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

Song-Nam Hong and Giuseppe Caire

Ming Hsieh Department of EE, University of Southern California, Los Angeles CA

Seville, Spain, Sep 9-13, 2013
Motivations

- Compute-and-Forward converts a Gaussian network into a finite-field linear deterministic network

- Precoding Based Network Alignment (in wired networks)
  - (Random) linear network coding at intermediate nodes yields a finite-field interference network

- The study of deterministic linear finite-field networks can provide insights to solve open problems in wireless networks such as finite SNR and finite channel diversity.
Definitions and Notations

- \( \mathbb{F}_{p^m} \) denote a finite-field of order \( p^m \) with elements
  \[ \{0, 1, \alpha, \ldots, \alpha^{p^m-1}\} \]
  where \( \alpha \) is a primitive element

- \( \mathbb{F}_{p^m}^* \) denotes the multiplicative group of \( \mathbb{F}_{p^m} \)

- For \( \beta \in \mathbb{F}_{p^m} \), \( \pi_\beta(x) \) denotes the minimal polynomial of \( \beta \)

- For a primitive element \( \alpha \), the minimal polynomial \( \pi_\alpha(x) \) has degree \( m \) and is called primitive polynomial
Definitions and Notations

**Definition:** The companion matrix of a primitive polynomial

\[ \pi_\alpha(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + x^m \]

is the \( m \times m \) matrix over \( \mathbb{F}_p \)

\[
C \triangleq \begin{bmatrix}
0 & 0 & \cdots & 0 & -a_0 \\
1 & 0 & \cdots & 0 & -a_1 \\
0 & 1 & \cdots & 0 & -a_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -a_{m-1}
\end{bmatrix}.
\]

Then, the set of matrices

\[
C(p, m) \triangleq \{0 = C^\infty, I = C^0, C, \ldots, C^{p^m-1}\}
\]

is a finite-field under matrix addition and multiplication.

Notice that \( C^\ell \) is **full-rank** over \( \mathbb{F}_p \) for \( \ell = 1, \ldots, p^m - 1 \).
Definitions and Notations

- **Vector Representation**
  
  one-to-one mapping $\Phi : \mathbb{F}_p^m \rightarrow \mathbb{F}_p^m$:
  
  $$\Phi(\alpha^\ell) = [b_0, b_1, \ldots, b_{m-1}]^T$$

  where $\alpha^\ell = b_0 + b_1 \alpha + \cdots + b_{m-1} \alpha^{m-1}$

- **Matrix Representation**
  
  one-to-one mapping $\Gamma : \mathbb{F}_p^m \rightarrow \mathcal{C}(p, m)$:
  
  $$\Gamma(\alpha^\ell) = C^\ell$$
Example

- Take $\pi_\alpha(x) = x^2 + x + 1$ over $\mathbb{F}_2$ with elements $\{0, 1, \alpha, \alpha^2\}$

- Vector representation

  $$\Phi(\{0, 1, \alpha, \alpha^2 = 1 + \alpha\}) = \{[0, 0]^T, [1, 0]^T, [0, 1]^T, [1, 1]^T\}$$

- Matrix representation

  $$\Gamma(\{0, 1, \alpha, \alpha^2 = 1 + \alpha\}) = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$
Lemma: Let $\mathbf{y} = \sum_{k=1}^{K} Q_k \mathbf{x}_k$ denote a deterministic linear MAC over $\mathbb{F}_{p^m}$, such that both the inputs $\{\mathbf{x}_k\}$ and the channel coefficients $\{Q_k\}$ are elements of $\mathbb{F}_{p^m}$.

