EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS
Euro. Trans. Telecomms. **00**: 1–14 (0000)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/ett.0000

Weight Properties of Network Codes

Shenghao Yang[1], Raymond W. Yeung[1]* and Zhen Zhang[2]

[1]*Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong*
[2]*Department of Electrical Engineering, University of Southern California, CA, USA*

SUMMARY

In this paper, we first study the error correction and detection capability of codes for a general transmission system inspired by network error correction. For a given weight measure on the error vectors, we define a corresponding minimum weight decoder. Then we obtain a complete characterization of the capability of a code for 1) error correction; 2) error detection; and 3) joint error correction and detection. Our results show that if the weight measure on the error vectors is the Hamming weight, the capability of a linear code is fully characterized by a single minimum distance. By contrast, for a nonlinear code, two different minimum distances are needed for characterizing the capabilities of the code for error correction and for error detection. This leads to the surprising discovery that for a nonlinear code, the number of correctable errors can be more than half of the number of detectable errors. We also present a framework that captures joint error correction and detection. We further define equivalence classes of weight measures with respect to a channel. Specifically, for any given code, the minimum weight decoders for two different weight measures are equivalent if the two weight measures belong to the same equivalence class. In the special case of linear network coding, we study three weight measures, and show that they are in the same equivalence class of the Hamming weight and induce the same minimum distance as the Hamming weight. Copyright © 0000 AEIT

1. INTRODUCTION

Consider multicasting information transmission in a directed acyclic communication network, where a source node transmits the same information to a set of sink nodes. It was shown by Ahlswede *et al.* [1] that the network capacity for multicast satisfies the max-flow min-cut theorem, and this capacity can be achieved by network coding. Li, Yeung, and Cai [2] further showed that it is sufficient to consider linear network codes only. Subsequently, Koetter and Médard [3] developed a matrix framework for network coding. Jaggi *et al.* [4] proposed a deterministic polynomial-time algorithm to construct network codes. Ho *et al.* [5] showed that linear network codes can be effectively constructed by a randomized algorithm with an exponentially decreasing probability of error.

In practical communication networks, transmission suffers from *errors* due to link failure, traffic congestion, malicious modifications, etc. The concept of network error correction, introduced by Cai and Yeung [6, 7, 8], is to correct the errors in the network by means of network coding. In this work, they generalized the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound in classical error correction coding to network coding. The relation between network coding and maximum distance separation (MDS) codes in classical algebraic coding has been clarified in [9].

Network coding in the presence of link failure has been considered by Koetter and Médard [3], where they introduced the static network code. Network error detection by random network coding has been studied by Ho *et al.* [10]. Jaggi et al. [11, 12, 13] have developed random network coding algorithms for network error

*Correspondence to: Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong. E-mail: whyeung@ie.cuhk.edu.hk

Received
Prepared using ettauth.cls *[Version: 2007/01/05 v1.00]*

correction with various assumptions on the adversaries. Network error correction in packet networks has been studied in [14, 15] by Zhang, where he introduced an algebraic definition of minimum distance for linear network codes and studied the decoding problem. By contrast, Yang and Yeung [16] introduced a geometric definition of minimum distance, and they showed that it is equivalent to the definition of minimum distance in [14, 15]. Recently, Koetter and Kschischang [17] have introduced a general framework for network error correction over an underlying network that performs random network coding.

Except for the works of Cai and Yeung [6, 8], all prior works on network error correction focused on linear network codes. In this work, we first study a general transmission system which includes network error correction, hence, classical error correction, as a special case. We focus on how to characterize error correction and error detection as well as joint error correction and detection when applying minimum weight decoding. Such characterizations are more complicated than their classical counterparts where only the minimum distance is sufficient, because here different "minimum distances" may need to be employed for error correction and error detection. Specifically, this will be illustrated by an example of a nonlinear network code for which the number of correctable errors is more than half of the number of detectable errors. We also obtain a new parameter which can completely characterize both the error correction and error detection capabilities as well as the joint error correction and detection capability of a code. This parameter reduces to the minimum distance when the channel is linear and the weight measure is the Hamming weight.

Our characterization of the capability of a code for error correction and/or error detection depends on the weight measure, or equivalently, the minimum weight decoder chosen for the problem. Even though the definition of the weight measure we give is general, the actual choice of the weight measure affects the performance of the corresponding minimum weight decoder. For example, the original purpose of introducing the Hamming weight measure for error vectors is to capture the probabilistic property of a channel by assuming that an error vector with lower weight occurs with higher probability, so that minimum Hamming weight decoding is optimal, i.e., equivalent to maximum *a priori* decoding, when the point-to-point channel is a discrete memoryless channel and the codeword $\mathbf{x}$ is chosen uniformly from the codebook $\mathcal{C}$.

How to find a good weight measure is rather problem specific. Nevertheless, we obtain for the general case an equivalence relation on weight measures and show that weight measures belonging to the same equivalence class lead to the same minimum weight decoder. We show that all the four weight measures for linear network codes that have appeared in the network error correction literature are in fact equivalent for error correction and detection.

This paper is organized as follows. In the next section, we formulate the network error correction problem in a general setting. In Section 2, we study the error correction, error detection, and joint error correction and detection for a general transmission system, and define an equivalence relation for weight measures. Specifically, if two weight measures are in the same equivalence class, they induce the same minimum weight decoder. In Section 3, we formulate the network error correction problem and illustrate an example of nonlinear network codes. We further show that two weight measures, the Hamming weight and a minimum cut induced by the error vector, are in the same equivalence class for general network codes. In Section 4, we discuss two more weight measures for linear network codes, the rank and the network Hamming weight, and show that all the four weight measures are in the same equivalence class for linear network codes and they induce the same minimum distance for error correction/detection and erasure correction. Two of these weight measures, namely the minimum cut and the rank, have previously been discussed in [14, 15]. In the last section, we summarize our work and discuss topics for further research.

2. ERROR CORRECTION AND DETECTION CAPABILITY

In this section, we study a general transmission system that includes network error correction as a special case. We are given a codebook $\mathcal{C}$, a set Σ whose elements are called *error vectors*, and a set Φ whose elements are called *received vectors*. For any $\mathbf{x} \in \mathcal{C}$ and $\mathbf{z} \in \Sigma$, the received vector is $F(\mathbf{x}, \mathbf{z})$ where $F : \mathcal{C} \times \Sigma \to \Phi$ is called the *transfer function*. The transfer function F models the communication channel. A *weight measure* of the error vectors is a mapping

$$w : \Sigma \to \mathbb{Z}^*, \tag{1}$$

where $\mathbb{Z}^*$ is the set of nonnegative integers.

DOI: 10.1002/ett

2.1. Error Correction Capability

With respect to a weight measure w, define

$$\Phi_w(\mathbf{x}, c) = \{F(\mathbf{x}, \mathbf{z}) : \mathbf{z} \in \Sigma,\ w(\mathbf{z}) \leq c\}, \qquad (2)$$

for a codeword $\mathbf{x}$ and a nonnegative integer c. This induces a distance-like measure between $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$ defined as

$$D^0_w(\mathbf{x}_1, \mathbf{x}_2) = \min\{c_1 + c_2 : |c_1 - c_2| \leq 1, \\ \Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset\}. \qquad (3)$$

By adopting the convention that the minimum of the empty set is ∞, $D^0_w(\mathbf{x}_1, \mathbf{x}_2)$ is well defined.

Note that D^0_w is not necessarily a metric even though it is symmetric. With respect to D^0_w, we define the minimum distance for the code $\mathcal{C}$ as

$$d^0_{\min,w} = \min\{D^0_w(\mathbf{x}_1, \mathbf{x}_2) : \mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}\}. \qquad (4)$$

Here, we call $d^0_{\min,w}$ the minimum distance because it is a generalization of the notion of minimum distance in classical coding theory, although D^0_w is not necessarily a metric.

The *minimum weight decoder* with respect to w, denoted by MWD_w, decodes a received vector $\mathbf{y}$ as follows: First, find all the solutions of equation

$$F(\mathbf{x}, \mathbf{z}) = \mathbf{y} \qquad (5)$$

with $\mathbf{x} \in \mathcal{C}$ and $\mathbf{z} \in \Sigma$ as variables. A pair $(\mathbf{x}, \mathbf{z})$, $\mathbf{x} \in \mathcal{C}$ and $\mathbf{z} \in \Sigma$, is said to be a solution if it satisfies (5), and furthermore a minimum weight solution if $w(\mathbf{z})$ achieves the minimum among all the solutions. If for all minimum weight solutions $(\mathbf{x}, \mathbf{z})$, the message part $\mathbf{x}$ are identical, then we say that the error is correctable and claim that the identical message part is the decoded message. Otherwise, we claim an uncorrectable error.

We also define another decoder related to MWD_w if we can find a collection of disjoint decoding spheres $\{\Phi_w(\mathbf{x}, c) : \mathbf{x} \in \mathcal{C}\}$ with integer parameter c. For any received vector $\mathbf{y} \in \Phi$, if $\mathbf{y} \in \Phi_w(\mathbf{x}, c)$ for only one $\mathbf{x} \in \mathcal{C}$, we say the error is correctable and claim $\mathbf{x}$ to be the decoded message. If $\mathbf{y}$ is not in any of the decoding spheres, we claim an uncorrectable error, or we say the error is detected. Such a decoder is denoted by $\mathrm{MWD}'_w(c)$.

Definition 1 *A code is* c-error-correcting *if* MWD_w *can correct all error vectors* $\mathbf{z}$ *with* $w(\mathbf{z}) \leq c$.

Lemma 1 *A code is* c*-error-correcting if and only if* $\mathrm{MWD}'_w(c)$ *exists.*

Proof First, consider a code and assume $\mathrm{MWD}'_w(c)$ exists. Let $\mathbf{x}$ be the transmitted codeword and $\mathbf{z}$ be the error vector occurred with $w(\mathbf{z}) \leq c$, and $\mathbf{y} = F(\mathbf{x}, \mathbf{z})$ be the received vector. Let $(\mathbf{x}^*, \mathbf{z}^*)$ be a minimum weight solution of (5). Since the decoding spheres in $\mathrm{MWD}'_w(c)$ are disjoint, for any codeword $\mathbf{x}' \neq \mathbf{x}$, and $\mathbf{z}'$ with $w(\mathbf{z}') \leq c$, $F(\mathbf{x}', \mathbf{z}') \neq \mathbf{y}$. That is, for any $\mathbf{z}'$ such that $w(\mathbf{z}') \leq c$, if $F(\mathbf{x}', \mathbf{z}') = \mathbf{y}$, than $\mathbf{x}' = \mathbf{x}$. In particular, this applies to $\mathbf{z}^*$ since $w(\mathbf{z}^*) \leq w(\mathbf{z}) \leq c$. Therefore, the message part of any minimum weight solution of (5) is $\mathbf{x}$, implying that the code is c-error-correcting.

