

## Multiuser Cooperative Diversity Through Network Coding Based on Classical Coding Theory

Authors: J. Rebelatto, B.Uchoa-Filho, Y. Li, B. Vucetic

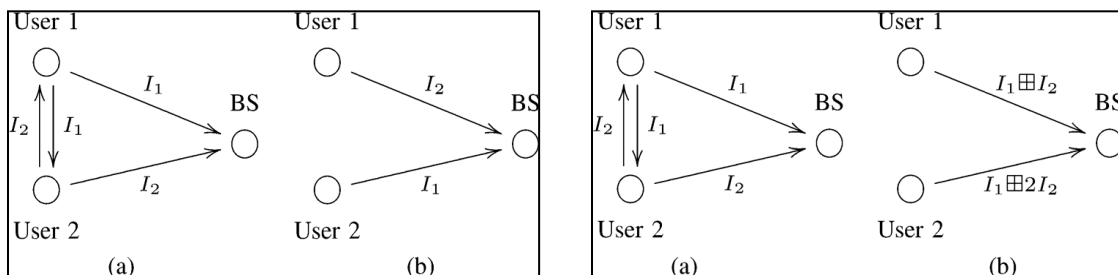
Publication: IEEE Trans. Sig. Processing, Feb. 2012.

Speaker: Jin-Taek Seong

**Short summary:** To increase the diversity order of cooperative wireless communication systems without sacrificing the system's rate, they propose the generalized dynamic-network code (GDNC). They showed that the problem of designing network codes that maximize the diversity order is related to that of designing optimal linear block codes, in the Hamming distance sense over finite fields.

### I. INTRODUCTION

In the network coding schemes, each user linearly combines the messages coming from other users, and generates a new message, and then forwards it to the destination.



- ❖ Each user broadcasts its own information
- ❖ With the routing protocol, each user transmits its partner's information after decoding,
- ❖ With network coding schemes, each user transmits a linear combination regenerated.

The contributions of this paper are:

- i) they investigate another relationship between network codes and classical error-correcting codes. They explain on the dynamic-network coding (DNC) scheme by first recognizing the associated network code design problem as equivalent to that

of designing linear block codes over for erasure correction. In particular, for perfect interuser channels, we note that the diversity order equals the minimum Hamming distance of the block code, so the network transfer matrix should correspond to the generator matrix of an optimal block code under the Hamming metric. The Singleton upper bound for the minimum Hamming distance of a linear block code appears as a natural limit to the diversity order, and this bound is achieved with a sufficiently large field size. The codes that achieve the Singleton bound are called *maximum distance separable* (MDS) codes.

- ii) Regarding the GDNC network code design, they show that if a generator matrix of a MDS code is used as the GDNC network code, the maximum diversity order is guaranteed. They also show that a much better tradeoff between rate and diversity order can be achieved, e.g., it is possible to improve both rate and diversity order over the DNC scheme.

## II. SYSTEM MODEL

### A. System Model

The received baseband codeword at User  $i$  at time  $t$  is given by

$$\mathbf{y}_{j,i,t} = h_{j,i,t} \mathbf{x}_{j,t} + \mathbf{n}_{j,i,t} \quad (1)$$

where  $j \in \{1, \dots, M\}$  represents the transmit user index and  $i \in \{0, 1, \dots, M\}$  the receive user index (0 corresponds to the BS).

The mutual information  $I_{j,i,t}$  between  $\mathbf{x}_{j,t}$  and  $\mathbf{y}_{j,i,t}$  is

$$I_{j,i,t} = \frac{1}{M} \log_2 \left( 1 + |h_{j,i,t}|^2 SNR \right) \quad (2)$$

where the factor  $1/M$  follows from the division of the channel's resources among the  $M$  users.

