

# Two-Unicast Two-Hop Interference Network: Finite-Field Model

Song-Nam Hong  
Dep. of Electrical Engineering  
University of Southern California  
CA, USA  
Email: songnamh@usc.edu

Giuseppe Caire  
Dep. of Electrical Engineering  
University of Southern California  
CA, USA  
Email: caire@usc.edu

**Abstract**—In this paper we present a novel framework to convert the  $K$ -user multiple access channel (MAC) over  $\mathbb{F}_{p^m}$  into the  $K$ -user MAC over ground field  $\mathbb{F}_p$  with  $m$  multiple inputs/outputs (MIMO). This framework makes it possible to develop coding schemes for MIMO channel as done in symbol extension for time-varying channel. Using aligned network diagonalization based on this framework, we show that the sum-rate of  $(2m-1) \log p$  is achievable for a  $2 \times 2 \times 2$  interference channel over  $\mathbb{F}_{p^m}$ . We also provide some relation between field extension and symbol extension.

## I. INTRODUCTION

In recent years, significant progress has been made on the understanding of the theoretical limits of wireless communication networks. In [1], the capacity of multiple multicast network (where every destination desires all messages) is approximated within a constant gap independent of SNR and of the realization of the channel coefficients. Also, for multiple flows over a single hop, new capacity approximations were obtained in the form of degrees of freedom (DoF), generalized degrees of freedom (GDoF), and  $O(1)$  approximations [2]–[4]. Yet, the study of multiple flows over multiple hops remains largely unsolved. The  $2 \times 2 \times 2$  Gaussian interference channel (IC) has received much attention recently, being one of the fundamental building blocks to characterize the DoFs of two-flows networks [5]. The optimal DoF was obtained in [6] using *aligned interference neutralization*, which appropriately combines interference alignment and interference neutralization. Also, there was the recent extension to the  $K \times K \times K$  Gaussian IC in [7], achieving the optimal  $K$  DoF using *aligned network diagonalization*.

In this paper we investigate interference networks over finite-field. This model can be meaningful in practical wireless communication systems, by the observation that the main bottleneck of a digital receiver is the Analog-to-Digital Conversion (ADC), which is power-hungry, and does not scale with Moore's law. Rather the number of bits per second produced by an ADC is roughly a constant that depends on the power consumption [8]. Therefore, it makes sense to consider the ADC as part of channel, which may produce the finite-field model, as shown in [10]. Also, Compute-and-Forward (CoF) in [11] enables to decode linear combinations of messages over finite-field at relays. By forwarding linear combinations,

the overall end-to-end “transfer function” between sources and destinations can be described by a system of linear equations over finite-field. Each destination can solve such equations to obtain desired messages as long as there exists a full-rank sub-system of equations involving the desired messages. In the setting of multiple flows (inference) over multiple hops, interference alignment (or neutralization and diagonalization) over finite-field is generally needed. However, current schemes developed for Gaussian channel may not be straightforwardly applicable for finite-field interference networks. For example, it is not so clear to apply the framework of real interference alignment [9] based on rational dimensions to finite-field interference networks.

**Our Contribution:** We show that the  $K$ -user multiple access channel (MAC) over  $\mathbb{F}_{p^m}$  is equivalent to the  $K$ -user MAC over  $\mathbb{F}_p$  with  $m$  multiple inputs/outputs (MIMO). In the transformed MIMO channel, the  $m \times m$  channel matrices are represented by the powers of *companion matrix* of primitive element of  $\mathbb{F}_{p^m}$ . This framework makes it possible to develop coding schemes for MIMO channel as done in symbol extension for time-varying channel. Next, we focus on a  $2 \times 2 \times 2$  IC over  $\mathbb{F}_{p^m}$  and show that the sum-rate of  $(2m-1) \log p$  is achievable by applying the concept of aligned network diagonalization to the transformed MIMO channel, under certain condition on channel coefficients. We also prove that this condition is satisfied with probability 1 if the channel coefficients are uniformly and independently drawn from non-zero elements of  $\mathbb{F}_{p^m}$  and either  $m$  or  $p$  goes to infinity. In addition, we consider the  $2 \times 2 \times 2$  MIMO IC over  $\mathbb{F}_p$  and show that symbol extension (i.e., coding over multiple time slots) is needed for the aligned network diagonalization scheme. We characterize the required symbol extension order (number of time slots over which coding takes place) that depends on the channel coefficients and is upper-bounded by the number of inputs/outputs.

## II. MIMO TRANSFORM OVER GROUND FIELD

Throughout the paper, it is assumed that  $\mathbb{F}_{p^m}$  denotes a finite-field of order  $p^m$ , generated by a primitive polynomial  $\pi(x) \triangleq a_0 + a_1x + \dots + a_{m-1}x^{m-1} + x^m$ . The elements of  $\mathbb{F}_{p^m}$  are given by the polynomial representation  $\{b_0 + b_1x + \dots + b_{m-1}x^{m-1} : b_0, \dots, b_{m-1} \in \mathbb{F}_p\}$ . Also, we can

represent the elements of  $\mathbb{F}_{p^m}$  using primitive element  $\alpha$  as  $\{0 = \alpha^\infty, 1 = \alpha^0, \alpha, \dots, \alpha^{p^m-2}\}$ . As usual,  $\mathbb{F}_{p^m}^*$  denotes the multiplicative group of  $\mathbb{F}_{p^m}$ , i.e., the set of non-zero elements of  $\mathbb{F}_{p^m}$ .

