Characterizations of Network Error Correction/Detection and Erasure Correction

Shenghao Yang
Department of Information Engineering
The Chinese University of Hong Kong
Email: shyang5@ie.cuhk.edu.hk

Raymond W. Yeung
Department of Information Engineering
The Chinese University of Hong Kong
Email: whyeung@ie.cuhk.edu.hk

***Abstract*— In classical algebraic coding theory, the minimum distance of black code completely determines the ability of the code in terms of error correction/detection and erasure correction. We have obtained generalizations of these results for network codes.**

I. Introduction

In the previous studies of network coding, the transmission over networks is mostly assumed to be error-free [1]. However, in practical communication networks, transmission suffers different kinds of errors, such as random errors, link failures, traffic congestion and malicious modifications. Some researchers have noticed that network coding can be used to detect and correct errors in networks [2]–[7]. The concept of network error correction coding, a generalization of classical error correction coding, was first introduced by Cai and Yeung [4]–[6]. They generalized the Hamming bound, the Singleton bound and the Gilber-Vashamov bound in classical error correction coding to network coding. Zhang [7] introduced the minimum rank for linear network codes, which plays a role similar to that of the minimum distance in decoding classical error-correcting codes. The relation between network coding and classical algebraic coding has been clarified in [1].

In this paper, the weight properties of linear network codes are investigated. We first introduce some new weight definitions, called the network Hamming weight, for error vectors, receive vectors and message vectors. All these network Hamming weights reduce to the usual Hamming weight in the special case of classical error correction. With these network Hamming weights, the minimum distance of a network code can be defined. The main contribution of this paper is to characterize the ability of network codes for error correction, error detection and erasure correction in terms of the minimum distances of the codes. Specifically, we show that the following properties of a linear network code are equivalent:

1) The multicast minimum distance of the code is larger than or equal to d.
2) The code can correct all error vectors with Hamming weight less than $d/2$.
3) The code can detect all non-zero error vectors with Hamming weight less than d.
4) The code can correct all erasures with Hamming weight less than d.

This paper is organized as follows. Section II formulates the network error correction problem. Section III defines the network Hamming weights and the minimum distances for network codes. The error correcting and detecting abilities of a network code are characterized in Section IV. Section V discusses the relation between minimum rank decoding and minimum distance decoding for network error correction. The erasure correction ability of a network code is characterized in Section VI. In the last section we summarize our work and discuss topics for further research.

II. Problem Formulation

We study network transmission in a directed acyclic communication network denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes in the network and $\mathcal{E}$ is the set of edges in the network. We assume an order on the edge set $\mathcal{E}$ which is consistent with the partial order induced by the acyclicity of $\mathcal{G}$. An edge from node a to b, denoted by (a, b), represents a communication channel from node a to node b. We call node a (node b) the input node (output node) of edge (a, b), and edge (a, b) an input edge (output edge) of node b (node a). Let $In(a) = \{(b, a) : (b, a) \in \mathcal{E}\}$ and $Out(a) = \{(a, b) : (a, b) \in \mathcal{E}\}$ be the sets of input edges and output edges of node a, respectively. There can be multiple edges between a pair of nodes, and each edge can transmit one symbol in a field $GF(q)$.

A multicast on $\mathcal{G}$ transmits information from a source node s to a set of sink nodes $\mathcal{U}$. Let $n_s = |Out(s)|$. The source node s modulates the information to be multicast into a row vector $\mathbf{x} \in GF(q)^{n_s}$ called the *message vector*. The vector is sent in one use of the network by mapping the n_s symbols of the vector onto each edges in $Out(s)$. Define an $n_s \times |\mathcal{E}|$ matrix $A = [A_{i,j}]$ as

$$A_{i,j} = \begin{cases} 1 & e_j \text{ is the } i\text{th edge in } Out(s), \\ 0 & \text{other wise.} \end{cases}$$

By applying the order on $\mathcal{E}$ to $Out(s)$, the n_s nonzero columns of A form an identity matrix. An error vector $\mathbf{z}$ is an $|\mathcal{E}|$-tuple with each component representing the error on an edge.

A network code for network $\mathcal{G}$ is specified by a set of local encoding functions $\{k_{e_i,e_j} : e_i, e_j \in \mathcal{E}\}$ and the message set $\mathcal{C}$. Only linear local encoding functions are considered in this

paper. Define the $|\mathcal{E}|\times|\mathcal{E}|$ one-step transformation matrix $K = [K_{i,j}]$ in network $\mathcal{G}$ as

$$K_{i,j} = \begin{cases} k_{e_i,e_j} & e_i \in In(a), e_j \in Out(a) \text{ for some } a \in \mathcal{V}, \\ 0 & \text{other wise.} \end{cases}$$

For an acyclic network, $K^N = \mathbf{0}$ for some positive integer N. Define the transfer matrix of the network by $F = (I-K)^{-1}$ [8], so that the symbols transmitted on the edges are given by the components of $(\mathbf{x}A + \mathbf{z})F$.

