Chapter 2
Network Error Correction Model

In the last chapter, we introduced network coding, and particularly, described linear network coding. From this chapter, we begin to discuss network error correction coding specifically. To be similar, let a communication network be represented by a finite acyclic directed graph with unit capacity channels. The network is used for single source multicast: there is a single source node, which produces messages, and multiple sink nodes, all of which demand the messages. All the remaining nodes are internal nodes. In this chapter, we will give the basic model of network error correction.

2.1 Basic Model

For the case that there is an error on a channel e, the channel model is additive, i.e., the output of the channel e is $\tilde{U}_e = U_e + z_e$, where $U_e \in \mathscr{F}$ is the message that should be transmitted on e and $z_e \in \mathscr{F}$ is the error occurred on e. Further, let error vector be an $|E|$-dimensional row vector $\mathbf{z} = [z_e : e \in E]$ over the field $\mathscr{F}$ with each component z_e representing the error occurred on the corresponding channel e.

Recall some notation in linear network coding, which will be used frequently during our discussion on network error correction coding. The system transfer matrix (also called one-step transfer matrix) $K = (k_{d,e})_{d\in E, e\in E}$ is an $|E| \times |E|$ matrix with $k_{d,e}$ being the local encoding coefficient for $head(d) = tail(e)$ and $k_{d,e} = 0$ for $head(d) \neq tail(e)$. As the transfer from all channels are accumulated, the overall transform matrix is $F = I + K + K^2 + K^3 + \cdots$. And further because the network is finite and acyclic, $K^N = 0$ for some positive integer N. Thus we can write

$$F = I + K + K^2 + K^3 + \cdots = (I - K)^{-1}.$$

X. Guang and Z. Zhang, *Linear Network Error Correction Coding*, SpringerBriefs in Computer Science, DOI 10.1007/978-1-4939-0588-1_2, © The Author(s) 2014

In addition, recall the $\omega \times |E|$ matrix $B = (k_{d,e})_{d\in In(s),e\in E}$ where $k_{d,e} = 0$ for $e \notin Out(s)$ and $k_{d,e}$ is the local encoding coefficient for $e \in Out(s)$. Let $\rho \subseteq E$ represent a set of channels, and for ρ, define a $|\rho| \times |E|$ matrix $A_\rho = (A_{d,e})_{d\in\rho,e\in E}$ satisfying:

$$A_{d,e} = \begin{cases} 1 & d = e; \\ 0 & \text{otherwise.} \end{cases} \tag{2.1}$$

This matrix for different ρ will be used frequently throughout the whole book. Moreover, we say that ρ is an *error pattern* if errors may occur on those channels in it.

Therefore, when a source message vector $\mathbf{x} \in \mathscr{F}^\omega$ is transmitted and an error vector $\mathbf{z} \in \mathscr{F}^{|E|}$ occurs, the received vector $\mathbf{y} \in \mathscr{F}^{|In(t)|}$ at the sink node t is

$$\mathbf{y} = \mathbf{x} \cdot B \cdot F \cdot A^\top_{In(t)} + \mathbf{z} \cdot F \cdot A^\top_{In(t)}. \tag{2.2}$$

Note that the decoding matrix $F_t = \begin{bmatrix} f_e : & e \in In(t) \end{bmatrix} = BFA^\top_{In(t)}$ and further let $G_t \triangleq FA^\top_{In(t)}$. Then the above Eq. (2.2) can be rewritten as

$$\mathbf{y} = \mathbf{x} \cdot F_t + \mathbf{z} \cdot G_t = \begin{pmatrix} \mathbf{x} \; \mathbf{z} \end{pmatrix} \begin{bmatrix} F_t \\ G_t \end{bmatrix} \triangleq \begin{pmatrix} \mathbf{x} \; \mathbf{z} \end{pmatrix} \tilde{F}_t.$$

Further, let $\mathscr{X}$ be the source message set and $\mathscr{Z}$ be the error vector set. Clearly,

$$\mathscr{X} = \mathscr{F}^\omega \text{ and } \mathscr{Z} = \mathscr{F}^{|E|}.$$

For any sink node $t \in T$, let $\mathscr{Y}_t$ be the received message set with respect to t, that is,

$$\mathscr{Y}_t = \left\{ (\mathbf{x}\; \mathbf{z})\tilde{F}_t : \; \text{all } \mathbf{x} \in \mathscr{X}, \; \mathbf{z} \in \mathscr{Z} \right\}.$$