**Definition 1:** The *companion matrix* of the polynomial  $\pi(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1} + x^m$  is defined to be  $m \times m$  matrix over  $\mathbb{F}_p$

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \cdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}.$$

Then,  $\mathcal{M} \triangleq \{0 = \mathbf{C}^\infty, \mathbf{I} = \mathbf{C}^0, \mathbf{C}, \dots, \mathbf{C}^{p^m-2}\}$  forms a finite-field of order  $p^m$ . From [12, Theorem 6], all finite fields of order  $p^m$  are isomorphic<sup>1</sup>. Then, we have one-to-one mappings:

- Vector representation (i.e., one-to-one mapping between polynomials and  $m$ -dimensional vectors over  $\mathbb{F}_p$ ):

$$\Phi(b_0 + b_1x + \dots + b_{m-1}x^{m-1}) = [b_0, \dots, b_{m-1}]^T. \quad (1)$$

- Matrix representation (i.e., one-to-one mapping between elements of  $\mathbb{F}_{p^m}$  and matrices over  $\mathbb{F}_p$ ):

$$\Psi(\alpha^\ell) = \mathbf{C}^\ell. \quad (2)$$

With these mappings, we have:

**Lemma 1:** For  $\mathcal{X}_k \in \mathbb{F}_{p^m}$ , let  $\mathcal{Y} = \sum_{k=1}^K q_k \mathcal{X}_k$  for some coefficients  $q_k \in \mathbb{F}_{p^m}$ . Also, set  $\mathbf{y} = \sum_{k=1}^K \mathbf{Q}_k \mathbf{x}_k$  where  $\mathbf{x}_k = \Phi(\mathcal{X}_k) \in \mathbb{F}_p^m$  and  $\mathbf{Q}_k = \Psi(q_k) \in \mathbb{F}_p^{m \times m}$  for  $k = 1, \dots, K$ . Then, we have  $\mathbf{y} = \Phi(\mathcal{Y})$ . ■

The above lemma shows that the  $K$ -user *scalar* MAC over  $\mathbb{F}_{p^m}$  can be transformed into the  $K$ -user MIMO MAC over ground field  $\mathbb{F}_p$  where all nodes have  $m$  multiple inputs/outputs.

### III. TWO-UNICAST TWO-HOP IC OVER $\mathbb{F}_{p^m}$

We consider a  $2 \times 2 \times 2$  IC over  $\mathbb{F}_{p^m}$  where all nodes have a single input/output. Notice that CoF framework produces a *noiseless* finite-field IC, while the symbol-by-symbol sampling (i.e., taking the ADC as part of channel) results in a finite-field IC with additive noise [10]. In this paper we only consider a *noiseless* model by focusing on interference management. In the first hop, the IC over  $\mathbb{F}_{p^m}$  is described by

$$\begin{bmatrix} \mathcal{Y}_1 \\ \mathcal{Y}_2 \end{bmatrix} = \begin{bmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{bmatrix} \begin{bmatrix} \mathcal{X}_1 \\ \mathcal{X}_2 \end{bmatrix} \quad (3)$$

and also, in the second hop, the IC over  $\mathbb{F}_{p^m}$  is described by

$$\begin{bmatrix} \mathcal{Y}_3 \\ \mathcal{Y}_4 \end{bmatrix} = \begin{bmatrix} q_{33} & q_{34} \\ q_{43} & q_{44} \end{bmatrix} \begin{bmatrix} \mathcal{X}_3 \\ \mathcal{X}_4 \end{bmatrix} \quad (4)$$

where  $\mathcal{X}_k \in \mathbb{F}_{p^m}, k = 1, 2, 3, 4$  and  $\mathcal{Y}_\ell \in \mathbb{F}_{p^m}, \ell = 1, 2, 3, 4$ . Here, the channel coefficients  $q_{\ell k} \in \mathbb{F}_{p^m}^*$  are fixed and known to all nodes. Also, it is assumed that each hop has full-rank  $2 \times 2$  channel matrices over  $\mathbb{F}_{p^m}$ .

<sup>1</sup>Two fields  $F, G$  are said to be *isomorphic* if there is a one-to-one mapping from  $F$  onto  $G$  which preserves addition and multiplication.

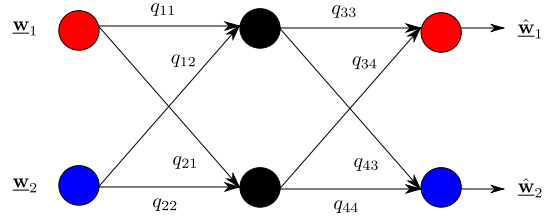


Fig. 1.  $2 \times 2 \times 2$  interference channel over  $\mathbb{F}_{p^m}$ .

