireless interference channel. As shown in Fig. 1b, the entire network can be viewed as a channel with a linear transfer function, albeit this function is no longer given by nature, as it is the case in wireless, but is determined by the network topology, routing and coding coefficients. This analogy enables us to apply the technique of precoding-based interference alignment.

1Considering three unicast sessions and SISO is the smallest, yet highly non-trivial, instance of the problem. Furthermore, we restrict our approach to precoding-based techniques while the middle of the network performs random network coding. Apart from being of interest on its own right, we hope that this can be used as a building block and for better understanding of the general network coding problem across multiple unicasts.
alignment, designed by Cadambe and Jafar [14] for wireless interference channels. We adapt this technique to our problem and we refer to it as precoding-based network alignment, or PBNA for short: Precoding occurs only at source nodes while all nodes in the middle of the network perform random network coding. One advantage of PBNA is complexity: it significantly simplifies network code design since the nodes in the middle of the network perform random network coding. Another advantage is that, unlike heuristic approaches, PBNA guarantees to each unicast session, asymptotic rate equal to one half of the minimum cut (in the information-theoretic sense [13]) between the sender and corresponding receiver. This rate is higher than one third of the min-cut, which can be achieved through time-sharing (i.e., the three unicast sessions taking turns transmitting); it is also optimal in networks where PBNA is feasible.

Indeed, an important difference between the SISO scenario and the wireless interference channel is that there may be algebraic dependencies (which we refer to as coupling relations) between elements of the transfer matrix (which we refer to as transfer functions). These are introduced by the network topology and make PBNA infeasible in some networks [16]. Such algebraic dependencies are not present in the wireless interference channel, where channel gains are independent from each other, thus making the precoding-based interference alignment scheme of [14] feasible almost surely. Another difference is that while channel gains in the wireless interference channel come from the real or complex field, network coding is performed over finite fields. Therefore, traditional interference alignment techniques, developed for the wireless interference channel, cannot be directly applied to DAGs with network coding but (i) they need to be properly adapted in the new setting and (ii) their feasibility needs to be characterized in terms of the network topology. Towards the second goal, we identify graph-related properties of the transfer functions, which together with a degree-counting technique, enable us to identify the minimal set of conditions for the feasibility of PBNA.

Our main contributions in this paper are the following:

- **PBNA Design**: We design the first precoding-based interference-alignment scheme for three unicast sessions over a DAG where intermediate nodes perform random network coding. The scheme is inspired by the Cadambe and Jafar scheme in [14] and asymptotically achieves a rate of half the min-cut for every unicast session.
- **Feasibility Conditions**: We identify the minimal set of coupling relations between network transfer functions, the presence of which makes PBNA infeasible. We further interpret these coupling relations in terms of network topology. We finally present a polynomial-time algorithm for checking the feasibility of PBNA, given the network topology and unicast sessions.
- **Rate Optimality**: We show that for any SISO scenario with non-zero channel coefficients, there are only three possible symmetric rates achievable by any precoding-based linear scheme (namely 1/3, 2/5 and 1/2), depending on the network topology. In the last case, PBNA is feasible and optimal, i.e., it achieves rate 1/2 per session.

The rest of the paper is organized as follows. In Section II, we review related work. In Section III, we present the problem setup and formulation. In Section IV, we present our proposed precoding-based interference alignment (PBNA) scheme for the network setting. In Section V, we present an overview of our main results. In Section VI, we discuss in depth the feasibility conditions of PBNA. In Section VII, we provide a polynomial-time algorithm to check the feasibility of PBNA. In Section VIII, we prove the optimal symmetric rates achieved by any linear precoding-based scheme. Section IX concludes the paper and outlines future directions.

II. RELATED WORK

A. Network Coding

Network coding was first proposed to achieve optimal throughput for single multicast scenario [1] [2] [3]. In contrast, for inter-session network coding, which includes the practical case of multiple unicasts, there have been only limited progresses. It is known that there exist networks in which network coding significantly outperforms routing schemes in terms of transmission rate [4]. However, there exist only approximation methods to characterize the rate region for this setting [6]. Moreover, it is known that finding linear network codes for this setting is NP-hard [10]. Therefore, only sub-optimal and heuristic methods exist to construct linear network code for this setting. For example, Ratnakar et al. [11] consider coding pairs of flows using poison-antidote butterfly structures and packing a network using these butterflies to improve throughput; Drskov et al. [12] further present a linear programming-based method to find butterfly structures in the network; Ho et al. [23] develop online and offline back pressure algorithms for finding approximately throughput-optimal network codes within the class of network codes restricted to XOR coding between pairs of flows; Effros et al. [22] described a tiling approach for designing network codes for wireless networks with multiple unicast sessions on a triangular lattice; Kim et al. [13] present an evolutionary approach to construct linear code. Unfortunately, most of these approaches don’t provide any guarantee in terms of performance. Moreover, most of these approaches are concerned about finding network codes by jointly considering code assignment and network topology at the same time. In contrast, our approach is oblivious to network topology in the sense that the design of encoding/decoding schemes is separated from network topology, and is predetermined regardless of network topology. The separation of code design from network topology greatly simplifies the code design of PBNA.

The part of our work that connects the algebraic feasibility conditions to network structure is related to some recent work
on network coding. Ebrahimi and Fragouli [23] found that the structure of a network polynomial, which is the product of the determinants of all transfer matrices, can be described in terms of certain subgraph structures; Weifei et al. [24] proposed the Edge-Reduction Lemma which makes connections between cut sets and the row and column spans of the transfer matrices.

B. Interference Alignment

The original concept of precoding-based interference alignment was first proposed by Cadambe and Jafar [14] to achieve the optimal degree of freedom (DoF) for K-user wireless interference channel. After that, various approaches to interference alignment have been proposed. For example, Nazer et al. proposed ergodic interference alignment [25]; Bresler, Parekh and Tse proposed lattice alignment [26]; Jafar introduced blind alignment [27] for the scenarios where the actual channel coefficient values are entirely unknown to the transmitters; Maddah-Ali and Tse proposed retrospective interference alignment [28] which exploits only delayed CSIT. Interference alignment has been applied to a wide variety of scenarios, including K-user wireless interference channel [14], compound broad channel [29], cellular networks [30], relay networks [31], and wireless networks supported by a wired backbone [32]. Recently, it was shown that interference alignment can be used to achieve exact repair in distributed storage systems [33, 34].

C. Network Alignment

Our work present an application of interference alignment to network coding for multiple unicasts by adapting the asymptotic precoding-based scheme of Cadambe and Jafar [14], originally developed for the wireless interference channel [35]. We also provided an algebraic formulation of feasibility conditions for PBNA for three unicast sessions. However, since the conditions proposed in [35] contain infinite number of conditions, it is difficult to check these conditions in practice.

In the follow-up work by Ramakrishnan et al. [16], we observe that the feasibility of PBNA depends on network topology and we conjectured that the (infinitely many) feasibility conditions in [35] can be simplified to just six conditions. Han et al. [36] stated that the conjecture is true for the simple case of three symbol extensions. They showed that three of the algebraic conditions are not possible due to the network structure and they provided graph interpretations of the two remaining conditions.

However, it emerged that the conjecture in [16] is incorrect, as observed independently both by us [37, 38] and by Han et al. [39]. There are three additional conditions which must be satisfied for PBNA to be feasible (See the Main Theorem of Section V). In our subsequent work, we reduce the infinite many conditions in [35] to the minimal set of nine conditions [37]. Using two graph-related properties, an algebraic degree-counting technique, and one of the results in [36] (namely the elimination of the three algebraic conditions mentioned above), we are able to identify the minimal set of coupling relations that are realizable in networks [37]. In the same paper, we also provided an interpretation of the six conditions in terms of graph structure, and an example of interpretation of the third condition (see Fig. 3(b) in this paper). In the technical report [38], we provide a full interpretation of all conditions in terms of graph structure. At the same time and independently, a technical report by Han et al [39] also provide a similar characterization.

This paper combines all our previous papers in this thread, namely [16, 35, 37, 38] and extends them by finding the optimal rates of precoding-based schemes. Compared to the most closely related work, namely [39], our work addresses a more general setting: (i) It enables the use of any precoding matrix, not only the one considered in Cadambe and Jafar [14] and (ii) it applies to all network topologies, which subsume the cases considered in [39]. In addition, in this paper, we prove that in networks where PBNA is feasible, it is also the optimal symmetric rate achieved by precoding-based schemes.

III. Problem Formulation

The network is represented by a directed acyclic graph $G = (V, E)$, where $V$ is the set of nodes and $E$ the set of edges. We consider the simplest non-trivial communication scenario where there are three unicast sessions coexisting in the network. The $i$th ($i = 1, 2, 3$) unicast session is represented by a tuple $\omega_i = (s_i, d_i, X_i)$, where $s_i$ and $d_i$ are the sender and the receiver of the $i$th unicast session, respectively; $X_i = (X_1^i, X_2^i, \ldots, X_n^i)$ is a vector of random variables, each of which represents a packet that $s_i$ sends to $d_i$. Each sender node $s_i$ is connected to the network via a single edge $\sigma_i$, called a sender edge, and each receiver node $d_i$ via a single edge $\tau_i$, called a receiver edge. We group these unicast sessions into a set $\Omega = \{\omega_1, \omega_2, \omega_3\}$, and refer to it as a single-input and single-output communication scenario, or a SISO scenario for short. An example of SISO scenario is shown in Fig. 1a. Clearly, in a SISO scenario, each sender node can transmit at most one symbol to its corresponding receiver node in a time slot.

Given an edge $e = (u, v) \in E$, let $u = $ head$(e)$ and $v = $ tail$(e)$ denote the head and the tail of $e$, respectively. Given a node $v \in V$, let $In(v) = \{e \in E : head(e) = v\}$ denote the set of incoming edges at $v$, and Out$(v) = \{e \in E : tail(e) = v\}$ the set of outgoing edges at $v$. Given two distinct edges $e, e' \in E$, a directed path from $e$ to $e'$ is a subset of edges $P = \{e_1, e_2, \ldots, e_k\}$ such that $e_1 = e, e_k = e'$, and head$(e_i) = $ tail$(e_{i+1})$ for $i \in \{1, 2, \ldots, k - 1\}$. The set of directed paths from $e$ to $e'$ is denoted by $P_{e,e'}$. For $i, j \in \{1, 2, 3\}$, we also use $P_{i,j}$ to represent $P_{\sigma_i, \tau_j}$.

We make the following simplifying assumptions:

1) The random variables transmitted in the network all take values from a finite field $\mathbb{F}_{2^m}$.
2) Each edge has unit capacity, i.e., can transmit one symbol of $\mathbb{F}_{2^m}$ in a time slot, and represents an error-free and delay-free channel.
3) Except for the sender nodes and the receiver nodes, all other nodes in the network have zero memory, and therefore cannot store any received data.
4) The sender nodes have no incoming edges, and the receiver nodes have no outgoing edges.
5) The random variables in all \( X_i \)'s are mutually independent. Each element of \( X_i \) has an entropy rate of \( m \) bits.
6) The transmissions within the network are all synchronized with respect to the symbol timing.

Each node in the network performs scalar linear network coding operations on the incoming symbols [2][3]. Let \( \hat{X}_e \) be the symbol injected at the sender node \( s_i \). Thus, for an edge \( e = (u, v) \in E \), the symbol transmitted along \( e \), denoted by \( Y_e \), is a linear combination of the incoming symbols at \( u \):

\[
Y_e = \begin{cases} 
\hat{X}_i & \text{if } e = \sigma_i; \\
\sum_{e' \in \text{In}(u)} x_{e'e} Y_{e'} & \text{otherwise.} 
\end{cases}
\]

where \( x_{e'e} \) denotes the coding coefficient that is used to combine the incoming symbol \( Y_{e'} \) into \( Y_e \). Following the algebraic framework of [3], we treat the coding coefficients as variables. Let \( x \) denote the vector consisting of all the coding coefficients in the network, i.e., \( x = (x_{e'e} : e' \in E, \text{head}(e') = \text{tail}(e)) \).

Due to the linear operations at each node, the network functions like a linear system such that the received symbol at \( \tau_i \) is a linear combination of the symbols injected at sender nodes:

\[
Y_{\tau_i} = m_{1i}(x) \hat{X}_i + m_{2i}(x) \hat{X}_2 + m_{3i}(x) \hat{X}_3
\]

In the above formula, \( m_{ji}(x) \) (\( j = 1, 2, 3 \)) is a multivariate polynomial in the ring \( \mathbb{F}_2[x] \), and is defined as follows [3]:

\[
m_{ji}(x) = \sum_{P \in P_{ji}} t_P(x)
\]

Each \( t_P(x) \) denotes a monomial in \( m_{ji}(x) \), and is the product of all the coding coefficients along path \( P \), i.e., for a given path \( P = \{e_1, e_2, \ldots, e_k\} \),

\[
t_P(x) = \prod_{i=1}^{k-1} x_{e_i e_{i+1}}
\]

Thus, \( t_P(x) \) represents the signal gain along a path \( P \), and \( m_{ji}(x) \) is simply the summation of the signal gains along all possible paths from \( \sigma_j \) to \( \tau_i \). We refer to \( m_{ji}(x) \) as the transfer function from \( \sigma_j \) to \( \tau_i \).

Each sender node \( s_i \) also performs linear network coding on the data \( X_i \) that is to be transmitted:

\[
\hat{X}_i = V_i X_i
\]

where \( V_i \) is an \( N \times k_i \) matrix defined on \( \mathbb{F}_{2^m} \), and is called the precoding matrix at \( s_i \). Both \( N \) and \( k_i \) are predetermined positive integers that are part of the transmission scheme.

In the next section, we will show how to set these two numbers. The symbols in \( X_i \) are then transmitted to the corresponding receivers through the network in \( N \) time slots. Let \( x^t \) denote the vector of coding coefficients for the time slot \( t \). In general, the precoding matrices may also contain indeterminate variables. Let \( \xi \) denote the vector consisting of all the variables in \( x^1, \ldots, x^N \), and the precoding matrices.

For an edge \( e \), let \( Y^t_e \) denote the symbol transmitted along \( e \) during time slot \( t \), and \( Y_e = (Y^1_e, Y^2_e, \ldots, Y^N_e)^T \) the vector of all the symbols transmitted along \( e \) during the \( N \) time slots.

Define the following \( N \times N \) diagonal matrix which includes all the transfer functions \( m_{ji}(x^t) \) for the \( N \) time slots:

\[
M_{ji} = \begin{pmatrix}
m_{ji}(x^1) & 0 & \cdots & 0 \\ 0 & m_{ji}(x^2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m_{ji}(x^N)
\end{pmatrix}
\]

Hence, the input-output equation of the network can be formulated in a matrix form as follows:

\[
Y_{\tau_i} = M_{1i} \hat{X}_1 + M_{2i} \hat{X}_2 + M_{3i} \hat{X}_3
\]

\[
= M_{1i} V_1 X_1 + M_{2i} V_2 X_2 + M_{3i} V_3 X_3
\]

\[
= M_i X
\]

where \( M_i = (M_{1i} V_1, M_{2i} V_2, M_{3i} V_3) \) and \( X = ((X_1)^T, (X_2)^T, (X_3)^T)^T \). Note that under the algebraic framework, \( M_i \) is a matrix defined on the field of rational functions \( \mathbb{F}_{2^m}(\xi) \). Given a network \( G \), and a SISO scenario \( \Omega \), we define \( (G, \Omega) \) as a network coding problem. Before proceeding, we introduce a simplified version of Schwartz-Zippel Lemma.

**Lemma IIII.** Let \( f(x_1, x_2, \cdots, x_n) \) be a non-zero polynomial in the polynomial ring \( \mathbb{F}[x_1, x_2, \cdots, x_n] \), where \( \mathbb{F} \) is a field. If \( |\mathbb{F}| \) is greater than the degree of \( p \) in every variable \( x_j \), there exists \( r_1, r_2, \cdots, r_n \in \mathbb{F} \) such that \( p(r_1, r_2, \cdots, r_n) \neq 0 \).