Conversely, if $\mathrm{MWD}'_w(c)$ does not exist, then we can find $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, $\mathbf{z}_1$ and $\mathbf{z}_2$ with $w(\mathbf{z}_1) \leq c$ and $w(\mathbf{z}_2) \leq c$ such that $F(\mathbf{x}_1, \mathbf{z}_1) = F(\mathbf{x}_2, \mathbf{z}_2)$. If $\mathbf{y} = F(\mathbf{x}_1, \mathbf{z}_1) = F(\mathbf{x}_2, \mathbf{z}_2)$ is received, then MWD_w cannot always decode correctly. Hence, the code is not c-error-correcting. ∎

Theorem 1 *A code is* c*-error correcting if and only if* $d^0_{\min,w} \geq 2c + 1$.

Proof We will prove the theorem by showing the equivalence of the following statements:

1) The existence of $\mathrm{MWD}'_w(c)$, i.e., for any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, $\Phi_w(\mathbf{x}_1, c) \cap \Phi_w(\mathbf{x}_2, c) = \emptyset$.
2) For any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, any c_1 and c_2 such that $\Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset$, satisfy either $c_1 > c$ or $c_2 > c$.
3) For any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, any c_1 and c_2 such that $|c_1 - c_2| \leq 1$ and $\Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset$, satisfy $\max\{c_1, c_2\} > c$.
4) For any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, any c' such that $\Phi_w(\mathbf{x}_1, c') \cap \Phi_w(\mathbf{x}_2, c') \neq \emptyset$, satisfies $c' > c$.
5) $d^0_{\min,w} \geq 2c + 1$.

Specifically, this will be done by showing that 1) ⇔ 2) ⇒ 3) ⇒ 4) ⇒ 2) and 3) ⇔ 5).

We show 1) ⇔ 2) by contradiction. If 2) is not true, there exist $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, $c_1 \leq c$ and $c_2 \leq c$ such that $\Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset$, i.e., 1) is false. This shows that 1) ⇒ 2). The converse can be proved by similar contradiction.

3) is a special case of 2) with the additional constraint $|c_1 - c_2| \leq 1$ and 4) is a special case of 3) with the constraint $c_1 = c_2$. We prove 4) ⇒ 2) by contradiction. Assume 2) does not hold, i.e., there exist $c_1 \leq c$ and $c_2 \leq c$ such that $\Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset$. Then we have $c' = \max\{c_1, c_2\} \leq c$ such that $\Phi_w(\mathbf{x}_1, c') \cap \Phi_w(\mathbf{x}_2, c') \neq \emptyset$, i.e., 4) does not hold.

Finally, 3) ⇔ 5) simply follows from the definition of $d^0_{\min,w}$. ∎

DOI: 10.1002/ett

Theorem 1 says that $d^0_{\min,w}$ can fully characterize the error correction capability of $\mathcal{C}$. In the special setting of classical error correction, $d^0_{\min,w}$ corresponds to the minimum distance of a classical error-correcting block code, which characterizes not only the error correction capability but also the error detection and erasure correction capabilities of the code. However, the situation is more complicated in the general setting.

2.2. Error Detection Capability

Within the discussion of this paper, we assume that there exists $\mathbf{z}_0$ such that $w(\mathbf{z}_0) = 0$. For general cases, we can replace w by the weight measure $w'(\mathbf{z}) = w(\mathbf{z}) - \min_{\mathbf{z}'} w(\mathbf{z}')$ without changing the problem. A justification is given in [18].

For two vectors $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$, define another distance-like measure

$$D^1_w(\mathbf{x}_1, \mathbf{x}_2) = \min\{c : \Phi_w(\mathbf{x}_1, 0) \cap \Phi_w(\mathbf{x}_2, c) \neq \emptyset\}. \tag{6}$$

Again, $D^1_w(\mathbf{x}_1, \mathbf{x}_2)$ is well defined with the convention that the minimum of the empty set is ∞.

We note that D^1_w is in general not symmetric. Even though we could have defined an alternative symmetric form for D^1_w, it is not necessary for D^1_w to possess this property for the purpose of our discussion. With respect to D^1_w, define minimum distance of the code $\mathcal{C}$ as

$$d^1_{\min,w} = \min\{D^1_w(\mathbf{x}_1, \mathbf{x}_2) : \mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}\}. \tag{7}$$

Definition 2 *A code is* c-error-detecting *if* $\mathrm{MWD}'_w(0)$ *exists and detects all error vector* $\mathbf{z}$ *with* $0 < w(\mathbf{z}) \leq c$.

Theorem 2 *A code is* c*-error detecting if and only if* $d^1_{\min,w} \geq c + 1$.

Proof The theorem can be proved by showing the equivalence of the following statements:

1) A code is c-error detecting.
2) For any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, $F(\mathbf{x}_2, 0) \notin \Phi_w(\mathbf{x}_1, c)$.
3) For any $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$, any c' such that $F(\mathbf{x}_2, 0) \in \Phi_w(\mathbf{x}_1, c')$, we have $c' > c$.
4) $d^1_{\min,w} \geq c + 1$.

It is straightforward from the definitions that 1) $\Leftrightarrow$ 2) $\Leftrightarrow$ 3) $\Leftrightarrow$ 4). ∎

Now we have two different minimum distances for error correction and error detection, namely $d^0_{\min,w}$ and $d^1_{\min,w}$, respectively. Subsection 3.2 gives an example of a nonlinear network code with $d^0_{\min,w} = 3$ and $d^1_{\min,w} = 2 > \frac{1}{2}d^0_{\min,w}$, where w is the Hamming weight. This example shows that the minimum distances defined here are not exactly the same as that in classical coding theory, which is defined as the minimum of a distance between two distinct codewords in the code. Nevertheless, we will show in Subsection 2.6 and Section 4 that $d^0_{\min,w}$ and $d^1_{\min,w}$ coincide for some cases.

2.3. A Unified Framework For Minimum Distances

We now develop a framework that captures the notions of the minimum distances $d^0_{\min,w}$ and $d^1_{\min,w}$ as special cases. Define the set

$$\Psi_w(\mathbf{x}_1, \mathbf{x}_2) = \{(c_1, c_2) \in (\mathbb{Z}^*)^2 : \Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset\}, \tag{8}$$

for $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$.

Lemma 2 *For* $c'_1 \geq c_1$ *and* $c'_2 \geq c_2$, *if* $(c_1, c_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$, *then* $(c'_1, c'_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$.

Proof By the property that $\Phi_w(\mathbf{x}, c) \subset \Phi_w(\mathbf{x}, c')$ for $c \leq c'$, under the condition of the lemma, $\Phi_w(\mathbf{x}_1, c'_1) \cap \Phi_w(\mathbf{x}_2, c'_2) \supset \Phi_w(\mathbf{x}_1, c_1) \cap \Phi_w(\mathbf{x}_2, c_2) \neq \emptyset$. ∎

In terms of the set $\Psi_w(\mathbf{x}_1, \mathbf{x}_2)$, we can rewrite the definitions of D^0_w and D^1_w as:

$$D^0_w(\mathbf{x}_1, \mathbf{x}_2) = \min_{(c_1,c_2)\in\Psi_w(\mathbf{x}_1,\mathbf{x}_2):|c_1-c_2|\leq 1}(c_1 + c_2), \tag{9}$$

and

$$D^1_w(\mathbf{x}_1, \mathbf{x}_2) = \min_{(c_1,c_2)\in\Psi_w(\mathbf{x}_1,\mathbf{x}_2):c_1=0}(c_1 + c_2). \tag{10}$$

Define

$$\Psi_w = \cup_{\mathbf{x}_1\neq\mathbf{x}_2\in\mathcal{C}}\Psi_w(\mathbf{x}_1, \mathbf{x}_2). \tag{11}$$

The set Ψ_w is symmetric in c_1 and c_2 because if $(c_1, c_2) \in \Psi_w$, then $(c_2, c_1) \in \Psi_w$. Thus for $c'_1 \geq c_1$ and $c'_2 \geq c_2$, if $(c_1, c_2) \in \Psi_w$, then $(c'_1, c'_2) \in \Psi_w$.

In terms of the set Ψ_w, we can rewrite the definitions of $d^0_{\min,w}$ and $d^1_{\min,w}$ as:

$$d^0_{\min,w} = \min_{(c_1,c_2)\in\Psi_w:|c_1-c_2|\leq 1}(c_1 + c_2), \tag{12}$$

and

$$d^1_{\min,w} = \min_{(c_1,c_2)\in\Psi_w:c_1=0}(c_1 + c_2). \tag{13}$$

DOI: 10.1002/ett

For a set $S \subset (\mathbb{Z}^*)^2$, let $\bar{S}$ be the complementary of S defined as

$$\bar{S} = (\mathbb{Z}^*)^2 \setminus S. \tag{14}$$

Then for $c_1' \leq c_1$ and $c_2' \leq c_2$, if $(c_1, c_2) \in \bar{\Psi}_w$, then $(c_1', c_2') \in \bar{\Psi}_w$.

