This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Binary Field Network Coding Design for Multiple-Source Multiple-Relay Networks

Jun Li, Jinhong Yuan, Robert Malaney
School of Electrical
Engineering and Telecommunications
University of New South Wales, AUSTRALIA
Email: {jun.li, j.yuan, r.malaney}@unsw.edu.au

Ming Xiao
ACCESS Linnaeus center
School of Electrical Engineering
Royal Institute of Technology, KTH, SWEDEN
Email: ming.xiao@ee.kth.se

***Abstract*—We study the design of network codes for M-source, N-relay wireless networks over slow fading channels. Specifically, vector-wise binary field network coding (BFNC) schemes are proposed. In the construction of our BFNC schemes, we utilize a diversity achieving criterion which can be expressed in terms of the linear independence of quasi-cyclic matrices. Our codes can be implemented with low-complexity encoders at the relays as only binary operations are used. Meanwhile at the destination, for small code lengths, ML decoding can be applied. For large code lengths, we propose a modified BP decoder with low decoding complexity. From analysis and simulations, we show that our proposed BFNC schemes can achieve full diversity for the ML decoder, as well as full diversity for the modified BP decoder we propose for large block lengths. Our simulations also show that our proposed BFNC schemes achieve a higher coding gain relative to previous network coding schemes.**

I. Introduction

The use of relays in wireless networks is recognized as an efficient technique to combat channel fading [1, 2]. By allowing information processing in the intermediate nodes, network coding (NC) schemes have been proved to achieve network multicast capacity bounds for computer networks [3]. Recently, how to leverage network coding in wireless relaying networks to enhance the achievable rates and combat the channel fading has drawn increasing interest [4–8].

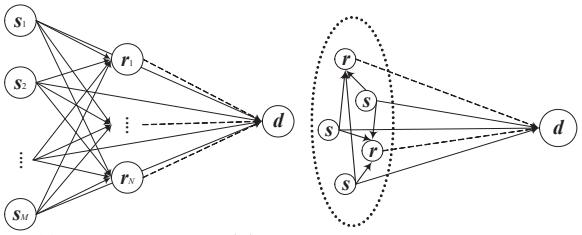
In multiple-source, one-relay and one-destination wireless systems ($M-1-1$ relaying networks), binary field network coding (BFNC) schemes have been proposed to achieve higher transmission rate without reducing the diversity gain [5]. In the BFNC schemes, messages of all the sources are XORed in binary field at the relay before retransmission. However, when extended to multiple-source, multiple-relay and one-destination wireless systems ($M-N-1$ relaying networks), the BFNC schemes designed for the $M-1-1$ relaying networks cannot achieve the full diversity [6].

To address this issue, the authors in [6] propose novel Galois field (with q elements, $q>2$) NC (GFNC) schemes. In the GFNC schemes, messages of the sources are superimposed in Galois field at the relays. By this way, full diversity can be achieved in the $M-N-1$ relaying networks. However, we note that the main drawback of the GFNC schemes is that the destination has to decode the messages from different channels (different sources or relays) separately. This is because joint decoding for frames with nontrivial length from different channels is generally infeasible for GFNC due to high complexity. This leads to a dramatic reduction in coding gain. In addition, the field size of network codes increases with the number of the sources M and the number of the relays N in a network. Thus, the encoding complexity of the GFNC schemes is high when M and N are large, since computation in large Galois fields generally has high complexity. Complex Field NC (CFNC) has also been studied in the context of relaying networks [7]. However, although full diversity can be achieved using CFNC, such schemes are also impacted negatively through low coding gain.

These drawbacks in GFNC and CFNC schemes motivate us to reconsider the BFNC scheme design in the $M-N-1$ relaying networks. The advantage of BFNC schemes is that they can be treated as instances of conventional low-density parity-check (LDPC) codes for slow fading channels. Using this fact, efficient belief propagation (BP) decoders (with reasonable complexity) can be applied to the destination so as to jointly decode the messages from different channels [8–10]. Specifically, in [8], LDPC-like BFNC schemes are designed to improve the error performance in the networks over ergodic fading channels. In [9, 10], LDPC based BFNC schemes are designed to obtain higher threshold in the networks over AWGN channels. Thus, high coding gain can be achieved, particularly for large block length. However, the previous works in [8–10] do not address the issue on how to guarantee the full diversity of the networks over slow fading channels.

In this paper, we will study the design of binary field NC (BFNC) schemes for an $M-N-1$ relaying network with slow fading channels to achieve full diversity and high coding gain. Firstly, we discuss a full-diversity-achieving criterion derived from treating the BFNC schemes as frame-wise cyclic-shift channel codes. We prove that the criterion can be applied to the BFNC schemes with both maximum likelihood (ML) decoding and belief propagation (BP) decoding. Secondly, based on the criterion, we propose an algorithm to design the low complexity encoders of BFNC schemes by exploiting the parity check matrices of quasi-cyclic LDPC codes, *i.e.* quasi-cyclic matrices. Finally, we focus on the network with large block length and design the practical decoder based on the BP decoding principle. Our codes have the following advantages.

978-1-61284-233-2/11/$26.00 ©2011 IEEE



(a) M-N-1 system model (b) A practical scenario

Fig. 1. System model of the $M-N-1$ relaying network.

(i) In terms of encoding complexity at the relays, the proposed BFNC schemes are binary and can be linearly encoded. (ii) In terms of decoding at the destination, for small block lengths, a maximum likelihood (ML) decoder can be utilized to achieve full diversity. For large block lengths where ML decoding becomes impractical, the proposed BFNC schemes with a modified BP decoder can still achieve full diversity and high coding gain due to the joint decoding of the observations of different channels.