For a sink node $u \in \mathcal{U}$, write $n_u = In(u)$, and define an $|\mathcal{E}| \times n_u$ matrix $B = [B_{i,j}]$ for sink node u as

$$B_{i,j} = \begin{cases} 1 & e_i \text{ is the } j\text{th edge in } In(u), \\ 0 & \text{other wise.} \end{cases}$$

The n_u nonzero rows of B form a permutation matrix. The received vector for a sink node u is

$$\begin{aligned} \mathbf{y}_u &= (\mathbf{x}A + \mathbf{z})FB, \\ &= \mathbf{x}F_{s,u} + \mathbf{z}F_u, \end{aligned} \tag{1}$$

where $F_{s,u} = AFB$ is the submatrix of F given by the intersection of the n_s rows corresponding to the edges in $Out(s)$ and the n_u columns corresponding to the edges in $In(u)$, and $F_u = FB$ is the columns of F corresponding to the input edges of u. $F_{s,u}$ and F_u are the transfer matrices of message transmission and error transmission, respectively, for the sink node u.

Equation (1) is our formulation of the multicast network error correction problem. The classical error correction problem is a special case in which both of $F_{s,u}$ and F_u reduce to identity matrices. The message transmission capacity is measured by the rank of the transfer matrix $F_{s,u}$. Denote the maximum flow between source node s and sink node u by maxflow(s,u). Evidently, for any linear network code on $\mathcal{G}$, the rank of $F_{s,u}$ is upper bounded by maxflow(s,u) [1]. Let $\mathcal{C}$ be the set of message vectors that can be transmitted by the source. When the network is error-free, the error correction problem is reduced to the usual network coding problem, for which the size of $\mathcal{C}$ is upper bounded by $q^{\min_{u\in\mathcal{U}} \text{maxflow}(s,u)}$ [9].

In this paper, the transmission problem formulated by (1) is studied in the scenario that there can be errors in the edges (channels), which may be due to channel noise, link failures, traffic congestion, malicious modifications, and so on. Classical coding theory refers to the message set $\mathcal{C}$ as the code. In network error correction coding, the code consists of the message set $\mathcal{C}$ as well as the local encoding functions of all the nodes in the network. If $\mathcal{C}$ is a linear space, we say the network code is linear, other wise, non-linear.

III. Network Hamming Weights

The Hamming weight and the Hamming distance are instrumental for quantifying the ability of a classical block code for error correction, error detection and erasure correction. We will introduce similar definitions of weights and distances for network codes in this section.

The idea behind the definition of the distance of two message vectors in the context of networks is that the distance should be measured by the weight of error vectors which can confuse the reception of these two messages at the sinks. In classical error correction, the weight of an error vector $\mathbf{z}$ is measured by the number of non-zero components of the error vector which is called the Hamming weight of $\mathbf{z}$ and is denoted by $w_H(\mathbf{z})$. This distance measure, however, cannot be applied to the network case, because only the linear transformation of an error vector affects the reception at the sinks. Thus, we should measure the weight of an error vector by some linear transformation of the error vector. Further, the definition of the weight of an error vector $\mathbf{z}$ should satisfy two conditions: 1) If $\mathbf{z}F_u = \mathbf{0}$, then the weight of $\mathbf{z}$ is zero; 2) If the difference of two error vectors is an error vector with weight $\mathbf{0}$, then these two error vectors have the same weight.

For any $u \in \mathcal{U}$, let $\Upsilon_u(\mathbf{y}) = \{\mathbf{z} : \mathbf{z}F_u = \mathbf{y}\}$ for a received vector $\mathbf{y} \in Im(F_u)$, the image space of F_u.

Definition 1: For any sink u, the network Hamming weight of a received vector $\mathbf{y}$ is defined by

$$W_u^{rec}(\mathbf{y}) = \min_{\mathbf{z}\in\Upsilon_u(\mathbf{y})} w_H(\mathbf{z}). \tag{2}$$

Definition 2: For any sink u, the network Hamming weight of an error vector $\mathbf{z}$ is defined by

$$W_u^{err}(\mathbf{z}) = W_u^{rec}(\mathbf{z}F_u). \tag{3}$$

In other words, $W_u^{err}(\mathbf{z})$ is the minimum Hamming weight of any error vector that causes the same confusion at sink u as the error vector $\mathbf{z}$. For any vector $\mathbf{z} \in \Upsilon_u(\mathbf{0})$, $W_u^{err}(\mathbf{z}) = W_u^{rec}(\mathbf{0}) = \min_{z\in\Upsilon_u(\mathbf{0})} w_H(\mathbf{z}) = w_H(\mathbf{0}) = 0$. If error vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ satisfy $\mathbf{z}_1 - \mathbf{z}_2 \in \Upsilon_u(\mathbf{0})$, then $W_u^{err}(\mathbf{z}_1) = W_u^{rec}(\mathbf{z}_1F_u) = W_u^{rec}(\mathbf{z}_2F_u) = W_u^{err}(\mathbf{z}_2)$. Thus Definition 2 satisfies the two conditions required for the definition of the weight of error vectors.

Definition 3: For any sink u, the network Hamming weight of a message vector x is defined by

$$W_u^{msg}(\mathbf{x}) = W_u^{rec}(\mathbf{x}F_{s,u}). \tag{4}$$

In other words, $W_u^{msg}(\mathbf{x})$ is the minimum Hamming weight of any error vector that has the same effect on sink u (when the message vector is $\mathbf{0}$) as the message vector $\mathbf{x}$ (when the error vector is $\mathbf{0}$).