For a set $S \subset (\mathbb{Z}^*)^2$, let $\partial(S)$ be the lower boundary of S defined as

$$\partial(S) = \{(c_1, c_2) \in S : (c_1 - 1, c_2) \text{ or } (c_1, c_2 - 1) \in \bar{S}\}. \tag{15}$$

Lemma 3 *The following statements hold:*

1) either

$$\left(\left\lceil \frac{D_w^0(\mathbf{x}_1, \mathbf{x}_2)}{2} \right\rceil, \left\lfloor \frac{D_w^0(\mathbf{x}_1, \mathbf{x}_2)}{2} \right\rfloor\right) \in \partial(\Psi_w(\mathbf{x}_1, \mathbf{x}_2))$$

or

$$\left(\left\lfloor \frac{D_w^0(\mathbf{x}_1, \mathbf{x}_2)}{2} \right\rfloor, \left\lceil \frac{D_w^0(\mathbf{x}_1, \mathbf{x}_2)}{2} \right\rceil\right) \in \partial(\Psi_w(\mathbf{x}_1, \mathbf{x}_2));$$

2) $(0, D_w^1(\mathbf{x}_1, \mathbf{x}_2)) \in \partial(\Psi_w(\mathbf{x}_1, \mathbf{x}_2))$*;*
3) $(\lfloor d_{\min,w}^0/2 \rfloor, \lceil d_{\min,w}^0/2 \rceil) \in \partial(\Psi_w)$*;*
4) $(0, d_{\min,w}^1) \in \partial(\Psi_w)$.

Proof By the definition of $D_w^0(\mathbf{x}_1, \mathbf{x}_2)$, either

$$(D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2, D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$$

or

$$(\lfloor D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rfloor, \lceil D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rceil) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2),$$

but both

$$(\lceil D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rceil - 1, \lfloor D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rfloor) \notin \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$$

and

$$(\lfloor D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rfloor, \lceil D_w^0(\mathbf{x}_1, \mathbf{x}_2)/2 \rceil - 1) \notin \Psi_w(\mathbf{x}_1, \mathbf{x}_2).$$

Thus 1) holds. Similar reasoning gives 2), 3) and 4). ∎

For each $(c_1, c_2) \in \partial(\Psi_w(\mathbf{x}_1, \mathbf{x}_2))$, we can define a distance-like measure for $\mathbf{x}_1$ and $\mathbf{x}_2$ given by $c_1 + c_2$. Accordingly, for each $(c_1, c_2) \in \partial(\Psi_w)$, we can define a minimum distance given by $c_1 + c_2$. In general, these minimum distances defined for different $(c_1, c_2) \in \partial(\Psi_w)$ are not equal.

2.4. Joint Error Correction and Detection Capability

For classical block codes, it is well-known that a code can correct c errors and detect additional c' errors as long as $d_{\min} \geq 2c + c' + 1$. Now we consider such a characterization for our general transmission system.

Definition 3 *A code is joint (c, c')-error-correcting if $\mathrm{MWD}_w'(c)$ exists (cf. Lemma 1) and detects all error vector $\mathbf{z}$ with $c < w(\mathbf{z}) \leq c + c'$.*

Theorem 3 *For a given weight measure w, a code is joint (c, c')-error-correcting if and only if $(c, c + c') \in \bar{\Psi}_w$.*

Proof We first prove that $(c, c + c') \in \bar{\Psi}_w$ is sufficient for the code to be joint (c, c')-error-correcting. If $(c, c + c') \in \bar{\Psi}_w$, we have $(c, c) \in \bar{\Psi}_w$, which implies $d_{\min,w}^0 > 2c$. Thus the code is c-error-correcting by Theorem 1, and hence $\mathrm{MWD}_w'(c)$ exists by Lemma 1.

We further need to show that for such a code, $\mathrm{MWD}_w'(c)$ can detect correctly all error vectors $\mathbf{z}$ with $c < w(\mathbf{z}) \leq c + c'$. Let $\mathbf{x} \in \mathcal{C}$ be transmitted and suppose an error vector $\mathbf{z}$ with $c < w(\mathbf{z}) \leq c + c'$ has occurred. Obviously, the received vector $\mathbf{y} = F(\mathbf{x}, \mathbf{z}) \notin \Phi_w(\mathbf{x}, c)$. Then for any $\mathbf{x}' \neq \mathbf{x} \in \mathcal{C}$, since $(c, c + c') \in \bar{\Psi}_w$, $\Phi_w(\mathbf{x}', c) \cap \Phi_w(\mathbf{x}, c + c') = \emptyset$. Thus, $\mathbf{y} \notin \Phi_w(\mathbf{x}', c)$. This means that the received vector $\mathbf{y}$ is not in any of the decoding spheres of $\mathrm{MWD}_w'(c)$, and hence the error vector $\mathbf{z}$ is detected.

We prove that $(c, c + c') \in \bar{\Psi}_w$ is necessary for the code to be joint (c, c')-error-correcting. Assume $(c, c + c') \in \Psi_w$. If $(c, c) \in \Psi_w$, the $\mathrm{MWD}_w'(c)$ decoder does not exist, and hence the code is not joint (c, c')-error-correcting. If $(c, c) \notin \Psi_w$, the $\mathrm{MWD}_w'(c)$ decoder exists. Since $(c, c + c') \in \Psi_w$, there exist $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{z}_1$, and $\mathbf{z}_2$ with $w(\mathbf{z}_1) \leq c$ and $c < w(\mathbf{z}_2) \leq c + c'$ such that $F(\mathbf{x}_1, \mathbf{z}_1) = F(\mathbf{x}_2, \mathbf{z}_2)$. If $\mathbf{y} = F(\mathbf{x}_1, \mathbf{z}_1) = F(\mathbf{x}_2, \mathbf{z}_2)$ is received, $\mathrm{MWD}_w'(c)$ always decodes $\mathbf{y}$ to $\mathbf{x}_1$ because $\mathbf{y} \in \Phi_w(\mathbf{x}_1, c)$. If $\mathbf{x}_2$ is transmitted and $\mathbf{z}_2$ has occurred, $\mathrm{MWD}_w'(c)$ cannot detect this error vector $\mathbf{z}_2$ with $c < w(\mathbf{z}_2) \leq c + c'$. ∎

The set $\bar{\Psi}_w$ fully characterizes the capability of a code for joint error correction and detection with respect to the weight measure w. In fact, Theorem 1 and Theorem 2 are special cases of Theorem 3 with $c' = 0$ and $c = 0$, respectively.

2.5. Equivalent Weight Measures

Definition 4 *Two weight measures w_1 and w_2 on Σ are* equivalent *with respect to F, denoted as $w_1 \overset{F}{\sim} w_2$, if for*

DOI: 10.1002/ett

any $\mathbf{x} \in \mathcal{C}$ *and any nonnegative integer* c*,*

$$\Phi_{w_1}(\mathbf{x}, c) = \Phi_{w_2}(\mathbf{x}, c). \tag{16}$$

Lemma 4 *The relation "*$\overset{F}{\sim}$*" is an equivalence relation.*

Proof It is easy to check that 1) $w \overset{F}{\sim} w$; 2) if $w_1 \overset{F}{\sim} w_2$, then $w_2 \overset{F}{\sim} w_1$; and 3) if $w_1 \overset{F}{\sim} w_2$ and $w_2 \overset{F}{\sim} w_3$, then $w_1 \overset{F}{\sim} w_3$. ∎

For w_1 and w_2 in the same equivalence class with respect to F, when there is no ambiguity, we just say that w_1 and w_2 are equivalent.

Lemma 5 *If two weight measures* w_1 *and* w_2 *are equivalent, then*

$$\Psi_{w_1}(\mathbf{x}_1, \mathbf{x}_2) = \Psi_{w_2}(\mathbf{x}_1, \mathbf{x}_2) \tag{17}$$

for any $\mathbf{x}_1$, $\mathbf{x}_2 \in \mathbb{F}^m$.

Proof

$$\begin{aligned}
&\Psi_{w_1}(\mathbf{x}_1, \mathbf{x}_2) \\
&= \{(c_1, c_2) : \Phi_{w_1}(\mathbf{x}_1, c_1) \cap \Phi_{w_1}(\mathbf{x}_2, c_2) \neq \emptyset\}, && (18)\\
&= \{(c_1, c_2) : \Phi_{w_2}(\mathbf{x}_1, c_1) \cap \Phi_{w_2}(\mathbf{x}_2, c_2) \neq \emptyset\}, && (19)\\
&= \Psi_{w_2}(\mathbf{x}_1, \mathbf{x}_2). && (20)
\end{aligned}$$

∎

The following theorem says that a code has the same error correction/detection capability with respect to equivalent weight measures.

Theorem 4 *If two weight measures* w_1 *and* w_2 *are equivalent, then*

$$\bar{\Psi}_{w_1} = \bar{\Psi}_{w_2}. \tag{21}$$

Proof

$$\begin{aligned}
\Psi_{w_1} &= \cup_{\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}} \Psi_{w_1}(\mathbf{x}_1, \mathbf{x}_2) && (22)\\
&= \cup_{\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}} \Psi_{w_2}(\mathbf{x}_1, \mathbf{x}_2) && (23)\\
&= \Psi_{w_2}. && (24)
\end{aligned}$$

∎

Theorem 5 *For two equivalent weight measures* w_1 *and* w_2*,* MWD_{w_1} *is equivalent to* MWD_{w_2} *in the sense that they generate the same output for the same received vector.*

Proof Let $\mathbf{y}$ be a received vector. Let $(\mathbf{x}_1, \mathbf{z}_1)$ be a minimum weight solution of MWD_{w_1}. Then $\mathbf{y} \in \Phi_{w_1}(\mathbf{x}_1, w_1(\mathbf{z}_1)) = \Phi_{w_2}(\mathbf{x}_1, w_1(\mathbf{z}_1))$, which means that there exists $\mathbf{z}_1'$ with $w_2(\mathbf{z}_1') \leq w_1(\mathbf{z}_1)$ such that $(\mathbf{x}_1, \mathbf{z}_1')$ is a solution of MWD_{w_2}. We show that $(\mathbf{x}_1, \mathbf{z}_1')$ is also the minimum weight solution of MWD_{w_2} by contradiction. Assume $(\mathbf{x}_2, \mathbf{z}_2)$ is a minimum weight solution of MWD_{w_2} and $w_2(\mathbf{z}_2) < w_2(\mathbf{z}_1')$. Then $\mathbf{y} \in \Phi_{w_2}(\mathbf{x}_2, w_2(\mathbf{z}_2)) = \Phi_{w_1}(\mathbf{x}_2, w_2(\mathbf{z}_2))$. Since $w_2(\mathbf{z}_2) < w_1(\mathbf{z}_1)$, $\mathbf{y} \in \Phi_{w_1}(\mathbf{x}_2, w_2(\mathbf{z}_2))$ is a contradiction to that $(\mathbf{x}_1, \mathbf{z}_1)$ is a minimum weight solution of MWD_{w_1}.