In this paper, we will consider the following method to construct a linear network code. At each source node, we use a precoding matrix to encode the data to be transmitted; and in the middle of the network, we use random linear network coding [19] to find an assignment of values to the variables in \( \xi \) in a suitable field \( \mathbb{F}_{2^m} \) such that each receiver node \( d_i \) can decode \( X_i \) from the received symbols, as formulated in Eq. (7). Specifically, if for each \( i = 1, 2, 3 \), there exists a matrix \( D_i \) on \( \mathbb{F}_{2^m}(\xi) \) such that \( X_i \) is a sub-vector of \( D_i M_i X \), we say that the network coding problem \( (G, \Omega) \) is solvable through precoding-based schemes. Due to Lemma [III], if \( (G, \Omega) \) is solvable through precoding-based schemes, for sufficiently large field \( \mathbb{F}_{2^m} \), we can use random network coding to find an assignment of values to \( \xi \), say \( \xi_0 \), such that \( X_i \) is a sub-vector of \( D_i M_i X \) under the assignment \( \xi = \xi_0 \). We call the tuple \( \lambda = (\xi_0, V_i, D_i : i = 1, 2, 3) \), where all the variables has been assigned values \( \xi_0 \), a precoding-based solution to the network coding problem \( (G, \Omega) \).

Note that the above framework is different from the interference-free framework defined in [3], where all the interfering signals must be cancelled out via suitable choice of \( \xi \). In the above definition, we allow the existence of interfering signals in the decoded data \( D_i M_i X \). As shown in the next section, by adopting a precoding-based approach, in which all coding happens at the source nodes, and intermediate nodes perform simply random network coding, this framework greatly simplifies the network code design problem.

**IV. Applying Precoding-Based Network Alignment to Networks**

In this section, we first present how to utilize precoding-based interference alignment technique to find a solution to
Fig. 2. Applying precoding-based interference alignment to the network setting: At each sender edge \( \sigma_i \) (\( i = 1, 2, 3 \)), the input vector \( \mathbf{X}_i \) is first encoded into \( 2n + 1 \) symbols through the precoding matrix \( \mathbf{V}_i \); then the encoded symbols are transmitted through the network in \( 2n + 1 \) time slots; at each receiver edge \( \tau_i \), the undesired symbols are aligned into a single linear space, which is linearly independent from the linear space spanned by the desired signals, such that the receiver can decode all the desired symbols.

the network coding problem \((\mathcal{G}, \Omega)\). Then, we propose an algebraic formulation to describe the feasibility conditions of our approach in a concise form. This formulation allows us to link the feasibility conditions to the underlying network topology. We then introduce the concept of “coupling relations,” and show that these relations are essential in determining the feasibility of our approach.

A. Precoding-Based Network Alignment Scheme

In this section, we present how to apply interference alignment to networks to find a solution to the network coding problem \((\mathcal{G}, \Omega)\) such that each unicast session can achieve a transmission rate close to 1/2. The basic idea is that under linear network coding, the network behaves like a wireless interference channel, which is shown below:

\[
U_i = H_j W_1 + H_2 W_2 + H_3 W_3 + N_i \quad i = 1, 2, 3
\]

(8)

where \( W_j, H_{ji}, U_i, \text{ and } N_i \) (\( j = 1, 2, 3 \)) are all complex numbers, representing the transmitted signal at sender \( j \), the channel gain from sender \( j \) to receiver \( i \), the received signal at receiver \( j \), and the noise term respectively. As we can see from Eq. (2), in a network equipped with linear network coding, \( X_j \)'s (\( j \neq i \)) play the roles of interfering signals, and transfer functions the roles of channel gains. This analogy enables us to borrow some techniques, such as precoding-based interference alignment, which is originally developed for the wireless interference channel, to the network setting.

We assume all \( m_{ij}(x) \)'s (\( i, j = 1, 2, 3 \)) are non-zeros. The case where some \( m_{ij}(x) \)'s (\( i \neq j \)) are zeros can be dealt with similarly, and is deferred to Section [14]. Let \( n \) be a positive integer. We set \( N = 2n + 1 \), \( k_1 = n + 1 \), and \( k_2 = k_3 = n \), and thus \( V_1 \) is \((2n+1) \times (n+1)\) matrix, and both \( V_2 \) and \( V_3 \) are \((2n+1) \times n\) matrices. We require the following conditions are satisfied [14]:

\[
\begin{align*}
\mathcal{A}_1 & : \text{span}(M_{21} V_2) = \text{span}(M_{31} V_3) \\
\mathcal{A}_2 & : \text{span}(M_{32} V_3) \subseteq \text{span}(M_{12} V_1) \\
\mathcal{A}_3 & : \text{span}(M_{23} V_3) \subseteq \text{span}(M_{13} V_1) \\
\mathcal{B}_1 & : \text{rank}(M_{12} V_1 \ M_{21} V_2) = 2n + 1
\end{align*}
\]

2The wireless interference channel that we consider here has only one sub-channel.

In the above conditions, for a matrix \( E \), we use \( \text{span}(E) \) to denote the linear space spanned by the column vectors contained in \( E \). \( \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3 \) are called the alignment conditions and \( \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \) the rank conditions. Basically, each alignment condition guarantees that the undesired symbols or interferences at each receiver are mapped into a single linear space, such that the dimension of received symbols or the number of unknowns is decreased. Moreover, each rank condition guarantees that the linear space spanned by the interferences is linearly independent from that spanned by the desired symbols, and thus each receiver can decode the desired symbols from the received symbols. In Fig. 2, we show a graphical illustration of these conditions. Clearly, when all these conditions are satisfied, the network coding problem \((\mathcal{G}, \Omega)\) is solvable through precoding-based schemes.

In order to find a solution to \((\mathcal{G}, \Omega)\), we choose a sufficiently large field \( \mathbb{F}_{2^m} \). We then apply random network coding [19] to find an assignment of values to \( \xi \) such that these conditions are all satisfied with high probability. Let \( \lambda_{na} \) denote a solution to \((\mathcal{G}, \Omega)\). It can be easily seen that the three unicast sessions can achieve a rate vector \( R_n \) \( \overset{\triangle}{=} \left( \frac{n}{2(n+1)}, \frac{n}{2(n+1)}, \frac{n}{2(n+1)} \right) \) via the solution \( \lambda_{na} \), which approaches \(( \frac{n}{2}, \frac{n}{2}, \frac{n}{2} \)) as \( n \to \infty \). We call a solution constructed in this way as a precoding-based network alignment scheme or a PBNA scheme for short. If there exists a PBNA scheme \( \lambda_{na} \) for \((\mathcal{G}, \Omega)\), we also say that \( R_n \) is feasible through PBNA.

B. Algebraic Formulation of the Feasibility Conditions

We can further simply the alignment conditions and rank conditions as follows. First, we reformulate \( \mathcal{A}_1 \sim \mathcal{A}_3 \) as follows:

\[
\begin{align*}
\mathcal{A}_1' & : M_{21} V_2 = M_{31} V_3 \ A \\
\mathcal{A}_2' & : M_{32} V_3 = M_{12} V_1 \ B \\
\mathcal{A}_3' & : M_{23} V_2 = M_{13} V_1 \ C
\end{align*}
\]

where \( A \) is an \( n \times n \) invertible matrix, and \( B, C \) are both \((n+1) \times n\) matrices with rank \( n \). A direct consequence of \( \mathcal{A}_2' \) and \( \mathcal{A}_3' \) is that the precoding matrices are not independent from each other. Both \( V_2 \) and \( V_3 \) are determined by \( V_1 \) through the following equations:

\[
V_2 = M_{12} M_{23}^{-1} V_1 C \quad V_3 = M_{12} M_{32}^{-1} V_1 B \quad (9)
\]

Substituting the above equations into \( \mathcal{A}_1' \), the three alignment conditions can be further condensed into a single equation:

\[
TV_1 C = V_1 BA \quad (10)
\]

where \( T = M_{13} M_{23} M_{32} M_{12}^{-1} M_{23}^{-1} M_{31}^{-1} \). Eq. (10) suggests that alignment conditions introduce self-constraint on \( V_1 \). Thus, in general, we cannot choose \( V_1 \) freely. Indeed, Eq. (10) is also the major restriction on \( V_1 \). Finally, using Eq. (9) and Eq. (10), the rank conditions are transformed into the
following equivalent equations:

\begin{align*}
\mathcal{B}_1 : & \quad \text{rank}(V_1 P_1 V_1 C) = 2n + 1 \\
\mathcal{B}_2 : & \quad \text{rank}(V_1 P_2 V_1 C) = 2n + 1 \\
\mathcal{B}_3 : & \quad \text{rank}(V_1 P_3 V_1 C A^{-1}) = 2n + 1
\end{align*}

where \( P_1 = M_{11} M_{22} M_{12}^{-1} M_{23}^{-1} \), \( P_2 = M_{11} M_{22} M_{12}^{-1} M_{13}^{-1} \), and \( P_3 = M_{11} M_{33} M_{13}^{-1} M_{32}^{-1} \). Thus, we have simplified the feasibility conditions into four equations, i.e., Eq. (10) and \( \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \). Note that all these equations are formulated in terms of \( V_1 \) and \( P_i \). We summarize this result into the following lemma:

**Lemma IV.1.** Assume all \( m_{ij}(x) \)'s \((i, j = 1, 2, 3)\) are non-zero. \( R_n \) is feasible through PBNA if and only if 1) Eq. (10) is satisfied, and 2) \( \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \) are satisfied.

We further define the following functions:

\[
\begin{align*}
p_1(x) &= \frac{m_{11}(x)m_{22}(x)}{m_{11}(x)m_{22}(x)} \\
p_2(x) &= \frac{m_{11}(x)m_{32}(x)}{m_{11}(x)m_{22}(x)} \\
p_3(x) &= \frac{m_{11}(x)m_{23}(x)m_{32}(x)}{m_{23}(x)m_{32}(x)} \\
\eta(x) &= \frac{m_{11}(x)m_{22}(x)m_{32}(x)}{m_{23}(x)m_{31}(x)}
\end{align*}
\]

Clearly, \( p_1(x) \) and \( \eta(x) \) form the elements along the diagonals of \( P_i \) and \( T \) respectively.

Next, we reformulate the feasibility conditions in terms of \( p_1(x) \) and \( \eta(x) \). To this end, we need to know the internal structure of \( V_1 \). We distinguish the following two cases:

**Case I:** \( \eta(x) \) is non-constant, and thus \( T \) is not an identity matrix. For this case, Eq. (10) becomes non-trivial, and we cannot choose \( V_1 \) freely. We use the following precoding matrices proposed by Cadambe and Jafar (14):

\[
\begin{align*}
V_1' &= (w T w \cdots T^n w) \\
V_2 &= M_{11} M_{22}^{-1} (w T w \cdots T^{n-1} w) \\
V_3 &= M_{12} M_{32}^{-1} (T w T^2 w \cdots T^n w)
\end{align*}
\]

where \( w \) is a column vector of \( 2n + 1 \) ones. It is straightforward to verify that the above precoding matrices satisfy the alignment conditions. Note that the above precoding matrices correspond to the configuration where \( A = I_n, C \) consists of the left \( n \) columns of \( I_{n+1} \), and \( B \) the right \( n \) columns of \( I_{n+1} \).

In order to reformulate the rank conditions, we consider the following matrix

\[
H = \begin{pmatrix}
f_1(y)^1 & f_2(y)^1 & \cdots & f_r(y)^1 \\
\vdots & \vdots & \ddots & \vdots \\
f_1(y)^r & f_2(y)^r & \cdots & f_r(y)^r
\end{pmatrix}
\]

where \( f_i(y) \) \((i = 1, 2, \cdots, r)\) is a rational function in \( \mathbb{F}_{2^m} \), and the \( j \)th row of \( H \) is simply a repetition of the vector \( (f_1(y), \cdots, f_r(y)) \), with \( y \) being replaced by \( y^j \). Due to the particular structure of \( H \), the problem of checking whether \( H \) is full rank can be simplified to checking whether \( f_1(y), \cdots, f_r(y) \) are linearly independent, as stated in the following lemma. Here, \( f_1(y), \cdots, f_r(y) \) are said to be linearly independent, if for any scalars \( a_1, \cdots, a_r \in \mathbb{F}_q \), which are not all zeros, \( a_1 f_1(y) + \cdots + a_r f_r(y) \neq 0 \).

**Lemma IV.2.** \( \det(H) \neq 0 \) if and only if \( f_1(y), \cdots, f_r(y) \) are linearly independent.

*Proof:* See Theorem 1 of [36].

An important observation is that using the precoding matrices defined in Eq. (12)-(14), all of the matrices involved in \( \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \) have the same form as \( H \). Specifically, each row of the matrix in \( \mathcal{B}_1 \) is of the form:

\[
(1 \eta(x) \cdots \eta(x)^{n-1}) p_1(x) \cdots p_1(x) \eta(x)^{n-1}(x)
\]

(15)

Hence, using Lemma IV.2, we can quickly derive:

**Lemma IV.3.** Assume all \( m_{ij}(x) \)'s \((i, j = 1, 2, 3)\) are non-zero, and \( \eta(x) \) is non-constant. \( R_n \) is feasible through PBNA if for each \( i = 1, 2, 3 \)

\[
p_1(x) \notin S_n = \left\{ \frac{f(g(x))}{g(g(x))} : f(z), g(z) \in \mathbb{F}_q[z], f(z)g(z) \neq 0, \gcd(f(z), g(z)) = 1, df \leq n, dg \leq n - 1 \right\}
\]

(16)

*Proof:* If Eq. (16) is satisfied, the rational functions in Eq. (15) are linearly independent. Therefore, due to Lemma IV.2 condition \( \mathcal{B}_1 \) is satisfied. Meanwhile, the precoding matrix \( V_1 \) defined in Eq. (12) satisfies Eq. (10). Hence, \( R_n \) is feasible through PBNA by Lemma IV.1.

Note that each rational function \( \frac{f(g(x))}{g(g(x))} \in S_n \) represents a constraint on \( p_1(x) \), i.e., \( p_1(x) \neq \frac{f(g(x))}{g(g(x))} \), the violation of which invalidates the use of the PBNA through the precoding matrices defined in Eq. (12)-(14). Also note that Eq. (16) only guarantees that PBNA is feasible for a fixed value of \( n \), i.e., each unicast session only achieves a transmission rate close to one half. In order for each unicast session to asymptotically achieve a transmission rate of one half, we simply combine the conditions of Lemma IV.3 for all possible values of \( n \), and get the following result:

**Theorem IV.1.** Assume all \( m_{ij}(x) \)'s \((i, j = 1, 2, 3)\) are non-zero, and \( \eta(x) \) is non-constant. The three unicast sessions can asymptotically achieve the rate tuple \((1/2, 1/2, 1/2)\) through PBNA if for each \( i = 1, 2, 3 \).

\[
p_1(x) \notin S' = \left\{ \frac{f(g(x))}{g(g(x))} : f(z), g(z) \in \mathbb{F}_q[z], f(z)g(z) \neq 0, \gcd(f(z), g(z)) = 1 \right\}
\]

(17)

*Proof:* If Eq. (17) is satisfied, \( R_n \) is feasible through PBNA for all possible values of \( n \). Thus, each unicast session can asymptotically achieve one half rate as \( n \to \infty \).

**Case II:** \( \eta(x) \) is constant, and thus \( T \) is an identity matrix. For this case, Eq. (10) becomes trivial. In fact, we set \( BA = C \), and hence Eq. (10) can be satisfied by any arbitrary \( V_1 \).

3Notation: For two polynomials \( f(x) \) and \( g(x) \), let \( \gcd(f(x), g(x)) \) denote their greatest common divisor, and \( df \) the degree of \( f(x) \).
Thus the conditions of Theorem IV.2 are violated. Moreover, let’s first consider start by illustrating that through examples of networks whose matrices correspond to the configuration where $A$ are linearly independent, and therefore Theorem IV.2. Assume all if for each $i$ zeros, and $\eta(x)$ is constant. $R_n$ is feasible through PBNA for any $n$. This example suggests that there exists significant redundancy in the feasibility conditions of Theorem IV.1, which is applicable for most networks.

One interesting observation is that not all coupling relations are realizable. For example, consider the coupling relation $p_1(x) = \eta^3(x)$, where both $p_1(x)$ and $\eta(x)$ are non-constants. Let $p_1(x) = \frac{u(x)}{v(x)}, \eta(x) = \frac{w(x)}{t(x)}$ denote the unique forms of $p_1(x)$ and $\eta(x)$ respectively. Consider a coding variable $x_{ee'}$ that appears in both $\frac{u(x)}{v(x)}$ and $\frac{w(x)}{t(x)}$. Because the maximum degree of each coding variable in a transfer function is at most one, according to Eq. (11), the maximum of the degrees of $x_{ee'}$ in $u(x)$ and $v(x)$ is at most two. However, it can be easily seen that the maximum of the degrees of $x_{ee'}$ in $s^3(x)$ and $t^3(x)$ is at least three. Therefore, it is impossible that $p_1(x) = \eta^3(x)$. This example suggests that there exists significant redundancy in the feasibility conditions of Theorem IV.1.