Definition 4: For any $u \in \mathcal{U}$, the network Hamming distance between two received vectors $\mathbf{y}_1$ and $\mathbf{y}_2$ is defined by

$$D_u^{rec}(\mathbf{y}_1, \mathbf{y}_2) = W_u^{rec}(\mathbf{y}_1 - \mathbf{y}_2). \tag{5}$$

Definition 5: For any $u \in \mathcal{U}$, the network Hamming distance between two message vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ is defined by

$$D_u^{msg}(\mathbf{x}_1, \mathbf{x}_2) = W_u^{msg}(\mathbf{x}_1 - \mathbf{x}_2). \tag{6}$$

When $F_u = F_{s,u} = I$, these definitions reduce to the usual Hamming weight and Hamming distance.

Theorem 1 (Basic properties): Let $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2 \in \text{GF}(q^{n_s})$ be message vectors, $\mathbf{y}, \mathbf{y}_1, \mathbf{y}_2 \in Im(F_u)$ be received vectors, and $\mathbf{z} \in \text{GF}(q^{|\mathcal{E}|})$ be an error vector. Then

1) $W_u^{err}(\mathbf{z}) \le w_H(\mathbf{z})$, $W_u^{msg}(\mathbf{x}) = W_u^{err}([\mathbf{x}\ \mathbf{0}])$, and $W_u^{msg}(\mathbf{x}) \le w_H(\mathbf{x})$, where $[\mathbf{x}\ \mathbf{0}]$ is the error vector obtained by concatenating the message vector $\mathbf{x}$ by the zero vector.

2) $D_u^{msg}(\mathbf{x},\mathbf{x}_1) = D_u^{msg}(\mathbf{x}_1,\mathbf{x}) = D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}_1F_{s,u})$ $= D_u^{rec}(\mathbf{x}_1F_{s,u},\mathbf{x}F_{s,u})$.
3) (Triangle inequality)

$$D_u^{rec}(\mathbf{y}_1,\mathbf{y}) + D_u^{rec}(\mathbf{y},\mathbf{y}_2) \geq D_u^{rec}(\mathbf{y}_1,\mathbf{y}_2),$$

and

$$D_u^{msg}(\mathbf{x}_1,\mathbf{x}) + D_u^{msg}(\mathbf{x},\mathbf{x}_2) \geq D_u^{msg}(\mathbf{x}_1,\mathbf{x}_2).$$

Proof: The first inequality in Property 1) is a direct consequence of the definitions. The equality in Property 1) can be obtained from the fact that $[\mathbf{x}\ \mathbf{0}]F_u = \mathbf{x}F_{s,u}$. The second inequality holds since $W_u^{msg}(\mathbf{x}) = W_u^{err}([\mathbf{x}\ \mathbf{0}]) \leq w_H([\mathbf{x}\ \mathbf{0}]) = w_H(\mathbf{x})$.

The symmetry of the distances in Property 2) is obvious. The other part of this property holds since $D_u^{msg}(\mathbf{x},\mathbf{x}_1) = W_u^{msg}(\mathbf{x}-\mathbf{x}_1) = W_u^{rec}((\mathbf{x}-\mathbf{x}_1)F_{s,u}) = D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}_1F_{s,u})$.

We now prove the third property. Consider $\mathbf{z}_1 \in \Upsilon_u(\mathbf{y}_1-\mathbf{y})$ and $\mathbf{z}_2 \in \Upsilon_u(\mathbf{y}-\mathbf{y}_2)$ such that $D_u^{rec}(\mathbf{y}_1,\mathbf{y}) = w_H(\mathbf{z}_1)$ and $D_u^{rec}(\mathbf{y},\mathbf{y}_2) = w_H(\mathbf{z}_2)$. Since $\mathbf{z}_1+\mathbf{z}_2 \in \Upsilon_u(\mathbf{y}_1-\mathbf{y}_2)$, we have

$$\begin{aligned} D_u^{rec}(\mathbf{y}_1,\mathbf{y}_2) &= W_u^{rec}(\mathbf{y}_1-\mathbf{y}_2) \\ &\leq w_H(\mathbf{z}_1+\mathbf{z}_2) \\ &\leq w_H(\mathbf{z}_1)+w_H(\mathbf{z}_2) \\ &= D_u^{rec}(\mathbf{y}_1,\mathbf{y}) + D_u^{rec}(\mathbf{y},\mathbf{y}_2). \end{aligned}$$

The triangle inequality for the distance of message vectors can be obtained by considering

$$\begin{aligned} & D_u^{msg}(\mathbf{x}_1,\mathbf{x}) + D_u^{msg}(\mathbf{x},\mathbf{x}_2) \\ &= D_u^{rec}(\mathbf{x}_1F_{s,u},\mathbf{x}F_{s,u}) + D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}_2F_{s,u}) \\ &\geq D_u^{rec}(\mathbf{x}_1F_{s,u},\mathbf{x}_2F_{s,u}) \\ &= D_u^{msg}(\mathbf{x}_1,\mathbf{x}_2). \end{aligned}$$

■

A message set $\mathcal{C}$ for a multicast in network $\mathcal{G}$ is a subset of the vector space $GF(q)^{n_s}$. Note that we do not require $\mathcal{C}$ to be a linear space.