∎

For two equivalent weight measures w_1 and w_2, the equivalence of $\mathrm{MWD}'_{w_1}(c)$ and $\mathrm{MWD}'_{w_2}(c)$ comes from the fact that $\mathrm{MWD}'_{w_1}(c)$ and $\mathrm{MWD}'_{w_2}(c)$ depend only on $\Phi_{w_1}(\mathbf{x}, c) = \Phi_{w_2}(\mathbf{x}, c)$ for all codeword $\mathbf{x}$.

2.6. Linear Channels and the Hamming Weight

Let $\mathbb{F}$ be any finite field with q elements, and let m, n and l be positive integers. In this subsection, we consider $\mathcal{C} \subset \mathbb{F}^m$ and $\Sigma = \mathbb{F}^n$. We say a channel is *linear* if

$$F(\mathbf{x}, \mathbf{z}) = \mathbf{x}\mathbf{F} + \mathbf{z}\mathbf{F}' \tag{25}$$

for all $\mathbf{x} \in \mathcal{C}$ and all $\mathbf{z} \in \Sigma$, where $\mathbf{F}$ is an $m \times l$ matrix and $\mathbf{F}'$ is an $n \times l$ matrix.

The definition of $\Phi_w(\mathbf{x}, c)$ in (2) can be applied for $\mathbf{x} \in \mathbb{F}^m \setminus \mathcal{C}$, which in general is nonempty for linear channels. Then we can regard Φ_w as a mapping from $(\mathbb{F}^m \times \mathcal{Z}^*)$ to $2^{\mathbb{F}^l}$. In the same way, we can extend all the definitions related to $\Phi_w(\mathbf{x}, c)$, and the discussion from Subsections 2.1 to 2.5 continues to hold for linear channels.

For two subsets $V_1, V_2 \subset \mathbb{F}^k$, their sum is the set defined by

$$V_1 + V_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2\}. \tag{26}$$

For $\mathbf{v} \in \mathbb{F}^k$ and $V \subset \mathbb{F}^k$, we also write $\{\mathbf{v}\} + V$ as $\mathbf{v} + V$.

For linear channel,

$$\begin{aligned}
\Phi_w(\mathbf{x}, c) &= \mathbf{x}\mathbf{F} + \{\mathbf{z}\mathbf{F}' : \mathbf{z} \in \Sigma,\ w(\mathbf{z}) \leq c\}, && (27)\\
&= \mathbf{x}\mathbf{F} + \Phi_w(\mathbf{0}, c) && (28)
\end{aligned}$$

The Hamming weight w is a weight measure with $w(\mathbf{z})$ equal to the non-zero components of $\mathbf{z}$.

Lemma 6 *If the channel is linear and the weight measure* w *is the Hamming weight, then*

$$\begin{aligned}
\partial(\Psi_w(\mathbf{x}_1, \mathbf{x}_2)) = \{&(c_1, c_2) \in (\mathbb{Z}^*)^2 : \\
&c_1 + c_2 = D_w^1(\mathbf{x}_1, \mathbf{x}_2)\}.
\end{aligned} \tag{29}$$

DOI: 10.1002/ett

Proof First we show that for any $(c_1, c_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$, we can find $c_1' \le c_1$ and $c_2' \le c_2$ such that $c_1' + c_2' = D_w^1(\mathbf{x}_1, \mathbf{x}_2)$. Let $(c_1, c_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$. There exist $\mathbf{z}_1$ and $\mathbf{z}_2$ with $w(\mathbf{z}_1) = c_1$ and $w(\mathbf{z}_2) = c_2$ such that $\mathbf{x}_1\mathbf{F} + \mathbf{z}_1\mathbf{F}' = \mathbf{x}_2\mathbf{F} + \mathbf{z}_2\mathbf{F}'$. Thus, $\mathbf{x}_1\mathbf{F} + \mathbf{0}\mathbf{F}' = \mathbf{x}_2\mathbf{F} + (\mathbf{z}_2 - \mathbf{z}_1)\mathbf{F}'$. Therefore, $c_1 + c_2 = w(\mathbf{z}_1) + w(\mathbf{z}_2) \ge w(\mathbf{z}_2 - \mathbf{z}_1) = w(\mathbf{0}) + w(\mathbf{z}_2 - \mathbf{z}_1) \ge D_w^1(\mathbf{x}_1, \mathbf{x}_2)$.

Then we need to prove that $(c_1, c_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$ if $c_1 + c_2 \ge D_w^1(\mathbf{x}_1, \mathbf{x}_2)$. Find $c_1' \le c_1$ and $c_2' \le c_2$ such that $c_1' + c_2' = D_w^1(\mathbf{x}_1, \mathbf{x}_2)$. Since there exists $\mathbf{z}$ with $w(\mathbf{z}) = D_w^1(\mathbf{x}_1, \mathbf{x}_2)$ such that $\mathbf{x}_1\mathbf{F} = \mathbf{x}_2\mathbf{F} + \mathbf{z}\mathbf{F}'$, we can find $\mathbf{z}_1$ and $\mathbf{z}_2$ such that $\mathbf{z}_2 - \mathbf{z}_1 = \mathbf{z}$, $w(\mathbf{z}_1) = c_1'$, and $w(\mathbf{z}_2) = c_2'$. Thus, $\mathbf{x}_1\mathbf{F} + \mathbf{z}_1\mathbf{F}' = \mathbf{x}_2\mathbf{F} + \mathbf{z}_2\mathbf{F}'$, which implies $(c_1', c_2') \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$. Hence, by Lemma 2, $(c_1, c_2) \in \Psi_w(\mathbf{x}_1, \mathbf{x}_2)$.

■

Corollary 1 *If the channel is linear and the weight measure w is the Hamming weight, then, for any $(c_1, c_2) \in \partial(\Phi_w)$, $c_1 + c_2 = d_{\min,w}^1$.*

Thus by Theorem 3, a code for linear channel is (c, c')-error-correcting if and only if $d_{\min,w} \ge 2c + c' + 1$ when the weight measure w is the Hamming weight.

Lemma 7 *If the channel is linear and the weight measure w is the Hamming weight, then D_w^1 is a translation-invariant metric.*

Proof Using the definition of D_w^1 in (6), we have

$$D_w^1(\mathbf{x}_1, \mathbf{x}_2) = \min\{c : \mathbf{x}_1\mathbf{F} \in \mathbf{x}_2\mathbf{F} + \Phi_w(\mathbf{0}, c)\} \quad (30)$$
$$= \min\{c : (\mathbf{x}_1 - \mathbf{x}_2)\mathbf{F} \in \Phi_w(\mathbf{0}, c)\}. \quad (31)$$

First, it is clear from (31) that D_w^1 is translation invariant, i.e.,

$$D_w^1(\mathbf{x}_1 + \mathbf{x}, \mathbf{x}_2 + bx) = D_w^1(\mathbf{x}_1, \mathbf{x}_2). \quad (32)$$

Then we show that D_w^1 satisfies the triangle inequality. Find $\mathbf{z}$ and $\mathbf{z}'$ such that $(\mathbf{x}_1 - \mathbf{x}_2)\mathbf{F}_{s,t} = \mathbf{z}\mathbf{F}_t$, $D_w^1(\mathbf{x}_1, \mathbf{x}_2) = w(\mathbf{z})$, $(\mathbf{x}_2 - \mathbf{x}_3)\mathbf{F}_{s,t} = \mathbf{z}'\mathbf{F}_t$ and $D_w^1(\mathbf{x}_2, \mathbf{x}_3) = w(\mathbf{z}')$. The existence of such $\mathbf{z}$ and $\mathbf{z}'$ follows from (31). Thus $(\mathbf{x}_1 - \mathbf{x}_3)\mathbf{F} = (\mathbf{z} + \mathbf{z}')\mathbf{F}'$. Hence, from (31),

$$D_w^1(\mathbf{x}_1, \mathbf{x}_3) \le w(\mathbf{z} + \mathbf{z}') \quad (33)$$
$$\le w(\mathbf{z}) + w(\mathbf{z}') \quad (34)$$
$$= D_w^1(\mathbf{x}_1, \mathbf{x}_2) + D_w^1(\mathbf{x}_2, \mathbf{x}_3). \quad (35)$$

■

3. NETWORK ERROR CORRECTION

3.1. Formulation of Network Coding

A directed acyclic communication network is represented by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes 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 associated partial order of the directed acyclic network $\mathcal{G}$. An edge from node a to node b, say edge e, represents a communication channel from node a to node b. We call node a (node b) the tail (head) of edge e, denoted by $tail(e)$ ($head(e)$). Let $In(a) = \{e \in \mathcal{E} : head(e) = a\}$ and $Out(a) = \{e \in \mathcal{E} : tail(e) = a\}$ be the sets of incoming edges and outgoing edges of node a, respectively. There can be multiple edges between a pair of nodes, and each edge can transmit one symbol in a finite field $\mathbb{F}$.

Without loss of generality, we assume $In(s) = \emptyset$. Let $n_s = |Out(s)|$. The source node s encodes the information to be multicast into a row vector $\mathbf{x} \in \mathbb{F}^{n_s}$, called the *codeword*. We will write $\mathbf{x} = [x_e, e \in Out(s)]$. The set of all codewords is the *codebook*, denoted by $\mathcal{C}$. Note that we do not require $\mathcal{C}$ to be a linear space. The source node s transmits the codeword by mapping its n_s components onto the edges in $Out(s)$.

An *error vector* $\mathbf{z}$ is an $|\mathcal{E}|$-dimensional row vector over the field $\mathbb{F}$ with the ith component representing the error on the ith edge in $\mathcal{E}$. An *error pattern* is a subset of $\mathcal{E}$. An error vector is said to match an error pattern if all the errors occur on the edges in the error pattern. The set of all error vectors that *match* error pattern ρ is denoted by ρ^*. Let $\rho_{\mathbf{z}}$ be the error pattern corresponding to the non-zero components of an error vector $\mathbf{z}$.