II. System Model and Preliminaries

Fig. 1(a) shows an $M-N-1$ relaying network, where M sources, $s_1, \cdots, s_M$, transmit messages to their common destination d with the help of N half-duplexing relays, $r_1, \cdots, r_N$. We assume that all the transmitting nodes access the channels using time division multiple access (TDMA). We consider the frequency-nonselective slow fading channels with block length of l_{block} symbols. During a block period, there are two transmission phases. In the first phase, the sources $s_1, \cdots, s_M$ take turns to broadcast their *uncoded* frames to the relays and the destination with the frame length of l symbols. Each relay tries to decode the frames of all the sources and encode the messages by an NC scheme. In the second phase, the relays $r_1, \cdots, r_N$ take turns forwarding the network coded frames to the destination with the same frame length l, and all the sources keep silent. Thus, $l_{block} = (M+N)l$. After the second phase, the destination tries to decode the messages of the sources by combining the received signals of the two phases.

Since reference [6] has shown that the network coding designed for perfect source-to-relay channels can still achieve full diversity in the non-perfect source-to-relay channels, here we consider the scenario shown as Fig. 1(b), where the sources and the relays are close to each other, but far from the destination. We assume the source-to-relay channels are error free. Note that this assumption does not change the network coding design method. We denote the channel coefficient between the m-th sources s_m and the destination as $\hbar_m$, and the channel coefficient between the n-th relay r_n and the destination as h_n. We assume that all the channel magnitudes $|\hbar_m|$ and $|h_n|$ are independent, identically distributed $(i.i.d)$ Rayleigh random variables with zero mean and unit variance. All channel coefficients are randomly distributed, but remain constant for one or more blocks.

Messages of all the transmitting nodes are BPSK modulated. We denote $\boldsymbol{b}_{s_m} = [b_{s_m,1}, \cdots, b_{s_m,l}]^T$ as the information bit vector of s_m and $\boldsymbol{x}_{s_m} = [x_{s_m,1}, \cdots, x_{s_m,l}]^T$ as the transmitting frame after modulation, where the superscript T represents the transpose of a vector. All the symbols transmitted by each source are uniformly distributed. We denote $\boldsymbol{b}_{r_n} = [b_{r_n,1}, \cdots, b_{r_n,l_r}]^T$ as the network coded bit vector of r_n, which is generated based on source messages by a binary field network coding (BFNC) scheme. Correspondingly, the modulated frame transmitted by r_n is $\boldsymbol{x}_{r_n} = [x_{r_n,1}, \cdots, x_{r_n,l_r}]^T$. For BPSK, we have $\boldsymbol{x}_{s_m} = (-1)^{\boldsymbol{b}_{s_m}}$ and $\boldsymbol{x}_{r_n} = (-1)^{\boldsymbol{b}_{r_n}}$. We suppose that the average power of the transmitted symbols at both the sources and the relays is the same and denoted as P. The additive channel noise at destination receiver is Gaussian distributed with variance σ^2. So the average signal-to-noise ratio (SNR) is defined as $\rho \triangleq P/\sigma^2$. During a block period, we denote $\boldsymbol{y}_{1m}$ as the received frame from s_m in the first phase and $\boldsymbol{y}_{2n}$ as the received frame from r_n in the second phase. Then we have $\boldsymbol{y}_{1m} = \hbar_m \boldsymbol{x}_{s_m} + \boldsymbol{v}_{1m}, m = 1, \cdots, M$ and $\boldsymbol{y}_{2n} = h_n \boldsymbol{x}_{r_n} + \boldsymbol{v}_{2n}, n = 1, \cdots, N$, where $\boldsymbol{v}_{1m}$ and $\boldsymbol{v}_{2n}$ are the two vectors of noise variables.

With the BFNC schemes at the relays, the average mutual information between s_m and the destination is normalized among all the sources. Then we have

$$I_{BFNC}^{s_m} = \frac{M}{M+N}\left(\log\left(1+|\hbar_m|^2\rho\right) + \frac{1}{M}\sum_{n=1}^{N}\log\left(1+|h_n|^2\rho\right)\right). \quad (1)$$

Since the N parity check messages are shared by the M sources, the transmission rate of each source is $R = M/(M+N)$. Given the transmission rate R and the channel realization $\boldsymbol{h} = [\hbar_1, \cdots, \hbar_m, h_1, \cdots, h_n]$ in a block period, the conditional outage probability of s_m is defined as $P_r(\mathcal{O}_{s_m}) = P_r(I_{BFNC}^{s_m} < R|\boldsymbol{h})$, where $\mathcal{O}_{s_m}$ represents the outage event of s_m. Then the outage probability of the network is $P_o = P_r(\mathcal{O}_{s_1} \cup \cdots \cup \mathcal{O}_{s_M})$, which can be seen as the lower bound of the block error probability P_e. We define the diversity gain as $\lambda \triangleq -\lim_{\rho\to\infty} \log P_e/\log\rho$. In the $M-N-1$ relaying network, the full diversity is $N+1$, since each source message is transmitted through $N+1$ independent paths [6].

III. Full Diversity Achieving BFNC Schemes

The reason that an $M-N-1$ relaying network with conventional BFNC schemes cannot achieve full diversity is because the schemes are operated in a single bit-wise fashion [6]. In the following, we will show that if a BFNC scheme can be operated in a frame-wise fashion, the $M-N-1$ relaying network may achieve full diversity. We are interested in design of the BFNC schemes that can achieve full diversity with either the maximum likelihood (ML) decoder or the belief propagation (BP) decoder at the destination.