Definition 6: The *unicast minimum distance* of a network code with message set $\mathcal{C}$ for sink node u is defined by

$$d_{\min,u} = \min\{D_u^{msg}(\mathbf{x},\mathbf{x}') : \mathbf{x},\mathbf{x}' \in \mathcal{C}, \mathbf{x} \neq \mathbf{x}'\}.$$

Definition 7: The *multicast minimum distance* of a network code with message set $\mathcal{C}$ is defined by

$$d_{\min} = \min_{u\in\mathcal{U}} d_{\min,u}.$$

IV. Error Correction and Detection Capacities

In this section, we study the performance of a network code for correcting and detecting errors. We assume that a sink node u knows the message set $\mathcal{C}$ as well as the transfer matrices $F_{s,u}$ and F_u.

A. Unicast Case

Theorem 2: For a sink node u, the following three properties of a network code are equivalent:

1) The code can correct any error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq t$.
2) The code can correct any error vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq t$.
3) The code has $d_{\min,u} \geq 2t+1$.

Proof: To prove 3) ⇒ 2), we assume $d_{\min,u} \geq 2t+1$. When the message vector is $\mathbf{x}$ and the error vector is $\mathbf{z}$, the received vector at sink u is $\mathbf{y}_u = \mathbf{x}F_{s,u}+\mathbf{z}F_u$. We then declare the transmitted message vector to be

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathcal{C}} D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{y}_u). \tag{7}$$

We will show that this decoding algorithm can always decode correctly for any message vector $\mathbf{x}$ and any error vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq t$. To this end, by means of the triangle inequality, we obtain

$$D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{y}_u) + D_u^{rec}(\mathbf{x}'F_{s,u},\mathbf{y}_u) \geq D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}'F_{s,u}),$$

where $\mathbf{x}'$ is any other message vector not equal to $\mathbf{x}$. Since $D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}'F_{s,u}) = D_u^{msg}(\mathbf{x},\mathbf{x}') \geq d_{\min,u} \geq 2t+1$ and $D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{y}_u) = W_u^{rec}(\mathbf{x}F_{s,u}-\mathbf{y}_u) = W_u^{rec}(\mathbf{z}F_u) = W_u^{err}(\mathbf{z}) \leq t$, we have

$$\begin{aligned} & D_u^{rec}(\mathbf{x}'F_{s,u},\mathbf{y}_u) \\ &\geq D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{x}'F_{s,u}) - D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{y}_u) \\ &\geq t+1 \\ &> D_u^{rec}(\mathbf{x}F_{s,u},\mathbf{y}_u). \end{aligned}$$

So the decoding algorithm gives $\hat{\mathbf{x}} = \mathbf{x}$. Thus 2) is true.

For any error vector $\mathbf{z}$, $W_u^{err}(\mathbf{z}) \leq w_H(\mathbf{z})$. Thus, 2) ⇒ 1).

Now we prove 1) ⇒ 3). Assume 3) does not hold, i.e., $d_{\min,u} \leq 2t$. We will show that the network code cannot correct all error vectors $\mathbf{z}$ with $w_H(\mathbf{z}) \leq t$. First, we find two messages $\mathbf{x}_1$, $\mathbf{x}_2$ such that $D_u^{msg}(\mathbf{x}_1,\mathbf{x}_2) \leq 2t$. Since $W_u^{rec}((\mathbf{x}_1-\mathbf{x}_2)F_{s,u}) = D_u^{rec}(\mathbf{x}_1F_{s,u},\mathbf{x}_2F_{s,u}) = D_u^{msg}(\mathbf{x}_1,\mathbf{x}_2) \leq 2t$, there exists an error vector $\mathbf{z}$ such that $(\mathbf{x}_1-\mathbf{x}_2)F_{s,u} = \mathbf{z}F_u$ and $w_H(\mathbf{z}) \leq 2t$. Thus, we can construct two new error vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ which satisfy $w_H(\mathbf{z}_1) \leq t$, $w_H(\mathbf{z}_2) \leq t$, and $\mathbf{z}_2-\mathbf{z}_1 = \mathbf{z}$. It follows that $\mathbf{x}_1F_{s,u}+\mathbf{z}_1F_u = \mathbf{x}_2F_{s,u}+\mathbf{z}_2F_u$. Then under the condition that the message vector is $\mathbf{x}_1$ and the error vector is $\mathbf{z}_1$, or the condition that the message vector is $\mathbf{x}_2$ and the error vector is $\mathbf{z}_2$, $\mathbf{y}_u = \mathbf{x}_1F_{s,u}+\mathbf{z}_1F_u = \mathbf{x}_2F_{s,u}+\mathbf{z}_2F_u$ is received at sink node u. Therefore, no matter what decoding algorithm is used, the algorithm cannot decode correctly in both cases, i.e., 1) does not hold. Hence, 1) ⇒ 3). This completes the proof. ■

Equation (7) gives a decoding algorithm for network codes. The proof of Theorem 2 verifies that this algorithm can correct any vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq t$ at sink u if the code has $d_{\min,u} \geq 2t+1$. This decoding algorithm can be regarded as the minimum distance decoding in the network case.