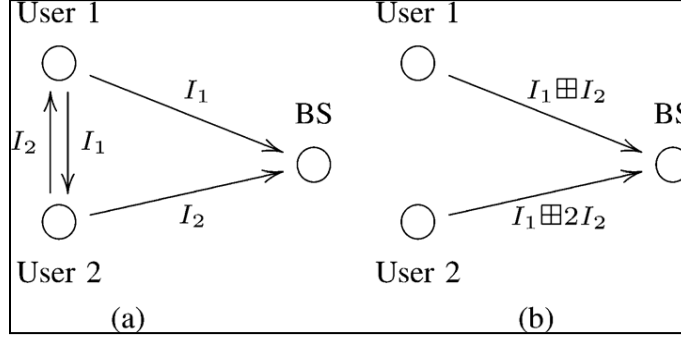
For Rayleigh fading, the outage probability is calculated as

$$P_e = \Pr \left\{ |h_{j,i,t}|^2 < g \right\} = 1 - e^{-g} \approx g \quad (3)$$

The diversity order  $D$  is defined as

$$D \triangleq \lim_{SNR \rightarrow \infty} \frac{-\log P_0}{\log SNR} \quad (4)$$

### B. Binary vs. Nonbinary Network Coded Cooperation



The network codes for both schemes are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}_{\text{Binary}} \begin{bmatrix} I_1 \\ I_2 \end{bmatrix} \quad (5)$$

and

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 2 \end{bmatrix}_{4\text{-ary}} \begin{bmatrix} I_1 \\ I_2 \end{bmatrix} \quad (6)$$

For the binary and 4-ary network coding schemes, the general and exact form of the outage probability of the  $I_1$  message at the BS are obtained as follows [1]

$$P_{o,4\text{-ary}} \approx \frac{A_1}{P_1^2 P_2} + \frac{A_2}{P_1 P_2^2} + \frac{A_3}{P_1^3} \quad (7)$$

and

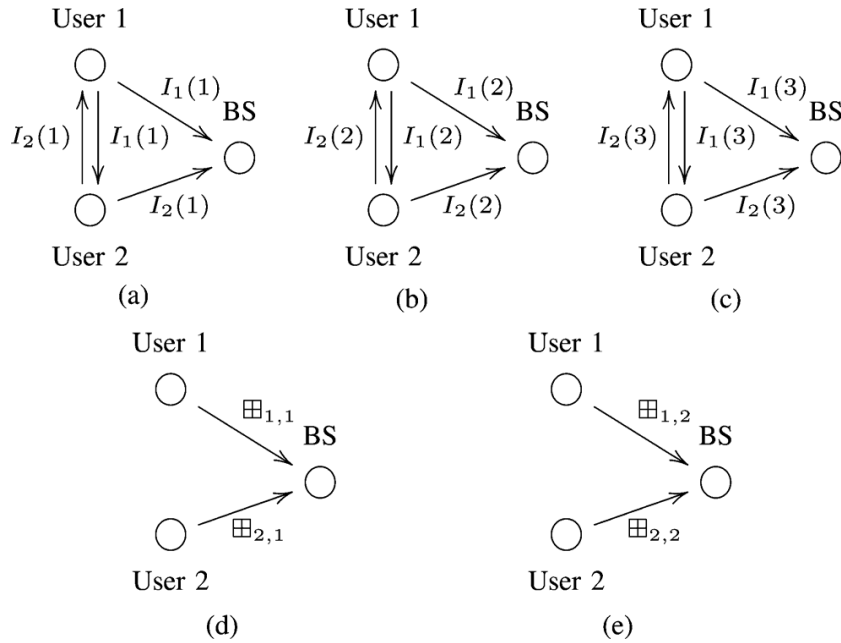
$$P_{o,\text{binary}} \approx \frac{B_1}{P_1 P_2} + \frac{B_2}{P_1^2 P_2} + \frac{B_3}{P_1 P_2^2} + \frac{B_4}{P_1^3} \quad (8)$$

where the constants  $A_c$  and  $B_c$  are determined by the variances of channel gains and transmission rates.

### III. GENERALIZED DYNAMIC-NETWORK CODES

In the DNC scheme [2], [3], the diversity order is related to the minimum number of correctly received packets at the BS from which the information packets from all users can be recovered.