Furthermore, note that $A_{In(t)}G_t = I_{|In(t)|}$, an $|In(t)| \times |In(t)|$ identity matrix. Hence, for any $\mathbf{y} \in \mathscr{F}^{|In(t)|}$, we at least can choose an error vector $\mathbf{z} \in \mathscr{Z}$ satisfying $\mathbf{z}_{In(t)} = \mathbf{y}$ and $z_e = 0$ for all $e \in E \setminus In(t)$, where $\mathbf{z}_{In(t)}$ only consists of the components corresponding to the channels in $In(t)$, i.e., $\mathbf{z}_{In(t)} = [z_e : \; e \in In(t)]$, such that

$$\begin{pmatrix} \mathbf{0} \; \mathbf{z} \end{pmatrix} \cdot \tilde{F}_t = \mathbf{0}F_t + \mathbf{z}G_t = \mathbf{z}G_t = \mathbf{z}_{In(t)} \cdot A_{In(t)} \cdot G_t = \mathbf{z}_{In(t)} = \mathbf{y}.$$

This shows

$$\begin{aligned} \mathscr{Y}_t &= \left\{ (\mathbf{x}\; \mathbf{z})\tilde{F}_t : \; \text{all } \mathbf{x} \in \mathscr{X}, \; \mathbf{z} \in \mathscr{Z} \right\} \\ &= \{ \mathbf{x}F_t + \mathbf{z}G_t : \; \text{all } \mathbf{x} \in \mathscr{X}, \; \mathbf{z} \in \mathscr{Z} \} \\ &= \mathscr{F}^{|In(t)|}. \end{aligned}$$

Consequently, for each sink node $t \in T$, we define an encoding function $\mathrm{En}^{(t)}$ as follows:

$$\begin{aligned} \mathrm{En}^{(t)} : \; \mathscr{X} = \mathscr{F}^\omega &\mapsto \mathscr{Y}_t = \mathscr{F}^{|In(t)|} \\ \mathbf{x} &\mapsto \mathbf{x} \cdot F_t. \end{aligned}$$

Definition 2.1. A linear network code is called a regular code, if for any sink node $t \in T$, $\mathrm{Rank}(F_t) = \omega$.

If the considered linear network code is regular, i.e., $\mathrm{Rank}(F_t) = \omega$, $\mathrm{En}^{(t)}$ is an injection, and hence $\mathrm{En}^{(t)}$ is well-defined. Otherwise, if the linear network code is not regular, i.e., $\mathrm{Rank}(F_t) < \omega$ for at least one sink node $t \in T$, then even in the error-free case, the code is not decodable at least one sink node $t \in T$, let alone network error correction. Therefore, we assume that codes considered below are regular. Now, we can define a linear network error correction (LNEC) code as

$$\mathrm{En}^{(t)}(\mathscr{X}) \triangleq \{\mathrm{En}^{(t)}(\mathbf{x}) : \ \mathbf{x} \in \mathscr{X}\}.$$

To be specific, for any message vector $\mathbf{x} \in \mathscr{F}^{\omega}$, $\mathbf{x}F_t$ is called a *codeword* for the sink node t, and let

$$\mathscr{C}_t \triangleq \{\mathbf{x}F_t : \ \text{all } \mathbf{x} \in \mathscr{F}^{\omega}\},$$

which is the set of all codewords for the sink node $t \in T$, say *codebook* for t.

2.2 Distance and Weight

Similar to the classical coding theory, we can also define the distance between two received vectors at each sink node $t \in T$ in order to characterize their discrepancy.

Definition 2.2. For any two received vectors $\mathbf{y}_1, \mathbf{y}_2 \in \mathscr{F}^{|In(t)|}$ at the sink node $t \in T$, the *distance* between $\mathbf{y}_1$ and $\mathbf{y}_2$ with respect to t is defined as:

$$d^{(t)}(\mathbf{y}_1,\ \mathbf{y}_2) \triangleq \min\{w_H(\mathbf{z}) : \ \mathbf{z} \in \mathscr{F}^{|E|} \text{ such that } \mathbf{y}_1 = \mathbf{y}_2 + \mathbf{z}G_t\},$$

where $w_H(\mathbf{z})$ represents the Hamming weight of the error vector $\mathbf{z}$, i.e., the number of nonzero components of $\mathbf{z}$.