A. BFNC Design Criterion with ML Decoder

Note that a block $\boldsymbol{x}$ is composed of the frames transmitted by all the sources and the relays. So we have $\boldsymbol{x} = [\boldsymbol{x}_{s_1}^T, \cdots, \boldsymbol{x}_{s_M}^T, \boldsymbol{x}_{r_1}^T, \cdots, \boldsymbol{x}_{r_N}^T]^T$. We define that the pairwise error

probability (PEP), *i.e.* $P_e(\boldsymbol{x} \rightarrow \hat{\boldsymbol{x}})$, of the network is the average error probability of the event that a block $\boldsymbol{x}$ is decoded into another block $\hat{\boldsymbol{x}} = [\hat{\boldsymbol{x}}_{s_1}^T, \cdots, \hat{\boldsymbol{x}}_{s_M}^T, \hat{\boldsymbol{x}}_{r_1}^T, \cdots, \hat{\boldsymbol{x}}_{r_N}^T]^T$ with the ML decoder. We can investigate the diversity gain from the PEP of the $M-N-1$ relaying network. We have the following lemma.

Lemma 1: When ρ is large enough, the PEP of the $M-N-1$ relaying network with an ML decoder is

$$P_e(\boldsymbol{x} \rightarrow \hat{\boldsymbol{x}}) = \frac{K}{\prod_{m=1}^{M}(1+||\boldsymbol{u}_{s_m}||^2\rho)\prod_{n=1}^{N}(1+||\boldsymbol{u}_{r_n}||^2\rho)}, \tag{2}$$

where K is a constant relative to SNR, $\boldsymbol{u}_{s_m} = \frac{1}{\sqrt{P}}(\boldsymbol{x}_{s_m} - \hat{\boldsymbol{x}}_{s_m})$, $m = 1, \cdots, M$, and $\boldsymbol{u}_{r_n} = \frac{1}{\sqrt{P}}(\boldsymbol{x}_{r_n} - \hat{\boldsymbol{x}}_{r_n})$, $n = 1, \cdots, N$. Frobenius 2-norm $||\boldsymbol{z}||$ of a vector $\boldsymbol{z} = [z_1, \cdots, z_l]^T$ is calculated as $||\boldsymbol{z}|| = \sqrt{z_1^2 + \cdots + z_l^2}$.

Proof: In this work we omit all of our proofs due to space considerations. Full proofs will appear in an extended version of this paper.

We define the *frame-wise Hamming distance* between two blocks $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$ as the number of different frames between the two blocks. From *Lemma 1*, the diversity gain of the $M-N-1$ relaying network is determined by the minimum frame-wise Hamming distance between two arbitrary blocks $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$. For a conventional BFNC scheme, since each network coded bit at a relay is XORed in bit-wise fashion, all the relays generate the same network coded frame as $\boldsymbol{b}_{s_1} \oplus \boldsymbol{b}_{s_2} \oplus \cdots \oplus \boldsymbol{b}_{s_M}$. Therefore, we can see that in the conventional BFNC scheme, the minimum distance is two, and by *Lemma 1* we see that the diversity gain of the conventional BFNC scheme in the $M-N-1$ relaying network is two.

In order to achieve full diversity in the $M-N-1$ relaying network, we consider the frame-wise BFNC schemes. In these schemes, the network coded frame at the relay r_n, *i.e.* $\boldsymbol{b}_{r_n}$ is represented as $\boldsymbol{H}_{r_n}\boldsymbol{b}_{r_n} = \sum_{m=1}^{M} \oplus \boldsymbol{H}_{s_m,n}\boldsymbol{b}_{s_m}$, where $\boldsymbol{H}_{r_n}, \boldsymbol{H}_{s_1,n}, \cdots, \boldsymbol{H}_{s_M,n}$ are the $l \times l$ binary matrices and $\sum \oplus$ represents the summation in the binary field. Then we have $\boldsymbol{H}\boldsymbol{b} = \boldsymbol{o}$, where $\boldsymbol{o}$ represents the all-zero vector of length l_{block}, $\boldsymbol{b} = [\boldsymbol{b}_{s_1}^T, \cdots, \boldsymbol{b}_{s_M}^T, \boldsymbol{b}_{r_1}{}^T, \cdots, \boldsymbol{b}_{r_N}{}^T]^T$, and

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_{s_1,1} & \cdots & \boldsymbol{H}_{s_M,1} & \boldsymbol{H}_{r_1} & \boldsymbol{O} & \cdots & \boldsymbol{O} \\ \boldsymbol{H}_{s_1,2} & \cdots & \boldsymbol{H}_{s_M,2} & \boldsymbol{O} & \boldsymbol{H}_{r_2} & \cdots & \boldsymbol{O} \\ & & \cdots & & & & \cdots \\ \boldsymbol{H}_{s_1,N} & \cdots & \boldsymbol{H}_{s_M,N} & \boldsymbol{O} & \boldsymbol{O} & \cdots & \boldsymbol{H}_{r_N} \end{bmatrix}, \tag{3}$$

with $\boldsymbol{O}$ representing the $l \times l$ all-zero matrix. Each BFNC scheme corresponds to a particular binary matrix $\boldsymbol{H}$ in (3). We call the matrix $\boldsymbol{H}$ the parity check matrix of a BFNC scheme. We can rewrite $\boldsymbol{H}$ as $\boldsymbol{H} = [\boldsymbol{H}_1, \cdots, \boldsymbol{H}_M, \boldsymbol{H}_{M+1}, \cdots, \boldsymbol{H}_{M+N}]$. The following theorem provides a design criterion for $\boldsymbol{H}$, by which, the corresponding BFNC scheme can achieve $(N+1)$-order diversity in the network with an ML decoder.