A packet which is not received correctly may be thought of as an erasure, and is discarded by the receiver. The receiver's ability to recover the information packets from the non-erased packets is thus equivalent to the erasure correction capability of the associated (network) block code. It is well-known that the transmitted codeword of a linear block code with minimum Hamming distance can be recovered if no more than of its positions have been erased by the channel.



**For example:** Each user broadcasts three packets of its own in the broadcast phase, and then each user transmits two nonbinary linear combinations (of the six previously broadcasted packets) over in the cooperative phase, where is an integer greater than zero. The receiver collects the 10 packets, which can be seen as a codeword of a systematic 6/10 linear block code.

In this case, the outage probability of  $I_1(1)$  message can be approximately derived,

$$P_{o,1} = P_e P_{f,1} + (1 - P_e) P_{p,1} \approx P_e^4 \quad (9)$$

where the outage probability  $P_{f,1} \approx P_e^3$  is from fact that the 3 outage events (direct transmission and two parity messages) occur when User 2 cannot correctly decode  $I_1(1)$ , the outage probability  $P_{p,1} \approx P_e^5$  is obtained from that when User 2 can decode  $I_1(1)$ , one direct

transmission plus four parity messages are erased in the worst case. We can also verify that the outage probability is dominated by the term related to the interuser channel being in outage, when User 2 cannot help User 1.

The GDNC overall rate is given by

$$R_{GDNC} = \frac{k_1 M}{k_1 M + k_2 M} = \frac{k_1}{k_1 + k_2} \quad (10)$$

In general, for a rate  $k/n$  linear block code, the minimum Hamming distance is upper bounded by the Singleton bound,

$$d_{\min} \leq n - k + 1 \quad (11)$$

Thus, we can see that the diversity order of the GDNC scheme is upper bounded by

$$D_{GDNC} \leq k_2 M + 1 \quad (12)$$

However, due to outages in interuser channels, this upper bound cannot be achieved.

#### IV. ON THE NETWORK CODE DESIGN

**Theorem 1:** The diversity order of the GDNC scheme for an appropriately designed network code with sufficiently large field size is  $D_{GDNC} = M + k_2$ .

**Proof:** Let  $D_{j,t} \subseteq \{1, \dots, M\}$  be the index set corresponding the users that correctly decoded the information packet  $I_j(t)$ . We define a new set  $\mathcal{D}_{j,t}(I)$  as the set of all messages correctly decoded by the users in  $D_{j,t}$  in the broadcast phase, including  $I_j(t)$  itself. There are at least  $|\mathcal{D}_{j,t}(I)| + |D_{j,t}| k_2$  packets containing messages of  $\mathcal{D}_{j,t}(I)$ . For a fixed  $D_{j,t}$ , the message  $I_j(t)$  is declared and erased at the BS only if the direct transmission  $I_j(t)$  and the at least  $|D_{j,t}| k_2$  out of the remaining  $|\mathcal{D}_{j,t}(I)| + |D_{j,t}| k_2 - 1$  received packets are not correctly decoded by the BS which occurs with probability

$$\begin{aligned}
P_{o,j}(\bar{D}_{j,t}) &= P_e \left[ \sum_{F=|\bar{D}_{j,t}|k_2}^{|\mathcal{D}_{j,t}(I)|+|\bar{D}_{j,t}|k_2-1} \binom{|\mathcal{D}_{j,t}(I)|+|\bar{D}_{j,t}|k_2-1}{F} P_e^F (1-P_e)^{(|\mathcal{D}_{j,t}(I)|+|\bar{D}_{j,t}|k_2-1)-F} \right] \\
&\approx P_e \left[ \binom{|\mathcal{D}_{j,t}(I)|+|\bar{D}_{j,t}|k_2-1}{|\bar{D}_{j,t}|k_2} P_e^{|\bar{D}_{j,t}|k_2} \right] \\
&= \gamma(k_1, k_2, \bar{D}_{j,t}) P_e^{(M-|\bar{D}_{j,t}|)k_2+1}, \quad \gamma(k_1, k_2, \bar{D}_{j,t}) = \binom{|\mathcal{D}_{j,t}(I)|+|\bar{D}_{j,t}|k_2-1}{|\bar{D}_{j,t}|k_2}
\end{aligned} \tag{13}$$