More formally, it raises the following important question:

\[ f(m_{ij1}(x), m_{ij2}(x), \cdots, m_{ijk}(x)) = 0 \] (22)

where $f(z_1, z_2, \cdots, z_k)$ is a polynomial in $\mathbb{F}_2^m [z_1, \cdots, z_k]$. We call such relation a coupling relation. As shown in Theorem IV.1, each rational function $f(\eta(x)) \in S'$ represents a coupling relation $p_1(x) = f(\eta(x))$. Given a coupling relation, if there are networks for which it holds, we say that it is realizable.

The existence of coupling relations greatly complicates the feasibility problem of PBNA. As shown previously, most of the coupling relations, such as $p_1(x) = 1$ and $p_1(x) = \frac{\eta(x)}{1+\eta(x)}$, are harmful to PBNA, because their presence violates the feasibility conditions. The only exception is $\eta(x) = 1$, which does help simplify the construction of precoding matrices, and thus is beneficial to PBNA. Indeed, as we will see in Section VII, this coupling relation allows interferences to be perfectly aligned at each receiver, and thus each unicast session can achieve one half rate in exactly two time slots. Unfortunately, as we will see in Section VII, this coupling relation requires that the network possesses particular structures, which are not present in most networks. For this reason, we will mainly focus on Theorem IV.1, which is applicable for most networks.

\[ \sigma_1 \quad \sigma_2 \quad \sigma_3 \]
\[ \tau_2 \quad \tau_1 \quad \tau_3 \quad \epsilon \]

Fig. 3. Examples of realizable coupling relations: The left network realizes the coupling relations $p_1(x) = \eta(x) = 1$ such that the conditions of Theorem IV.2 are violated; in the right network, $\eta(x) \neq 1$, but $p_1(x) = \frac{\eta(x)}{1+\eta(x)}$, which violates the conditions of Theorem IV.1. It can be easily verified that for this network, $\eta(x) \neq 1$, and $p_1(x) = \frac{\eta(x)}{1+\eta(x)}$. Thus the conditions of Theorem IV.1 are violated. Moreover, by exchanging $\sigma_1 \leftrightarrow \sigma_2$ and $\tau_1 \leftrightarrow \tau_2$, we obtain another example, where $p_2(x) = 1 + \eta(x)$, and thus the conditions of Theorem IV.1 are again violated. While the key feature of the first example can be easily identified, it is not obvious what are the defining features of the second example. Nevertheless, both examples demonstrate an important difference between networks and wireless interference channel: In networks, due to the internal structure of transfer functions, network topology might introduce dependence between different transfer functions, e.g., $p_1(x) = 1$ or $p_1(x) = \frac{\eta(x)}{1+\eta(x)}$; in contrast, in wireless channel, channel gains are algebraically independent almost surely such that precoding-based interference alignment is always feasible.

Note that the above dependence relations between transfer functions can be generalized to the following form:

\[ x_1(x) = x_2(x) = x_3(x) = 0 \] (22)

where $f(z_1, z_2, \cdots, z_k)$ is a polynomial in $\mathbb{F}_2^m [z_1, \cdots, z_k]$. We call such relation a coupling relation. As shown in Theorem IV.1, each rational function $f(\eta(x)) \in S'$ represents a coupling relation $p_1(x) = f(\eta(x))$. Given a coupling relation, if there are networks for which it holds, we say that it is realizable.

The existence of coupling relations greatly complicates the feasibility problem of PBNA. As shown previously, most of the coupling relations, such as $p_1(x) = 1$ and $p_1(x) = \frac{\eta(x)}{1+\eta(x)}$, are harmful to PBNA, because their presence violates the feasibility conditions. The only exception is $\eta(x) = 1$, which does help simplify the construction of precoding matrices, and thus is beneficial to PBNA. Indeed, as we will see in Section VII, this coupling relation allows interferences to be perfectly aligned at each receiver, and thus each unicast session can achieve one half rate in exactly two time slots. Unfortunately, as we will see in Section VII, this coupling relation requires that the network possesses particular structures, which are not present in most networks. For this reason, we will mainly focus on Theorem IV.1, which is applicable for most networks.

One interesting observation is that not all coupling relations are realizable. For example, consider the coupling relation $p_1(x) = \eta^3(x)$, where both $p_1(x)$ and $\eta(x)$ are non-constants. Let $p_1(x) = \frac{u(x)}{v(x)}, \eta(x) = \frac{w(x)}{t(x)}$ denote the unique forms of $p_1(x)$ and $\eta(x)$ respectively. Consider a coding variable $x_{ee'}$ that appears in both $\frac{u(x)}{v(x)}$ and $\frac{w(x)}{t(x)}$. Because the maximum degree of each coding variable in a transfer function is at most one, according to Eq. (11), the maximum of the degrees of $x_{ee'}$ in $u(x)$ and $v(x)$ is at most two. However, it can be easily seen that the maximum of the degrees of $x_{ee'}$ in $s^3(x)$ and $t^3(x)$ is at least three. Therefore, it is impossible that $p_1(x) = \eta^3(x)$. This example suggests that there exists significant redundancy in the feasibility conditions of Theorem IV.1.

More formally, it raises the following important question:

4For a non-zero rational function $h(y) \in \mathbb{F}_q(y)$, its unique form is defined as $h(y) = \frac{f(y)}{g(y)}$, where $f(y), g(y) \in \mathbb{F}_q[y]$ and $\gcd(f(y), g(y)) = 1$. 

C. Coupling Relations and Feasibility of PBNA

In the previous section, we reformulated the feasibility conditions in terms of the functions $p_1(x)$ and $\eta(x)$. One critical question is: What is the connection between the reformulated feasibility conditions and network topology? We start by illustrating that through examples of networks whose structure violates the feasibility conditions. Let’s first consider the network shown in Fig. 3a. Due to the bottleneck $e$, it can be easily verified that $p_1(x) = p_2(x) = p_3(x) = \eta(x) = 1$, and thus the conditions of Theorem IV.2 are violated. Moreover,
Q1: Which coupling relations \( p_i(x) = \frac{f(x)}{g(x)} \in S' \) are realizable?

The answer to this question allows us to reduce the set \( S' \) defined in Theorem \([V,1]\) to its minimal size. For \( i = 1, 2, 3 \), we define the following set, which represents the minimal set of coupling relations we need to consider:

\[
S'_i = \left\{ \frac{f(x)}{g(x)} \in S' : p_i(x) = \frac{f(x)}{g(x)} \text{ is realizable} \right\}
\]  

(23)

Then the next important question is:

Q2: Given \( p_i(x) = \frac{f(x)}{g(x)} \in S'_i \), what are the defining features of the networks for which this coupling relation holds?

As we will see in the rest of this paper, the answers to Q1 and Q2 both lie in a deeper understanding of the properties of transfer functions. Intuitively, because each transfer function is defined on a graph, it usually possesses special properties. The graph-related properties not only allow us to reduce \( S' \) to the minimal set \( S'_i \), but also enable us to identify the defining features of the networks that realize the coupling relations represented by \( S'_i \).

In the derivation of Theorem \([V,1]\), we only consider the precoding matrices defined in Eq. (12)-14. However, the choices of precoding matrices are not limited to these matrices. In fact, as we will see in Section [VI] given different \( A, B, \) and \( C \), we can derive different precoding matrix \( V_1 \) such that Eq. (10) is satisfied. This raises the following important question:

Q3: Assume some coupling relation \( p_i(x) = \frac{f(x)}{g(x)} \in S'_i \), is present in the network. Is it still possible to utilize PBNA via other precoding matrices instead of those defined in Eq. (12)-14?

As we will see in Section [VI] the answer to this question is negative. The basic idea is that each precoding matrix \( V_1 \) that satisfies Eq. (10) can be transformed into the precoding matrix in Eq. (12) through a transform equation \( V_1 = G^{-1}V_1F^{-1} \), where \( G \) is a diagonal matrix and \( F \) a full-rank matrix (See Lemma [VI,3]). Using this transform equation, we can prove that if the precoding matrices cannot be used due to the presence of a coupling relation, then any precoding matrices cannot be used.

V. OVERVIEW OF MAIN RESULTS

In this section, we state our main results. Proofs are deferred to Sections [VI] and [VIII] and Appendices.

A. Feasibility Conditions of PBNA

Since the construction of \( V_1 \) depends on whether \( \eta(x) \) is constant, we distinguish two cases.

1) \( \eta(x) \) Is Not Constant:

Theorem V.1 (The Main Theorem). Assume all \( m_{ij}(x) \)’s \((i, j = 1, 2, 3)\) are non-zeros, and \( \eta(x) \) is not constant. The three unicast sessions can asymptotically achieve the rate tuple \((\frac{1}{2}, \frac{1}{2}, \frac{1}{2})\) through PBNA if and only if the following conditions are satisfied:

\[
\begin{align*}
& m_{11}(x) \neq \frac{m_{13}(x)m_{21}(x)}{m_{23}(x)}, \frac{m_{12}(x)m_{31}(x)}{m_{32}(x)}, \\
& \quad \frac{m_{13}(x)m_{21}(x)}{m_{23}(x)} + \frac{m_{12}(x)m_{31}(x)}{m_{32}(x)} \quad (24) \\
& m_{22}(x) \neq \frac{m_{12}(x)m_{23}(x)}{m_{13}(x)}, \frac{m_{32}(x)m_{21}(x)}{m_{31}(x)} + \frac{m_{12}(x)m_{21}(x)}{m_{31}(x)} \quad (25) \\
& m_{33}(x) \neq \frac{m_{23}(x)m_{31}(x)}{m_{32}(x)}, \frac{m_{13}(x)m_{32}(x)}{m_{12}(x)} + \frac{m_{13}(x)m_{32}(x)}{m_{12}(x)} \quad (26)
\end{align*}
\]

Proof: See Appendix B

Note that in the Main Theorem, we have reduced the feasibility conditions of Theorem [VI] to its minimal size.

The conditions of the Main Theorem can be understood from the perspective of the interference channel. As shown in Section [V-A] under linear network coding, the network behaves as a 3-user wireless interference channel, where the channel coefficients \( m_{ij}(x) \) are all non-zeros. Let \( H \) denote the matrix with the \((i, j)\)-element being \( m_{ij}(x) \). It is easy to see that the first two inequalities in Eq. (27)-(29) can be rewritten as \( M_{kl}(H) \neq 0 \) for some \( k \neq l \), where \( M_{kl}(H) \) denotes the \((k, l)\)-Minor of \( H \). For example, \( m_{11}(x) \neq \frac{m_{13}(x)m_{21}(x)}{m_{33}(x)} \) is equivalent to \( M_{32}(H) \neq 0 \), and \( m_{11}(x) \neq \frac{m_{13}(x)m_{31}(x)}{m_{33}(x)} \) is equivalent to \( M_{32}(H) \neq 0 \). Suppose that there exists \( M_{kl}(H) = 0 \) for some \( k \neq l \). For such a channel, it is known that the sum-rate achieved by the three unicast sessions cannot be more than 1 in the information theoretical sense (see Lemma 1 of [40]), i.e., no precoding-based scheme, linear or non-linear, can achieve a rate beyond 1/3 per user. Therefore, given that channel coefficients are always non-zero, the condition \( M_{kl}(H) \neq 0 \) is information theoretically necessary for rate 1/2 feasibility. Hence, the first two inequalities of Eq. (27)-(29) are simply the information theoretic necessary conditions, so they must hold for any achievable precoding-based scheme. The third condition involves a sum of the first two, which is not information theoretically necessary, but is needed for the precoding-based scheme we utilize.

2) \( \eta(x) \) Is Constant: In this case, we can choose \( V_1 \) freely by setting \( BA = C \), and thus the feasibility conditions of PBNA are significantly simplified. Moreover, each unicast session can achieve one half rate in exactly two time slots, as stated in the following theorem:

Theorem V.2. Assume all \( m_{ij}(x) \)'s \((i, j = 1, 2, 3)\) are non-zeros, and \( \eta(x) \) is constant. The three unicast sessions can achieve the rate tuple \((\frac{1}{2}, \frac{1}{2}, \frac{1}{2})\) in exactly two time slots through PBNA if and only if the following conditions are satisfied:

\[
\begin{align*}
& m_{11}(x) \neq \frac{m_{13}(x)m_{21}(x)}{m_{23}(x)}, \frac{m_{12}(x)m_{31}(x)}{m_{32}(x)} \quad (27) \\
& m_{22}(x) \neq \frac{m_{12}(x)m_{23}(x)}{m_{13}(x)}, \frac{m_{32}(x)m_{21}(x)}{m_{31}(x)} \quad (28)
\end{align*}
\]

\(^3\)In the precoding-based scheme mentioned here, the encoding/decoding process at each sender/receiver might be linear or non-linear, but the operations at each internal node are linear.
Theorem V.3. \( \eta(x) = 1 \) if and only if \( \alpha_{213} = \alpha_{312} \) and \( \beta_{213} = \beta_{312} \).

In [36], the authors independently discovered a similar result. Consider the example shown in Fig. 3a. It is easy to see that in this example, \( \alpha_{213} = \alpha_{312} = \beta_{213} = \beta_{312} = e \), and thus \( \eta(x) = 1 \). In Fig. 3b, we show another example, where \( \alpha_{213} = \alpha_{312} = e_1, \beta_{213} = \beta_{312} = e_2 \), and thus \( \eta(x) = 1 \).

Given two subsets of edges, \( S \) and \( D \), a cut-set \( C \) between \( S \) and \( D \) is a subset of the edges, the removal of which will disconnect every directed path from \( S \) to \( D \). The capacity of cut-set \( C \) is defined as the summation of the capacities of the edges contained in \( C \). The minimum cut between \( S \) and \( D \) is the minimum capacity of all cut-sets between \( S \) and \( D \).

Theorem V.4. The following statements hold:

1) \( p_1(x) = 1 \) if and only if the minimum cut between \( \{\sigma_1, \sigma_2\} \) and \( \{\tau_1, \tau_3\} \) equals one; \( p_1(x) = \eta(x) \) if and only if the minimum cut between \( \{\sigma_1, \sigma_3\} \) and \( \{\tau_1, \tau_2\} \) equals one.

2) \( p_2(x) = 1 \) if and only if the minimum cut between \( \{\sigma_1, \sigma_2\} \) and \( \{\tau_2, \tau_3\} \) equals one; \( p_2(x) = \eta(x) \) if and only if the minimum cut between \( \{\sigma_2, \sigma_3\} \) and \( \{\tau_1, \tau_2\} \) equals one.

3) \( p_3(x) = 1 \) if and only if the minimum cut between \( \{\sigma_1, \sigma_3\} \) and \( \{\tau_2, \tau_3\} \) equals one; \( p_3(x) = \eta(x) \) if and only if the minimum cut between \( \{\sigma_1, \sigma_3\} \) and \( \{\tau_2, \tau_3\} \) equals one.

For instance, in Fig. 3a, the cut-set with minimum capacity between \( \{\sigma_2, \sigma_3\} \) and \( \{\tau_1, \tau_2\} \) contains only one edge \( e \), and thus \( p_2(x) = \eta(x) \).

Given two edges \( e_1 \) and \( e_2 \), we say that they are parallel with each other if there is no directed paths from \( e_1 \) to \( e_2 \), or from \( e_2 \) to \( e_1 \). As shown below, two edges are important in defining the networks that realizes the third coupling relation in Eq. (30)-(32), e.g., \( \alpha_{213} \) and \( \alpha_{312} \) are used to define the networks that realize \( p_1(x) = \frac{\eta(x)}{1+\eta(x)} \), and so on.

Theorem V.5. Assume \( \eta(x) \) is not constant. The following statements hold:

1) \( p_1(x) = \frac{\eta(x)}{1+\eta(x)} \) if and only if the following conditions are satisfied: a) \( \alpha_{312} \) is a bottleneck between \( \sigma_1 \) and \( \tau_2 \); b) \( \alpha_{213} \) is a bottleneck between \( \sigma_1 \) and \( \tau_3 \); c) \( \alpha_{312} \) is parallel with \( \alpha_{213} \); d) \( \{\alpha_{312}, \alpha_{213}\} \) forms a cut-set between \( \sigma_1 \) from \( \tau_1 \).

2) \( p_2(x) = 1 + \eta(x) \) if and only if the following conditions are satisfied: a) \( \alpha_{123} \) is a bottleneck between \( \sigma_2 \) and \( \tau_3 \); b) \( \alpha_{321} \) is a bottleneck between \( \sigma_2 \) and \( \tau_1 \); c) \( \alpha_{123} \) is parallel with \( \alpha_{321} \); d) \( \{\alpha_{123}, \alpha_{321}\} \) forms a cut-set between \( \sigma_2 \) from \( \tau_2 \).