Theorem 1: The $M-N-1$ relaying network with an ML decoder can achieve $(N+1)$-order diversity if the columns in any N (*i.e.* total Nl columns) of matrices $\boldsymbol{H}_1, \cdots, \boldsymbol{H}_{M+N}$ are linearly independent.

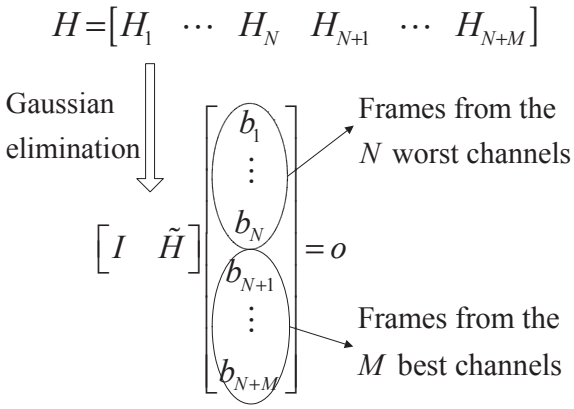


Fig. 2. The parity check matrix $\boldsymbol{H}'$ derived from $\boldsymbol{H}$ by Gaussian elimination.

B. BFNC Design Criterion with BP Decoder

We now consider the full diversity-achieving BFNC scheme design for the $M-N-1$ relaying network with a BP decoder. To achieve $(N+1)$-order diversity in the network, the destination needs to recover the source's frames even arbitrary N channels are in deep fading. Note that the destination knows the channel gains of all the M source-to-destination channels and all the N relay-to-destination channels.

Without loss of generality, we suppose that the matrices $\boldsymbol{H}_1, \cdots, \boldsymbol{H}_N$ are related to the N frames (denoted as $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_N$) that are transmitted through the worst N channels, *i.e.* N channels with the lowest channel gains. We also suppose that the matrices $\boldsymbol{H}_{N+1}, \cdots, \boldsymbol{H}_{N+M}$ are related to the M bit frames (denoted as $\boldsymbol{b}_{N+1}, \cdots, \boldsymbol{b}_{N+M}$) that are transmitted through the best M channels, *i.e.* M channels with the highest channel gains. If $\boldsymbol{H}_1, \cdots, \boldsymbol{H}_N$ are constructed to be linearly independent, we can transfer the matrix $\boldsymbol{H}$ to $\boldsymbol{H}' = [\boldsymbol{I}\ \widetilde{\boldsymbol{H}}]$ by Gaussian elimination, where $\boldsymbol{I}$ is an $Nl \times Nl$ identity matrix and $\widetilde{\boldsymbol{H}}$ is an $Nl \times Ml$ binary matrix. We can see that both $\boldsymbol{H}$ and $\boldsymbol{H}'$ are the parity check matrices of the transmitted bit blocks. Refers to Fig. 2 for the transferring process.

According to the concept of root-check LDPC codes [12], if $\boldsymbol{H}'$ is used as a parity check matrix, all the bits transmitted in the N worst channels corresponding to the identical matrix $\boldsymbol{I}$ in $\boldsymbol{H}'$ can obtain the extrinsic mutual information from the M best channels corresponding to the matrix $\widetilde{\boldsymbol{H}}$ in $\boldsymbol{H}'$ with one iteration of the BP decoder. Thus, all the bits in a block are equivalently transmitted in the M best channels and the network achieves $(N+1)$-order diversity based on the diversity evolution of the root-check LDPC codes. Note that the N worst channels are randomly distributed in all the source-to-destination channels and all the relay-to-destination channels for different transmission blocks. Therefore, the BFNC scheme design criterion with a BP decoder is that, the columns in arbitrary N of matrices $\boldsymbol{H}_1, \cdots, \boldsymbol{H}_{M+N}$ are linearly independent. It is obvious that the criterion to achieve full diversity with the ML decoder and the BP decoder are the same. We refer to this criterion as the *linearly independent criterion* (LIC).

IV. Low Complexity BFNC Encoder Design based on Quasi-Cyclic Matrices

We will design $\boldsymbol{H}$ based on the parity check matrices of quasi-cyclic LDPC (QC-LDPC) codes, *i.e.* QC matrices, that satisfy the LIC. The reasons are as follows. Firstly, QC matrices are semi-deterministic. Therefore, we can design the matrices that satisfy the LIC rather than using an exhaustive search. Secondly, QC-LDPC code structures are binary and enable linear encoding at the relays. This offers a low-complexity encoding solution. A QC matrix is composed of sub-matrices that are either zero matrices or circulant permutation matrices [13]. We denote $\boldsymbol{I}^l(\alpha)$ as the circulant permutation matrix which shifts the $l \times l$ identity matrix to the right by α times for any non-negative integer α. In addition, we denote $\boldsymbol{I}^l(0)$ as an $l \times l$ identity matrix and denote $\boldsymbol{I}^l(\infty)$ as an $l \times l$ zero matrix.