The outage probability of the information message  $I_j(t)$  is given by

$$\begin{aligned}
P_{o,j} &= \sum_{\bar{D}_{j,t}} P_e^{|\bar{D}_{j,t}|} (1-P_e)^{(M-1)-|\bar{D}_{j,t}|} P_{o,j}(\bar{D}_{j,t}) \\
&\approx \sum_{\bar{D}_{j,t}} P_e^{(M-|\bar{D}_{j,t}|)k_2+|\bar{D}_{j,t}|+1} \gamma(k_1, k_2, |\bar{D}_{j,t}|) \\
&\approx \binom{M-1}{|\bar{D}_{j,t}|^*} P_e^{(M-|\bar{D}_{j,t}|^*)k_2+|\bar{D}_{j,t}|^*+1} \gamma(k_1, k_2, |\bar{D}_{j,t}|^*)
\end{aligned} \tag{14}$$

For  $k_2 \geq 2$ ,  $|\bar{D}_{j,t}|^* = M-1$  since the lowest exponent achieves. Thus, the exponent of (14) is  $M+k_2$ .

**Theorem 2:** An  $(n, k, d_{\min})$  code  $\mathcal{C}$  with generator matrix  $\mathbf{G} = [\mathbf{I} | \mathbf{P}]$ , is minimum distance separable (MDS) if and only if every square submatrix of  $\mathbf{P}$  is nonsingular.

We consider network codes in the light of classical coding theory. Let  $\mathcal{C}$  be an  $(n, k, d_{\min})$  linear block code over  $\text{GF}(q)$  with systematic generator matrix  $\mathbf{G}$  given by

$$\mathbf{G} = \left[ \begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & p_{1,1} & p_{1,2} & \cdots & p_{1,n-k} \\ 0 & 1 & \cdots & 0 & p_{2,1} & p_{2,2} & \cdots & p_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{k,1} & p_{k,2} & \cdots & p_{k,n-k} \end{array} \right] = [\mathbf{I}_k | \mathbf{P}_{k \times n-k}] \tag{15}$$

### A. A Theory of Faulty Generator Matrices

We study some properties of new block codes obtained from systematic MDS codes by zeroing some entries of its generator matrix, and we refer to the obtained generator matrix as *faulty generator matrix*.

**Theorem 3:** Let  $\mathcal{C}$  be an  $(n, k, d_{\min})$  MDS code with systematic generator matrix  $\mathbf{G} = [\mathbf{I} | \mathbf{P}]$ . The replacement by zeros of  $\delta$  entries in any row of the matrix  $\mathbf{P}$  gives rise to  $(n, k, d_{\min} - \delta)$  code  $\mathcal{C}$ .

**Theorem 4:** If a systematic generator matrix of a MDS code  $\mathcal{C}$  with minimum Hamming distance  $d_{\min} = Mk_2 + 1$  is used as a transfer matrix of the GDNC scheme, the diversity order  $D_{GDNC} = M + k_2$  is guaranteed.

**Proof:** One fault corresponds to one interuser channel being in outage. When that happens, the user's receiver cannot correctly decode its partner's information, so, when forming  $k_2$  linear combinations to generate its  $k_2$  parity-check packets, this user replaces this erroneous packet with an all-zero packet, or equivalently, sets to zero the  $k_2$  coefficients associated with this partner. This amounts to replacing by zeros the  $k_2$  corresponding entries (in same row) of the parity matrix  $\mathbf{P}$ , i.e.,  $|A| = k_2$ . Since each user knows its own information,  $k_2$  entries in each row of  $\mathbf{P}$  are immune to faults, while the other  $k_2(M - 1)$  entries are subject to faults. In the worst scenario, when all the possible faults happen, the generator matrix takes the form