3) \( p_3(x) = 1 + \eta(x) \) if and only if the following conditions are satisfied: a) \( \alpha_{231} \) is a bottleneck between \( \sigma_3 \) and \( \tau_1 \); b) \( \alpha_{132} \) is a bottleneck between \( \sigma_3 \) and \( \tau_2 \); c) \( \alpha_{231} \) is parallel with \( \alpha_{132} \); d) \( \{\alpha_{231}, \alpha_{132}\} \) forms a cut-set between \( \sigma_3 \) from \( \tau_3 \).

Consider the network as shown in Fig. 3b. It is easy to see that \( e_2 = \alpha_{312} \) and \( e_1 = \alpha_{213} \), and all the conditions in 1) of Theorem V.5 are satisfied. Therefore, this network realizes...
the coupling relation \( p_1(x) = \frac{\eta(x)}{1 + \eta(x)} \). Note that these three coupling relations are mutually exclusive when \( \eta(x) \) is not constant. If any two of these coupling relation were to occur in the same network, then it would induce a graph structure that forces \( \eta(x) \) to be a constant \(^{36}\).

C. Optimal Symmetric Linear Rates

For SISO networks with all non-zero channel coefficients considered in this paper, there are only three possible rates achievable through any precoding-based network coding schemes. We classify the networks based on the type of conditions they satisfy (or violate).

- **Type I**: Networks that fail to satisfy one or more of the six basic conditions: \( p_i(x) \neq 1 \) and \( p_i(x) \neq \eta(x) \) \( \forall i \in \{1, 2, 3\} \).
- **Type II**: Networks that satisfy the six basic conditions shown in **Type I**, but fail to satisfy one of the following three mutually exclusive conditions: \( p_1(x) \neq \frac{\eta(x)}{1 + \eta(x)} \), \( p_2(x) \neq 1 + \eta(x) \), and \( p_3(x) \neq 1 + \eta(x) \).
- **Type III**: Networks that satisfy all the nine conditions shown in (30), (31) and (32).

**Theorem V.6.** The following statements hold:

1) The optimal symmetric rate achieved by precoding-based network coding schemes for **Type I** networks is 1/3 per unicast session.
2) The optimal symmetric rate achieved by precoding-based network coding schemes for **Type II** networks is 2/5 per unicast session.
3) The optimal symmetric rate achieved by precoding-based network coding schemes for **Type III** networks is 1/2 per unicast session.

**Proof:** See Section VIII.

Basically, **Type III** are the only networks whose topology satisfies all the feasibility conditions for the PBNA scheme; in those networks, the PBNA scheme achieves the optimal linear precoding-based rates for these networks. **Type I** and **Type II** networks do not satisfy all the three feasibility conditions; however, it is possible to achieve their optimal linear precoding based rates using simpler schemes described in Section VIII.

VI. FEASIBILITY CONDITIONS OF PBNA

In this section, we explain the main ideas behind the proofs regarding the feasibility conditions for PBNA \(^{V}\). Consistently with Section \(^{V}\) we distinguish two cases based on whether \( \eta(x) \) is constant.

A. \( \eta(x) \) Is Not Constant

In this subsection, we first present a simple method to quickly identify a class of networks, for which PBNA is feasible. Then, we sketch the outline of the proof for the sufficiency of the Main Theorem. Next, we explain the main idea behind the proof for the necessity of the Main Theorem.

1) **A Simple Method Based on Theorem \(^{IV.I}\)** As shown in Theorem \(^{IV.I}\), the set \( S' \) contains an infinite number of rational functions, and thus it is impossible to check the feasibility conditions of Theorem \(^{IV.I}\) in practice. Interestingly, the theorem directly yields a simple method to quickly identify a class of networks for which PBNA is feasible. The major idea of the method is to exploit the asymmetry between \( p_i(x) \) and \( \eta(x) \) in terms of effective variables. Here, given a rational function \( f(y) \), we define a variable as an effective variable of \( f(y) \) if it appears in the unique form of \( f(y) \). Let \( \mathcal{V}(f(y)) \) denote the set of effective variables of \( f(y) \). Intuitively, this asymmetry allows us more freedom to control the values of \( p_i(x) \) and \( \eta(x) \) such that they can change independently, which makes the network behave more like a wireless channel.

The formal description of the method is presented below:

**Corollary VI.1.** Assume all \( m_{ij}(x) \)'s \( (i, j = 1, 2, 3) \) are non-zeros, and \( \eta(x) \) is not constant. Each unicast session can asymptotically achieve one half rate through PBNA if for \( i = 1, 2, 3, p_i(x) \neq 1 \) and \( \mathcal{V}(\eta(x)) \neq \mathcal{V}(p_i(x)) \).

**Proof:** If the above conditions are satisfied, we must have \( p_i(x) \neq \frac{\eta(x)}{1 + \eta(x)} \in S' \). Thus, the theorem holds.

In Fig. 6a and 6b we present two examples for which the simple method is applicable. As shown in these examples, due to edge \( e \), \( \eta(x) \) contains effective variables \( x_{\sigma_2 e}, x_{e r_2} \), which are absent in the unique form of \( p_i(x) \) \( (i = 1, 2, 3) \). Thus, by Corollary VI.1, each unicast session can asymptotically achieve one half rate through PBNA. However, Corollary VI.1 doesn’t subsume all possible networks for which PBNA is feasible. For instance, in Fig. 6c we show a counter example, where \( \mathcal{V}(\eta(x)) = \mathcal{V}(p_1(x)) \), and thus Corollary VI.1 is not applicable. Nevertheless, it is easy to verify the network satisfies the conditions of the Main Theorem, and thus PBNA is still feasible.
2) Sufficiency of the Main Theorem: As shown in Section IV, not all coupling relations \( p_i(x) = \frac{f_i(x)}{g_i(x)} \in S' \) are realizable due to the special properties of transfer functions. Indeed, since the transfer functions are defined on graphs, they exhibit special properties due to the graph structure. As we will see, these properties are essential in identifying the minimal sub-set of realizable coupling relations. In fact, we only need two such properties, namely Linearization Property and Square-Term Property.

We consider the general form of \( p_i(x) \) as below

\[
h(x) = \frac{m_{ab}(x)m_{pq}(x)}{m_{aq}(x)m_{pb}(x)}
\]  
(33)

where \( a, b, p, q = 1, 2, 3 \) and \( a \neq p, b \neq q \). Moreover, by the definition of transfer function, the numerator and denominator of \( h(x) \) can be expanded respectively as follows:

\[
m_{ab}(x)m_{pq}(x) = \sum_{(p_1, p_2) \in P_{ab} \times P_{pq}} t_{p_1}(x) t_{p_2}(x)
\]

\[
m_{aq}(x)m_{pb}(x) = \sum_{(p_3, p_4) \in P_{aq} \times P_{pb}} t_{p_3}(x) t_{p_4}(x)
\]

Hence, each path pair in \( P_{ab} \times P_{pq} \) contributes a term in \( m_{ab}(x)m_{pq}(x) \), and each path pair in \( P_{aq} \times P_{pb} \) contributes a term in \( m_{aq}(x)m_{pb}(x) \).

The first property, Linearization Property, is stated in the following lemma. According to this property, if \( p_i(x) \neq 1 \), it can be transformed into its simplest non-trivial form, i.e., a linear function or the inverse of a linear function, through a partial assignment of values to \( x \).

**Lemma VI.1 (Linearization Property).** Assume \( h(x) \) is not constant. Let \( h(x) = \frac{u(x)}{v(x)} \) such that \( \gcd(u(x), v(x)) = 1 \). Then, we can assign values to \( x \) other than a variable \( x_{ee'} \) such that \( u(x) \) and \( v(x) \) are transformed into either \( u(x_{ee'}) = c_1 x_{ee'} + c_0 \), \( v(x_{ee'}) = c_2 \) or \( u(x_{ee'}) = c_3 \), \( v(x_{ee'}) = c_4 \). Then, \( c_0, c_1, c_2, c_3, c_4 \) are constants in \( \mathbb{F}_2^m \), and \( c_1 c_2 \neq 0 \).

**Proof:** See Appendix A.

The second property, namely Square-Term Property, is presented in the following lemma. According to this property, the coefficient of \( x_{ee'}^2 \) in the numerator of \( h(x) \) equals its counterpart in the denominator of \( h(x) \). Thus, if \( x_{ee'}^2 \) appears in the numerator of \( h(x) \) under some assignment to \( x \), it must also appear in the denominator of \( h(x) \), and vice versa.

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

**Proof:** See Appendix A.

Now, we sketch the outline for the proof of the sufficiency of the Main Theorem. The proof consists of three steps:

First, we use Linearization Property and a simple degree-counting technique to reduce \( S' \) to the following set \( S'' \):

\[
S'' = \left\{ \frac{a_0 + a_1 \eta(x)}{b_0 + b_1 \eta(x)} \in S' : a_0, a_1, b_0, b_1 \in \mathbb{F}_q \right\}
\]  
(34)

Note that \( S'' \) only includes a finite number of rational functions.

Next, we iterate through all possible configurations of \( a_0, a_1, b_0, b_1 \), and utilize Linearization Property and Square-Term Property to further reduce \( S'' \) to just four rational functions:

\[
S_2'' = \left\{ 1, \eta(x), 1 + \eta(x), \frac{\eta(x)}{1 + \eta(x)} \right\}
\]  
(35)

Finally, we use a recent result from [36] to rule out the fourth redundant rational function in \( S_2'' \), resulting in the minimal set \( S_2 \) defined in the Main Theorem. The detailed proof is deferred to Appendix B.

3) Necessity of the Feasibility Conditions: We first show that the choices of precoding matrices are not limited to those defined in Eq. (12). In fact, given \( A, B, C \), we can always construct a precoding matrix \( V_1 \) such that Eq. (10) is satisfied.

The construction of \( V_1 \) involves solving a system of linear equations defined on \( \mathbb{F}_2^m(z) \):

\[
r(z)(zC - BA) = 0 \]  
(36)

where \( r(z) = (r_1(z), \ldots, r_{n+1}(z)) \in \mathbb{F}_2^{n+1}(z) \). Assume \( r_0(z) \) is a non-zero solution to Eq. (36). Substitute \( z \) with \( \eta(x) \), and we have \( \eta(x)r_0(\eta(x))C = r_0(\eta(x))BA \). Finally, construct the following precoding matrix

\[
V_1^T = (r_0^T(\eta(x^1))) \ r_0^T(\eta(x^2)) \ \cdots \ r_0^T(\eta(x^{2n+1}))
\]  
(37)

Apparently, \( V_1 \) satisfies Eq. (10). Hence, each non-zero solution to Eq. (36) corresponds to a row of \( V_1 \) satisfying Eq. (10). Conversely, it is straightforward to see that each row of \( V_1 \) satisfying Eq. (10) corresponds to a solution to Eq. (36).

As an example, consider the case where \( n = 2 \) and \( 2m = 4 \). Let \( \alpha \) be the primitive element of \( \mathbb{F}_4 \) such that \( \alpha^3 = 1 \) and \( \alpha^2 + \alpha + 1 = 0 \). Moreover, let \( A = I_2 \) and

\[
C = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix}, \quad B = \begin{pmatrix} \alpha^2 & \alpha \\ 1 & 1 \end{pmatrix}
\]

It’s easy to verify that \( r(z) = (\alpha^2 z^2 + z + \alpha, z^2 + \alpha z + \alpha^2) \) satisfies Eq. (36). Thus, we substitute \( z \) with \( \eta(x^1) \) and construct \( V_1^T = (r^T(\eta(x^1))) \ r^T(\eta(x^2)) \ \cdots \ r^T(\eta(x^{2n+1})) \). Apparently, Eq. (10) is satisfied. From this example, we can see that given different \( A, B, C \), we can construct different precoding matrix \( V_1 \), and thus the choices of precoding matrices are not limited to those defined in Eq. (12) through (14). An interesting observation is that the above precoding matrix \( V_1 \) is closely related to Eq. (12) through a transform equation:

\[
V_1 = GV_1^*F
\]  
(38)

where \( V_1^* \) is defined in Eq. (12). \( F \) is an \((n + 1) \times (n + 1)\)
matrix, and $G$ is a $(2n+1) \times (2n+1)$ diagonal matrix, with the $(i, i)$ element being $f_i(\eta(x'))$, where $f_i(z)$ is an arbitrary non-zero rational function in $\mathbb{F}_2[z]$. Moreover, the $(n+1)$th row of $FC$ and the 1st row of $FBA$ are both zero vectors.

**Proof:** See Appendix B.

Using Lemma VI.3 we can prove that when PBNA is infeasible via the precoding matrices defined in Eq. (12)-(14) due to the presence of a coupling relation, it is infeasible via any precoding matrices which satisfy the alignment conditions. This implies that the conditions of the Main Theorem are also necessary for the feasibility of PBNA. We defer the detailed proof to Appendix B.

**B. $\eta(x)$ Is Constant**

For this case, we use a scheme that is slightly different from that of Section IV. In this scheme, at each sender edge $\sigma_i$ ($i = 1, 2, 3$), we encode source symbol $X_i$ into two encoded symbols, which are then transmitted through the network in two time slots. The precoding matrices are defined as follows:

$$V_1 = (\theta_1 \theta_2)^T \tag{39}$$
$$V_2 = M_{12}M_{32}^{-1}(\theta_1 \theta_2)^T \tag{40}$$
$$V_3 = M_{12}M_{32}^{-1}(\theta_1 \theta_2)^T \tag{41}$$

where $\theta_1, \theta_2$ are arbitrary variables. Because $T$ is an identity matrix, it can be easily verified that at each receiver, the interferences are perfectly aligned, i.e.,

$$M_{21}V_2 = M_{31}V_3$$
$$M_{32}V_3 = M_{12}V_1$$
$$M_{23}V_3 = M_{13}V_1$$

Moreover, the rank conditions can be reformulated to similar forms as $\mathcal{B}_1', \mathcal{B}_2', \mathcal{B}_3'$.

**Proof of Theorem V.2** First, assume $p_i(x)$ is not constant. Using the above construction, the rank condition for the $i$th unicast session is equivalent to

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

Thus $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ is feasible through PBNA. Conversely, if $p_i(x)$ is constant and thus $P_i = I_2$, the rank condition for the $i$th unicast session is violated, and thus $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ is not feasible through PBNA.

In Fig. 7 we show an example of this case. One interesting observation is that in this example, each unicast session can achieve unit rate by using pure routing. Hence, PBNA doesn’t provide any advantage over routing in terms of transmission rate.

**Algorithm 1: Calculate $C_{ee'}$**

1. Use BFS algorithm to calculate the set of edges reachable from $e$, denoted by $E_1$.
2. Use reverse BFS algorithm to calculate the set of edges which is connected to $e'$, denoted by $E_2$.
3. $E_{ee'} \leftarrow E_1 \cap E_2$.
4. $C_{ee'} \leftarrow \{\sigma_i\}, C \leftarrow \{\sigma_i\}$.
5. for each $e \in E_{ee'}$ in the topological order do
   6. $C \leftarrow C - \{e\}$;
   7. for each $e'$ such that head($e$) = tail($e'$) do
      8. if $e' \in E_{ee'}$ then $C \leftarrow C \cup \{e'\}$;
   9. end
10. if $C$ contains one edge then $C_{ee'} \leftarrow C_{ee'} \cup C$;
11. end

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

In this section, since the number of interfering signals is reduced, at least one alignment conditions can be removed, and thus the restriction on $V_1$ imposed by Eq. (10) vanishes. Therefore, we can choose $V_1$ freely, and the feasibility conditions of PBNA can be greatly simplified. For example, assume $m_{21}(x) = 0$ and all other transfer functions are non-zeros. Hence, the alignment condition for the first unicast session vanishes. Using a scheme similar to above, we set $V_1 = (\theta_1 \ theta_2)^T, V_2 = M_{13}M_{23}^{-1}(\theta_1 \ theta_2)^T$ and $V_3 = M_{12}M_{32}^{-1}(\theta_1 \ theta_2)^T$, and thus the interferences at $\tau_2$ and $\tau_3$ are all perfectly aligned. It is easy to see that $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ is feasible through PBNA if and only if $p_i(x)$ is not constant for every $i = 1, 2, 3$. Using similar arguments, we can discuss other cases.