To change the matrix $\boldsymbol{H}$ to a quasi-cyclic matrix, we replace its sub-matrices, *e.g.* $\boldsymbol{H}_{s_m,n}$, $\boldsymbol{H}_{r_n}$ in (3), $n = 1, \cdots, N$, $m = 1, \cdots, M$, with either circulant permutation matrices, or square quasi-cyclic matrices. If we put the circulant permutation matrices into the matrix $\boldsymbol{H}$ in (3), then we have $\boldsymbol{H}_{s_m,n} = \boldsymbol{I}^l(\alpha_{nm})$, $\boldsymbol{H}_{r_n} = \boldsymbol{I}^l(\alpha_n)$, and

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{I}^l(\alpha_{11}) & \cdots & \boldsymbol{I}^l(\alpha_{1M}) & \boldsymbol{I}^l(\alpha_1) & \cdots & \boldsymbol{I}^l(\infty) \\ & \cdots & & & \cdots & \\ \boldsymbol{I}^l(\alpha_{N1}) & \cdots & \boldsymbol{I}^l(\alpha_{NM}) & \boldsymbol{I}^l(\infty) & \cdots & \boldsymbol{I}^l(\alpha_N) \end{bmatrix}. \tag{4}$$

In (4), the numbers α_n, $n = 1, \cdots, N$, are positive integers and α_{nm}, $m = 1, \cdots, M$, are either positive integers or ∞. Also, we can set $\boldsymbol{H}_{s_m,n}$ and $\boldsymbol{H}_{r_n}$ as the square quasi-cyclic matrices. For example, $\boldsymbol{H}_{s_m,n}$ can be composed of a combination of four $l/2 \times l/2$ circulant permutation matrices and $l/2 \times l/2$ zero matrices, such that $\boldsymbol{H}_{s_m,n} = [\boldsymbol{I}^{l/2}(0)\ \boldsymbol{I}^{l/2}(1); \boldsymbol{I}^{l/2}(2)\ \boldsymbol{I}^{l/2}(\infty)]$.

In the matrix $\boldsymbol{H}$, by replacing the zero matrix with 0, and replacing all the other non-zero circulant matrices with 1, we obtain a basic binary matrix $\hat{\boldsymbol{H}}$. If $\boldsymbol{H}_{s_m,n}$ and $\boldsymbol{H}_{r_n}$ are the circulant permutation matrices, then $\hat{\boldsymbol{H}}$ is an $N \times (M+N)$ matrix. If both $\boldsymbol{H}_{s_m,n}$ and $\boldsymbol{H}_{r_n}$ are composed of $k \times k$ circulant permutation matrices of size $l/k \times l/k$ (l is an integer multiple of k), then $\hat{\boldsymbol{H}}$ is an $Nk \times (M+N)k$ matrix. According to [11], to design a matrix $\boldsymbol{H} = [\boldsymbol{H}_1, \cdots, \boldsymbol{H}_{M+N}]$ to satisfy the LIC, a sufficient condition is that we need to design its basic matrix $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}]$ so that the columns in arbitrary N of matrices $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}$ are linearly independent. We call this sufficient condition the basic-matrix linearly independent criterion (BLIC). Thus, in our QC matrix based BFNC scheme design, we construct a basic matrix $\hat{\boldsymbol{H}}$ that satisfies the BLIC (instead of searching for a matrix $\boldsymbol{H}$ that satisfies the LIC). To facilitate illustration, we first consider a multiple-source 2-relay network. We then extend to the general case of an $M-N-1$ relaying network.

A. Basic Matrix Design for the $M-2-1$ relaying network

There are two steps to construct a basic matrix $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+2}]$ such that the columns in any 2 matrices of $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+2}$ are linearly independent. First of all, we need to ensure that the columns inside of each $\hat{\boldsymbol{H}}_k$, $k = 1, \cdots, M+2$, are linearly independent, *i.e.* each matrix $\hat{\boldsymbol{H}}_k$ is of full column rank. *Algorithm 4.1* generates a series of full column rank binary matrices.

Algorithm 4.1:
1: Choose υ linearly independent binary columns $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_\upsilon$, with column length equal or larger than υ.
2: Generate $\boldsymbol{b}_{\upsilon+1} = \boldsymbol{b}_1 \oplus \boldsymbol{b}_2$, $\boldsymbol{b}_{\upsilon+2} = \boldsymbol{b}_2 \oplus \boldsymbol{b}_3$, $\cdots$, $\boldsymbol{b}_{2^\upsilon-1} = \boldsymbol{b}_{2^\upsilon-1-\upsilon} \oplus \boldsymbol{b}_{2^\upsilon-\upsilon}$.
3: Obtain $2^\upsilon - 1$ binary matrices as $\boldsymbol{G}_{2,1} = [\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_\upsilon]$, $\boldsymbol{G}_{2,2} = [\boldsymbol{b}_2, \boldsymbol{b}_3, \cdots, \boldsymbol{b}_{\upsilon+1}]$, $\cdots$, $\boldsymbol{G}_{2,2^\upsilon-1} = [\boldsymbol{b}_{2^\upsilon-1}, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{\upsilon-1}]$.

Algorithm 4.2:
1: Get 2υ linearly independent binary columns of length 2υ, *e.g.* columns from the $2\upsilon \times 2\upsilon$ identity matrix.
2: Split the 2υ columns into two matrices $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$, with υ columns in each matrix.
3: Generate $2^\upsilon - 1$ matrices $\boldsymbol{G}_{2,1}, \cdots, \boldsymbol{G}_{2,2^\upsilon-1}$ based on the columns in $\boldsymbol{G}_2$ according to *Algorithm 4.1*. Set $\boldsymbol{G}_{2,1} = \boldsymbol{G}_2$.
4: Generate another $2^\upsilon - 1$ matrices by $\boldsymbol{G}_3 = \boldsymbol{G}_1 \oplus \boldsymbol{G}_{2,1}$, $\boldsymbol{G}_4 = \boldsymbol{G}_1 \oplus \boldsymbol{G}_{2,2}$, $\cdots$, $\boldsymbol{G}_{2^\upsilon+1} = \boldsymbol{G}_1 \oplus \boldsymbol{G}_{2,2^\upsilon-1}$. There are now a total of $2^\upsilon + 1$ matrices, *i.e.* $\boldsymbol{G}_1$, $\boldsymbol{G}_2$, $\boldsymbol{G}_3$, $\cdots$, $\boldsymbol{G}_{2^\upsilon+1}$.
5: Within each matrix $\boldsymbol{G}_k$, $k = 1, \cdots, 2^\upsilon + 1$, randomly combine the columns by XOR to generate $\sum_{k=2}^{\upsilon} C_\upsilon^k = 2^\upsilon - \upsilon - 1$ new binary columns. Added to original υ columns to generate a new matrix $\boldsymbol{B}_k$ composed of these $2^\upsilon - 1$ columns.
6: Within each matrix $\boldsymbol{B}_k$, randomly choose υ linearly independent columns to construct $\hat{\boldsymbol{H}}_k$, and thus $\hat{\boldsymbol{H}}$ is obtained.