Let

$$\mathbf{y} = \sum_{k=1}^{K} Q_k \mathbf{x}_k$$

where $\mathbf{x}_k = \Phi(\mathbf{x}_k) \in \mathbb{F}_p^m$ and $Q_k = \Gamma(Q_k) \in \mathbb{F}_{p^m \times m}$, for $k = 1, \ldots, K$. Then, we have:

$$\mathbf{y} = \Phi(\mathbf{y}).$$

♦
System Model: $2 \times 2 \times 2$ IC

- All nodes have $m$ multiple inputs/outputs

- Channel matrices $Q_{\ell k} \in \mathbb{F}_p^{m \times m}$ (considering 3-different structures)

- Channel inputs $x_k \in \mathbb{F}_p^m$, $k = 1, 2, 3, 4$, and channel outputs $y_\ell \in \mathbb{F}_p^m$, $\ell = 1, 2, 3, 4$
Three Channel Structures

- MIMO ground-field model

- \( x_k \in \mathbb{F}_p^m \), \( y_\ell \in \mathbb{F}_p^m \), and \( Q_{\ell k} \in \text{GL}(p, m) \) (set of full-rank matrices)
Three Channel Structures

- **MIMO ground-field model**
  - \( x_k \in \mathbb{F}_p^m, \ y_\ell \in \mathbb{F}_p^m, \) and \( Q_{\ell k} \in \text{GL}(p, m) \) (set of full-rank matrices over \( \mathbb{F}_p \))

- **Scalar \( m \)-th extension field model**
  - channel inputs \( \mathcal{X}_k \in \mathbb{F}_{p^m}, \) channel outputs \( \mathcal{Y}_\ell \in \mathbb{F}_{p^m}, \) and channel coefficients \( Q_{\ell k} \in \mathbb{F}_{p^m}^* \)
  - MIMO Representation: \( x_k = \Phi(\mathcal{X}_k), \ y_\ell = \Phi(\mathcal{Y}_\ell), \) and \( Q_{\ell k} = \Gamma(Q_{\ell k}) \)
Three Channel Structures

- **MIMO ground-field model**
  - $x_k \in \mathbb{F}_p^m$, $y_\ell \in \mathbb{F}_p^m$, and $Q_{\ell k} \in \text{GL}(p, m)$ (set of full-rank matrices)

- **Scalar $m$-th extension field model**
  - channel inputs $\mathcal{X}_k \in \mathbb{F}_{p^m}$, channel outputs $\mathcal{Y}_\ell \in \mathbb{F}_{p^m}$, and channel coefficients $Q_{\ell k} \in \mathbb{F}_{p^m}^*$
  - MIMO Representation: $x_k = \Phi(\mathcal{X}_k)$, $y_\ell = \Phi(\mathcal{Y}_\ell)$, and $Q_{\ell k} = \Gamma(Q_{\ell k})$

- **Scalar $m$-th symbol extension model**
  - channel inputs $x_k[t] \in \mathbb{F}_p$, channel outputs $y_\ell[t] \in \mathbb{F}_p$, and time-varying channel coefficients $q_{\ell k}[t] \in \mathbb{F}_p^*$
  - MIMO Representation: $x_k = [x_k[1], \ldots, x_k[m]]$, $y_\ell = [y_\ell[1], \ldots, y_\ell[m]]$, and $Q_{\ell k} = \text{diag}(q_{\ell k}[1], \ldots, q_{\ell k}[m])$
Sources 1 and 2 choose the precoding matrices $V_1, V_2 \in \mathbb{F}_p^{m \times m}$ such that the received signals at relays are aligned:

\[
\begin{align*}
y_1 &= Q_{11} V_1 w_1 + Q_{12} V_2 w_2 \\
    &= Q_{11} V_1 u_1 \\
y_2 &= Q_{21} V_1 w_1 + Q_{22} V_2 w_2 \\
    &= Q_{21} V_1 u_2
\end{align*}
\]

where

\[
\begin{align*}
u_1 &= \begin{bmatrix} w_{1,1} \\
                    w_{1,2} + w_{2,1} \\
                    \vdots \\
                    w_{1,m} + w_{2,m-1} \end{bmatrix} \\
u_2 &= \begin{bmatrix} w_{1,1} + w_{2,1} \\
                    \vdots \\
                    w_{1,m-1} + w_{2,m-1} \\
                    w_{1,m} \end{bmatrix}
\end{align*}
\]

Notice that $u_1$ and $u_2$ are fixed, independently from channel matrices.
• Relays 1 and 2 obtain $u_1$ and $u_2$ (assuming that $V_1$ is full-rank)