$$\mathbf{G} = \left[ \begin{array}{c|ccc} & P_1 & & \\ \hline I & & \ddots & \\ & & & P_M \end{array} \right] \quad (16)$$

where the  $(k_1 \times k_2)$  submatrix  $P_i$  contains the immune entries associated with User  $i$ . From Theorem 2, we know that every submatrix of  $P_i$  is nonsingular. Thus, the **least minimum Hamming distance** of a block code obtained from the original MDS code  $\mathcal{C}$  due to the occurrence of faults is  $k_2 + 1$ . Nevertheless, the same minimum Hamming distance can be

achieved with a much lower number of faults. We can see that the minimum number of faults for a code with minimum distance  $k_2 + 1$  is  $M - 1$ , when all of these faults occur in the same row of  $\mathbf{P}$ , for example.

For all the possible minimum distances in the range  $k_2 + 1 \leq d_{\min} \leq Mk_2 + 1$ , a sufficient condition for the worst possible scenario (the lowest number of faults that result in this minimum distance) is when all the faults are located in the same row of  $\mathbf{P}$ . Thus, we can observe that the larger the number of faults in a given row (and consequently the lower the minimum distance of the resulting code), the lower the composite minimum distance. This assures that the code with minimum distance  $k_2 + 1$  is the one that generates the least composite minimum distance, with is then given by, see the Appendix in detail,

$$\begin{aligned}
 d_{\min}^{comp} &= \min_{B_x \in \mathcal{B}} \left\{ d_{\min} \left( C(B_x) \right) + |B_x| / |A| \right\} \\
 &= (k_2 + 1) + (M - 1) \\
 &= M + k_2
 \end{aligned} \tag{17}$$

It is easy to see the connection between the two terms in the composed minimum distance and the exponents of  $P_e$ .



## V. SIMULATION RESULTS

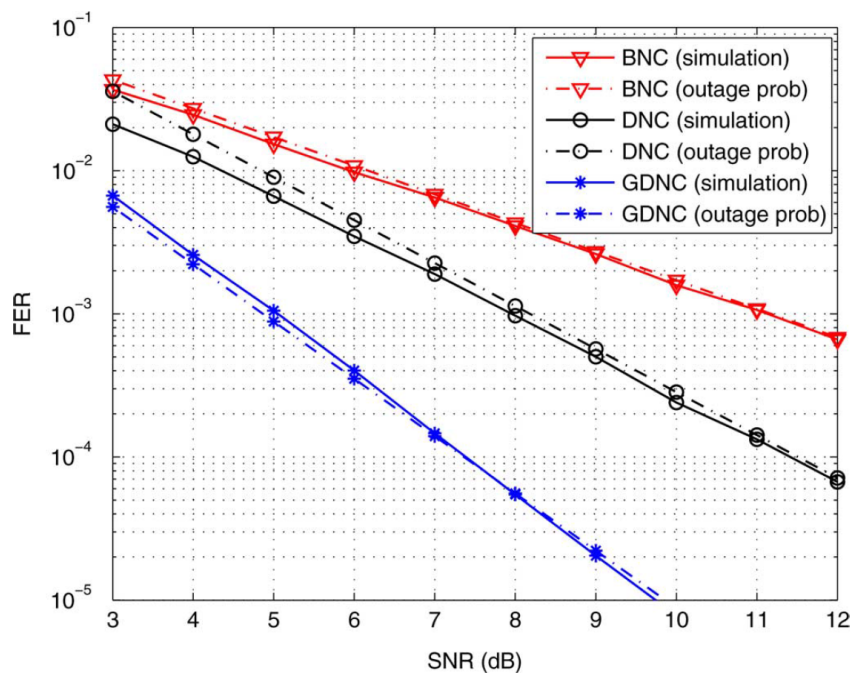


Fig. 5. FER versus SNR (dB) of a 2-user system with the BNC scheme, DNC scheme [in GF(4)] and the proposed GDNC scheme (with  $k_1 = k_2 = 2$  and in GF(8), according to Table I), all with rate 1/2.