We have two lemmas based on the *Algorithm 4.1* as follows.

Lemma 2: Columns in each $\boldsymbol{G}_{2,k}$, $k = 1, \cdots, 2^\upsilon - 1$ are linearly independent.

Lemma 3: Among $\boldsymbol{G}_{2,1}$, $\cdots$, $\boldsymbol{G}_{2,2^\upsilon-1}$, each matrix is the XOR combination of the other two matrices.

In the sequel, we present *Algorithm 4.2* to generate a basic matrix $\hat{\boldsymbol{H}}$ based on *Algorithm 4.1*.

Theorem 2: If we construct a basic matrix $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+2}]$ by *Algorithm 4.2*, then the columns in every two matrices of $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+2}$ are linearly independent, and the basic matrix $\hat{\boldsymbol{H}}$ satisfies the BLIC.

By *Algorithm 4.2*, we can generate a basic matrix as $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{2^\upsilon+1}]$, where $2^\upsilon + 1 = M + 2$. That is, *Algorithm 4.2* can support an $M - 2 - 1$ relaying network with $M \leq 2^\upsilon - 1$ to achieve full diversity.

B. Basic Matrix Design for the $M-N-1$ relaying network

Note that in the $M-N-1$ relaying network, the BLIC for the basic matrix $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}]$ is that the columns in every N of matrices $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}$ are linearly independent. Here, we consider the cases where $M \leq N$. To generate a basic matrix that satisfies the BLIC, we have *Algorithm 4.3*.

We now present a theorem regarding to the linearly independent property of the columns in any N of matrices $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}$.

Theorem 3: If we construct a basic matrix $\hat{\boldsymbol{H}} = [\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}]$ by *Algorithm 4.3*, then the columns in ev-

Algorithm 4.3: 1: Get $N\upsilon$ linearly independent binary columns of length $N\upsilon$, *e.g.* columns from the $N\upsilon \times N\upsilon$ identity matrix.
2: Split the $N\upsilon$ columns into N matrices $\boldsymbol{G}_1, \boldsymbol{G}_2, \cdots, \boldsymbol{G}_N$, with υ columns in each column.
3: For a given n, $n = 2, \cdots, N$, generate $2^\upsilon - 1$ matrices $\boldsymbol{G}_{n,0}, \cdots, \boldsymbol{G}_{n,2^\upsilon-2}$ based on the columns in $\boldsymbol{G}_n$ according to *Algorithm 4.1*. Note that $\boldsymbol{G}_{n,0} = \boldsymbol{G}_n$.
4: Generate $2^\upsilon - 1$ matrices by $\boldsymbol{G}_{N+1} = \boldsymbol{G}_1 \oplus \sum_{n=2}^{N} \oplus \boldsymbol{G}_{n,0}, \cdots, \boldsymbol{G}_{N+k} = \boldsymbol{G}_1 \oplus \sum_{n=2}^{N} \oplus \boldsymbol{G}_{n,(k-1)(n-1) \bmod (2^\upsilon-1)}, \cdots, \boldsymbol{G}_{N+2^\upsilon-1} = \boldsymbol{G}_1 \oplus \sum_{n=2}^{N} \oplus \boldsymbol{G}_{n,(2^\upsilon-2)(n-1) \bmod (2^\upsilon-1)}$.
5: Within each matrix $\boldsymbol{G}_k, k = 1, \cdots, N+2^\upsilon+1$ columns are randomly XORed to generate $\sum_{k=2}^{\upsilon} C_\upsilon^k = 2^\upsilon - \upsilon - 1$ new binary columns. Added to the original υ columns, we obtain a matrix $\boldsymbol{B}_k$ composed of these $2^\upsilon - 1$ columns.
6: Within each matrix $\boldsymbol{B}_k$, randomly choose υ linearly independent columns to construct $\hat{\boldsymbol{H}}_k$, and thus $\hat{\boldsymbol{H}}$ is obtained.

ery N of matrices $\hat{\boldsymbol{H}}_1, \cdots, \hat{\boldsymbol{H}}_{M+N}$ are linearly independent and the basic matrix $\hat{\boldsymbol{H}}$ satisfies the BLIC.

If we allocate the N original sets to the relays, then *Algorithm 4.3* can support an $M - N - 1$ relaying network with $M \leq 2^\upsilon - 1$.

V. Modified BP Decoder for Large Block Length

After obtaining the basic matrix $\hat{\boldsymbol{H}}$, we can easily extend $\hat{\boldsymbol{H}}$ to generate the parity check matrix $\boldsymbol{H}$ with a large block length. When the channel block length is large the ML decoder becomes impractical. The BP decoder is more efficient for large block length provided that the code has a low-density parity-check matrix. Recall that the parity check matrix $\boldsymbol{H}'$ in Section III is designed to achieve full diversity gain with a BP decoder. However, the matrix $\boldsymbol{H}'$ generated through $\boldsymbol{H}$ by Gaussian elimination could be very dense, which does not suit for BP decoding. In what follows, we modify the decoder to obtain full diversity and improve the error performance.