**Definition 2:** The *minimal polynomial* over  $\mathbb{F}_p$  of  $\beta \in \mathbb{F}_{p^m}$  is the lowest degree monic polynomial  $\mu(x)$  with coefficients from  $\mathbb{F}_p$  such that  $\mu(\beta) = 0$ . We denote the degree of polynomial  $\mu(\beta)$  by  $\deg(\mu(\beta))$ . ■

With this definition, we have:

**Theorem 1:** For  $2 \times 2 \times 2$  IC over  $\mathbb{F}_{p^m}$ , the sum-rate of  $(2m - 1) \log p$  is achievable if  $\deg(\mu(\gamma)) = m$  and  $\deg(\mu(\gamma')) = m$  where

$$\gamma = q_{11}^{-1} q_{12} q_{22}^{-1} q_{21} \text{ and } \gamma' = s_{11}^{-1} s_{12} s_{22}^{-1} s_{21} \quad (5)$$

and

$$\begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} = \begin{bmatrix} q_{33} & q_{34} \\ q_{43} & q_{44} \end{bmatrix}^{-1}.$$

*Proof:* See Section III-A. ■

Also, we derive a normalized achievable sum-rate with respect to interference-free channel capacity  $m \log p$  when either  $m$  or  $p$  goes to infinity. This metric is analogous to degrees-of-freedom of Gaussian channels.

**Corollary 1:** If the channel coefficients  $q_{\ell k}$  are uniformly and independently drawn from  $\mathbb{F}_{p^m}^*$ , the following normalized sum-rates are achievable with probability 1:

$$d_{\text{sum}}(p) = \lim_{m \rightarrow \infty} \frac{R_{\text{sum}}(p, m)}{m \log p} = 2 \quad (6)$$

$$d_{\text{sum}}(m) = \lim_{p \rightarrow \infty} \frac{R_{\text{sum}}(p, m)}{m \log p} = \frac{2m - 1}{m} \quad (7)$$

where  $R_{\text{sum}}(p, m)$  denotes the achievable sum-rate for given finite-field  $\mathbb{F}_{p^m}$ .

*Proof:* The proof consists of showing that the conditions in Theorem 1 are satisfied with probability 1 in the limits. Let  $N(p, m)$  denote the number of *monic irreducible polynomials* of degree- $m$  over  $\mathbb{F}_p$ . From [12, Theorem 15], we have:

$$N(p, m) = \frac{1}{m} \sum_{d|m} \nu(d) p^{m/d}$$

where  $\nu(d)$  denotes the Möbius function, defined by

$$\nu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^r & \text{if } d \text{ is the product of } r \text{ distinct primes} \\ 0, & \text{otherwise.} \end{cases}$$

Notice that each degree- $m$  monic irreducible polynomial has  $m$  distinct roots in  $\mathbb{F}_{p^m}$  and is a degree- $m$  minimal polynomial of such roots. Thus, we have  $mN(p, m)$  distinct elements in  $\mathbb{F}_{p^m}$  with degree- $m$  minimal polynomial. Also, we can derive

a simple lower-bound on  $mN(p, m)$  by setting  $\nu(d) = -1$  for any  $d$  with  $d|m, d > 1$ :

$$mN(p, m) \geq p^m - \sum_{d|m, d>1} p^{m/d}.$$

Using this bound and the fact that  $\gamma$  defined in (5), is uniformly distributed over  $\mathbb{F}_{p^m}^*$ , we can compute:

$$\begin{aligned} \mathbb{P}(\{\deg(\mu(\gamma)) = m\}) &= \frac{mN(m, p)}{p^m - 1} \\ &\geq \frac{p^m - \sum_{d|m, d>1} p^{m/d}}{p^m} \\ &= 1 - \sum_{d|m, d>1} p^{m(1/d-1)}. \end{aligned}$$

This probability goes to 1 if either  $m$  or  $p$  goes to infinity. With the same procedures, we can also prove that  $\mathbb{P}(\{\deg(\mu(\gamma')) = m\})$  goes to 1 if either  $m$  or  $p$  goes to infinity. This completes the proof.  $\blacksquare$

*Remark 1:* We provide a brief comparison with the case of a  $2 \times 2 \times 2$  IC over  $\mathbb{F}_p$  with time varying channel and  $m$ -symbol extension. Similarly to the case of the degree- $m$  extension field, the symbol extension also yields a MIMO IC where  $m \times m$  channel matrices are the form of diagonal matrix with diagonal elements in  $\mathbb{F}_p^*$ . One may expect that the two MIMO channel models (namely, the one obtained by field extension and the other by symbol extension) are equivalent since they have about  $p^m$  possible channel matrices and these matrices belong to a commutative algebra (products of such matrices do not depend on the order of the factors). For the symbol extension, the same achievable scheme of Section III-A can be used under different feasibility conditions, namely, that the diagonal elements of the products of channel matrices (i.e.,  $\mathbf{Q} = \mathbf{Q}_{11}^{-1} \mathbf{Q}_{12} \mathbf{Q}_{22}^{-1} \mathbf{Q}_{21}$  in (9)) are distinct and non-zero [6]. We can compute the probability that this condition is satisfied. For  $p \rightarrow \infty$ , the condition is satisfied with probability 1, as for the case of field extension. However, when  $m \rightarrow \infty$  and  $p$  is finite, this probability is strictly less than 1, while we have seen before that in the field extension the feasibility probability goes to 1 also in this case. This shows that symbol extension and field extension are generally not equivalent.  $\diamond$