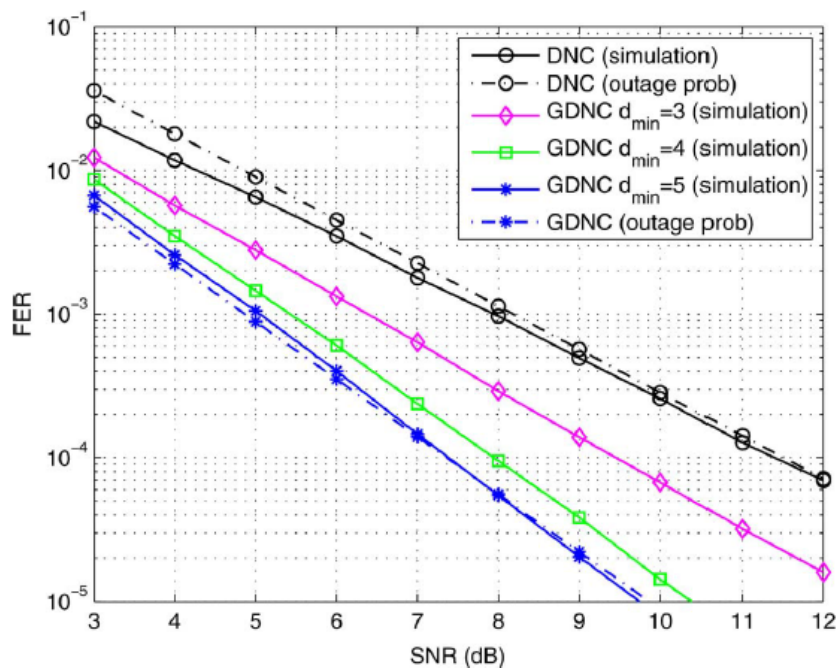


Fig. 6. FER versus SNR (dB) of a 2-user system with the DNC scheme [in GF(4)] and the proposed GDNC scheme (with  $k_1 = k_2 = 2$  and in GF(8), according to Tables I and III), all with rate 1/2.

TABLE 1  
NETWORK CODES OBTAINED FROM RS CODES FOR  $M = 2$  USERS

$k_1$	$k_2$	Code rate	Field size $q$	Parity matrix $\mathbf{P}$
1	1	2/4	4	$\begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$
1	2	2/6	8	$\begin{bmatrix} 3 & 5 & 1 & 7 \\ 2 & 4 & 3 & 6 \end{bmatrix}$
2	1	4/6	8	Obtained from the 4/8 code by puncturing the last 2 columns
2	2	4/8	8	$\begin{bmatrix} 3 & 7 & 3 & 6 \\ 5 & 7 & 7 & 4 \\ 2 & 4 & 6 & 1 \\ 5 & 5 & 3 & 2 \end{bmatrix}$
2	3	4/10	16	Obtained from the 4/12 code by puncturing the last 2 columns
2	4	4/12	16	$\begin{bmatrix} 14 & 5 & 7 & 10 & 4 & 10 & 8 & 9 \\ 12 & 4 & 14 & 5 & 12 & 12 & 14 & 7 \\ 13 & 6 & 12 & 15 & 8 & 1 & 4 & 10 \\ 14 & 6 & 4 & 1 & 1 & 6 & 3 & 5 \end{bmatrix}$
3	2	6/10	16	Obtained from the 6/12 code by puncturing the last 2 columns
3	3	6/12	16	$\begin{bmatrix} 11 & 2 & 4 & 6 & 14 & 12 \\ 1 & 11 & 13 & 10 & 14 & 10 \\ 2 & 4 & 2 & 10 & 5 & 9 \\ 6 & 13 & 12 & 11 & 8 & 12 \\ 4 & 12 & 12 & 2 & 6 & 6 \\ 11 & 13 & 10 & 14 & 10 & 4 \end{bmatrix}$

## VI. DISCUSSION

After meeting, please write discussion in the meeting and update your presentation file.