The modified BP decoder, which possesses two concatenated BP decoders, is shown in Fig. 3. The first BP decoder receives the channel log-likelihood ratio (LLR) values and uses $\boldsymbol{H}'$ as the parity check matrix to obtain full diversity. According to [12], $\boldsymbol{H}'$ can be seen as a root check (RC) LDPC code. Thus, all the variable nodes can achieve full diversity gain after one iteration of the first BP decoder. Note that in the first BP decoder, we only do iteration once to obtain diversity gain. Since $\boldsymbol{H}'$ is a dense matrix, the error performance becomes worse when executing more iterations in the first BP decoder.

The output LLR values are then used as the input of the second BP decoder. In this second BP decoder, the parity check matrix $\boldsymbol{H}$ is used for multiple iteration processing to improve the error performance. We obtain a desired $\boldsymbol{H}$ in the AWGN channels by searching its corresponding basic matrix $\hat{\boldsymbol{H}}$. More specifically, due to the same degree distribution, the code generated by parity check matrix $\boldsymbol{H}$ keeps the same threshold as that of the code generated by the corresponding basic matrix $\hat{\boldsymbol{H}}$. Therefore, we use the reciprocal-channel approximation (RCA) introduced in [14] to search an basic matrix $\hat{\boldsymbol{H}}$ with a good threshold.

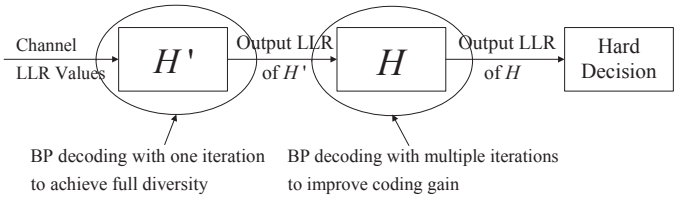


Fig. 3. The modified BP decoder based on the two concatenated BP decoders $\boldsymbol{H}'$ and $\boldsymbol{H}$. The parity check matrix $\boldsymbol{H}'$ is firstly used to achieve full diversity. Then the output LLR are used as the input of $\boldsymbol{H}$ to achieve high coding gain.

VI. Simulations

In the simulations, we focus on the two-source, two-relay network ($2 - 2 - 1$ relaying network). BPSK modulation is applied to all the network coding schemes in the simulations. We compare the proposed BFNC scheme with the GFNC scheme [6] and the CFNC scheme [7]. Firstly, we consider the network with small frame length *i.e.* $l = 3$ and $l_{block} = 12$. In this case, ML decoder is applied at the destination. We compare the proposed BFNC scheme with the GFNC scheme and the CFNC scheme. In the GFNC scheme, we choose the Galois field as GF(8) with 8 elements. At the relays, according to [6], we map a frame (three bits) into a Galois field element (GF symbol). At the first relay, we use the two Galois field elements 1 and 1 to combine the frames from the two sources. At the second relay, we use the two Galois field elements 1 and 2 to combine the frames from the two sources. In the CFNC scheme, space-time codes are applied to the relays to combine the frame from the two sources. The space-time coding matrix here is chosen according to [7].

In the BFNC scheme, we generate the 6×12 parity check matrix $\boldsymbol{H}$ by the proposed algorithms. Fig. 4 shows the block error probabilities (BLEP) of the $2 - 2 - 1$ relaying network with BFNC and CFNC. ML decoding is used at the destination. We can see that all the three schemes can achieve full diversity (3-order diversity). In addition, both the BFNC scheme and the GFNC scheme outperform the CFNC scheme. Even though the BFNC scheme and the GFNC scheme have almost the same performance, our BFNC scheme has lower encoding complexity than the GFNC scheme.

Then we consider the network with large block length. We assume that the frame length is $l = 300$. Therefore, the block length in the network is $l_{block} = 1200$. We compare the proposed BFNC scheme with the GFNC scheme. In the GFNC scheme, we choose the Galois field as GF(4). At the relays, we map every two bits of a frame into a GF symbol. Therefore, there are 150 GF symbols in a frame. At the first relay, we use the two GF(4) elements 1 and 1 to combine the two frames from the two sources. At the second relay, we use the two GF(4) elements 1 and 2 to combine the two frames from the two sources. At the destination, the j-th GF symbol, $j = 1, \cdots, 150$ of each frame are connected by the GFNC scheme (the network coded GF symbols at the relays can be seen as the parities of the GF symbols of the sources). Therefore, during a block period, ML decoder is

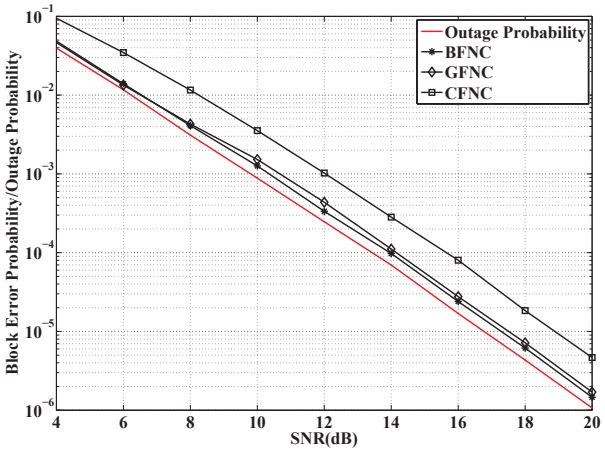


Fig. 4. Block error probabilities for the $2-2-1$ relaying network with block length 12. An ML decoder is used at the destination. We compare the BLEP performance for three network coding schemes, i.e., BFNC, GFNC, and CFNC.