• Relays 1 and 2 choose precoding matrices $V_3$ and $V_4$ such that the interferences at destinations are cancelled (possible by using the fact that $u_1$, $u_2$ are fixed):

\[
\begin{align*}
y_3 &= Q_{33} V_3 u_1 + Q_{34} V_4 u_2 \\
    &= V_3 w_1
\end{align*}
\]
\[
\begin{align*}
y_4 &= Q_{43} V_3 u_1 + Q_{44} V_4 u_2 \\
    &= V_4 w_2
\end{align*}
\]

• Destinations 1 and 2 can obtain their desired messages using $V_3^{-1} y_3$ and $V_4^{-1} y_4$ (assuming that $V_3$ and $V_4$ are full-rank)

◊ Feasibility Conditions: $V_1$, $V_3$, and $V_4$ are full-rank
Precoding matrix $V_1$ has the form:

$$V_1 = [v_{1,1}, Qv_{1,1}, \ldots, Q^{m-1}v_{1,1}]$$

where $Q = Q_{11}^{-1}Q_{12}Q_{21}^{-1}Q_{22}$ and $v_{1,1}$ is given by

- **Scalar $m$-th symbol extension model**
  $$v_{1,1} = 1$$

- **Scalar $m$-th extension field model**
  $$v_{1,1} = \Phi(1)$$

- **MIMO ground-field model**
  $$v_{1,1} = E1$$

where the columns of $E$ consist of eigenvectors of $Q$. 
MIMO ground-field model: symbol-extension

- Eigenvalues of $Q$ may not exist in the ground field $\mathbb{F}_p$, depending on characteristic polynomial of $Q$ (i.e., $c(x)$)

- Find eigenvalues of $Q$ in the splitting field of $c(x)$, i.e., $\mathbb{F}_{pr}$

- Construct the precoding matrix $V_1$ in the extension field $\mathbb{F}_{pr}$, i.e., it is the minimal field containing all roots of $c(x)$

- Accordingly, coding/decoding should be performed over extension-field ($\Rightarrow r$ channel uses)
The required symbol-extension \( r \) depends on characteristic polynomial \( c(x) \), i.e., the degree of splitting field of \( c(x) \)

\[
c(x) = \prod_{i=1}^{d} c_i(x)
\]

where \( c_i(x) \) denotes an irreducible factor over \( \mathbb{F}_p \)

\[
r = \text{lcm}(r_1, \ldots, r_d)
\]

where \( r_i \) is the degree of splitting field of \( c_i(x) \)

An upper bound on the degree \( r \) is the maximum of least common multiplies over all possible integer partitions of the integer \( m \) (unsolved problem in number theory)

A general bound on the degree of splitting field is known to be \( m! \)
This bound is quite loose as shown in the below

<table>
<thead>
<tr>
<th>$m$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>upper-bound</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>12</td>
<td>15</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>$m!$</td>
<td>2</td>
<td>6</td>
<td>24</td>
<td>120</td>
<td>720</td>
<td>5040</td>
<td>40320</td>
<td>362880</td>
<td>3628800</td>
</tr>
</tbody>
</table>

The upper bound in Table is computed by finding exhaustively the least common multiples over all integer partitions of $m$
Feasibility Conditions

In order to guarantee the full-rank of $V_k$, we have:

- **MIMO ground-field model**
  - $Q = Q_{11}^{-1} Q_{12} Q_{21}^{-1} Q_{22}$ and $Q' = Q_{33}^{-1} Q_{34} Q_{43}^{-1} Q_{44}$ have distinct eigenvalues

- **Scalar $m$-th symbol extension model**
  - the diagonal elements of the products of $Q$ and $Q'$ are distinct where
  $$Q_{\ell k} = \text{diag}(q_{\ell k}[1], \ldots, q_{\ell k}[m])$$

- **Scalar $m$-th extension field model**
  - $\deg(\pi_{\gamma}(x)) = m$ and $\deg(\pi_{\gamma'}(x)) = m$ where
  $$\gamma = Q_{11}^{-1} Q_{12} Q_{22}^{-1} Q_{21}$$ and $$\gamma' = Q_{33}^{-1} Q_{34} Q_{44}^{-1} Q_{43}$$
**Main Results**

**Theorem:** For all three channel models, the sum-rate of \((2m - 1) \log p\) is achievable with feasibility probability \(P(p, m)\)