**VII. CHECKING THE FEASIBILITY CONDITIONS OF PBNA**

In this section, we propose a polynomial-time algorithm to check the feasibility conditions of PBNA. We use $C_{e_1e_2}$ to denote the set of bottlenecks between two edges $e_1$ and $e_2$, and use $C_{ij}$ to represent $C_{e_1e_2}$. Using this notation, it can be easily seen that $\alpha_{ijk}$ is the last edge of the topological ordering of the edges in $C_{ij} \cap C_{ik}$, and $\beta_{ijk}$ is the first edge of the topological ordering of the edges in $C_{jk} \cap C_{ij,ik}$. We assume $G$ is stored as an adjacency list, i.e., for each node $v \in V'$, we associate it with the set of its incoming edges and the set of its outgoing edges. Moreover, we assume all the edges in $G$ have been arranged in topological order.

The checking process consists of the following steps: 1) Check if $\eta(x) = 1$; 2) if $\eta(x) = 1$, check the conditions of Theorem V.2; 3) otherwise, check the conditions of the Main Theorem. In the following discussion, we present the building blocks involved in these steps.

1) Calculating $C_{ee'}$: We use Algorithm 1 to calculate the set of bottlenecks $C_{ee'}$, which separates $e$ from $e'$. The algorithm consists of two steps: 1) Lines 1-3 are used to calculate the set of edges traversed by the paths in $P_{ee'}$, denoted by $E_{ee'}$. Note that in the reverse BFS algorithm, we start from $e'$.
Algorithm 2: Check if $p_1(x) = \frac{\eta(x)}{1 + \eta(x)}$

1. $\alpha_{312} \leftarrow$ the last edge of $C_{21} \cap C_{22}$;
2. $\alpha_{213} \leftarrow$ the last edge of $C_{21} \cap C_{32}$;
3. if $\alpha_{312} \not\in C_{12}$ or $\alpha_{213} \not\in C_{13}$ then return false;
4. Use BFS algorithm to check whether $\alpha_{312}$ is connected with $\alpha_{213}$ by a directed path;
5. if $\alpha_{312}$ is connected with $\alpha_{213}$ then return false;
6. Let $G_1$ denote the subgraph of $G'$ induced by $E' = \{\alpha_{312}, \alpha_{213}\}$;
7. Use BFS algorithm to check whether $\tau_1$ is connected to $\sigma_1$ in $G_1$;
8. if $\tau_1$ is connected to $\sigma_1$ in $G_1$ then return false;
9. else return true.

and move upwards by following the incoming edges associated with each node. 2) Lines 4-11 are used to calculate $C_{ee'}$. In this step, we iterate through each edge $e \in E_{ee'}$ in the topological order. In each iteration, we calculate $C$, which forms a cut separating $e$ from $e'$. If $C$ contains only one edge, we then incorporate $C$ into $C_{ee'}$. The running time of the algorithm is $O(h(|E|))$, where $h$ is the maximum in-degree of nodes in $G'$.

2) Checking if $\eta(x) = 1$: Using algorithm 1 and Theorem VIII.3, we can easily check whether this coupling relation holds. First, we calculate $C_{31} \cap C_{32}, C_{21} \cap C_{23}$, from which we get the two edges $\alpha_{312}$ and $\alpha_{213}$. Then, we calculate $C_{12} \cap C_{312}, C_{13} \cap C_{312}$, from which we get $\beta_{312}$ and $\beta_{213}$. Finally, we use Theorem VIII.3 to check if $\eta(x) = 1$ by checking whether $\alpha_{312} = \beta_{312}$ and $\alpha_{213} = \beta_{213}$.

3) Checking if $p_1(x) = 1$ or $p_2(x) = \eta(x)$: Due to Theorem VIII.4, we use Ford-Fulkerson Algorithm to check these coupling relations. For example, in order to check whether $p_1(x) = 1$, we add a super sender node $s'$, which is connected to $s_1$ and $s_2$ via two directed edges of capacity one, and a super receiver node $d'$, to which $d_1$ and $d_3$ are connected via two directed edges of capacity one. We then use Ford-Fulkerson Algorithm to calculate the maximum flow from $s'$ to $d'$, which is identical to $C_{12,13}$. Thus, by checking whether $C_{12,13} = 1$, we can identify whether $p_1(x) = 1$. Similarly, we can check other coupling relations.

4) Checking if $p_1(x) = \frac{\eta(x)}{1 + \eta(x)}$ or $p_2(x), p_3(x) = 1 + \eta(x)$: We use Algorithm 2 to check if $p_1(x) = \frac{\eta(x)}{1 + \eta(x)}$. The other two coupling relations can be checked similarly. Note that Line 4 consists of two steps: First, we start from $\alpha_{312}$ and use BFS to check if $\alpha_{312}$ is reachable from $\alpha_{312}$; then we start from $\alpha_{213}$ and use BFS to check if $\alpha_{312}$ is reachable from $\alpha_{213}$. The running time of the algorithm is $O(h(|E|))$.

VIII. OPTIMAL LINEAR PRECODING-BASED RATES

In this section, we prove that for SISO scenarios with all non-zero channel coefficients, there are only three possible rates achievable through any linear precoding schemes. In order to show this, we first prove that for the networks that violate one of the following three conditions: $p_1(x) \neq \frac{\eta(x)}{1 + \eta(x)}$, $p_2(x) \neq 1 + \eta(x)$, and $p_3(x) \neq 1 + \eta(x)$, it is not possible to achieve a symmetric rate of more than 2/5 per user, through any precoding-based scheme (the proof follows from [1]). We also show that this outer bound of 2/5 is achievable through our PBNA scheme and thus it is tight.

Let’s classify the networks based on the type of conditions they satisfy (or violate). This will be helpful for pointing to the different types of networks later in this section.

- **Type I**: Networks that fail to satisfy one or more of the six basic conditions: $p_i(x) \neq 1$ and $p_i(x) \neq \eta(x) \forall i \in \{1, 2, 3\}$.
- **Type II**: Networks that satisfy the six basic conditions shown in Type I, but fail to satisfy one of the following three mutually exclusive conditions: $p_1(x) \neq \frac{\eta(x)}{1 + \eta(x)}$, $p_2(x) \neq 1 + \eta(x)$, and $p_3(x) \neq 1 + \eta(x)$.
- **Type III**: Networks that satisfy all the nine condition shown in [27], [28] and [29].

Consider any linear precoding scheme over $n$ channel uses. Let $V_1, V_2, V_3$ represent the signal vector spaces along which user 1, 2, 3 send their signal , respectively. Let $v_1, \tilde{v}_2, \tilde{v}_3$ be vectors from the spaces $V_1, V_2, V_3$, respectively. Consider a Type II network, without loss of generality, we assume that the network realizes $p_1(x) = \frac{\eta(x)}{1 + \eta(x)}$ (see Fig. 3b). This relation can be equivalently represented in matrix form as

$$M_{11} = M_{31}M_{32}^{-1}M_{12} + M_{21}M_{23}^{-1}M_{13}$$ (42)

**Lemma VIII.1.** If $\tilde{v}_1$ aligns with $\tilde{v}_3$ at Receiver 2 and with $\tilde{v}_2$ at Receiver 3, then $\tilde{v}_1$ must align in the space spanned by $\tilde{v}_2$ and $\tilde{v}_3$ at Receiver 1.

**Proof:** Given $\tilde{v}_1$ aligns with $\tilde{v}_3$ at Receiver 2 and with $\tilde{v}_2$ at Receiver 3, i.e.,

$$Rx2: \quad M_{12}\tilde{v}_1 = a \ M_{32}\tilde{v}_3$$ (43)

$$Rx3: \quad M_{13}\tilde{v}_2 = b \ M_{23}\tilde{v}_3$$ (44)

where $a, b$ are scalars. At Receiver 1, we see the vector $M_{11}\tilde{v}_1$. Using (42), (43) and (44) we get,

$$M_{11}\tilde{v}_1 = M_{31}M_{32}^{-1}M_{12}\tilde{v}_1 + M_{21}M_{23}^{-1}M_{13}\tilde{v}_1$$

$$= a M_{31}\tilde{v}_2 + b M_{21}\tilde{v}_2$$

This shows that the desired vector at Receiver 1 aligns with the space spanned by the interference.

**Theorem VIII.1.** For a Type II network the symmetric rate achievable per user through any precoding-based scheme cannot be more than 2/5.

**Proof:** Suppose every user sends $d$ symbols over $n$ dimensions, through any linear precoding scheme. Consider User 1, let use $d_{12}$ and $d_{13}$ to represent the number of dimensions of signal space of User 1 that align with User 2 at Receiver 3 and User 3 at Receiver 2 respectively, and $V_{12}$ and $V_{13}$ to represent their corresponding spaces. From Lemma VIII.1 we know that $V_{12}$ and $V_{13}$ must have no intersection, otherwise the intersection part will contain vectors that will align with interference at Receiver 1. Therefore, we must have $d_{12} + d_{13} \leq d$. Now consider User 2, we already know that there is a $d_{13}$ dimensional space where interference from User 1 and 3 are aligned. So the number of interference dimension.
is given as \((d + d - d_{13}) = 2d - d_{13}\). The number of desired dimensions at Receiver 2 is \(d\), and this \(d\) dimensional desired signal space should remain resolvable from the interference space, so we have \(3d - d_{13} \leq n\). Similarly, consider User 3 to obtain another inequality \(3d - d_{12} \leq n\). Combining these inequalities we get \(6d - (d_{13} + d_{12}) \leq n\). But we know \(d_{12} + d_{13} \leq d\), so \(6d - d \leq 2n \Rightarrow d/n \leq 2/5\), which implies it is not possible to achieve a symmetric rate more than 2/5 per user.

**Corollary VIII.1.** For Type II networks, it is possible to achieve a rate of 2/5 per user through user's and through a finite timeslot precoding based network alignment scheme, i.e., the outer bound is tight.

**Proof:** Without loss of generality, assume the Type II networks has a coupling relation \(p_1(x) = \frac{\eta(x)}{\eta(x)}\). This scheme can be easily modified to fit the other coupling relations too. Suppose we use a \(2n+1 = 5\) symbol extension, then according to the PBNA scheme in Section [V] we have precoding vectors 
\(V_1 = (wTw^{T}w)\), 
\(V_2 = (wTw)\) and 
\(V_3 = (TwTw^{T}w)\). The given coupling relation only affects User 1, so the rates at Receiver 2 and 3 will remain unaffected. The matrix equivalent of the coupling relation is given in [42], which can be rewritten as,

\[
M_{11} = M_{31}M_{32}^{-1}M_{12} + M_{31}M_{32}^{-1}M_{12}T
\]

At Receiver 1, the desired signal space is given \(M_{11}V_1\) and the interference space is given by \(M_{31}V_3\) (Note: The interference from transmitter 2 and 3 are aligned, i.e., \(M_{21}V_2 = M_{31}V_3\)). Substituting the alignment equation from Receiver 2 for \(V_3\) we get,

\[
M_{31}V_3 = M_{31}M_{32}^{-1}M_{12}(TwTw^{T}w)
\]

From [45] and [46], it can be seen that the second column of the desired signal space \((M_{11}V_1)\) can be written as a linear combination of the two columns of the interference space. The other two columns of the desired space are linearly independent of the column of interference space. User 1 could use these two dimension to send its signal without interference. In other words, each user would be able to achieve a rate of 2/5.

**Proof of Theorem VIII.1.** Type I networks fail to satisfy certain conditions which are information theoretically necessary to achieve any rate more than 1/3 user, this was explained in a remark under the Main Theorem in Section [V] The outer bound for Type II networks was derived in Theorem VIII.1 and the achievability was shown in Corollary VIII.1 Type III networks were the main focus of this paper, previous sections discussed in detail about schemes and their feasibility for achieving 1/2 rate per user in detail and it is a well known fact that it is not possible to achieve more than 1/2 per user for SISO scenarios in fully connected networks [14].

IX. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we consider the problem of network coding for the SISO scenarios with three unicast sessions. We apply precoding-based interference alignment [14] to this network setting, in which each source node performs precoding operations while intermediate nodes simply perform random network coding. We show that network topology may introduce algebraic dependence (“coupling relations”) between different transfer functions, which can potentially make PBNA infeasible. Using two graph-related properties and a recent result from [59], we identify the minimal set of coupling relations that are realizable in networks. Moreover, we show that each of these coupling relations has a unique interpretation in terms of network topology. Based on these interpretations, we present a polynomial-time algorithm to check the feasibility of PBNA.

This work is limited to three unicast sessions in the SISO scenario (i.e. with min-cut one per session) and following a precoding-based approach (all precoding is performed at the end nodes, while intermediate nodes perform random network coding). This is the simplest, yet highly non-trivial instance of the general problem of network coding across multiple unicasts. Apart from being of interest on its own right, we hope that it can be used as a building block and provide insight into the general problem.

There are still many problems that remain to be solved regarding applying interference alignment techniques to the network setting. For example, one important problem is the complexity of PBNA, which arises in two aspects, i.e., precoding matrix and field size, and is inherent in the framework of PBNA. One direction for future work is to apply other alignment techniques (with lower complexity) to the network setting. The extensions to other network scenarios beyond SISO with more than three unicast sessions are highly non-trivial. Finally, the current paper applies precoding at the sources only, while intermediate nodes performed simply random network coding; an open direction for future work is alignment by network code design in the middle of the network as well.

APPENDIX A

PROOFS OF GRAPH-RELATED PROPERTIES

A. Linearization Property and Square-Term Property

The following lemma plays an important role in the proof of Linearization Property and the interpretation of the coupled relations, \(p_1(x) = 1\) and \(p_1(x) = \eta(x)\). The basic idea of this lemma is that we can multicast two symbols from two senders to two receivers via network coding if and only if the minimum cut separating the senders from the receivers is greater than one.

**Lemma A.1.** \(m_{ab}(x)m_{pq}(x) \neq m_{aq}(x)m_{pb}(x)\) if and only if there is disjoint path pair \((P_1, P_2) \in P_{ab} \times P_{pq}\) or \((P_3, P_4) \in P_{aq} \times P_{pb}\).

**Proof:** We add a super sender \(s\) and connect it to \(s_p\) via two edges of unit capacity, and a super receiver \(d\), to which we connect \(d_p\) and \(d_q\) via two edges of unit capacity. Thus, the transfer matrix at \(d\) is

\[
M = \begin{pmatrix}
m_{ab}(x) & m_{aq}(x) \\
m_{pb}(x) & m_{pq}(x)
\end{pmatrix}
\]
On the other hand, if $d(e) = 0$, then $P_1$ is disjoint from $P_2$. Similarly, there exist edges $e, e' \in P$ such that the path segment between $e$ and $e'$ is disjoint with $P_1 \cup P_2$. Let $P_3 = P_1 \cup \{e, e'\} \cup P_2$ and $P_4 = P_1 \cup \{e, e'\} \cup P_2$, respectively. Then construct two new paths: $P_3' = P_3[\sigma_a : e_1 \cup P_2[e_2 ; \tau_1] \cup P_2[e_2 : \tau_1] \cup P_2[e_2 : \tau_1]$ and $P_4' = P_4[\sigma_p : e_3 \cup P_2[e_3 : \tau_0] \cup P_2[e_3 : \tau_0]$ (see Fig. 8). Let $H$ denote the subgraph of $G'$ induced by $P_1 \cup P_2 \cup P_3' \cup P_4'$. We then prove that the theorem holds for $H$. If $d(e_2) > o(e_3)$ (Fig. 8a and 8b), the variables along $P_2[e_2 : e_2]$ are absent in $h_2(x_{H})$. We then arbitrarily select a variable $x_{e_{ee}}$ from $P_2[e_2 : e_2]$, and write $h_1(x_{H}) = f(x_{H})x_{ee} + g(x_{H})$, where $x_{H}$ includes all the variables in $x_{H}$ other than $x_{ee}$. Meanwhile, $h_2(x_{H})$ can be written as $h_2(x_{H}')$. Clearly, $x_{ee}$ will not show up in $d(x_{H})$ and thus it can also be written as $d(x_{H})$. We then find values for $x_{H}'$, denoted by $r$, such that $f(r)h_2(r)d(r) = 0$. Finally, denote $c_0 = c_0(r)d^{-1}(r)$, $c_1 = c_1(r)d^{-1}(r)$, and $c_2 = c_2(r)d^{-1}(r)$ and the theorem holds.

On the other hand, if $d(e_2) < o(e_3)$ (see Fig. 8c), the variables along $P_4[e_1 : e_4]$ are absent in $h_2(x_{H})$. We then select a variable $x_{e_{ee}}$ from $P_4[e_1 : e_4]$. Similar to above, it's easy to see that $u(x)$ and $v(x)$ can be transformed into $c_0$ and $c_1 x_{e_{ee}} + c_0$ respectively.