Theorem 3: For a sink node u, the following three properties of a network code are equivalent:

1) The code can detect any error vector $\mathbf{z}$ with $0 < w_H(\mathbf{z}) \leq c$.
2) The code can detect any error vector $\mathbf{z}$ with $0 < W_u^{err}(\mathbf{z}) \leq c$.
3) The code has $d_{\min,u} \geq c+1$.

Remark: In classical coding, an error vector with Hamming weight zero means no error has occurred. However, in the network case, an error vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) = 0$ does not imply that $\mathbf{z} = \mathbf{0}$. Rather, it means $\mathbf{z}F_u = 0$, i.e., the error vector $\mathbf{z}$ has no effect on sink node u. Such an "invisible" error vector can by no means (perhaps does not need to) be detected at sink node u.

Proof: To prove 3) $\Rightarrow$ 2), we assume $d_{\min,u} \geq c+1$. Let $\mathbf{x} \in \mathcal{C}$ be a message vector, and $\mathbf{z}$ be an error vector with $W_u^{err}(\mathbf{z}) \leq c$. At sink node u, if the received vector $\mathbf{y}_u \neq \mathbf{x}'F_{s,u}$ for any $\mathbf{x}' \in \mathcal{C}$, we declare that at least one error has occurred during the transmission. If the error vector $\mathbf{z}$ cannot been detected, then there exists $\mathbf{x}' \in \mathcal{C}$ such that $\mathbf{y}_u = \mathbf{x}F_{s,u} + \mathbf{z}F_u = \mathbf{x}'F_{s,u}$. Thus $D_u^{msg}(\mathbf{x},\mathbf{x}') = D_u^{rec}(\mathbf{x}F_{s,u}, \mathbf{x}'F_{s,u}) = W_u^{rec}(\mathbf{z}F_u) = W_u^{err}(\mathbf{z}) \leq c < d_{\min,u}$. This is a contradiction to the definition of $d_{\min,u}$. So we conclude that all the error vectors $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq c$ can be detected.

The proof of 2) $\Rightarrow$ 1) is immediate because $W_u^{err}(\mathbf{z}) \leq w_H(\mathbf{z})$.

To prove 1) $\Rightarrow$ 3), we assume 3) does not hold, i.e., $d_{\min,u} \leq c$. Similar to the proof of Theorem 2, we can find two message vectors $\mathbf{x}$, $\mathbf{x}'$ and an error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq c$ and $(\mathbf{x}-\mathbf{x}')F_{s,u} = \mathbf{z}F_u$. This means when the message vector $\mathbf{x}'$ is transmitted, the error vector $\mathbf{z}$ cannot be detected. Thus 1) does not hold. Hence, 1) $\Rightarrow$ 3). The proof is complete. ■

B. Multicast Case

In the multicast case, for a particular network code, an error vector may have different weights for different sink nodes, so that the code may have different unicast minimum distance for different sink nodes. Applying Theorem 2 to all the sink nodes, we obtain that a network code can correct all the error vectors in the set

$$\Theta = \{\mathbf{z} : W_u^{err}(\mathbf{z}) < d_{\min,u}/2 \text{ for all } u \in \mathcal{U}\}. \quad (8)$$

In practice, we are very often concerned about correcting all error vectors whose Hamming weights do not exceed a certain threshold. However, it is not clear how the condition specifying the set Θ in (8) is related to the Hamming weights of the error vectors in that set. Therefore, we also obtain the following theorem which is the multicast version of Theorem 2.

The *multicast Hamming weight* of an error vector $\mathbf{z}$ is defined by $W^{err}(\mathbf{z}) = \max_{u\in\mathcal{U}} W_u^{err}(\mathbf{z})$.

Theorem 4: The following three properties of a network code are equivalent:

1) The code can correct any error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq t$ at all the sink nodes.
2) The code can correct any error vector $\mathbf{z}$ with $W^{err}(\mathbf{z}) \leq t$ at all the sink nodes.
3) The code has $d_{\min} \geq 2t+1$.

Proof: Assume 3) holds. Then $d_{\min,u} \geq 2t+1$ at all the sink nodes. If $\mathbf{z}$ is any error vector with $W^{err}(\mathbf{z}) \leq t$, i.e., $W_u^{err}(\mathbf{z}) \leq t$ at all the sink nodes, then by Theorem 2, the network code can correct error vector $\mathbf{z}$ at all the sink nodes. Hence, 3) $\Rightarrow$ 2).

Since $W^{err}(\mathbf{z}) = \max_{u\in\mathcal{U}} W_u^{err}(\mathbf{z}) \leq w_H(\mathbf{z})$, 2) $\Rightarrow$ 1) is immediate.