#### A. Proof of Theorem 1: Achievable scheme

We prove Theorem 1 using aligned network diagonalization, under the assumption that  $\gamma$  and  $\gamma'$  have degree- $m$  minimal polynomial. From Section II, we can transform the  $2 \times 2 \times 2$  scalar IC over  $\mathbb{F}_{p^m}$  in (3) and (4) into MIMO IC over  $\mathbb{F}_p$  with channel coefficients  $\mathbf{Q}_{\ell k} = \Psi(q_{\ell k}) \in \mathbb{F}_p^{m \times m}$ . Notice that  $\mathbf{Q}_{\ell k}$  is always full rank over  $\mathbb{F}_p$ . The proposed coding scheme is performed for the transformed MIMO channel and the one-to-one mapping  $\Phi(\cdot)$  is used to transmit coded messages via the channels. In order to transmit  $(2m-1)$  streams, source 1 sends  $m$  independent messages  $\{w_{1,\ell} \in \mathbb{F}_p : \ell = 1, \dots, m\}$  to destination 1 and source 2 sends  $m-1$  independent messages  $\{w_{2,\ell} \in \mathbb{F}_p : \ell = 1, \dots, m-1\}$  to destination 2. For simplicity, we also use the vector representation of messages as  $\mathbf{w}_1 = [w_{1,1}, \dots, w_{1,m}]^T$  and  $\mathbf{w}_2 = [w_{2,1}, \dots, w_{2,m-1}]^T$ .

*1) Encoding at the sources:* We let  $\mathbf{V}_1 = [\mathbf{v}_{1,1}, \dots, \mathbf{v}_{1,m}] \in \mathbb{F}_p^{m \times m}$  and  $\mathbf{V}_2 = [\mathbf{v}_{2,1}, \dots, \mathbf{v}_{2,m-1}] \in \mathbb{F}_p^{m \times m-1}$  denote the precoding matrices used at sources 1 and 2, respectively, chosen to satisfy the *alignment conditions*:

$$\begin{aligned} \mathbf{Q}_{11} \mathbf{v}_{1,\ell+1} &= \mathbf{Q}_{12} \mathbf{v}_{2,\ell} \\ \mathbf{Q}_{21} \mathbf{v}_{1,\ell} &= \mathbf{Q}_{22} \mathbf{v}_{2,\ell} \end{aligned} \quad (8)$$

for  $\ell = 1, \dots, m-1$ . For alignment, we use the construction method proposed in [6]:

$$\mathbf{v}_{1,\ell+1} = (\mathbf{Q}_{11}^{-1} \mathbf{Q}_{12} \mathbf{Q}_{22}^{-1} \mathbf{Q}_{21})^\ell \mathbf{v}_{1,1} \quad (9)$$

$$\mathbf{v}_{2,\ell} = (\mathbf{Q}_{22}^{-1} \mathbf{Q}_{21} \mathbf{Q}_{11}^{-1} \mathbf{Q}_{12})^{\ell-1} \mathbf{Q}_{22}^{-1} \mathbf{Q}_{21} \mathbf{v}_{1,1} \quad (10)$$

for  $\ell = 1, \dots, m-1$ . Using  $\Psi(\cdot)$  and  $\gamma$  defined in (5), the above constructions can be rewritten as

$$\mathbf{v}_{1,\ell+1} = \Psi(q_{11}^{-1} q_{12} q_{22}^{-1} q_{21})^\ell \mathbf{v}_{1,1} = \Psi(\gamma^\ell) \mathbf{v}_{1,1} \quad (11)$$

$$\mathbf{v}_{2,\ell} = \Psi(q_{22}^{-1} q_{21}) \Psi(\gamma^{\ell-1}) \mathbf{v}_{1,1} \quad (12)$$

for  $\ell = 1, \dots, m-1$ .

#### Encoding:

- Source  $k$  precodes its message over  $\mathbb{F}_p$  as  $\mathbf{x}_k = \mathbf{V}_k \mathbf{w}_k$  and produces the channel input

$$\mathcal{X}_k = \Phi^{-1}(\mathbf{x}_k) \in \mathbb{F}_{p^m}, \quad k = 1, 2. \quad (13)$$

Then,  $\mathcal{X}_1$  and  $\mathcal{X}_2$  are transmitted over channels.

*2) Relaying operations:* Relays decode linear combinations of source messages and forward the precoded linear combinations to destination.