For the case where $(P_3, P_4) \in P_{ao} \times P_{pb}$ is a disjoint path pair, we can show that $u(x)$ and $v(x)$ can be transformed into $c_0$ and $c_1 x_{e_{ee}} + c_0$ respectively.

The basic idea of Square-Term Property is to construct a one-to-one mapping between the square terms in the numerator of $h(x)$ and those in the denominator of $h(x)$.

**Proof of Square-Term Property:** First, we define two sets $Q_1 = \{(P_1, P_2) \in P_{ab} \times P_{pq} \mid t_{P_1}(x)t_{P_2}(x)\}$ and $Q_2 = \{(P_3, P_4) \in P_{ap} \times P_{pb} \mid t_{P_3}(x)t_{P_4}(x)\}$. Consider a path pair $(P_3, P_4) \in Q_1$. Since the degree of $x_{ee}$ in $t_{P_3}(x)$ and $t_{P_4}(x)$ is at most one, we must have $x_{ee} \in t_{P_3}(x)$ and $x_{ee} \in t_{P_4}(x)$. Thus $e, e' \in P_3 \cup P_4$. Let $P_1 \times P_2$ be the parts of $P_1$ before $e$ and after $e'$ respectively. Similarly, define $P_3' \times P_2'$ and $P_3' \times P_4'$ in $Q_2$ (see Fig. 9). Clearly, $t_{P_1}(x)t_{P_2}(x) = t_{P_3}(x)t_{P_4}(x)$, and thus $(P_3, P_4) \in Q_2$. The above method establishes a one-to-one mapping $\phi : Q_1 \rightarrow Q_2$, such that $\phi((P_1, P_2)) = (P_3, P_4)$, $t_{P_1}(x)t_{P_2}(x) = t_{P_3}(x)t_{P_4}(x)$, and $(P_3, P_4) \in Q_2$. Hence, $f_1(x) = \frac{1}{x_{ee}} \sum_{(P_1, P_2) \in Q_1} t_{P_1}(x)t_{P_2}(x) = f_2(x)$.

**B. Other Graph-Related Properties**

In this section, we present other graph-related properties, which reveal more microscopic structures of transfer functions, and are to be used in the proofs of Theorems V.3 and V.5. Before proceeding, we first extend the concept of transfer function to any two edges $e, e' \in E'$, i.e., $m_{ee}(x) = \sum_{P \in P_{ee'}} t_P(x)$, where $P_{ee'}$ is the set of paths from $e$ to $e'$. The following lemma states that any transfer function $m_{ee}(x)$ is fully determined by the two edges $e, e'$.

**Lemma A.2.** Consider two transfer functions $m_{e_1e_2}(x)$ and $m_{e_3e_4}(x)$. Then $m_{e_1e_2}(x) = m_{e_3e_4}(x)$ if and only if $e_1 = e_3$ and $e_2 = e_4$.

**Proof:** Apparently, the “if” part holds trivially. Now assume $e_1 \neq e_3$ or $e_2 \neq e_4$. Then, there must be some edge which appears exclusively in $P_{e_1e_2}$ or $P_{e_3e_4}$, implying $m_{e_1e_2}(x) \neq m_{e_3e_4}(x)$. Thus, the lemma holds.

The following result was first proved by Han et al. [36]. It states that each transfer function $m_{ee}(x)$ can be uniquely...
factorized into a product of irreducible polynomials according to the bottlenecks between \( e \) and \( e' \).

**Lemma A.3.** We arrange the bottlenecks in \( C_{ee'} \) in topological order: \( e_1, e_2, \ldots, e_k \), such that \( e = e_1, e' = e_k \). Then, \( m_{ee'}(x) \) can be factorized as \( m_{ee'}(x) = \prod_{i=1}^{k-1} m_{e_i, e_{i+1}}(x) \), where \( m_{e_i, e_{i+1}}(x) \) is an irreducible polynomial.

In addition, as shown below, any transfer function \( m_{ee'}(x) \) can be partitioned into a summation of products of transfer functions according to a cut between \( e \) and \( e' \).

**Lemma A.4.** Assume \( U = \{e_1, e_2, \ldots, e_k\} \) is a cut which separates \( e \) from \( e' \). If \( e_i \notin U \) or \( e_j \notin U \), we have \( m_{ee'}(x) = \sum_{i=1}^{k} m_{e_i, e'}(x) \). Otherwise, the above equality doesn’t hold.

**Proof:** For \( e_i \in U \), let \( P_{ee'}^i \) denote the set of paths in \( P_{ee'} \) that pass through \( e_i \). Because \( e_i \notin U \), \( P_{ee'}^i \) is disjoint with \( P_{ee'}^j \). Hence, \( m_{ee'}(x) = \sum_{i=1}^{k} \sum_{p \in P_{ee'}} t_p(x). \) Note that \( m_{e_i, e'}(x) = \sum_{(p_1, p_2) \in P_{ee'}^i \times P_{ee'}^j} t_{p_1}(x) t_{p_2}(x). \) Moreover, each monomial \( t_{p_1}(x) t_{p_2}(x) \) in \( m_{e_i, e'}(x) \) corresponds to a monomial \( t_{p_1}(x) t_{p_2}(x) \) in \( m_{ee'}(x) \). Hence, \( m_{ee'}(x) = \sum_{p \in P_{ee'}} t_p(x) \), and the lemma holds. On the other hand, if some \( e_i \) is upstream of \( e_j \), \( P_{ee'}^i \cap P_{ee'}^j \neq \emptyset \), and thus \( m_{ee'}(x) \neq \sum_{i=1}^{k} \sum_{p \in P_{ee'}} t_p(x) \), indicating that the lemma doesn’t hold.

**APPENDIX B**

**PROOFS OF FEASIBILITY CONDITIONS OF PBN A**

**A. Reducing \( S' \) to \( S'_i \)**

In order to utilize the degree-counting technique, we use the following lemma. Basically, it allows us to recompute each \( f(\eta(x)) \) to \( S' \) to its unique form \( \alpha(x) \), such that we can compare the degree of a coding variable in \( \alpha(x) \) and \( \beta(x) \) with its degrees in the numerator and denominator of \( p_i(x) \) respectively.

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

**Proof:** See Appendix

We use the following three steps to reduce \( S' \) to \( S'_i \).

**Step 1:** \( S' \Rightarrow S'_i \). Assume \( p_i(x) = \frac{f(\eta(x))}{g(\eta(x))} \in S' \). We will prove that \( d = \max\{|d_f, d_g|\} = 1 \). Let \( \eta(x) = \frac{w(x)}{z(x)} \), \( \eta(x) = \frac{s(x)}{t(x)} \) denote the unique forms of \( p_i(x) \) and \( \eta(x) \) respectively.

Without loss of generality, let \( f(z) = \sum_{j=0}^{k} a_j z^j \), \( g(z) = \sum_{j=0}^{l} b_j z^j \) where \( a_b h_i \neq 0 \). We first consider the case where \( l \leq k \) and thus \( d = k \). Define the following two polynomials:

\[
\alpha(x) = f(\eta(x)) x^k = \sum_{j=0}^{k} a_j \eta^{k-j}(x) y^j \\
\beta(x) = g(\eta(x)) x^k = \sum_{j=0}^{l} b_j \eta^{k-j}(x) y^j
\]

Due to Lemma B.1, we have \( \alpha(x) = c u(x) \), \( \beta(x) = c v(x) \), where \( c \) in a non-zero constant in \( F_q \). Moreover, according to Linearization Property, we assign values to \( x \) other than a coding variable \( x_{ee'} \) such that \( u(x) \) and \( v(x) \) are transformed into:

\[
u(x_{ee'}) = c_1 x_{ee'} + c_0 \quad v(x_{ee'}) = c_2
\]

or

\[
u(x_{ee'}) = c_2 \quad v(x_{ee'}) = c_1 x_{ee'} + c_0
\]

where \( c_0, c_1, c_2 \in F_q \) and \( c_1 c_2 \neq 0 \). We only consider the first case. The proof for the other case is similar. In this case, \( \alpha(x) \) and \( \beta(x) \) are transformed into \( \alpha(x_{ee'}) = c_1 x_{ee'} + c_0 \) and \( \beta(x_{ee'}) = c_2 \) respectively.

By contradiction, assume \( d \geq 2 \). We first consider the case where \( l \leq k \) and thus \( d = k \). In this case, we have

\[
\alpha(x_{ee'}) = \sum_{j=0}^{k} a_j x^{k-j}(x_{ee'}) s^j(x_{ee'}) = c c_1 x_{ee'} + c_0 \\
\beta(x_{ee'}) = \sum_{j=0}^{l} b_j x^{k-j}(x_{ee'}) s^j(x_{ee'}) = c_2
\]

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

**Case I:** \( r \neq r' \). If \( r > r' \), \( d_r = kr' - l(r' - r) = 1 \). Contradicting that \( d_r = 1 \). 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 \( d_r = kr' - l_1 (r' - r) = 1 \). Clearly, \( l_2 > 0 \) due to \( d_r = 0 \). If \( r > 0 \), \( kr' - l_2 (r' - r) > kr' - l_2 r' \geq 0 \), contradicting \( d_r = 0 \). Hence, \( r = 0 \), and \( l_2 = k \) due to \( d = 0 \). Meanwhile, \( d_r = (k - l_1) r_r = 1 \), which implies that \( l_1 = k - 1 \) and \( r_r = 1 \). Thus, \( k - 1 \) is a common divisor of \( f(z) \) and \( g(z) \), contradicting \( \gcd(f(z), g(z)) = 1 \).

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

\[
\sum_{j=0}^{k} a_j \eta^{k-j}(x_{ee'}) t_r^j \sum_{j=0}^{l} b_j \eta^{k-j}(x_{ee'}) s_r^j = t_r f(\eta(x)) = 0
\]

Hence \( z - \frac{c_r}{c_r} x_{ee'} \) 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 \( d = 1 \) whenever \( l > k \). This implies that \( \frac{f(\eta(x))}{g(\eta(x))} \) can only be of the form \( \frac{\alpha(x)}{\beta(x)} \). Hence, we have reduced \( S' \) to \( S'_i \).

**Step 2:** \( S'_i \Rightarrow S'_2 \). We consider the coupling relation \( p_i(x) = \frac{f(\eta(x))}{g(\eta(x))} \). The coupling relations \( p_2(x) = \frac{f(\eta(x))}{g(\eta(x))} \) and \( p_3(x) = \frac{f(\eta(x))}{g(\eta(x))} \) can be dealt with similarly. Define \( q_1(x) = \frac{f(\eta(x))}{g(\eta(x))} = \frac{m_{11}(x) m_{23}(x)}{m_{13}(x) m_{21}(x)} \). Assume the characteristic of
$\mathbb{F}_q$ is $p$. Given an integer $m$, let $m_p$ denote the remainder of $m$ divided by $p$. Since $S''_1$ only consists of a finite number of rational functions, we iterate all possible configurations of $a_0, a_1, b_0, b_1$ as follows:

Case I: $\frac{f(z)}{g(z)} = \frac{a_0+a_1z+b_1}{b_0+b_1z}$, where $a_1a_0b_1b_0 \neq 0$, and $a_0b_1 \neq a_1b_0$. For this case, we have $p_1(x_{ee'}) = \frac{a_0+a_1p_1(x_{ee'})q_1(x_{ee'})}{b_0+b_1p_1(x_{ee'})q_1(x_{ee'})}$.

It immediately follows

$$q_1(x_{ee'}) = \frac{a_0c_2^2 - b_0c_0c_2 - b_0c_1c_2x_{ee'}}{b_1c_1^2x_{ee'}^2 + 2b_0c_1c_0c_2x_{ee'} + b_1c_0^2 - a_1c_0c_2}$$

Let $u_1(x_{ee'})$, $v_1(x_{ee'})$ denote the numerator and denominator of the above expression respectively. Assume $u_1(x_{ee'}) \mid v_1(x_{ee'})$ and thus $x_{ee'} = \frac{a_0c_2-b_0c_0c_2}{b_0c_1c_2}x_{ee'} + \frac{b_1c_0^2 - a_1c_0c_2}{b_1c_1^2x_{ee'}^2}$ is a solution to $v_1(x_{ee'}) = 0$.

However, $\frac{a_0c_2-b_0c_0c_2}{b_0c_1c_2} = \frac{a_0c_2}{b_0}(a_0b_1 - a_1b_0) \neq 0$. Hence, $u_1(x_{ee'}) \nmid v_1(x_{ee'})$. Thus, by the definition of $q_1(x)$ and Square-Term Property, $x_{ee'}$ must appear in $u_1(x_{ee'})$, which contradicts the formulation of $u_1(x_{ee'})$.

Case II: $\frac{f(z)}{g(z)} = \frac{a_0+a_1z}{b_1}$, where $a_0a_1b_0 \neq 0$. Similar to Case I, we can derive

$$q_1(x_{ee'}) = \frac{a_0c_2^2}{b_1c_1^2x_{ee'}^2 + 2b_0c_1c_0c_2x_{ee'} + b_1c_0^2 - a_1c_0c_2}$$

which contradicts Square-Term Property.

Case III: $\frac{f(z)}{g(z)} = \frac{a_0}{b_1}$, where $a_0b_1 \neq 0$. Thus $\frac{1}{p_1(x)} = \frac{b_0}{a_0} = \frac{1}{a_1}$. Since the coefficient of each monomial in the denominators and numerators of $p_1(x)$ and $\eta(x)$ equals one, it follows $\frac{a_0}{b_0} = \frac{a_1}{a_0} = 1$. This indicates that $p_1(x) = \eta(x)\frac{a_1}{a_0}$.

Case IV: $\frac{f(z)}{g(z)} = \frac{a_0}{b_0+b_1z}$, where $a_0b_0 \neq 0$. It follows that

$$q_1(x_{ee'}) = \frac{a_0c_2^2 - b_0c_0c_2 - b_0c_1c_2x_{ee'}}{b_1c_1^2x_{ee'}^2 + 2b_0c_1c_0c_2x_{ee'} + b_1c_0^2 - a_1c_0c_2}$$

Similar to Case I, this also contradicts Square-Term Property.

Case V: $\frac{f(z)}{g(z)} = \frac{a_0}{z}$, where $a_0 \neq 0$. Hence, $q_1(x_{ee'}) = \frac{a_0c_2^2}{c_1x_{ee'}^2 + 2c_0c_2x_{ee'} + c_0^2}$, contradicting Square-Term Property.

Case VI: $\frac{f(z)}{g(z)} = a_0 + a_1z$, where $a_0a_1 \neq 0$. Thus, it follows $p_1(x) = a_0 + a_1\eta(x)$. Similar to Case III, $a_1 = a_0 = 1$, implying that $p_1(x) = 1 + \eta(x)$.

Case VII: $\frac{f(z)}{g(z)} = a_1z$, where $a_1 \neq 0$. Similar to Case III, $a_1 = 1$ and hence $p_1(x) = \eta(x)$.

Therefore, we have proved that $\frac{f(\eta(x))}{g(\eta(x))}$ can only take the form of the four rational functions in $S''_1$. Thus, we have reduced $S''_1$ to $S''_1$.

Step 3: $S''_1 \Rightarrow S''_1$. We note that in Proposition 3 of [36], it was proved that $p_1(x) \neq 1 + \eta(x)$, $p_2(x) \neq \frac{\eta(x)}{1+\eta(x)}$ and $p_3(x) \neq \frac{\eta(x)}{1+\eta(x)}$. Combined with the above results, we have reduced $S''_1$ to $S''_1$.

In summary, according to Theorem [V.1] if the conditions of the Main Theorem are satisfied, the three unicast sessions can asymptotically achieve the rate tuple $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$ through PBNA.

B. Necessity of the Feasibility Conditions

As shown previously, each row of $V_1$ satisfying the alignment conditions corresponds to a non-zero solution to Eq. (36). The following lemma reveals that any non-zero solution to Eq. (36) is linearly dependent on the particular vector $(1, z, z^2, \ldots, z^n)$, which forms each row of the preceding matrix $V_1^*$.

Lemma B.2. Eq. (36) has a non-zero solution in $\mathbb{F}_{q+1}[z]$ in the form of $r(z) = (1, z, z^2, \ldots, z^n)\mathbf{F}$, where $\mathbf{F}$ is an $(n+1) \times (n+1)$ matrix in $\mathbb{F}_{2^n}$. Moreover, any solution to Eq. (36) is linearly dependent on $(1, z, \ldots, z^n)$.$\mathbf{F}$.