To prove 1) $\Rightarrow$ 3), assume 1) holds. By Theorem 2, we have $d_{\min,u} \geq 2t+1$ at all the sink nodes. Thus, $d_{\min} \geq 2t+1$, i.e., 3) holds. This completes the proof. ■

Remark: From Theorem 4, we see that a network code can correct all the error vectors in the set

$$\Theta' = \{\mathbf{z} : W^{err} < d_{\min}/2\}.$$

We now show that $\Theta' \subset \Theta$. Consider any error vector $\mathbf{z} \in \Theta'$, i.e., $\mathbf{z}$ satisfies $W^{err}(\mathbf{z}) < d_{\min}/2$, or $\max_{u\in\mathcal{U}} W_u^{err}(\mathbf{z}) < (1/2)\min_{u\in\mathcal{U}} d_{\min,u}$, which implies $W_u^{err}(\mathbf{z}) < d_{\min,u}/2$ for all the sink nodes. Therefore $\mathbf{z} \in \Theta$, and hence $\Theta' \subset \Theta$. However, $\Theta \subset \Theta'$ does not hold in general.

Using a similar argument, we can prove the following error detection theorem for multicast. The details are omitted here.

Theorem 5: The following three properties of a network code are equivalent:

1) The code can detect any error vector $\mathbf{z}$ with $0 < w_H(\mathbf{z}) \leq c$ at all the sink nodes.
2) The code can detect any error vector $\mathbf{z}$ with $0 < W^{err}(\mathbf{z}) \leq c$ at all the sink nodes.
3) The code has $d_{\min} \geq c+1$.

V. Relation between the Minimum Rank and the Minimum Distance

Zhang [7] has defined the *minimum rank* for linear network codes and presented a minimum rank decoding algorithm based on this notion. In this section, we will generalize the notion of minimum rank to non-linear message sets and prove that the minimum rank is equal to the minimum distance. We will also prove that under certain conditions, minimum rank decoding is equivalent to minimum distance decoding.

An error pattern is a subset of $\mathcal{E}$, denoted by ρ. An error vector is said to match an error pattern if all the errors occur on the edges in the error pattern. Note that if an error vector $\mathbf{z}$ matches an error pattern ρ', it also matches any error pattern ρ if $\rho' \subset \rho$. The set of all error vectors that match ρ is denoted by ρ^*. Let $\rho_{\mathbf{z}}$ be the error pattern corresponding to the non-zero components of an error vector $\mathbf{z}$. Define

$$\Delta_u(\rho) = \{\mathbf{z}F_u : \mathbf{z} \in \rho^*\}$$

and

$$\Phi_u = \{(\mathbf{x}-\mathbf{x}')F_{s,u} : \mathbf{x},\mathbf{x}' \in \mathcal{C}, \mathbf{x} \neq \mathbf{x}'\}.$$

The rank of an error pattern ρ for the sink node u, denoted by $rank_u(\rho)$, is defined as the dimension of the subspace $\Delta_u(\rho)$. For $\rho' \subset \rho$, since $\Delta_u(\rho') \subset \Delta_u(\rho)$, we have $rank_u(\rho') \leq rank_u(\rho)$. The *unicast minimum rank* of a network code for sink node u is defined by

$$r_{\min,u} = \min\{rank_u(\rho) : \Delta_u(\rho) \cap \Phi_u \neq \emptyset\}. \quad (9)$$

Lemma 1 ([7]): For any sink node u and any error pattern ρ, there exists a subset $\rho' \subset \rho$ such that $|\rho'| = rank_u(\rho')$ and $\Delta_u(\rho') = \Delta_u(\rho)$.

Proof: The subspace $\Delta_u(\rho)$ is spanned by the row vectors in F_u which correspond to the edges in ρ. Therefore, there exists a subset $\rho' \subset \rho$ such that these vectors corresponding to the edges in ρ' form a basis of $\Delta_u(\rho)$. This implies that $\Delta_u(\rho') = \Delta_u(\rho)$ and $rank_u(\rho') = |\rho'|$. ∎

Theorem 6: $r_{\min,u} = d_{\min,u}$.

Proof: Fix a sink node u. Let $\Omega = \{\rho : \Delta_u(\rho) \cap \Phi_u \neq \emptyset\}$ and $\Gamma = \{\mathbf{z} : \mathbf{z}F_u \in \Phi_u\}$. It is obvious that $r_{\min,u} = \min\{rank_u(\rho) : \rho \in \Omega\}$ and $d_{\min,u} = \min\{w_H(\mathbf{z}) : \mathbf{z} \in \Gamma\}$.

Consider any $\mathbf{z} \in \Gamma$. Since $\mathbf{z}F_u \in \Delta_u(\rho_{\mathbf{z}})$, we have $\rho_{\mathbf{z}} \in \Omega$ and $rank_u(\rho_{\mathbf{z}}) \leq |\rho_{\mathbf{z}}| = w_H(\mathbf{z})$. Now we will show that $w_H(\mathbf{z}) \geq r_{\min,u}$ by contradiction. By assuming that $w_H(\mathbf{z}) < r_{\min,u}$, we have $rank_u(\rho_{\mathbf{z}}) \leq w_H(\mathbf{z}) < r_{\min,u}$, which is a contradiction to the definition of the minimum rank. Thus we must have $w_H(\mathbf{z}) \geq r_{\min,u}$. Hence, $d_{\min,u} = \min_{\mathbf{z}\in\Gamma} w_H(\mathbf{z}) \geq r_{\min,u}$.