#### Decoding:

- Relay 1 observes:

$$\mathcal{Y}_1 = q_{11} \mathcal{X}_1 + q_{12} \mathcal{X}_2 \in \mathbb{F}_{p^m}$$

and maps the received signal onto ground field  $\mathbb{F}_p$ :

$$\begin{aligned} \Phi(\mathcal{Y}_1) &= \mathbf{Q}_{11} \Phi(\mathcal{X}_1) + \mathbf{Q}_{12} \Phi(\mathcal{X}_2) \\ &= \mathbf{Q}_{11} \mathbf{V}_1 \mathbf{w}_1 + \mathbf{Q}_{12} \mathbf{V}_2 \mathbf{w}_2 \\ &\stackrel{(a)}{=} \mathbf{Q}_{11} \mathbf{V}_1 \underbrace{\begin{bmatrix} w_{1,1} \\ w_{1,2} + w_{2,1} \\ \vdots \\ w_{1,m} + w_{2,m-1} \end{bmatrix}}_{\triangleq \mathbf{u}_1} \end{aligned} \quad (14)$$

where (a) is due to the fact that precoding vectors satisfy the alignment conditions in (8). Since  $\mathbf{V}_1$  is full-rank over  $\mathbb{F}_p$  by Lemma 2, relay 1 can decode  $\mathbf{u}_1$  (i.e., linear combinations of source messages).

- Similarly, relay 2 observes the aligned signals over  $\mathbb{F}_p$ :

$$\begin{aligned} \Phi(\mathcal{Y}_2) &= \mathbf{Q}_{21} \Phi(\mathcal{X}_1) + \mathbf{Q}_{22} \Phi(\mathcal{X}_2) \\ &= \mathbf{Q}_{21} \mathbf{V}_1 \mathbf{w}_1 + \mathbf{Q}_{22} \mathbf{V}_2 \mathbf{w}_2 \\ &\stackrel{(a)}{=} \mathbf{Q}_{21} \mathbf{V}_1 \underbrace{\begin{bmatrix} w_{1,1} + w_{2,1} \\ \vdots \\ w_{1,m-1} + w_{2,m-1} \\ w_{1,m} \end{bmatrix}}_{\triangleq \mathbf{u}_2} \end{aligned} \quad (15)$$

where (a) is due to the fact that precoding vectors satisfy the alignment conditions in (8). Since  $\mathbf{V}_1$  is full-rank over  $\mathbb{F}_p$  by Lemma 2, relay 2 can decode  $\mathbf{u}_2$ .

*Lemma 2:* Assume that  $\deg(\mu(\gamma)) = m$ .  $\mathbf{V}_1$  has rank  $m$  if we choose  $\mathbf{v}_{1,1} = \Phi(1)$ .

*Proof:* Using  $\mathbf{v}_{1,1} = \Phi(1)$ , we have:

$$\Psi(\gamma^\ell)\mathbf{v}_{1,1} = \Phi(\Psi^{-1}(\Psi(\gamma)^\ell)\Phi^{-1}(\mathbf{v}_{1,1})) = \Phi(\gamma^\ell). \quad (16)$$

From (11) and (16), the precoding matrix  $\mathbf{V}_1$  can be written as

$$\begin{aligned} \mathbf{V}_1 &= [\mathbf{v}_{1,1}, \dots, \mathbf{v}_{1,m}] \\ &= [\Phi(1), \Phi(\gamma), \Phi(\gamma^2), \dots, \Phi(\gamma^{m-1})]. \end{aligned}$$

Since  $\gamma$  is assumed to have degree- $m$  minimal polynomial, the following holds:

$$b_0 + b_1\gamma + \dots + b_{m-1}\gamma^{m-1} \neq \mathbf{0}$$

for any non-zero coefficients vector  $(b_0, \dots, b_{m-1}) \in \mathbb{F}_p^m$ . Using this, we can prove that  $\mathbf{V}_1$  has  $m$  linearly independent columns:

$$\begin{aligned} &b_0\Phi(1) + b_1\Phi(\gamma) + \dots + b_{m-1}\Phi(\gamma^{m-1}) \\ &= \Phi(b_0) + \Phi(b_1\gamma) + \dots + \Phi(b_{m-1}\gamma^{m-1}) \\ &= \Phi(b_0 + b_1\gamma + \dots + b_{m-1}\gamma^{m-1}) \neq \mathbf{0} \end{aligned}$$

for any non-zero coefficients vector  $(b_0, \dots, b_{m-1}) \in \mathbb{F}_p^m$ . This completes the proof.  $\blacksquare$

#### Encoding:

- Relay 1 precodes the decoded linear combinations as  $\mathbf{x}_3 = \mathbf{S}_{11}\mathbf{V}_3\mathbf{u}_1$  and produces the channel input

$$\mathcal{X}_3 = \Phi^{-1}(\mathbf{x}_3) \in \mathbb{F}_{p^m} \quad (17)$$

- Likewise, relay 2 precodes the decoded linear combinations as  $\mathbf{x}_4 = \mathbf{S}_{21}\mathbf{V}_3\mathbf{u}_2$  and produces the channel input