## VII. APPENDIX

When a set of entries of the generator matrix  $\mathbf{P}$  of the MDS code  $\mathcal{C}$  is replaced by zeros, the new code  $\mathcal{C}'$  produced is no longer MDS. Let  $A = \{(a_1, b_1), (a_2, b_2), \dots\}$  be a subset of entries of  $\mathbf{P}$  that are replaced by zeros, where  $(a, b)$  is the entry in row  $a$  and column  $b$  of the matrix  $\mathbf{P}$ . We call  $A$  as a *fault*. Let  $\mathcal{A} = \{A_0, A_1, \dots, A_{f-1}\}$  be a collection of  $f$  faults. We consider that two different faults  $A_i$  and  $A_j$  cannot contain a common entry of the matrix  $\mathbf{P}$ . That is,  $A_i \cap A_j = \emptyset$ . It is also considered that every fault has fixed cardinality, i.e.,  $|A_i| = |A| \forall i$ .

Let  $\chi = (\chi_0, \chi_1, \dots, \chi_{f-1})$  be the binary indicator vector associated with the occurrence of faults, where

$$\begin{cases} \chi_i = 1, & \text{if } A_i \text{ occurs} \\ \chi_i = 0, & \text{if } A_i \text{ does not occur} \end{cases} \quad (18)$$

For a nonnegative integer  $i$ , let  $b(i)$  denote the binary (vector) representation of  $i$ . We denote the collection of all possible combinations of faults by  $\mathcal{B} = \{B_{b(0)}, B_{b(1)}, \dots, B_{b(2^f-1)}\}$ , with  $B_\chi = \{(a, b) | (a, b) \in \bigcup_{i: \chi_i=1} A_i\}$ . Each event  $B_\chi$ , which consists of the occurrence of  $|\mathcal{B}_\chi|/|A|$ , gives rise to a new generator matrix of a block code  $\mathcal{C}(B_\chi)$  with minimum Hamming distance  $d_{\min}(\mathcal{C}(B_\chi))$ . We also define the *minimum composite distance* of the code  $\mathcal{C}(B_\chi)$  as

$$d_{\min}^{\text{comp}}(\mathcal{C}(B_\chi)) \triangleq d_{\min}(\mathcal{C}(B_\chi)) + |\mathcal{B}_\chi|/|A| \quad (19)$$

which is composed of its minimum Hamming distance  $d_{\min}(\mathcal{C}(B_\chi))$  plus a ‘‘compensation’’ term related to the number of faults in the combination  $B_\chi$ .

A parameter of fundamental importance to indicate the performance of a MDS code subject to a set of faulty generator matrices is the least minimum composite distance of any possible

combination of faults. In particular, given a MDS code  $\mathcal{C}$  and a collection of  $f$  faults  $\mathcal{A}$ , this distance is defined as

$$d_{\min}^{\text{comp}}(\mathcal{C}, \mathcal{A}) \triangleq \min_{B_\chi \in \mathcal{B}} \left\{ d_{\min}^{\text{comp}}(\mathcal{C}(B_\chi)) \right\} \quad (20)$$

where, when there is no confusion, it is simply called minimum composite distance.

### Reference

- [1] J.T. Seong and H.N. Lee, "4-ary Network Coding for Two Nodes in Cooperative Wireless Networks: Exact Outage Probability and Coverage Expansion," To appear EURASIP Wirel. Comm. Networking.
- [2] M. Xiao and M. Skoglund, "M-user cooperative wireless communications based on nonbinary network codes," in *Proc. IEEE Inf. Theory Workshop (ITW'09), Jun. 2009*, pp. 316–320.
- [3] M. Xiao and M. Skoglund, "Multiple-user cooperative communications based on linear network coding," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3345–3351, Dec. 2010