On the other hand, for any $\rho \in \Omega$, there exists an error vector $\mathbf{z} \in \rho^*$ such that $\mathbf{z}F_u \in \Phi_u$. Thus $\mathbf{z} \in \Gamma$, which means that the set $\rho^* \cap \Gamma$ is not empty. By Lemma 1, there exists an error pattern $\rho' \subset \rho$ such that $|\rho'| = rank_u(\rho)$ and $\Delta(\rho) = \Delta(\rho')$. Furthermore, $\rho' \in \Omega$. Now we will show that $rank_u(\rho) \geq w_H(\mathbf{z})$ for some $\mathbf{z} \in \rho^* \cap \Gamma$ by contradiction. Assume $rank_u(\rho) < w_H(\mathbf{z})$ for all $\mathbf{z} \in \rho^* \cap \Gamma$. Then we have $|\rho'| < w_H(\mathbf{z})$ for all $\mathbf{z} \in \rho^* \cap \Gamma$. If there exists $\mathbf{z}' \in \rho'^* \cap \Gamma \subset \rho^* \cap \Gamma$, then $w_H(\mathbf{z}') \leq |\rho'|$ which contradicts to what we have obtained. Thus, we have $\rho'^* \cap \Gamma = \emptyset$, which is a contradiction to $\rho' \in \Omega$. So, $rank_u(\rho) \geq w_H(\mathbf{z}) \geq d_{\min,u}$ for some $\mathbf{z} \in \rho^* \cap \Gamma$. Hence, $r_{\min,u} = \min_{\rho\in\Omega} rank_u(\rho) \geq d_{\min,u}$. The proof is complete. ∎

Zhang [7] presented a minimum rank decoding algorithm and proved that for any error pattern ρ with $rank_u(\rho) \leq (r_{\min,u} - 1)/2$, the algorithm always decodes correctly. We now show that for an error pattern ρ with $rank_u(\rho) \leq (r_{\min,u} - 1)/2$, an error vector $\mathbf{z} \in \rho^*$ has $W_u^{err}(\mathbf{z}) \leq (d_{\min,u} - 1)/2$, so that by Theorem 2 the minimum distance decoding can also decode correctly. By Lemma 1, there exists $\rho' \subset \rho$ such that $|\rho'| = rank_u(\rho)$ and $\Delta_u(\rho') = \Delta_u(\rho)$. Thus for any $\mathbf{z} \in \rho^*$, there exists $\mathbf{z}' \in \rho'^*$ such that $\mathbf{z}F_u = \mathbf{z}'F_u$. Hence, $W_u^{err}(\mathbf{z}) = W_u^{err}(\mathbf{z}') \leq w_H(\mathbf{z}') \leq |\rho'| = rank_u(\rho) \leq (r_{\min,u} - 1)/2 = (d_{\min,u} - 1)/2$.

For any error vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq (d_{\min,u} - 1)/2$, we cannot determine whether $rank_u(\rho_{\mathbf{z}}) \leq (r_{\min,u} - 1)/2$ holds or not. Nevertheless, we know that there exists $\mathbf{z}' \in \Upsilon_u(\mathbf{z}F_u)$ with $w_H(\mathbf{z}') \leq (d_{\min,u} - 1)/2$. Thus, $rank_u(\rho_{\mathbf{z}'}) \leq |\rho_{\mathbf{z}'}| = w_H(\mathbf{z}') \leq (d_{\min,u} - 1)/2$. When the error vector is $\mathbf{z}'$, minimum rank decoding always decodes correctly. Now if the error vector is $\mathbf{z}$ instead, since $\mathbf{z}'F_u = \mathbf{z}F_u$, the impact to the sink node u is exactly the same as if the error vector is $\mathbf{z}'$. Thus minimum rank decoding also decodes correctly. Therefore, minimum rank decoding always decodes correctly not only for $\mathbf{z}$ with $rank_u(\rho_{\mathbf{z}}) \leq (d_{\min,u} - 1)/2$ (as shown in [7]), but more generally for $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq (d_{\min,u} - 1)/2$. By Theorem 2, minimum distance decoding always decodes correctly for error vector $\mathbf{z}$ with $W_u^{err}(\mathbf{z}) \leq (d_{\min,u} - 1)/2$. Hence, under this condition, minimum rank decoding and minimum distance decoding are equivalent.

VI. Network Erasure

In classical algebraic coding, erasure correction is equivalent to error correction with the potential positions of the errors in the codewords known by the decoder. In this section, we extend this theme to network coding by assuming that the set of channels in each of which an error may have occurred during the transmission is known by the sink nodes, and we refer to this set of channels as the *erasure pattern*. As before, we assume that each sink node u knows the message set $\mathcal{C}$ as well as the transfer matrices $F_{s,u}$ and F_u.