$$\mathcal{X}_4 = \Phi^{-1}(\mathbf{x}_4) \in \mathbb{F}_{p^m} \quad (18)$$

where

$$\mathbf{S} = \begin{bmatrix} \mathbf{S}_{11} & \mathbf{S}_{12} \\ \mathbf{S}_{21} & \mathbf{S}_{22} \end{bmatrix} = \begin{bmatrix} \mathbf{Q}_{33} & \mathbf{Q}_{34} \\ \mathbf{Q}_{43} & \mathbf{Q}_{44} \end{bmatrix}^{-1} \quad (19)$$

and  $\mathbf{V}_3$  are chosen to satisfy the alignment conditions in (8) with respect to  $\mathbf{S}$ :

$$\mathbf{v}_{3,\ell+1} = \Psi(\gamma'^\ell)\mathbf{v}_{3,1} \quad (20)$$

$$\mathbf{v}_{4,\ell} = \Psi(s_{22}^{-1}s_{21})\Psi(\gamma'^{\ell-1})\mathbf{v}_{3,1} \quad (21)$$

for  $\ell = 1, \dots, m-1$  where  $s_{ij} = \Psi^{-1}(\mathbf{S}_{ij})$  and where  $\gamma'$  is defined in (5).

From Lemma 2, we can immediately prove that  $\mathbf{V}_3$  and  $\mathbf{V}_4$  are full rank by choosing  $\mathbf{v}_{3,1} = \Phi(1)$  since  $\deg(\mu(\gamma')) = m$ . The other precoding vectors are completely determined by the (20) and (21).

From (14) and (15), we can observe that the coefficients of the linear combinations only depend on alignment conditions, independent of channel coefficients. From this, we can produce the received signal for which the channel matrix is equal to the

inverse of second-hop channel matrix. This is the key property to enable the network diagonalization. That is,  $\mathbf{x}_3$  and  $\mathbf{x}_4$  are equal to received signals with channel coefficients  $\mathbf{S}$ :

$$\begin{aligned} \begin{bmatrix} \mathbf{x}_3 \\ \mathbf{x}_4 \end{bmatrix} &= \begin{bmatrix} \mathbf{S}_{11}\mathbf{V}_3\mathbf{u}_1 \\ \mathbf{S}_{21}\mathbf{V}_3\mathbf{u}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{S}_{11}\mathbf{V}_3\mathbf{w}_1 + \mathbf{S}_{12}\mathbf{V}_4\mathbf{w}_2 \\ \mathbf{S}_{21}\mathbf{V}_3\mathbf{w}_1 + \mathbf{S}_{22}\mathbf{V}_4\mathbf{w}_2 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{Q}_{33} & \mathbf{Q}_{34} \\ \mathbf{Q}_{43} & \mathbf{Q}_{44} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{V}_3\mathbf{w}_1 \\ \mathbf{V}_4\mathbf{w}_2 \end{bmatrix}. \end{aligned} \quad (22)$$

3) *Decoding at the destinations:* Destinations 1 and 2 observe:

$$\begin{bmatrix} \mathcal{Y}_3 \\ \mathcal{Y}_4 \end{bmatrix} = \begin{bmatrix} q_{33} & q_{34} \\ q_{43} & q_{44} \end{bmatrix} \begin{bmatrix} \mathcal{X}_3 \\ \mathcal{X}_4 \end{bmatrix}.$$

By mapping the received signals onto ground field  $\mathbb{F}_p$ , we can get:

$$\begin{aligned} \begin{bmatrix} \Phi(\mathcal{Y}_3) \\ \Phi(\mathcal{Y}_4) \end{bmatrix} &= \begin{bmatrix} \mathbf{Q}_{33} & \mathbf{Q}_{34} \\ \mathbf{Q}_{43} & \mathbf{Q}_{44} \end{bmatrix} \begin{bmatrix} \mathbf{S}_{11}\mathbf{V}_3\mathbf{u}_1 \\ \mathbf{S}_{21}\mathbf{V}_3\mathbf{u}_2 \end{bmatrix} \\ &\stackrel{(a)}{=} \begin{bmatrix} \mathbf{V}_3\mathbf{w}_1 \\ \mathbf{V}_4\mathbf{w}_2 \end{bmatrix} \end{aligned}$$

where (a) is due to the precoding at relays to satisfy (22). This shows that destination 1 can decode  $\mathbf{w}_1$  using  $\mathbf{V}_3^{-1}\Phi(\mathcal{Y}_3)$  and destination 2 can decode  $\mathbf{w}_2$  using  $\mathbf{V}_4^{-1}\Phi(\mathcal{Y}_4)$ . This completes the proof of Theorem 1.

#### IV. TWO-UNICAST TWO-HOP MIMO IC OVER $\mathbb{F}_p$

We consider a  $2 \times 2 \times 2$  MIMO IC over  $\mathbb{F}_p$  where all nodes have  $m$  multiple inputs/outputs. Here, the  $m \times m$  channel matrices are denoted by  $\mathbf{Q}_{\ell k} \in \mathbb{F}_p^{m \times m}$ . Notice that they are neither diagonal matrices nor in the form of powers of companion matrix, and do not commute. Therefore, it is not possible to apply straightforwardly the same approach developed before. Instead, we have to resort to symbol extension by going to an extension field in order to obtain aligned network diagonalization.