Proof: Denote $D = \mathbf{BA}$. First, we will prove that $\text{rank}(zC - D) = n$. Let $c_i$ and $d_i$ denote the $i$th column of $C$ and $D$ respectively. Hence, $c_1, c_2, \ldots, c_n$ are linearly independent and so are $d_1, \ldots, d_n$. Assume there exist $f_1(z), \ldots, f_n(z) \in \mathbb{F}_{2^n}(z)$ such that $\sum_{i=1}^n f_i(z)(z c_i - d_i) = 0$. Without loss of generality, assume $f_i(z) = \frac{g_i(z)}{k(z)}$ for $i \in \{1, 2, \ldots, n\}$, where $g_i(z), b_i(z) \in \mathbb{F}_{2^n}[z]$. Thus, $\sum_{i=1}^n g_i(z)(z c_i - d_i) = 0$. Let $k = \max_{i \in \{1, 2, \ldots, n\}} |d_i|$, and assume $g_i(z) = \sum_{t=0}^{k} a_{i,t}z^t$. Then, it follows

$$\sum_{i=1}^n g_i(z)(z c_i - d_i) = \sum_{i=1}^n \sum_{t=0}^{k-1} (a_{i,t}z^{t+1}c_i - a_{i,t}z^td_i) = -z^{k+1} \sum_{i=1}^n a_{i,k}c_i + \sum_{i=1}^n \sum_{l=0}^{k-1} (a_{i,l}c_i - a_{i+l,1}d_i).$$

Therefore, the following equations must hold:

$$\sum_{i=1}^n a_{i,k}c_i = 0 \quad \sum_{i=1}^n a_{i,0}d_i = 0$$

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

Then, there must be an $n \times n$ invertible submatrix in $zC - D$. Without loss of generality, assume this submatrix consists of the top $n$ rows of $zC - D$ and denote this submatrix by $E_{n+1}$. Let $b$ denote the $(n+1)$th row of $zC - D$. In order to get a non-zero solution to equation (36), we first fix $r_{n+1}(z) = -1$. Therefore, equation (36) is transformed into $(r_1(z), \ldots, r_n(z))E_{n+1} = b$. Let $E_i$ denote the submatrix acquired by replacing the $i$th row of $E_{n+1}$ with $b$. Hence, we get a non-zero solution to (36), $r(z) = (\det E_1, \ldots, \det E_{n+1}, -1)$. Moreover, $r(z) = (\det E_1, \ldots, \det E_{n+1}, -\det E_{n+1})$ is also a solution. Note that the degree of $z$ in each det $E_i$ is at most $n$. Thus, $r(z)$ can be formulated as $(1, z, \ldots, z^n)\mathbf{F}$, where $\mathbf{F}$ is an $(n+1) \times (n+1)$ matrix. Since $\text{rank}(zC - D) = n$, all the solutions to equation (36) form a one-dimensional linear space. Thus, all solutions must be linearly dependent on $r(z)$. $\blacksquare$

Based on Lemma B.2, we can easily derive that each $V_1$ satisfying Eq. (10) is related to $V_1^*$ through a transform equation, as defined in Lemma VI.3

Proof of Lemma VI.3 Let $r_i$ be the $i$th row of $V_1$, which satisfies Eq. (10). According to Lemma B.2, $r_i$ must have the form $f_i(\eta(x^i))(1, \eta(x^i), \ldots, \eta^n(x^i))\mathbf{F}$, where $f_i(z)$ is a non-
zero rational function in \( F_{2m}(z) \). Hence, \( V_1 \) can be written as \( GV_1^*F \). Moreover, Eq. (56) can be rewritten as follows:

\[
(z, z^2, \ldots, z^{n+1})FC = (1, z, \ldots, z^n)FBA
\]

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

Now assume the coupling relation \( p_i(x) = f(\eta(x)) \in S_i' \) holds for the network. We will prove that \( S_i' \) is violated for \( n > 1 \), and thus it is impossible for the three unicast sessions to asymptotically achieve the rate tuple \((\frac{1}{2}, \frac{1}{2}, \frac{1}{2})\) via PBNA. Without loss of generality, assume \( f(z) = \sum_{k=0}^{n-1} a_k z^k \) and \( g(z) = \sum_{k=0}^{n-1} b_k z^k \). Apparently, if \( \text{rank}(V_1) < n+1 \), \( S_i' \) is violated. Thus, in the rest of this proof, we assume \( \text{rank}(V_1) = n+1 \). By Lemma VI.3, \( V_1 = GV_1^*F \), where \( F \) is an \((n+1) \times (n+1)\) invertible matrix. The \( j \)th row of \( V_1 \) is \( r_j = f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^n(x^j))F \). Since the \((n+1)\)th row of \( FC \) is zero, we have \( r_j C = f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^n(x^j))H \), where \( H \) consists of the top \( n \) rows of \( FC \) and \( \text{rank}(H) = n \). Let \( a = (a_0, a_1, \ldots, a_{n-1})^T \) and \( b = (b_0, b_1, \ldots, b_{n-1})^T \). For \( i = 1, 2 \), we define \( a' = F^{-1}a \) and \( b' = H^{-1}b \). It follows

\[
r_j a' = f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^n(x^j))Fa' = f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^n(x^j))a = f_j(\eta(x^j))f(\eta(x^j)) = f_j(\eta(x^j))p_i(\eta(x^j))\eta(\eta(x^j)) = p_i(\eta(x^j))f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^{n-1}(x^j))b = p_i(\eta(x^j))x f_j(\eta(x^j))(1, \eta(x^j), \ldots, \eta^{n-1}(x^j))Hb' = p_i(\eta(x^j))r_j Cb'
\]

Hence, the columns of \( V_1 - P, V_1 \)C \) are linearly dependent, violating \( S_i' \). Similarly, we can prove the case of \( i = 3 \).

APPENDIX C

PROOFS OF INTERPRETATIONS OF FEASIBILITY CONDITIONS OF PBNA

A. \( \eta(x) = 1 \)

First, note that \( \eta(x) \) can be rewritten as a ratio of two rational functions \( \eta(x) = \frac{f_{31}(x)}{f_{312}(x)} \), where \( f_{ij}(x) \triangleq \frac{m_{ij}(x)m_{jk}(x)}{m_{ik}(x)} \). Hence, in order to interpret \( \eta(x) = 1 \), we first study the properties of \( f_{ij}(x) \).

The following lemma is to be used to derive the general structure of \( f_{ijk}(x) \). Basically, it provides an easy method to calculate the greatest common divisor of two transfer functions with one common starring edge or ending edge.

**Lemma C.1.** The following statements hold:

1) For \( e_1, e_2, e_3 \in E' \) such that \( e_2, e_3 \) are both downstream of \( e_1 \). Let \( e \) be the last edge of the topological ordering of the edges in \( C_{e_1e_2} \cap C_{e_2e_3} \). Then \( m_{e_1e}(x) = \gcd(m_{e_1e_2}(x), m_{e_2e_3}(x)) \).

2) For \( e_1, e_2, e_3 \in E' \) such that \( e_1, e_2 \) are both upstream of \( e_3 \). Let \( e \) be the first edge of the topological ordering of the edges in \( C_{e_1e_3} \cap C_{e_2e_3} \). Then \( m_{e_2e}(x) = \gcd(m_{e_1e_3}(x), m_{e_2e_3}(x)) \).

**Proof:**

- **Case 1:** For \( e_1, e_2, e_3 \in E' \) such that \( e_2, e_3 \) are both downstream of \( e_1 \). Let \( e \) be the last edge of the topological ordering of the edges in \( C_{e_1e_2} \cap C_{e_2e_3} \). Then \( m_{e_1e}(x) = \gcd(m_{e_1e_2}(x), m_{e_2e_3}(x)) \).

- **Case 2:** For \( e_1, e_2, e_3 \in E' \) such that \( e_1, e_2 \) are both upstream of \( e_3 \). Let \( e \) be the first edge of the topological ordering of the edges in \( C_{e_1e_3} \cap C_{e_2e_3} \). Then \( m_{e_2e}(x) = \gcd(m_{e_1e_3}(x), m_{e_2e_3}(x)) \).

**Corollary C.1.** \( f_{ijk}(x) \) can be formulated as

\[
f_{ijk}(x) = \frac{m_{\sigma_j,\tau_j}(x)m_{\alpha_{ijk},\tau_j}(x)}{m_{\alpha_{ijk},\beta_{ijk}}(x)}(47)
\]

where \( \gcd(m_{\sigma_j,\tau_j}(x)m_{\alpha_{ijk},\tau_j}(x), m_{\alpha_{ijk},\beta_{ijk}}(x)) = 1 \).

**Proof:**

\[
f_{ijk}(x) = \frac{m_{\sigma_j,\alpha_{ijk}}(x)m_{\alpha_{ijk},\tau_j}(x)m_{\beta_{ijk}}(x)}{m_{\sigma_j,\beta_{ijk}}(x)m_{\alpha_{ijk},\tau_j}(x)}(47)
\]

By Lemma , \( \gcd(m_{\sigma_j,\tau_j}(x), m_{\alpha_{ijk},\tau_j}(x)) = 1 \) and thus \( \gcd(m_{\sigma_j,\beta_{ijk}}(x), m_{\alpha_{ijk},\tau_j}(x)) = 1 \). Meanwhile, \( \gcd(m_{\sigma_j,\alpha_{ijk}}(x), m_{\alpha_{ijk},\beta_{ijk}}(x)) = 1 \). Hence, we must have \( \gcd(m_{\sigma_j,\alpha_{ijk}}(x)m_{\alpha_{ijk},\tau_j}(x), m_{\alpha_{ijk},\beta_{ijk}}(x)) = 1 \).

According to Corollary C.1, the structure of \( f_{ijk}(x) \) must fall into one of the two types, as shown in Fig. 10. In Fig. 10a, \( \alpha_{ijk} \neq \beta_{ijk} \) and \( f_{ijk}(x) \) is a rational function, the denominator of which is a non-constant polynomial \( m_{\alpha_{ijk},\beta_{ijk}}(x) \). On the other hand, when \( \alpha_{ijk} \in C_{jk} \) and thus \( \alpha_{ijk} = \beta_{ijk} \), as shown in Fig. 10b, \( f_{ijk}(x) \) becomes a polynomial \( m_{\sigma_j,\alpha_{ijk}}(x)m_{\alpha_{ijk},\tau_j}(x) \).
Moreover, using Corollary C.1, we can easily check whether two $f_{ijk}(x)$’s are equivalent, as shown in the next corollary. It is easy to see that Theorem V.3 is just a special case of this corollary.

**Corollary C.2.** Assume $i, j, k, i', k' \in \{1, 2, 3\}$ such that $i \neq j, j \neq k$ and $i' \neq j, j \neq k'$. $f_{ijk}(x) = f_{i'j'k'}(x)$ if and only if $\alpha_{ijk} = \alpha_{i'j'k'}$ and $\beta_{ijk} = \beta_{i'j'k'}$.

**Proof:** By Corollary C.1 if $\alpha_{ijk} = \alpha_{i'j'k'}$ and $\beta_{ijk} = \beta_{i'j'k'}$, we must have $f_{ijk}(x) = f_{i'j'k'}(x)$. Conversely, if $f_{ijk}(x) = f_{i'j'k'}(x)$, $m_{\alpha_{ijk}, \beta_{ijk}}(x) = m_{\alpha_{i'j'k'}, \beta_{i'j'k'}}(x)$. Thus $\alpha_{ijk} = \alpha_{i'j'k'}$ and $\beta_{ijk} = \beta_{i'j'k'}$ by Lemma A.2.

**B.** $p_1(x) = 1$ and $p_1(x) = \eta(x)$

Using Lemma A.1, we can easily prove Theorem V.4 as shown below.

**Proof of Theorem V.4.** Apparently, by Lemma A.1 and the definition of $p_1(x)$, $p_1(x) = 1$ if and only if the minimum cut separating $\sigma_1, \sigma_2$ from $\tau_1$ and $\tau_2$ is one, i.e., $C_{12,13} = 1$. In order to interpret $p_1(x) = \eta(x)$, we consider $q_1(x) = p_1(x) | q_1(x) = x_{\eta(x)} = m_{11}(x)m_{12}(x)$. Hence $p_1(x) = \eta(x)$ is equivalent to $q_1(x) = 1$. Similarly, using Lemma A.1 it is easy to see that $p_1(x) = \eta(x)$ if and only if the minimum cut separating $\sigma_1, \sigma_3$ from $\tau_1, \tau_2$ is one, i.e., $C_{13,12} = 1$.

**C.** $p_1(x) = \eta(x)$ and $p_2(x) = 1 + \eta(x)$

Note that the three coupling relations can be respectively reformulated in terms of $f_{ijk}(x)$ as follows:

\[
m_{11}(x) = f_{312}(x) + f_{213}(x)
\]

\[
m_{22}(x) = f_{123}(x) + f_{231}(x)
\]

\[
m_{33}(x) = f_{321}(x) + f_{132}(x)
\]

Thus, as shown above, the three coupling relations can also be interpreted by the properties of $f_{ijk}(x)$.

**Proof of Theorem V.5.** We only prove statement 1). The other statements can be proved similarly. First, we prove the “if” part. Due to $\alpha_{312} \in C_{12}$ and $\alpha_{213} \in C_{13}$, $f_{312}(x) = \sigma_{\alpha_{312}}(x)m_{\alpha_{312}, \tau_1}(x)$ and $f_{213}(x) = \sigma_{\alpha_{213}}(x)m_{\alpha_{213}, \tau_1}(x)$. Hence, $f_{312}(x) + f_{213}(x) = \sigma_{\alpha_{312}}(x)m_{\alpha_{312}, \tau_1}(x) + \sigma_{\alpha_{213}}(x)m_{\alpha_{213}, \tau_1}(x)$. On the other hand, because $\alpha_{312} | \alpha_{213}$ and $\{\alpha_{312}, \alpha_{213}\}$ forms a cut which separates $\tau_1$, $m_{11}(x) = m_{\alpha_{312}}(x)m_{\alpha_{213}, \tau_1}(x) + m_{\alpha_{213}}(x)m_{\alpha_{312}, \tau_1}(x)$ by Lemma A.4 Therefore, $m_{11}(x) = f_{312}(x) + f_{213}(x)$.

Next we prove the “only if” part. Assume $m_{11}(x) = f_{312}(x) + f_{213}(x)$. If $\alpha_{312} \notin C_{12}$ but $\alpha_{213} \in C_{13}$, $f_{312}(x)$ is a rational function whose denominator is non-constant polynomial, while $f_{213}(x)$ is a polynomial. Hence $f_{312}(x) + f_{213}(x)$ must be a rational function with non-constant denominator, and thus $m_{11}(x) \neq f_{312}(x) + f_{213}(x)$. Similarly, if $\alpha_{312} \in C_{12}$ but $\alpha_{213} \notin C_{13}$, we can also prove that $m_{11}(x) \neq f_{312}(x) + f_{213}(x)$.

Now assume $\alpha_{312} \notin C_{12}$ and $\alpha_{213} \notin C_{13}$. It follows that $f_{312}(x) = m_{\alpha_{312}, \beta_{213}}(x)m_{\alpha_{213}, \tau_1}(x)$ and $f_{213}(x) = m_{\alpha_{213}, \beta_{312}}(x)m_{\alpha_{312}, \tau_1}(x)$. Because $\eta(x) \neq 1$, we have $f_{312}(x) \neq f_{213}(x)$, which indicates that $\alpha_{312} \neq \alpha_{213}$ or $\beta_{312} \neq \beta_{213}$ by Corollary C.2 and $m_{\alpha_{312}, \beta_{312}}(x) \neq m_{\alpha_{213}, \beta_{213}}(x)$. Therefore, by Lemma A.3, one of the following cases must hold: 1) There exists an irreducible polynomial $m_{ee}(x)$ such that $m_{ee}(x) \mid m_{\alpha_{312}, \beta_{312}}(x)$ but $m_{ee}(x) \nmid m_{\alpha_{213}, \beta_{213}}(x)$; 2) there exists an irreducible polynomial $m_{ee}(x)$ such that $m_{ee}(x) \nmid m_{\alpha_{312}, \beta_{312}}(x)$ but $m_{ee}(x) \mid m_{\alpha_{213}, \beta_{213}}(x)$.