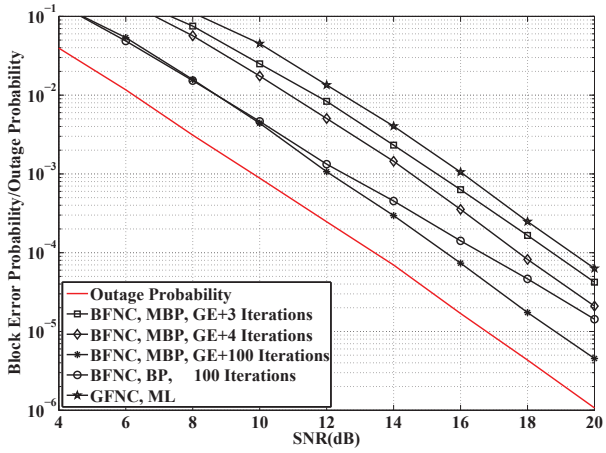


Fig. 5. Block error probabilities for the $2-2-1$ relaying network with block length 1200. For the BFNC scheme, the proposed BP decoder is used at the destination. For the GFNC scheme, an ML decoder is used at the destination.

utilized among the j-th symbols of all the frames. Since there are 150 GF symbols in a frame, we have 150 ML decoding processes within each block.

For the BFNC scheme with the block length 1200, we generate the 600×1200 parity check matrix $\boldsymbol{H}$ by the proposed algorithms. The modified BP decoder is applied to the destination. Fig. 5 shows the BLEP of the $2-2-1$ relaying network with both the BFNC scheme and the GFNC scheme. In the BFNC scheme, we compare the proposed modified BP deocoder (MBP) with the conventional BP (BP) decoder, which is based on the parity check matrix $\boldsymbol{H}$. We consider $3, 4, 100$ iterations of the parity check matrix $\boldsymbol{H}$ in the MBP decoder and 100 iterations in the BP decoder. From Fig. 5, we can see that due to the parity check matrix $\boldsymbol{H}'$, the MBP decoder with '3 Iterations', '4 Iterations' and '100 Iterations' can all achieve the full diversity gain (3-order diversity). The 100 iterations in $\boldsymbol{H}$ facilitates the system to achieve a higher coding gain. We can also see that due to the absence of $\boldsymbol{H}'$, the BP decoder with '100 Iterations' cannot achieve full diversity. Also in Fig. 5, the GFNC scheme with ML decoder can achieve full diversity. However, when compared to the BFNC scheme, the coding gain of GFNC is much worse. This is because the BFNC scheme with a BP decoder enables the joint decoding among all symbols of a block, while the GFNC scheme only decodes among every 4 GF symbols of a block.

VII. Conclusion

In this paper, we have studied a binary field network coding design for a multiple-source, multiple-relay wireless network with slow fading channels. We discussed a diversity-achieving criterion for the BFNC schemes with either an ML decoder or a BP decoder at the destination. Based on this criterion, we proposed an algorithm that constructs low complexity encoders, which are then used to generate our new BFNC schemes. Our simulation results show that our proposed BFNC schemes can achieve full diversity using ML decoding. In addition, our BFNC schemes can obtain improved coding gain relative to both the GFNC and the CFNC schemes.

References

[1] A. Sendonaris, E. Erkip, and B. Azhang, "User cooperation diversity - part I: system description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927-1938, Nov. 2003.

[2] A. Sendonaris, E. Erkip, and B. Azhang, "User cooperation diversity - part II: implementation aspects and performance analysis," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1939-1948, Nov. 2003.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network infomation flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.

[4] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: physical layer network coding," in *Proc. 12th MobiCom*, pp. 358C365, New York, NY, USA, 2006.

[5] M. Xiao and T. Aulin, "Optimal decoding and performance analysis of a noisy channel network with network coding," *IEEE Trans. on Commun.*, vol. 57, pp. 1402-1412, May 2009.

[6] M. Xiao and M. Skoglund, "Design of network codes for multiple-user multiple-relay wireless networks," *IEEE International Symposium on Information Theory (ISIT)*, pp. 2562-2566, Jun. 2009.

[7] T. Wang and G. B. Giannakis, "Complex Field Network Coding for Multiuser Cooperative Communications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 3, pp. 561-571, Apr. 2008.

[8] X. Bao, J. Li, "Adaptive network coded cooperation (ANCC) for wireless relay networks: matching code-on-graph with network-on-graph," *IEEE Trans. Wireless Commun.*, vol. 7, no. 2, pp. 574-583, Feb. 2008.

[9] J. Kim, S. Park, J. Kim, Y. Kim, and H. Song, "Joint LDPC codes for multi-user relay channel," *Fourth Workshop on Network Coding, Theory and Applications (NetCod)*, pp. 1-6, Jan. 2008.

[10] Y. Li, G. Song, and L. Wang, "Design of joint network-low density parity check codes based on the EXIT charts," *IEEE Communications Letters*, vol. 13, no. 8, pp. 600-602, Aug. 2009.

[11] S.-N. Hong, S. Kim, D.-J. Shin, and I. Lee, "Quasi-cyclic low-density parity check codes for space-time bit-interleaved coded modulation," *IEEE Communications Letters*, vol. 12, no. 10, pp. 767-769, Oct. 2008.

[12] J. J. Boutros, A. G. Fabregas, E. Biglieri, and G. Zemor, "Low-density paritycheck codes for nonergodicblock-fading channels," *submitted to IEEE Trans. Inf. Theory*, arXiv:0710.1182v1.

[13] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894-2901, Aug. 2005.

[14] S.-Y. Chung, *On the Construction of Some Capacity-Approaching Coding Schemes*, Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, Massachusetts, September 2000.