Consider the codeword $\mathbf{x}$ and the error vector $\mathbf{z}$. If the input to an edge e is $\bar{F}_e(\mathbf{x}, \mathbf{z})$ and the error on the edge is z_e, the output of the edge $F_e(\mathbf{x}, \mathbf{z})$ is

$$F_e(\mathbf{x}, \mathbf{z}) = \bar{F}_e(\mathbf{x}, \mathbf{z}) + z_e. \quad (36)$$

For any set of edges ρ, form two row vectors

$$F_\rho(\mathbf{x}, \mathbf{z}) = [F_e(\mathbf{x}, \mathbf{z}), e \in \rho], \quad (37)$$

and

$$\bar{F}_\rho(\mathbf{x}, \mathbf{z}) = [\bar{F}_e(\mathbf{x}, \mathbf{z}), e \in \rho]. \quad (38)$$

A network code on network $\mathcal{G}$ is a codebook $\mathcal{C} \subseteq \mathbb{F}^{n_s}$ and a family of local encoding functions $\{\bar{\beta}_e : e \in \mathcal{E} \setminus Out(s)\}$, where $\bar{\beta}_e : \mathbb{F}^{|In(tail(e))|} \to \mathbb{F}$, such that

$$\bar{F}_e = \bar{\beta}_e(F_{In(tail(e))}). \quad (39)$$

DOI: 10.1002/ett

Communication over the network with the code defined above is in an upstream-to-downstream order consistent with the partial order of the edges. The family of local encoding functions induces global transfer functions $\bar{F}_e$ and F_e for each edge e by the iterative functions (36) and (39) with boundary condition

$$\bar{F}_{Out(s)}(\mathbf{x},\mathbf{z}) = \mathbf{x}. \tag{40}$$

This is the general form of the network error correction problem [6].

If $\bar{\beta}_e$ is a linear function for all $e \in \mathcal{E} \setminus Out(s)$, i.e.,

$$\bar{F}_e = \sum_{e' \in \mathcal{E}} \beta_{e',e} F_{e'} \tag{41}$$

we say the network code is *linear*, where $\beta_{e',e}$ is called *local encoding kernel*. The local encoding kernel $\beta_{e',e}$ can be non-zero only if $e' \in In(tail(e))$. Define the $|\mathcal{E}| \times |\mathcal{E}|$ one-step transformation matrix $\mathbf{K} = [K_{i,j}]$ in network $\mathcal{G}$ as $K_{i,j} = \beta_{e_i,e_j}$. For an acyclic network, $\mathbf{K}^N = \mathbf{0}$ for some positive integer N. Define the transfer matrix of the network by $\mathbf{F} = (\mathbf{I} - \mathbf{K})^{-1}$ [3].

For a set of edges ρ, define a $|\rho| \times |\mathcal{E}|$ matrix $\mathbf{A}_\rho = [A_{i,j}]$ by

$$A_{i,j} = \begin{cases} 1 & e_j \text{ is the } i\text{th edge in } \rho, \\ 0 & \text{otherwise.} \end{cases} \tag{42}$$

By applying the order on $\mathcal{E}$ to ρ, the $|\rho|$ nonzero columns of $\mathbf{A}_\rho$ form an identity matrix. To simplify notation, we write $\mathbf{A}_\rho \mathbf{F} \mathbf{A}_{\rho'}^{\mathrm{T}} = \mathbf{F}_{\rho,\rho'}$. For input $\mathbf{x}$ and error vector $\mathbf{z}$, the output of the edges in ρ is

$$F_\rho(\mathbf{x},\mathbf{z}) = (\mathbf{x}\mathbf{A}_{Out(s)} + \mathbf{z})\mathbf{F}\mathbf{A}_\rho^{\mathrm{T}}. \tag{43}$$

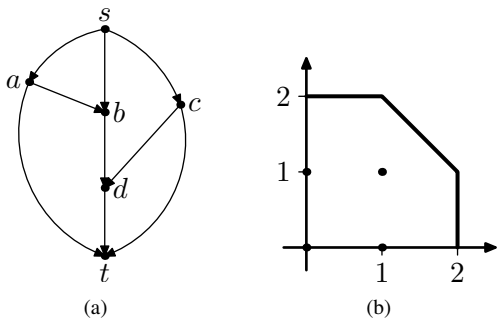
Writing $F_v(\mathbf{x},\mathbf{z}) = F_{In(v)}(\mathbf{x},\mathbf{z})$ for a node v, the received vector for a sink node t is

$$F_t(\mathbf{x},\mathbf{z}) = (\mathbf{x}\mathbf{A}_{Out(s)} + \mathbf{z})\mathbf{F}\mathbf{A}_{In(t)}^{\mathrm{T}}, \tag{44}$$

$$= \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}\mathbf{F}_t, \tag{45}$$

where $\mathbf{F}_{s,t} = \mathbf{F}_{Out(s),In(t)}$, and $\mathbf{F}_t = \mathbf{F}\mathbf{A}_{In(t)}^{\mathrm{T}}$. Here $\mathbf{F}_{s,t}$ and $\mathbf{F}_t$ are the transfer matrices for message transmission and error transmission, respectively, for sink node t.

When there is only one sink node t and both $\mathbf{F}_{s,t}$ and $\mathbf{F}_t$ are the identity matrix, the problem becomes that of classical error correction. Therefore, classical error correction is a special case of the linear network error correction problem.



(a) (b)

Figure 1. (a) is an example of non-linear network code with $d^1_{\min,w} \neq d^0_{\min,w}$. In (b), the black points are in $\bar{\Psi}_w$.

3.2. An Example of Nonlinear Network Code

Consider a network coding problem over the network shown in Fig. 1(a), where s is the source node and t is the sink node. The network code is over the finite field $\mathbb{F}_3 = \{0,1,2\}$. Define the codebook $\mathcal{C} = \{\mathbf{x}_0 = (0,0,0), \mathbf{x}_1 = (1,1,1)\}$. The network code is specified as follows: $\bar{F}_{(a,t)} = F_{(s,a)}$, $\bar{F}_{(a,b)} = F_{(s,a)}$, $\bar{F}_{(c,t)} = F_{(s,c)}$, $\bar{F}_{(c,d)} = F_{(s,c)}$ and the local encoding functions $\bar{\beta}_{(b,d)}$ and $\bar{\beta}_{(d,t)}$ are given in Tables 1 and 2, respectively. For this network, $\Sigma = \mathbb{F}_3^9$. The weight measure w on Σ is the Hamming weight.

For this problem, first we can calculate that

$$\Phi_w(\mathbf{x}_0,1) = \{(0,0,0),(1,0,0)(0,1,0),\\ (0,0,1),(2,0,0),(0,2,0),(0,0,2)\}, \tag{46}$$

and

$$\Phi_w(\mathbf{x}_1,1) = \{(0,1,1),(1,0,1),(1,1,0),\\ (1,1,1),(1,0,2),(2,0,1),\\ (2,1,1),(1,2,1),(1,1,2)\}. \tag{47}$$

Thus

$$\Phi_w(\mathbf{x}_0,1) \cap \Phi_w(\mathbf{x}_1,1) = \emptyset, \tag{48}$$

which gives $\Phi_w(\mathbf{x}_0,0) \cap \Phi_w(\mathbf{x}_1,1) = \emptyset$ and $\Phi_w(\mathbf{x}_0,1) \cap \Phi_w(\mathbf{x}_1,0) = \emptyset$.

Let $\mathbf{z}$ be an error vector such that $z_{(s,a)} = z_{(s,c)} = 2$ and all other components are equal to 0. Then, $F_t(\mathbf{x}_1,\mathbf{z}) = (0,0,0) = F_t(\mathbf{x}_0,\mathbf{0})$. Thus

$$\Phi_w(\mathbf{x}_0,0) \cap \Phi_w(\mathbf{x}_1,2) \neq \emptyset. \tag{49}$$

Fig. 1(b) shows $\partial(\Psi_w)$. We see that for this code, $d^1_{\min,w} = 2$ and $d^0_{\min,w} = 3$, i.e., the code $\mathcal{C}$ can correct and detect one error in this network. This is rather surprising that the number of correctable errors can be more than half of the number of detectable errors.

Table 1. Local encoding function of node b

$F_{(s,b)}$	0	0	0	1	1	1	2	2	2
$F_{(a,b)}$	0	1	2	0	1	2	0	1	2
$\bar{F}_{(b,d)}$	0	0	0	2	1	0	0	0	0

Table 2. Local encoding function of node c

$F_{(b,d)}$	0	0	0	1	1	1	2	2	2
$F_{(c,d)}$	0	1	2	0	1	2	0	1	2
$\bar{F}_{(d,t)}$	0	0	0	1	1	0	0	1	0

3.3. Weight Measures for General Network Codes

In this section, we consider the network coding problem with the codebook $\mathcal{C} \subset \mathbb{F}^{n_s}$ and the set of error vectors $\Sigma = \mathbb{F}^{|\mathcal{E}|}$. For any $t \in \mathcal{T}$, the transfer function F_t induced by local encoding functions gives an instance of the general transmission system studied in Section 2.

To apply the general results in Section 2 to network error correction, we need to specify the weight measure on Σ. One natural such weight measure is the Hamming weight, the number of non-zero components in an error vector $\mathbf{z}$, denoted by $w_H(\mathbf{z})$. With respect to the Hamming weight w_H, for a sink node t, define the set

$$\Phi^t_{w_H}(\mathbf{x}, c) = \{F_t(\mathbf{x}, \mathbf{z}) : w_H(\mathbf{z}) \le c\} \tag{50}$$

in view of (2).

An error pattern, which is a set of edges, can be measured using the concept of minimum cut (min-cut) which has been used in [12, 15]. We say a set of edges ρ is a *cut-set* separating node u and node v if any directed path from u to v crosses ρ. Since each edge has unit capacity, the capacity of a cut-set is just its cardinality. Further, define a cut-set and the associated cut-set capacity between a set of edges ρ and a node v by introducing an auxiliary node u_ρ and the auxiliary edges $(u_\rho, head(e))$ for all $e \in \rho$. A cut-set between ρ and v is then a cut-set between u_ρ and v. It follows that the min-cut between source node s (a set of edges ρ) and a sink node t is the minimum cut-set capacity among all cut sets that separates s (ρ) and t, denoted by $\mathrm{mincut}_t(s)$ ($\mathrm{mincut}_t(\rho)$).