From (11), we can define the precoding matrix  $\mathbf{V}_1$  to satisfy the alignment conditions as function of  $\mathbf{v}_{1,1}$ :

$$\mathbf{V}_1 = [\mathbf{v}_{1,1}, \mathbf{Q}\mathbf{v}_{1,1}, \dots, \mathbf{Q}^{m-1}\mathbf{v}_{1,1}] \quad (23)$$

where  $\mathbf{Q} = \mathbf{Q}_{11}^{-1}\mathbf{Q}_{12}\mathbf{Q}_{22}^{-1}\mathbf{Q}_{21}$ . We cannot use the result in Section III-A since  $\mathbf{Q}$  is not mapped onto the element of  $\mathbb{F}_{p^m}$ . For the time being, we assume that  $\mathbf{Q}$  has  $m$  distinct eigenvalues. Following [6], [13], we can prove that  $\mathbf{V}_1$  is full rank if we choose  $\mathbf{v}_{1,1} = \mathbf{E}\mathbf{1}$  where  $\mathbf{E}$  consists of  $m$  linearly independent eigenvectors of  $\mathbf{Q}$ . In case of complex-valued Gaussian channel, we can always find  $m$  distinct eigenvalues in the given complex field. However, in the finite field  $\mathbb{F}_p$ , some eigenvalues of  $\mathbf{Q}$  may not exist in the ground field  $\mathbb{F}_p$ , depending on characteristic polynomial of  $\mathbf{Q}$  (denoted by  $C(\lambda)$ ). Suppose that this polynomial is factored in the following way:

$$C(\lambda) = \prod_i \pi_i(\lambda) \quad (24)$$

where  $\deg(\pi_i(\lambda)) \geq \deg(\pi_j(\lambda))$  if  $i \leq j$ . If  $\deg(\pi_1(\lambda)) = r > 1$  then some eigenvalues of  $\mathbf{Q}$  do not exist in  $\mathbb{F}_p$ . Also, we

can see that  $\pi_1(\lambda)$  is a degree- $r$  irreducible polynomial over  $\mathbb{F}_p$ . Thus,  $L = \mathbb{F}_p[\lambda]/\pi_1(\lambda)$  generates an extension field of  $\mathbb{F}_p$  with order  $p^r$  and is isomorphic to  $\mathbb{F}_{p^r}$ . We can notice that  $r$  is the minimum order for which the corresponding extension field contains the roots of  $\pi_1(\lambda)$ . Since  $\deg(\pi_1(\lambda)) \leq r$  for  $i > 1$ , we are able to find all roots of  $C(\lambda)$  in  $\mathbb{F}_{p^r}$ . In short,  $\mathbb{F}_{p^r}$  is the *splitting field*<sup>2</sup> of  $C(\lambda)$ . Assume that  $\mathbf{Q}$  has  $m$  distinct eigenvalues  $\{\lambda_i \in \mathbb{F}_{p^r} : i = 1, \dots, m\}$  and corresponding eigenvectors  $\{\mathbf{e}_i \in \mathbb{F}_{p^r}^m : i = 1, \dots, m\}$ . Since  $\mathbf{Q}$  is diagonalizable, we have  $\mathbf{Q} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^{-1}$  where  $\mathbf{E}$  has  $\mathbf{e}_i$  as its the  $i$ -th column and  $\mathbf{\Lambda}$  has  $\lambda_i$  as its  $i$ -th diagonal element. Then, we choose  $\mathbf{v}_{1,1} = \mathbf{E}\mathbf{1} \in \mathbb{F}_{p^r}^m$ . Following [13], we can show that  $\mathbf{V}_1$  is full rank over  $\mathbb{F}_{p^r}$  as follows. Since  $\mathbf{Q} = \mathbf{E}\mathbf{\Lambda}\mathbf{E}^{-1}$  and  $\mathbf{v}_{1,1} = \mathbf{E}\mathbf{1}$ , we have:

$$\mathbf{V}_1 = \mathbf{E} \underbrace{\begin{bmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_m & \cdots & \lambda_m^{m-1} \end{bmatrix}}_{\triangleq \mathbf{J}}. \quad (25)$$

Since  $\mathbf{J}$  is a Vandermonde matrix, the determinant of  $\mathbf{V}_1$  is computed by

$$\begin{aligned} \det(\mathbf{V}_1) &= \det(\mathbf{E})\det(\mathbf{J}) \\ &= \det(\mathbf{E}) \prod_{1 \leq i < j \leq m} (\lambda_j - \lambda_i) \neq 0. \end{aligned}$$

Therefore,  $\mathbf{V}_1$  is full rank.

Next, we present our coding scheme over the  $r$ -symbol extension (i.e., over  $r$  time slots).

#### Encoding at the sources:

- Source 1 precodes its message  $\mathbf{w}_1 \in \mathbb{F}_{p^r}^m$  using precoding matrix  $\mathbf{V}_1 \in \mathbb{F}_{p^r}^{m \times m}$ :

$$\mathbf{x}_1 = \mathbf{V}_1 \mathbf{w}_1 \in \mathbb{F}_{p^r}^m$$

and transmits the  $t$ -th column of  $\Phi^T(\mathbf{x}_1) \in \mathbb{F}_p^{m \times r}$  at time slot  $t$  for  $t = 1, \dots, r$  where  $\Phi^T : \mathbb{F}_{p^r} \rightarrow [\mathbb{F}_p, \dots, \mathbb{F}_p]$  (notice that differently from (1), it maps the elements of  $\mathbb{F}_{p^r}$  to the  $r$ -dimensional row vectors).