Two quantities will be employed to characterize the ability of a network code for erasure correction. The first one is the Hamming weight of an erasure pattern ρ, denoted by $|\rho|$. The second one, called the network Hamming weight of an error pattern ρ, is defined as $W_u^{esr}(\rho) = \max_{\mathbf{z}\in\rho^*} W_u^{err}(\mathbf{z})$. Since $W_u^{err}(\mathbf{z}) \leq w_H(\mathbf{z}) \leq |\rho|$ for any $\mathbf{z} \in \rho^*$, we have

$$W_u^{esr}(\rho) \leq |\rho|. \tag{10}$$

Theorem 7: At a sink node u, the following three properties of a network code are equivalent:

1) The code can correct any erasure pattern ρ with $|\rho| \leq r$.
2) The code can correct any erasure pattern ρ with $W_u^{esr}(\rho) \leq r$.
3) The code has $d_{\min,u} \geq r + 1$.

Proof: To prove 3) ⇒ 2), assume $d_{\min,u} \geq r + 1$. Let ρ be an erasure pattern with $W_u^{esr}(\rho) \leq r$. We try to find a message vector $\mathbf{z} \in \mathcal{C}$ and an error vector $\mathbf{z} \in \rho^*$ that satisfy the equation $\mathbf{y}_u = \mathbf{x}F_{s,u} + \mathbf{z}F_{\rho,u}$. We call such a $(\mathbf{x}, \mathbf{z})$ pair a solution. If there exists only one $\mathbf{x} \in \mathcal{C}$ such that this equation is solvable, we claim that $\mathbf{x}$ is the decoded message vector. If this equation has two solutions $(\mathbf{x}_1, \mathbf{z}_1)$ and $(\mathbf{x}_2, \mathbf{z}_2)$, where $\mathbf{x}_1 \neq \mathbf{x}_2$, we can check that $D_u^{msg}(\mathbf{x}_1, \mathbf{x}_2) = W_u^{rec}((\mathbf{x}_1 - \mathbf{x}_2)F_{s,u}) = W_u^{rec}((\mathbf{z}_2 - \mathbf{z}_1)F_u) = W_u^{err}(\mathbf{z}_2 - \mathbf{z}_1) \leq r$ since $\mathbf{z}_2 - \mathbf{z}_1 \in \rho^*$. This a contradiction to $d_{\min,u} \geq r + 1$. Hence, the code can correct any erasure pattern ρ with $W_u^{esr}(\rho) \leq r$, i.e., 2) holds.

Since $W_u^{esr}(\rho) \leq w_H(\rho)$ for (10) , 2) ⇒ 1) is immediate.

Finally we prove 1) ⇒ 3) by contradiction. Assume a code has $d_{\min,u} \leq r$. We will find an erasure pattern ρ with $|\rho| \leq r$ that cannot be corrected. Since $d_{\min,u} \leq r$, there exists an error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq r$ such that $D_u^{msg}(\mathbf{x}_1, \mathbf{x}_2) = w_H(\mathbf{z})$, where $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$, $\mathbf{x}_1 \neq \mathbf{x}_2$. Thus we can construct $\mathbf{z}_1, \mathbf{z}_2 \in \rho_z$ such that $\mathbf{z}_2 - \mathbf{z}_1 = \mathbf{z}$. If $y_u = \mathbf{x}_1F_{s,u} + \mathbf{z}_1F_u = \mathbf{x}_2F_{s,u} + \mathbf{z}_2F_u$ is received, by means of an argument similar to that in Theorem 2, we see that sink node u cannot correct the erasure pattern $\rho_{\mathbf{z}}$ with $|\rho_{\mathbf{z}}| \leq r$. This completes the proof. ∎

For an erasure pattern ρ, define the multicast weight as

$$W^{esr}(\rho) = \max_{u\in\mathcal{U}} W_u^{esr}(\rho).$$

Using Theorem 7, we can easily obtain the multicast theorem for erasure correction.

Theorem 8: The following three properties of a network code are equivalent:

1) The code can correct any erasure pattern ρ with $|\rho| \leq r$ at all the sink nodes.
2) The code can correct any erasure pattern ρ with $W^{esr}(\rho) \leq r$ at all the sink nodes.
3) The code has $d_{\min} \geq r + 1$.

VII. Concluding Remarks

In this work, we have defined the minimum distance of a network code. Based on this minimum distance, the ability of a network code in terms of error correction/detection and erasure correction can be fully characterized. These results are network generalizations of the corresponding results in classical algebraic coding theory. With the introduction of network error correction in [5], [6] and our results, any question that may be raised in classical algebraic coding theory can be raised in the more general setting of network coding. Thus there is a host of problems to be investigated in the direction of our work.

References

[1] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory," *Foundation and Trends in Communications and Information Theory*, vol. 2, no. 4 and 5, pp. 241–381, 2005.

[2] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in *Proc. IEEE ISIT'04*, June 2004.

[3] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," in *Proc. IEEE ISIT'05*, July 2005.

[4] N. Cai and R. W. Yeung, "Network codig and error correction," in *Proc. IEEE ITW'02*, 2002.

[5] R. W. Yeung and N. Cai, "Network error correction, part I: basic concepts and upper bounds," to appear in *Communications in Information and Systems*.

[6] N. Cai and R. W. Yeung, "Network error correction, part II: lower bounds," to appear in *Communications in Information and Systems*.

[7] Z. Zhang, "Network error correction coding in packetized networks," preprint.

[8] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[9] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.