Recall that $\rho_{\mathbf{z}}$ is the error pattern corresponding to the non-zero components of an error vector $\mathbf{z}$. In terms of the min-cut of an error pattern, we define another weight measure with respect to sink node t as

$$w^t_c(\mathbf{z}) = \mathrm{mincut}_t(\rho_{\mathbf{z}}). \tag{51}$$

Lemma 8 *For any error vector* $\mathbf{z}$ *and sink node* t*,*

$$w_H(\mathbf{z}) \ge w^t_c(\mathbf{z}). \tag{52}$$

Proof The lemma holds since $w^t_c(\mathbf{z}) = \mathrm{mincut}_t(\rho_{\mathbf{z}}) \le |\rho_{\mathbf{z}}| = w_H(\mathbf{z})$. ∎

Recall that ρ^* is the set of all error vectors that match an error pattern ρ.

Lemma 9 *If* ρ' *is a cut-set between* ρ *and* t *with* $|\rho'| = \mathrm{mincut}_t(\rho)$*, then for any* $\mathbf{x} \in \mathbb{F}^{n_s}$ *and* $\mathbf{z} \in \rho^*$*, there exists* $\mathbf{z}' \in (\rho')^*$ *such that* $F_t(\mathbf{x}, \mathbf{z}) = F_t(\mathbf{x}, \mathbf{z}')$*.*

Proof

Find a cut-set ρ'' separating s and t as follows. At the beginning, let $\rho'' = Out(s) \cup \rho'$. Then, for an edge e in $\rho'' \setminus \rho'$, if $\rho'' \setminus \{e\}$ is a cut-set separating s and t, we remove e from ρ'' and reassign ρ'' to be the remaining set. Repeat this procedure until no edge in $\rho'' \setminus \rho'$ can be removed.

It is easy to check that $(\rho'' \setminus \rho') \cap \rho = \emptyset$, so that the outputs of the edges in $\rho'' \setminus \rho'$ are not affected by the errors on ρ. Thus for any $\mathbf{z} \in \rho^*$, we have

$$F_{\rho'' \setminus \rho'}(\mathbf{x}, \mathbf{z}) = F_{\rho'' \setminus \rho'}(\mathbf{x}, \mathbf{0}). \tag{53}$$

Find an error vector $\mathbf{z}' \in (\rho')^*$ such that $F_{\rho'}(\mathbf{x}, \mathbf{z}) = F_{\rho'}(\mathbf{x}, \mathbf{z}')$ as follows. Apply the order on $\mathcal{E}$ to ρ' and label the edges in ρ' as $e'_1, e'_2, \cdots, e'_{|\rho'|}$. Let error vector $\mathbf{z}^0 = \mathbf{0}$. From $i = 1$ to $|\rho'|$, let $z'_i = F_{e'_i}(\mathbf{x}, \mathbf{z}) - F_{e'_i}(\mathbf{x}, \mathbf{z}^{i-1})$, and $\mathbf{z}^i$ be $\mathbf{z}^{i-1}$ except the value of the component corresponding to e'_i is z'_i. At the end of the process, let $\mathbf{z}' = \mathbf{z}^{|\rho'|}$.

Now we verify that $\mathbf{z}'$ as constructed meets our requirement. Since for $\mathbf{z}^{i-1}$, the error on e'_i is zero, $F_{e'_i}(\mathbf{x}, \mathbf{z}^{i-1}) = \bar{F}_{e'_i}(\mathbf{x}, \mathbf{z}^{i-1})$. Together with the fact that $\bar{F}_{e'_i}(\mathbf{x}, \mathbf{z}^{i-1}) = \bar{F}_{e'_i}(\mathbf{x}, \mathbf{z}^i)$, we obtain

$$F_{e'_i}(\mathbf{x}, \mathbf{z}) = F_{e'_i}(\mathbf{x}, \mathbf{z}^{i-1}) + z'_i \tag{54}$$

$$= \bar{F}_{e'_i}(\mathbf{x}, \mathbf{z}^i) + z'_i \tag{55}$$

$$= F_{e'_i}(\mathbf{x}, \mathbf{z}^i). \tag{56}$$

Further, the error on e'_j for $j > i$ does not affect the output of e'_i, i.e., $F_{e'_i}(\mathbf{x}, \mathbf{z}^i) = F_{e'_i}(\mathbf{x}, \mathbf{z}^{|\rho'|})$, thus

$$F_{e'_i}(\mathbf{x}, \mathbf{z}) = F_{e'_i}(\mathbf{x}, \mathbf{z}^{|\rho'|}), \tag{57}$$

for all $1 \le i \le |\rho'|$.

DOI: 10.1002/ett

Since the output of the edges in $\rho'' \setminus \rho'$ are not affected by the errors on ρ', we have

$$F_{\rho''\setminus\rho'}(\mathbf{x},\mathbf{z}') = F_{\rho''\setminus\rho'}(\mathbf{x},\mathbf{0}). \tag{58}$$

Then,

$$\begin{aligned} F_{\rho''}(\mathbf{x},\mathbf{z}) &= \begin{bmatrix} F_{\rho''\setminus\rho'}(\mathbf{x},\mathbf{z}) & F_{\rho'}(\mathbf{x},\mathbf{z}) \end{bmatrix} && (59)\\ &= \begin{bmatrix} F_{\rho''\setminus\rho'}(\mathbf{x},\mathbf{0}) & F_{\rho'}(\mathbf{x},\mathbf{z}) \end{bmatrix} && (60)\\ &= \begin{bmatrix} F_{\rho''\setminus\rho'}(\mathbf{x},\mathbf{z}') & F_{\rho'}(\mathbf{x},\mathbf{z}') \end{bmatrix} && (61)\\ &= F_{\rho''}(\mathbf{x},\mathbf{z}'). && (62) \end{aligned}$$

Since ρ'' is a cut-set separating $Out(s) \cup \rho$ and t, F_t is a function on the outputs of the edges in ρ''. Thus, $F_t(\mathbf{x},\mathbf{z}) = F_t(\mathbf{x},\mathbf{z}')$. ∎

For a sink t, with respect to w_c^t, define the set

$$\Phi^t_{w_c^t}(\mathbf{x},c) = \{F_t(\mathbf{x},\mathbf{z}) : w_c^t(\mathbf{z}) \le c\} \tag{63}$$

in view of (2).

Lemma 10 *For any network code,*

$$w_H \overset{F_t}{\sim} w_c^t, \tag{64}$$

where $t \in \mathcal{T}$.

Proof First, for any $\mathbf{y} \in \Phi^t_{w_H}(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_H(\mathbf{z}) \le c$ such that $\mathbf{y} = F_t(\mathbf{x},\mathbf{z})$. Since $w_c^t(\mathbf{z}) \le w_H(\mathbf{z}) = c$, we have $\mathbf{y} = F_t(\mathbf{x},\mathbf{z}) \in \Phi_{w_c^t}(c)$. Thus, $\Phi^t_{w_H}(c) \subset \Phi^t_{w_c^t}(c)$.

On the other hand, for any $\mathbf{y} \in \Phi^t_{w_c^t}(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_c^t(\mathbf{z}) \le c$ such that $\mathbf{y} = F_t(\mathbf{x},\mathbf{z})$. By Lemma 9, if ρ' is a cut-set between $\rho_{\mathbf{z}}$ and t with $|\rho'| = \mathrm{mincut}_t(\rho_{\mathbf{z}})$, there exists $\mathbf{z}' \in \rho'$ such that $F_t(\mathbf{x},\mathbf{z}'') = F_t(\mathbf{x},\mathbf{z}) = \mathbf{y}$. Further, $w_H(\mathbf{z}') \le |\rho'| = \mathrm{mincut}_t(\rho_{\mathbf{z}}) = w_c^t(\mathbf{z}) \le c$. Therefore, $\mathbf{y} \in \Phi_{w_H}(c)$. Hence, $\Phi^t_{w_c^t}(c) \subset \Phi^t_{w_H}(c)$. ∎

4. WEIGHT MEASURES FOR LINEAR NETWORK CODES

4.1. Rank of Error Vectors

For linear network codes, the *rank* of an error pattern ρ with respect to a sink node t [14] is

$$\mathrm{rank}_t(\rho) = \mathrm{rank}(\mathbf{F}_{\rho,In(t)}). \tag{65}$$

In terms of the rank of an error pattern, we define a weight measure for the error vectors as

$$w_r^t(\mathbf{z}) = \mathrm{rank}_t(\rho_{\mathbf{z}}), \tag{66}$$

for $\mathbf{z} \in \Sigma$.

For an error pattern ρ and an error vector $\mathbf{z}$, let $\mathbf{z}_\rho \in \mathbb{F}^{|\rho|}$ be the vector formed by the components of $\mathbf{z}$ corresponding to the edges in ρ. If $\mathbf{z} \in \rho^*$, $\mathbf{z}_\rho$ contains all the components in $\mathbf{z}$ that can be non-zero. Note that $\mathbf{F}_{\rho,In(t)}$ is a submatrix of $\mathbf{F}_t$ given by the rows corresponding to the edges in ρ. Thus, for $\mathbf{z} \in \rho^*$,

$$\mathbf{z}\mathbf{F}_t = \mathbf{z}_\rho \mathbf{F}_{\rho,In(t)}. \tag{67}$$

Lemma 11 *Let ρ' be any cut-set between an error pattern ρ and a sink node t. Then, $rank_t(\rho) \le rank_t(\rho')$.*

Proof By Lemma 9, for $\mathbf{x} = \mathbf{0}$ and any $\mathbf{z} \in \rho^*$, there exists $\mathbf{z}' \in (\rho')^*$ such that $\mathbf{z}\mathbf{F}_t = \mathbf{z}'\mathbf{F}_t$ (cf. (45)), which together with (67) implies

$$\mathbf{z}_\rho \mathbf{F}_{\rho,In(t)} = \mathbf{z'}_{\rho'} \mathbf{F}_{\rho',In(t)}. \tag{68}$$

Since (68) holds for all $\mathbf{z} \in \rho^*$, the subspace spanned by the row vectors of $\mathbf{F}_{\rho,In(t)}$ is a subset of the subspace spanned by the row vectors of $\mathbf{F}_{\rho',In(t)}$. Thus, $\mathrm{rank}(\mathbf{F}_{\rho,In(t)}) \le \mathrm{rank}(\mathbf{F}_{\rho',In(t)})$. ∎

Lemma 12 *For any error vector $\mathbf{z}$ and sink node t,*

$$w_r^t(\mathbf{z}) \le w_c^t(\mathbf{z}). \tag{69}$$

Proof Let ρ' be any cut-set between $\rho_{\mathbf{z}}$ and sink node t. Then, $w_r^t(\mathbf{z}) = \mathrm{rank}_t(\rho_{\mathbf{z}}) \le \mathrm{rank}_t(\rho') \le |\rho'|$. Minimize over all ρ', we obtain $w_r^t(\mathbf{z}) \le \mathrm{mincut}_t(\rho_{\mathbf{z}}) = w_c^t(\mathbf{z})$. ∎

Lemma 13 *If the network code is linear,*

1) *for any error pattern ρ, there exists a subset $\rho' \subset \rho$ such that $|\rho'| = rank_t(\rho)$; and*
2) *for any $\mathbf{z} \in \rho^*$, there exists $\mathbf{z}' \in (\rho')^*$ such that $\mathbf{z}\mathbf{F}_t = \mathbf{z}'\mathbf{F}_t$.*

Proof Find a maximal linearly independent subset of the row vectors of $\mathbf{F}_{\rho,In(t)}$. Let ρ' be the corresponding edges in that linearly independent subset. Thus $\rho' \subset \rho$ and $|\rho'| = rank_t(\rho)$.