- Scalar ground-field model with \(m\) symbol extension

\[
P_{SE}(p, m) = \left( (p - 1)^{-m} \prod_{i=1}^{m} (p - i) \right)^2
\]
Main Results

**Theorem:** For all three channel models, the sum-rate of \((2m - 1) \log p\) is achievable with feasibility probability \(\mathbb{P}(p, m)\)

- Scalar \(m\)-th extension field model

\[
\mathbb{P}_{FE} = \left( \frac{p^m + \sum_{d | m, d > 1} \nu(d) p^{m/d}}{p^m - 1} \right)
\]

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

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

In particular when \(m\) is a prime,

\[
\mathbb{P}_{FE}(p, m) = \left( \frac{p^m - p}{p^m - 1} \right)^2
\]
Main Results

**Theorem:** For all three channel models, the sum-rate of \((2m - 1) \log p\) is achievable with feasibility probability \(\mathbb{P}(p, m)\)

- **MIMO ground-field model**

\[
\mathbb{P}_{\text{MIMO}} = (s_{\text{GL}}(p, m))^2
\]

where \(s_{\text{GL}}(p, m)\) denotes the proportion of separable elements\(^1\) in \(\text{GL}(p, m)\)

In [Fulman-Neumann-Praeger], the lower and upper bounds on \(s_{\text{GL}}(p, m)\) is given by

\[
1 - p^{-1} - \frac{8(p-1)}{(2p-3)} \left(\frac{2}{3p}\right)^{-m} \leq s_{\text{GL}}(p, m) \leq 1 - p^{-1} + \frac{8(p-1)}{(2p-3)} \left(\frac{2}{3p}\right)^{-m}
\]

\(^1\)An \(m \times m\) matrix \(Q\) over a finite-field \(\mathbb{F}_p\) is said to be *separable* if its characteristic polynomial has no repeated roots in the algebraic closure of \(\mathbb{F}_p\)
Main Results

**Theorem:** For all three channel models, the sum-rate of \((2m - 1) \log p\) is achievable with feasibility probability \(P(p, m)\)

- Scalar ground-field model with \(m\) symbol extension

\[
P_{SE}(p, m) = \left((p - 1)^{-m} \prod_{i=1}^{m}(p - i)\right)^2
\]

- Scalar \(m\)-th extension field model (for prime \(m\))

\[
P_{FE}(p, m) = \left(\frac{p^m - p}{p^m - 1}\right)^2
\]

- MIMO ground-field model

\[
\left(1 - p^{-1} - \frac{8(p - 1)}{(2p - 3)} \left(\frac{2}{3}p\right)^{-m}\right)^2 \leq P_{MIMO}(p, m) \leq \left(1 - p^{-1} + \frac{8(p - 1)}{(2p - 3)} \left(\frac{2}{3}p\right)^{-m}\right)^2
\]
Field-extension and Symbol-extension

Ground field size (p)
Feasibility Probability
Field-extension (m=2)
Symbol-extension (m=2)
Field-extension (m=7)
Symbol-extension (m=7)
Main Results: In the limit

Feasibility probabilities in the limit (either $p$ or $m$ goes to infinity):

<table>
<thead>
<tr>
<th></th>
<th>$p \rightarrow \infty$</th>
<th>$m \rightarrow \infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{FE}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$P_{SE}$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$P_{MIMO}$</td>
<td>1</td>
<td>$(1 - p^{-1})^2$</td>
</tr>
</tbody>
</table>

Corollary: In case of scalar $m$-th extension field model, the optimal sum-capacity is achieved for any prime $p$ as long as $m$ goes to infinity.
Concluding Remarks

- Use companion matrix representation of extension-field to convert $K$-user linear deterministic MAC over $\mathbb{F}_{p^m}$ into a $K$-user MAC over ground field $\mathbb{F}_p$.

- Show the necessity of symbol-extension (multiple channel uses) for MIMO ground-field model, differently from complex Gaussian channel.

- Compute the feasibility probabilities for finite $p$ and $m$.

- Find some applications (i.e., wired networks and Gaussian networks) of this work in our journal paper (http://arxiv.org/abs/1308.0870).
Thank You!