Consider case 1). Define the following polynomials: $f(x) = \text{lcm}(m_{\alpha_{312}, \beta_{312}}(x), m_{\alpha_{213}, \beta_{213}}(x))$ and $f_1(x) = f(x)/m_{\alpha_{312}, \beta_{312}}(x)$ and $f_2(x) = f(x)/m_{\alpha_{213}, \beta_{213}}(x)$.

This implies that $m_{ee}(x) \nmid m_{\alpha_{312}, \beta_{312}}(x)$ and $m_{ee}(x) \mid m_{\alpha_{213}, \beta_{213}}(x)$.

Similarly, for case 2), we can also prove that $m_{11}(x) \neq f_{312}(x) + f_{213}(x)$.

Thus, we have proved that $\alpha_{312} \notin C_{12}$ and $\alpha_{213} \notin C_{13}$. It immediately follows that $m_{11}(x) = m_{\alpha_{312}}(x)m_{\alpha_{213}, \tau_1}(x) + m_{\alpha_{213}}(x)m_{\alpha_{312}, \tau_1}(x)$. Hence each path $P$ in $P_{\tau_1, \tau_2}$ either pass through $\alpha_{312}$ or $\alpha_{213}$, implying that $\{\alpha_{312}, \alpha_{213}\}$ forms a cut separating $\tau_1$ from $\tau_2$. Moreover, according to Lemma A.4, $\alpha_{312} \nmid \alpha_{213}$.

**APPENDIX D**

**Proofs of Lemmas on Multivariate Polynomials**

In this section, we present the proof of Lemma B.1. We first prove that Lemma B.1 holds for the case where $s(x)$ and $t(x)$ are both univariate polynomials. In order to extend this result to multivariate polynomials, we employ a simple idea that each multivariate polynomial can be viewed as an equivalent univariate polynomial on a field of rational functions. Specifically, we prove that the problem of checking if two multivariate polynomials are co-prime is equivalent to checking if their equivalent univariate polynomials are co-prime. Finally, based on this result, we prove that Lemma B.1 also holds for the multivariate case.

**A. The Univariate Case**

In the following lemma, we show that Lemma B.1 holds for the univariate case.

**Lemma D.1.** Let $F$ be a field, and $z, y$ are two variables. Consider four non-zero polynomials $f(z), g(z) \in F[z]$ and $s(y), t(y) \in F[y]$, such that $\gcd(f(z), g(z)) = 1$ and $\gcd(s(y), t(y)) = 1$. Denote $d = \max\{d_z, d_y\}$. Define two polynomials $\alpha(y) = f^{(d_y)}(y)$ and $\beta(y) = g^{(d_y)}(y)$. Then $\gcd(\alpha(y), \beta(y)) = 1$.

**Proof:** Assume $w(x) = \gcd(\alpha(x), \beta(x))$ is non-trivial. Thus we can find an extension field $\tilde{F}$ of $F$ such that

\[7\text{We use lcm}(f(x), g(x)) to denote the least common multiple of two polynomials f(x) and g(x).}
there exists \( x_0 \in \mathbb{F} \) 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 \( \mathbb{F} \). Note that \( \gcd(f(z), g(z)) = 1 \) and \( \gcd(s(x), t(x)) = 1 \) also hold for \( \mathbb{F} \). Assume \( t(x_0) = 0 \) and thus \( x - x_0 \) \( \parallel \) \( t(x) \). Since \( \gcd(s(x), t(x)) = 1 \), it follows that \( x - x_0 \) \( \parallel \) \( s(x) \) and thus \( s(x_0) \neq 0 \). Hence, either \( \alpha(x_0) \neq 0 \) or \( \beta(x_0) \neq 0 \), contradicting that \( \alpha(x_0), \beta(x_0) \) are both zeros. Hence, we have proved that \( t(x_0) \neq 0 \). Then we have \( f \left( \frac{s(x_0)}{t(x_0)} \right) = 0 \) and \( g \left( \frac{s(x_0)}{t(x_0)} \right) = 0 \), which implies that \( z - \frac{s(x_0)}{t(x_0)} \) is a common divisor of \( f(z) \) and \( g(z) \), contradicting \( \gcd(f(z), g(z)) = 1 \). Thus, we have proved that \( \gcd(\alpha(y), \beta(y)) = 1 \).

\[ \text{Let } g(y_i) \in \mathbb{F}[y_i]. \text{ It follows} \]
\[ \gcd(g(y_i), f_1(y), \ldots, f_l(y)) = \gcd(g(y_i), f_{01}(y_1), \ldots, f_{pl}(y_l), \ldots, f_{s0}(y_1), \ldots, f_{sp}(y_l)) \]

**Proof:** We have the following equations
\[ \gcd(g(y_1), f_1(y), \ldots, f_l(y)) = \gcd(g(y_1), f_{01}(y_1), \ldots, f_{pl}(y_l)) \]
\[ = \gcd(g(y_1), f_{01}(y_1), \ldots, f_{pl}(y_l), f_{02}(y_2), \ldots, f_{sp}(y_l)) \]
\[ = \gcd(g(y_1), f_{01}(y_1), \ldots, f_{pl}(y_l), \ldots, f_{s0}(y_1), \ldots, f_{sp}(y_l)) \]

**Lemma D.3.** For \( t \in \{1, 2, \ldots, s\} \), let \( a_t(y), b_t(y) \in \mathbb{F}[y] \) such that \( b_t(y) \neq 0 \) and \( \gcd(a_t(y), b_t(y)) = 1 \). For \( t \in \{1, 2, \ldots, s\} \), let \( v_t(y) = \text{lcm}(b_1(y), \ldots, b_t(y)) \). Then we have
\[ \gcd \left( a_1(y), v_1(y), \ldots, a_s(y), v_s(y) \right) = 1 \]

**Proof:** We use induction on \( s \) to prove this lemma. Apparently, the lemma holds for \( s = 1 \) due to \( \gcd(a_1(y), b_1(y)) = 1 \). Assume it holds for \( s - 1 \). Thus it follows
\[ \gcd \left( a_1(y), v_1(y), \ldots, a_{s-1}(y), v_{s-1}(y), v_s(y) \right) \]
\[ = \gcd \left( a_1(y), v_1(y), \ldots, a_{s-1}(y), v_{s-1}(y), v_s(y) \right) \]
\[ = \gcd \left( a_1(y), v_1(y), \ldots, a_{s-1}(y), v_{s-1}(y), v_s(y) \right) \]
\[ = \gcd \left( a_1(y), v_1(y), \ldots, a_{s-1}(y), v_{s-1}(y), v_s(y) \right) \]

\[ = \gcd \left( a_1(y), v_1(y), \ldots, a_{s-1}(y), v_{s-1}(y), v_s(y) \right) \]

**Corollary D.2.** For \( t \in \{1, 2, \ldots, s\} \), let \( f_t(y) \in \mathbb{F}[y] \) be defined as \( f_t(y) = \sum_{j=0}^{p_t} f_{i_j}(y_j)y_j^{q_t} \), where \( f_{i_j}(y_j) \in \mathbb{F}[y_j] \).

**Proof:** Note that any divisor of \( g(y_i) \) must be a polynomial in \( \mathbb{F}[y_i] \). Let \( d(y_i) = \gcd(g(y_i), f_i(y_i)) \) and \( d_i(y_i) = \gcd(g(y_i), f_0(y_i), \ldots, f_{p_i}(y_i)) \). By Lemma D.2,
\[ d_i(y_i) \mid f_j(y_i) \text{ for any } j \in \{0, 1, \ldots, p_i\}, \text{ implying that} \]
\[ d_i(y_i) \mid d(y_i). \text{ On the other hand,} \]
\[ d_i(y_i) \mid f_i(y_i) \text{ and thus} \]
\[ d_i(y_i) \mid d(y_i). \text{ Hence,} \]
\[ d_i(y_i) = d(y_i). \]

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

In general, each polynomial \( h(y_i) \in \mathbb{F}[y_i][y] \) is of the form \( h(y_i) = a_0(y_i) + a_1(y_i) y_i + \cdots + a_p(y_i) y_i^p \), where for each \( j \in \{0, 1, \ldots, p\} \), \( a_j(y_i), b_j(y_i) \in \mathbb{F}[y_i] \), \( b_j(y_i) \neq 0 \), \( \gcd(a_j(y_i), b_j(y_i)) = 1 \), and \( a_p(y_i) \neq 0 \). Note that for each \( y_i^t \) which is absent in \( h(y_i) \), we let \( a_j(y_i) = 0 \) and \( b_j(y_i) = 1 \). Moreover, define the following polynomial \( \mu_h(y_i) = \text{lcm}(b_0(y_i), b_1(y_i), \ldots, b_p(y_i)). \)

**Corollary D.3.** For \( j \in \{1, 2, \ldots, s\} \), let \( f_j(y_i) \in \mathbb{F}[y_i][y_j] \). Define \( v(y_i) = \text{lcm}(\mu_{f_j}(y_i), \ldots, \mu_{f_j}(y_i)) \) and \( \bar{f}_j(y) = v(y_i)f_j(y_i) \). Thus \( \gcd(v(y_i), \bar{f}_j(y_i)) = 1 \).

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

\[
\bar{f}_j(y) = \sum_{i=1}^{p_j} a_{ij}(y_i) y_i^{t_j} \]

where for any \( j \in \{1, 2, \ldots, s\} \) and \( t \in \{0, 1, \ldots, p_j\} \), \( a_{ij}(y_i), b_{ij}(y_i) \in \mathbb{F}[y_i] \), \( b_{ij}(y_i) \neq 0 \) and \( \gcd(a_{ij}(y_i), b_{ij}(y_i)) = 1 \). Apparently, \( v(y_i) \) is the least common multiple of all \( b_{ij}(y_i) \)'s. Define \( u_{ij}(y_i) = \frac{u_{ij}(y_i)}{b_{ij}(y_i)} \in \mathbb{F}[y_i] \). Hence, we have \( \bar{f}_j(y) = \sum_{i=1}^{p_j} a_{ij}(y_i) u_{ij}(y_i) y_i^{t_j} \). Then it follows:

\[
\gcd(v(y_i), \bar{f}_j(y_i), \ldots, \bar{f}_j(y)) = \gcd(v(y_i), a_{i0}(y_i) u_{i0}(y_i), \ldots, a_{ip}(y_i) u_{ip}(y_i), \ldots, a_{i0}(y_i) u_{i0}(y_i), \ldots, a_{ip}(y_i) u_{ip}(y_i)) \]

\[
= 1
\]

where (a) is due to Corollary D.2 and (b) follows from Lemma D.3.

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

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

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

Then, assume \( \gcd(f(y), g(y)) = 1 \) and we also use contradiction to prove that for any \( i \in \{1, 2, \ldots, k\} \), \( \gcd(f(y), g(y_i)) = 1 \). Assume there exists \( i \in \{1, 2, \ldots, k\} \) such that \( v(y_i) = \gcd(f(y_i), g(y_i)) \) is non-trivial. Define \( w(y) = \mu_{v_i}(y_i) v(y_i) \in \mathbb{F}[y] \). Clearly, \( w(y_i) | f(y_i) \) and \( w(y_i) | g(y_i) \). Thus, there exists \( p(y_i), q(y_i) \in \mathbb{F}[y_i][y_i] \) such that

\[
f(y_i) = w(y_i)p(y_i) \quad g(y_i) = w(y_i)q(y_i)
\]

Let \( s(y_i) = \text{lcm}(\mu_{v_i}(y_i), \mu_{q_i}(y_i)) \). Define \( \bar{p}(y) = s(y_i)p(y_i) \) and \( \bar{q}(y) = s(y_i)q(y_i) \). Apparently, \( \bar{p}(y), \bar{q}(y) \in \mathbb{F}[y] \). It follows that

\[
s(y_i)f(y) = w(y_i)\bar{p}(y) \quad s(y_i)g(y) = w(y_i)\bar{q}(y)
\]

Then the following equation holds

\[
s(y_i)\gcd(f(y), g(y)) = w(y_i)\gcd(\bar{p}(y), \bar{q}(y))
\]

Due to Corollary D.3, \( \gcd(s(y_i), \gcd(\bar{p}(y), \bar{q}(y))) = \gcd(s(y_i), \bar{p}(y), \bar{q}(y)) = 1 \). Hence \( s(y_i) | w(y_i) \). Let \( \bar{w}(y) = \frac{w(y)}{w(y_i)} \). According to Lemma D.2, \( \bar{w}(y) \) is a non-trivial polynomial in \( \mathbb{F}[y] \). Thus, \( \bar{w}(y) | \gcd(f(y), g(y)) \), contradicting \( \gcd(f(y), g(y)) = 1 \).

**C. The Multivariate Case**

Now, we are in the place of extending Lemma D.1 to the multivariate case.
Proof of Lemma D.1. Note that if we substitute $F$ with $F(y_i)$ and gcd with $gcd_1$ in Lemma D.1, the lemma also holds. Apparently, $f(z), g(z) \in F(y_i)[z]$. We will prove that $gcd_1(f(z), g(z)) = 1$. By contradiction, assume $r(z) = gcd_1(f(z), g(z)) \in F(y_i)[z]$ is non-trivial. Let $f(z) = \frac{f_1(z)}{r(z)}$ and $g(z) = \frac{g_1(z)}{r(z)}$. Clearly, $f(z)$ and $g(z)$ are both non-zero polynomials in $F(y_i)[z]$. Then we can find an assignment to $y_i$, denoted by $y_i^*$, such that the coefficients of the maximum powers of $z$ in $r(z), f(z)$ and $g(z)$ are all non-zeros. Let $r(z)$ denote the univariate polynomial acquired by assigning $y_i = y_i^*$ to $r(z)$. Clearly, $r(z)$ is a common divisor of $f(z)$ and $g(z)$ in $F[z]$, contradicting $gcd(f(z), g(z)) = 1$. Moreover, due to $gcd(s(y), t(y)) = 1$ and Theorem D.2, $gcd_1(s(y_i), t(y_i)) = 1$. Thus, by Lemma D.1, $gcd_1(\alpha(y_i), \beta(y_i)) = 1$. Since $i$ can be any integer in $\{1, 2, \ldots, k\}$, it follows that $gcd(\alpha(y), \beta(y)) = 1$ by Theorem D.2.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” IEEE Trans. Inform. Theory, vol. 46, pp. 1204–1216, 2000.
[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.
[3] R. Koetter and M. Médard, “An algebraic approach to network coding,” IEEE/ACM Trans. Networking, vol. 11, pp. 782–795, 2003.
[4] Z. Li and B. Li, “Network coding: The case of multiple unicast sessions,” in the Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing, 2004.
[5] A. Ramaswami-Lehman and E. Lehman, “Complexity classification of network information flow problems,” in 15th Annual ACM-SIAM SODA.
[6] S. Rouillier, “Linear versus non-linear boolean functions in network flow,” in Proc. of CISS.
[7] M. Médard, M. Effros, T. Ho, and S. Karger, “On coding for non-multicast networks,” in Proc. of 41st Allerton Conference, Oct 2003.
[8] R. Dougherty, C. Freiling, and K. Zeger, “Linearity and solvability in multicast networks,” Proc. CISS, 2004.
[9] F. Kschischang and R. Koetter, “Coding for errors and erasures in random network coding,” [arXiv:0709.0651v2].
[10] A. R. Lehman and E. Lehman, “Complexity classification of network information flow problems,” in Proceedings of the fifteenth annual ACM-SIAM symposium on Discrete algorithms, pp. 142–150.
[11] N. Ratnakar, R. Koetter, and T. Ho, “Linear flow equations for network coding in the multiple unicast case,” in Proc. DIMACS Working Group Network Coding.
[12] 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. IEEE ISIT 2006.
[13] M. Kim, M. Médard, U.-M. O'Reilly, and D. Traskov, “An evolutionary approach to inter-session network coding,” in IEEE INFOCOM, 2009, pp. 450–458.
[14] V. R. Cadambe and S. A. Jafar, “Interference alignment and the degrees of freedom for the k-user interference channel,” IEEE Transactions on Information Theory, vol. 54, no. 8, pp. 3425–3441, August 2008.
[15] T. M. Cover and J. A. Thomas, Elements of Information Theory, Wiley Series in Telecommunications, 1991.
[16] 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 on Communication, Control, and Computing, 2010, pp. 1054–1061.
[17] Z. Li, B. Li, and L. C. Lau, “On achieving maximum multicast throughput in undirected networks,” IEEE/ACM Transactions on Networking (TON), vol. 14, pp. 2467–2485, 2006.
[18] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” IEEE Transactions on Information Theory, vol. 51, no. 6, pp. 1973–1982, 2005.
[19] 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 Transactions on Information Theory, vol. 52, no. 10, pp. 4413–4430, 2006.