The second part of the lemma follows from the fact that the row vectors of $\mathbf{F}_{\rho,In(t)}$ and $\mathbf{F}_{\rho',In(t)}$ span the same vector space. ∎

For a sink t, with respect to w_r^t, define the set

$$\Phi_{w_r^t}^t(\mathbf{x}, c) = \{F_t(\mathbf{x}, \mathbf{z}) : w_r^t(\mathbf{z}) \leq c\} \tag{70}$$

in view of (2).

Lemma 14 *For any linear network code,*

$$w_c^t \overset{F_t}{\sim} w_r^t, \tag{71}$$

where $t \in \mathcal{T}$.

Proof

First, for any $\mathbf{y} \in \Phi_{w_c^t}^t(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_c^t(\mathbf{z}) \leq c$ such that $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z})$. Since $w_r^t(\mathbf{z}) \leq w_c^t(\mathbf{z}) = c$, we have $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z}) \in \Phi_{w_c^t}(c)$. Thus, $\Phi_{w_c^t}^t(c) \subset \Phi_{w_r^t}^t(c)$.

On the other hand, for any $\mathbf{y} \in \Phi_{w_r^t}^t(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_r^t(\mathbf{z}) \leq c$ such that $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z})$. By Lemma 13, there exists $\rho' \subset \rho_{\mathbf{z}}$ such that $|\rho'| = \text{rank}_t(\rho_{\mathbf{z}})$ and $\mathbf{z}' \in (\rho')^*$ such that $\mathbf{z}\mathbf{F}_t = \mathbf{z}'\mathbf{F}_t$. So $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z}) = \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}\mathbf{F}_t = \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}'\mathbf{F}_t = F_t(\mathbf{x}, \mathbf{z}')$. Further, $w_c^t(\mathbf{z}') \leq |\rho'| = \text{rank}_t(\rho_{\mathbf{z}}) = w_r^t(\mathbf{z}) \leq c$. Therefore, $\mathbf{y} \in \Phi_{w_c^t}(c)$. Hence, $\Phi_{w_c^t}^t(c) \subset \Phi_{w_r^t}^t(c)$. ∎

4.2. Network Hamming Weight

Network Hamming weight is a generalization of the Hamming weight for network codes [16]. For any $t \in \mathcal{T}$, let $\Upsilon_t(\mathbf{y}) = \{\mathbf{z} : \mathbf{z}\mathbf{F}_t = \mathbf{y}\}$ for a received vector $\mathbf{y} \in Im(\mathbf{F}_t)$, the image space of $\mathbf{F}_t$. For any sink t, the network Hamming weight of an error vector $\mathbf{z}$ is defined by

$$w_n^t(\mathbf{z}) = \min_{\mathbf{z}' \in \Upsilon_t(\mathbf{z}F_t)} w_H(\mathbf{z}'), \tag{72}$$

In other words, $w_n^t(\mathbf{z})$ is the minimum Hamming weight of any error vector that incurs the same input at sink node t as the error vector $\mathbf{z}$ when the transmitted codeword is $\mathbf{0}$. For any vector $\mathbf{z} \in \Upsilon_t(\mathbf{0})$, $w_n^t(\mathbf{z}) = \min_{z \in \Upsilon_t(\mathbf{0})} w_H(\mathbf{z}) = w_H(\mathbf{0}) = 0$. Evidently, if error vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ satisfy $\mathbf{z}_1 - \mathbf{z}_2 \in \Upsilon_t(\mathbf{0})$, then $w_n^t(\mathbf{z}_1) = w_n^t(\mathbf{z}_2)$. When $\mathbf{F}_t = \mathbf{F}_{s,t} = \mathbf{I}$, the definition reduces to the usual Hamming weight.

Lemma 15 *For any error vector $\mathbf{z}$ and sink node t,*

$$w_n^t(\mathbf{z}) \leq w_r^t(\mathbf{z}). \tag{73}$$

Proof Find an error vector $\mathbf{z}' \in (\rho')^*$ as in Lemma 13 where $\rho' \subset \rho_{\mathbf{z}}$, such that $w_r^t(\mathbf{z}) = |\rho'| \geq w_H(\mathbf{z}')$ and $\mathbf{z}\mathbf{F}_t = \mathbf{z}'\mathbf{F}_t$. Thus, $w_n^t(\mathbf{z}) \leq w_H(\mathbf{z}') \leq w_r^t(\mathbf{z})$. ∎

For a sink t, with respect to w_n^t, define the set

$$\Phi_{w_n^t}^t(\mathbf{x}, c) = \{F_t(\mathbf{x}, \mathbf{z}) : w_n^t(\mathbf{z}) \leq c\} \tag{74}$$

in view of (2).

Lemma 16 *For any linear network code,*

$$w_H \overset{F_t}{\sim} w_n^t, \tag{75}$$

where $t \in \mathcal{T}$.

Proof First, for any $\mathbf{y} \in \Phi_{w_H}^t(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_H(\mathbf{z}) \leq c$ such that $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z})$. Since $w_n^t(\mathbf{z}) \leq w_H(\mathbf{z}) = c$, we have $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z}) \in \Phi_{w_n^t}(c)$. Thus, $\Phi_{w_H}^t(c) \subset \Phi_{w_n^t}^t(c)$.

On the other hand, for any $\mathbf{y} \in \Phi_{w_n^t}^t(c)$, find $\mathbf{x} \in \mathbb{F}^{n_s}$ and any $\mathbf{z} \in \Sigma$ with $w_n^t(\mathbf{z}) \leq c$ such that $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z})$. By the definition of w_n^t, there exist $\mathbf{z}'$ with $w_H(\mathbf{z}') = w_n^t(\mathbf{z}) \leq c$ such that $\mathbf{z}'\mathbf{F}_t = \mathbf{z}\mathbf{F}_t$. So $\mathbf{y} = F_t(\mathbf{x}, \mathbf{z}) = \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}\mathbf{F}_t = \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}'\mathbf{F}_t = F_t(\mathbf{x}, \mathbf{z}')$. Therefore, $\mathbf{y} \in \Phi_{w_H}(c)$. Hence, $\Phi_{w_n^t}^t(c) \subset \Phi_{w_H}^t(c)$. ∎

4.3. Minimum Distance of Linear Network Codes

The results we have obtained regarding linear network codes can be summarized by the following theorem.

Theorem 6 *For any linear network code,*

1)

$$w_H(\mathbf{z}) \geq w_c^t(\mathbf{z}) \geq w_r^t(\mathbf{z}) \geq w_n^t(\mathbf{z}), \tag{76}$$

and

2)

$$w_H \overset{F_t}{\sim} w_c^t \overset{F_t}{\sim} w_r^t \overset{F_t}{\sim} w_n^t, \tag{77}$$

where $t \in \mathcal{T}$.

Proof The first part of the theorem follows from Lemmas 8, 12 and 15. The second part follows from Lemmas 10, 14 and 16. ∎

DOI: 10.1002/ett

4.4. Network Erasure Correction

In classical algebraic coding, erasure correction is error correction with the potential positions of the errors in the codewords known by the decoder. Here, we extend this theme to linear 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 this set of channels as the *erasure pattern*.

With respect to any weight measure w for the error vectors, define a weight measure for the erasure patterns as

$$w(\rho) = \max_{\mathbf{z}\in\rho^*} w(\mathbf{z}). \tag{78}$$

Thus, for linear network codes, each of the four weight measures on the error vectors we have discussed gives a weight measure on the erasure patterns defined by replacing w in (78) accordingly, namely

$$w_H(\rho) = |\rho|, \tag{79}$$

$$w_c^t(\rho) = \mathrm{mincut}_t(\rho), \tag{80}$$

$$w_r^t(\rho) = \mathrm{rank}_t(\rho), \tag{81}$$

and

$$w_n^t(\rho) = \max_{\mathbf{z}\in\rho^*} w_n^t(\mathbf{z}). \tag{82}$$

Lemma 17 *For any error vector* $\mathbf{z}$ *and any sink node* t*,*

$$w_H(\rho) \geq w_c^t(\rho) \geq w_r^t(\rho) \geq w_n^t(\rho). \tag{83}$$

Proof This is a direct result of the definitions and Theorem 6. ∎

A code can correct an erasure pattern ρ if there exists a decoding algorithm such that no matter which error vector matching ρ occurred, the algorithm can decode correctly.

Theorem 7 *At a sink node* t*, the following properties of a linear network code with codebook* $\mathcal{C}$ *are equivalent:*

1) *The code can correct all erasure pattern* ρ *with* $w_H(\rho) \leq c$*;*
2) *The code can correct all erasure pattern* ρ *with* $w_c^t(\rho) \leq c$*;*
3) *The code can correct all erasure pattern* ρ *with* $w_r^t(\rho) \leq c$*;*
4) *The code can correct all erasure pattern* ρ *with* $w_n^t(\rho) \leq c$*;*
5) $d_{\min,t} \geq c+1$.