- Similarly, source 2 precodes its message  $\mathbf{w}_2 \in \mathbb{F}_{p^r}^{m-1}$  using precoding matrix  $\mathbf{V}_2 \in \mathbb{F}_{p^r}^{(m-1) \times (m-1)}$ :

$$\mathbf{x}_2 = \mathbf{V}_2 \mathbf{w}_2 \in \mathbb{F}_{p^r}^{m-1}$$

and transmits the  $t$ -th column of  $\Phi^T(\mathbf{x}_2) \in \mathbb{F}_p^{(m-1) \times r}$  at time slot  $t$  for  $t = 1, \dots, r$ .

#### Decoding at the relays:

- Relay 1 observes:

$$\Phi^T(\mathbf{y}_1) = \mathbf{Q}_{11}\Phi^T(\mathbf{x}_1) + \mathbf{Q}_{12}\Phi^T(\mathbf{x}_2) \in \mathbb{F}_p^{m \times r}.$$

By mapping the received signal onto the element of  $\mathbb{F}_{p^r}$ , we have:

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{Q}_{11}\mathbf{V}_1\mathbf{w}_1 + \mathbf{Q}_{12}\mathbf{V}_2\mathbf{w}_2 \\ &= \mathbf{Q}_{11}\mathbf{V}_1\mathbf{u}_1 \end{aligned}$$

where the last step is due to the fact that precoding vectors satisfy the alignment conditions in (8).

- Similarly, relay 2 observes the aligned signal:

$$\mathbf{y}_2 = \mathbf{Q}_{21}\mathbf{V}_1\mathbf{u}_2.$$

At this point, we can follow Section III-A. In this case, we can achieve the sum-rate of  $(2m-1)\log p^r$  during  $r$  time slots. Therefore, we can achieve the sum-rate of  $(2m-1)\log p$  per time slot.

*Remark 2:* The number of required symbol extensions  $r \leq m$  depends on the channel coefficients. In general, we can always use the  $m$ -symbol extension to use the aligned network diagonalization, regardless of channel coefficients. In this way, the coding block length (symbol extension order) depends only on the number of inputs/outputs at each node, and it is independent of the channel coefficients.  $\diamond$

#### ACKNOWLEDGMENT

This work was supported by NSF Grant CCF 1161801.

#### REFERENCES

- [1] S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," *IEEE Transactions on Information Theory*, vol. 57, pp. 1872-1905, Apr. 2011.
- [2] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of the K user interference channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425-3441, Aug. 2008.
- [3] T. Gou and S. A. Jafar, "Capacity of a class of symmetric SIMO Gaussian interference channels within  $O(1)$ ," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, Jun-Jul. 2009.
- [4] S. A. Jafar and S. Vishwanath, "Generalized Degrees of Freedom of the Symmetric Gaussian K User Interference Channel," *IEEE Transactions on Information Theory*, vol. 56, pp. 3297-3303, Jul. 2010.
- [5] I. Shomorony and S. Avestimehr, "Two-Unicast Wireless Networks: Characterizing the Degrees-of-Freedom," *IEEE Transactions on Information Theory*, vol. 59, pp. 353-383, Jan. 2013.
- [6] T. Gou, S. A. Jafar, S.-W. Jeon, S.-Y. Chung, "Interference Alignment Neutralization and the Degrees of Freedom of the  $2 \times 2 \times 2$  Interference Channel," *IEEE Transactions on Information Theory*, vol. 58, pp. 4381-4395, July, 2012.
- [7] I. Shomorony and S. Avestimehr, "Degrees of Freedom of Two-Hop Wireless Networks: "Everyone Gets the Entire Cake", in *proceedings of 2012 Allerton Conference*.
- [8] R. Walden, "Analog-to-Digital Converter Survey and Analysis," *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 539-550, Apr. 1999.
- [9] A. S. Motahari, S. O. Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real Interference Alignment: Exploiting the Potential of Single Antenna Systems," *Submitted to IEEE Transactions on Information Theory* 2009.
- [10] S. Hong and G. Caire, "Compute-and-Forward Strategy for Cooperative Distributed Antenna Systems," *submitted to IEEE Transactions on Information Theory* 2012.
- [11] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference through Structured Codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 6463-6486, Oct. 2011.
- [12] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," Bell Laboratories Murray Hill.
- [13] S.-N. Hong and G. Caire, "Structured Lattice Codes for Some Two-User Gaussian Networks with Cognition, Coordination, and Two-Hops," *Submitted to IEEE Transactions on Information Theory*, Apr. 2013.

<sup>2</sup>A splitting field of a polynomial with coefficients in a field is a smallest field extension of that field over which the polynomial splits into linear factors.