Proof Fix a sink node t. To prove 5)⇒4), assume $d_{\min,t} \geq c+1$. Let ρ be an erasure pattern with $w_n^t(\rho) \leq c$. To decode a received vector $\mathbf{y}$, we try to find a codeword $\mathbf{x} \in \mathcal{C}$ and an error vector $\mathbf{z} \in \rho^*$ that satisfy the equation

$$\mathbf{y} = \mathbf{x}\mathbf{F}_{s,t} + \mathbf{z}\mathbf{F}_{\rho,t}. \tag{84}$$

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 codeword. 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 have $\mathbf{x}_1\mathbf{F}_{s,t} = \mathbf{x}_2\mathbf{F}_{s,t} + (\mathbf{z}_2 - \mathbf{z}_1)\mathbf{F}_t$. Thus, $d_{\min,t} \leq w_n^t(\mathbf{z}_2 - \mathbf{z}_1) \leq w_n^t(\rho) \leq c$. This a contradiction to $d_{\min,t} \geq c+1$. Hence, the code can correct all erasure pattern ρ with $w_n^t(\rho) \leq c$, i.e., 4) holds.

Since $w_H(\rho) \geq w_c^t(\rho) \geq w_r^t(\rho) \geq w_n^t(\rho)$, it is immediate that 4)⇒3) ⇒2)⇒1).

We prove 1)⇒5) by contradiction. Assume a code has $d_{\min,t} \leq c$. We will find an erasure pattern ρ with $w_H(\rho) \leq c$ that cannot be corrected. Since $d_{\min,t} \leq c$, there exists an error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq c$ such that $\mathbf{x}_1\mathbf{F}_{s,t} = \mathbf{x}_2\mathbf{F}_{s,t} + \mathbf{z}\mathbf{F}_t$, where $\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{C}$. Then we can construct $\mathbf{z}_1, \mathbf{z}_2 \in \rho_{\mathbf{z}}$ such that $\mathbf{z}_2 - \mathbf{z}_1 = \mathbf{z}$. If $\mathbf{y} = \mathbf{x}_1F_{s,u} + \mathbf{z}_1F_t = \mathbf{x}_2F_{s,u} + \mathbf{z}_2F_t$ is received, the equation (84) has two solutions. Thus we see that sink node t cannot correct the erasure pattern $\rho_{\mathbf{z}}$ with $w_H(\rho_{\mathbf{z}}) \leq c$. This completes the proof. ∎

5. CONCLUDING REMARKS

This paper is a thorough study of error correction and error detection in a general transmission system with network coding as a special case. Our characterization of the capability of a code for joint error correction and detection is in terms of the weight measure on the error vectors. Our work reveals the surprising fact that for a nonlinear network code, the number of correctable errors and the number of detectable errors are not related in a simple manner. In particular, for a nonlinear network code, the number of correctable errors can be more than half of the number of detectable errors, as illustrated by an example.

Together with the works by Yeung, Cai, and Zhang [7, 8, 14], we have shown that classical algebraic coding theory can naturally be generalized to networks. Therefore, any question that may be raised in classical algebraic coding can be raised in the more general setting of network coding.

DOI: 10.1002/ett

ACKNOWLEDGEMENT

Shenghao Yang would like to thank Min Tan, Salis L. Fang, Chi Kin Ngai and Hui Cheng for the helpful discussions. The work of Raymond W. Yeung was partially supported by a grant from the Research Grant Committee of the Hong Kong Special Administrative Region, China (RGC Ref. No. CUHK 2/06C) and a grant from Qualcomm China. The work of Zhen Zhang was supported in part by the National Science Foundation under Grant CCR 0326628.

REFERENCES

1. Ahlswede R, Cai N, Li SYR, Yeung RW. Network information flow. *IEEE Trans. Inform. Theory* Jul 2000; **46**(4):1204–1216.
2. Li SYR, Yeung RW, Cai N. Linear network coding. *IEEE Trans. Inform. Theory* Feb 2003; **49**(2):371–381.
3. Koetter R, Medard M. An algebraic approach to network coding. *IEEE/ACM Trans. Networking* Oct 2003; **11**(5):782–795.
4. Jaggi S, Sandrs P, Chou PA, Effros M, Egner S, Jain K, Tolhuizen L. Polynomial time algorithms for multicast network code construction. *IEEE Trans. Inform. Theory* Jun 2005; **51**(6):1973 – 1982.
5. Ho T, Leong B, Medard M, Koetter R, Chang Y, Effros M. The benefits of coding over routing in a randomized setting. *Proc. IEEE ISIT'03*, 2003.
6. Cai N, Yeung RW. Network coding and error correction. *Proc. IEEE Information Theory Workshop 2002*, Bangalore, India, 2002.
7. Yeung RW, Cai N. Network error correction, part I: basic concepts and upper bounds. *Communications in Information and Systems* 2006; **6**(1):19 – 36.
8. Cai N, Yeung RW. Network error correction, part II: lower bounds. *Communications in Information and Systems* 2006; **6**(1):37 – 54.
9. Yeung RW, Li SYR, Cai N, Zhang Z. Network coding theory. *Foundation and Trends in Communications and Information Theory* 2005; **2**(4 and 5):241–381.
10. Ho T, Leong B, Koetter R, Medard M, Effros M, Karger DR. Byzantine modification detection in multicast networks using randomized network coding. *Proc. IEEE ISIT'04*, 2004.
11. Jaggi S, Langberg M, Ho T, Effros M. Correction of adversarial errors in networks. *Proc. IEEE ISIT'05*, 2005.
12. Jaggi S, Langberg M, Katti S, Ho T, Katabi D, Medard M. Resilient network coding in the presence of byzantine adversaries. *INFOCOM'07*, 2007.
13. Jaggi S, Langberg M. Resilient network codes in the presence of eavesdropping byzantine adversaries. *Proc. IEEE ISIT'07*, 2007.
14. Zhang Z. Network error correction coding in packetized networks. *Proc. IEEE Information Theory Workshop 2006*, Chengdu, China, 2006.
15. Zhang Z. Linear network error correction codes in packet networks. *IEEE Trans. Inform. Theory* Jan 2008; **54**(1):209 – 218.
16. Yang S, Yeung RW. Characterizations of network error correction/detection and erasure correction. *Proc. Netcod Workshop 2007*, USA, 2007.
17. Koetter R, Kschischang FR. Coding for errors and erasures in random network coding Mar 2007. Submitted to *IEEE Trans. Inform. Theory*.
18. Yang S. Network coding and error correction. PhD Thesis, The Chinese University of Hong Kong 2008.

AUTHORS' BIOGRAPHIES

Shenghao Yang received the B.S. degree in Electronics Science from Nankai University, Tianjin, China, in 2001 and the M.S degree in Electronics Engineering from Peking University, Beijing, China, in 2004. From 2004 to 2005, he has held internship positions in Hitachi Research Center and Thomson Corporate Research Center, both at Beijing, China. Currently, he is a Ph.D. student at the Chinese University of Hong Kong, N.T., Hong Kong. His research interests are in the fields of information theory and network communications, as well as related combintorial problems.

Raymond W. Yeung was born in Hong Kong on June 3, 1962. He received the B.S., M.Eng., and Ph.D. degrees in electrical engineering from Cornell University, Ithaca, NY, in 1984, 1985, and 1988, respectively.

He was on leave at Ecole Nationale Supérieure des Télécommunications, Paris, France, during fall 1986. He was a Member of Technical Staff of AT&T Bell Laboratories from 1988 to 1991. Since 1991, he has been with the Department of Information Engineering, The Chinese University of Hong Kong, where he is now a chair professor. He is the author of the textbook *A First Course in Information Theory* (Kluwer Academic/Plenum, 2002). He has held visiting positions at Cornell University, Nankai University, the University of Bielefeld, the University of Copenhagen, Tokyo Institute of Technology, and Munich University of Technology. His research interests include information theory and network coding. He has been a Consultant in a project of Jet Propulsion Laboratory, Pasadena, CA, for salvaging the malfunctioning Galileo Spacecraft and a Consultant for NEC, USA.

Dr. Yeung was a member of the Board of Governors of the IEEE Information Theory Society from 1999 to 2001. He has served on the committees of a number of information theory symposiums and workshops. He was General Chair of the First and the Fourth Workshop on Network, Coding, and Applications (NetCod 2005 and 2008), a Technical Co-Chair for the 2006 IEEE International Symposium on Information Theory, and a Technical Co-Chair for the 2006 IEEE Information Theory Workshop, Chengdu, China. He currently serves as an Editor-at-Large of *Communications in Information and Systems*, an Editor of *Foundation and Trends in Communications and Information Theory* and of *Foundation and Trends in Networking*, and was an Associate Editor for Shannon Theory of *IEEE Transactions on Information Theory* from 2003 to 2005. He was a recipient of the Croucher Foundation Senior Research Fellowship for 2000/2001, the Best Paper Award (Communication Theory) of the 2004 International Conference on Communications, Circuits and System (with C. K. Ngai), the 2005 IEEE Information Theory Society Paper Award (for his paper "Linear network coding" co-authored with S.-Y. R. Li and N. Cai), and the Friedrich Wilhelm Bessel Research Award of the Alexander von Humboldt Foundation in 2007. He is a Fellow of the IEEE and the Hong Kong Institution of Engineers.

Zhen Zhang received his M.S. degree in mathematics from Nankai University, Tianjin, in 1980, his Ph.D. degree in applied mathematics from Cornell University, Ithaca, NY, in 1984, and Habilitation in mathematics from Bielefeld University, Bielefeld, Germany, in 1988.

He served as a lecturer, Department of Mathematics, Nankai University, from 1981 to 1982. He was a post-doctoral research associate with the School of Electrical Engineering, Cornell University, from 1984 to 1985 and with Information Systems Laboratory, Stanford University, in the Fall of 1985. From 1986 to 1988, he was with Mathematics Department, Bielefeld University, Bielefeld, Germany. He joined the faculty of University of Southern California in 1988, where he is currently a Professor of Electrical Engineering, Department of Electrical Engineering-systems. Dr. Zhang is a fellow of IEEE. His research interests include information theory, coding theory, data compression, network theory and applied mathematics.

DOI: 10.1002/ett