In particular, for any two codewords $\mathbf{x}_1F_t,\ \mathbf{x}_2F_t \in \mathscr{C}_t$ (or equivalently, any two message vectors $\mathbf{x}_1, \mathbf{x}_2 \in \mathscr{X}$), the distance between $\mathbf{x}_1F_t$ and $\mathbf{x}_2F_t$ at the sink node $t \in T$ is:

$$\begin{aligned} d^{(t)}(\mathbf{x}_1F_t,\ \mathbf{x}_2F_t) &= \min\{w_H(\mathbf{z}) : \ \mathbf{z} \in \mathscr{F}^{|E|} \text{ such that } \mathbf{x}_1F_t = \mathbf{x}_2F_t + \mathbf{z}G_t\} \\ &= \min\{w_H(\mathbf{z}) : \ \mathbf{z} \in \mathscr{F}^{|E|} \text{ such that } (\mathbf{x}_1 - \mathbf{x}_2)F_t = \mathbf{z}G_t\}. \end{aligned}$$

First, we show that this distance has the following property.

Proposition 2.1. *For any two received vectors $\mathbf{y}_1, \mathbf{y}_2 \in \mathscr{F}^{|In(t)|}$ at the sink node $t \in T$,*

$$0 \le d^{(t)}(\mathbf{y}_1,\ \mathbf{y}_2) \le |In(t)|.$$

Proof. We know

$$\begin{aligned} d^{(t)}(\mathbf{y}_1,\ \mathbf{y}_2) &= \min\{w_H(\mathbf{z}):\ \mathbf{z}\in\mathscr{F}^{|E|} \text{ such that } \mathbf{y}_1=\mathbf{y}_2+\mathbf{z}G_t\} \\ &= \min\{w_H(\mathbf{z}):\ \mathbf{z}\in\mathscr{F}^{|E|} \text{ such that } \mathbf{y}_1-\mathbf{y}_2=\mathbf{z}G_t\}, \end{aligned}$$

and recall that $A_{In(t)}G_t = I_{|In(t)|}$ is an $|In(t)|\times|In(t)|$ identity matrix. Furthermore, let $\mathbf{z}\in\mathscr{F}^{|E|}$ be an error vector satisfying $\mathbf{z}_{In(t)}=\mathbf{y}_1-\mathbf{y}_2$ and $z_e=0$ for all $e\in E\setminus In(t)$. It follows that

$$\mathbf{z}\cdot G_t = \mathbf{z}_{In(t)}\cdot A_{In(t)}G_t = \mathbf{z}_{In(t)} = \mathbf{y}_1-\mathbf{y}_2,$$

which implies

$$d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)\le w_H(\mathbf{z}) = w_H(\mathbf{y}_1-\mathbf{y}_2)\le |In(t)|.$$

On the other hand, it is evident that $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)\ge 0$ from $w_H(\mathbf{z})\ge 0$ for any $\mathbf{z}\in\mathscr{F}^{|E|}$. Combining the above, the proof is completed. □

Further, the following result shows that this distance is an actual metric.

Theorem 2.1. *This distance $d^{(t)}(\cdot,\cdot)$ defined in vector space $\mathscr{F}^{|In(t)|}$ is a metric, that is, the following three properties are qualified. For any $\mathbf{y}_1,\mathbf{y}_2,\mathbf{y}_3$ in $\mathscr{F}^{|In(t)|}$,*

1. **(Positive definiteness)** $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)\ge 0$, *and* $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=0$ *if and only if* $\mathbf{y}_1=\mathbf{y}_2$.
2. **(Symmetry)** $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=d^{(t)}(\mathbf{y}_2,\mathbf{y}_1)$.
3. **(Triangle inequality)** $d^{(t)}(\mathbf{y}_1,\mathbf{y}_3)\le d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)+d^{(t)}(\mathbf{y}_2,\mathbf{y}_3)$.

Thus, the pair $(\mathscr{F}^{|In(t)|},d^{(t)})$ is a metric space.

Proof. 1. It is evident that $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)\ge 0$ for any $\mathbf{y}_1,\mathbf{y}_2\in\mathscr{F}^{|In(t)|}$ because the Hamming weight is always nonnegative. Below we will show that $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=0$ if and only if $\mathbf{y}_1=\mathbf{y}_2$. First, it is easily seen that $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=0$ if $\mathbf{y}_1=\mathbf{y}_2$. On the other hand, assume that

$$0=d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=\min\{w_H(\mathbf{z}):\ \mathbf{z}\in\mathscr{F}^{|E|} \text{ such that } \mathbf{y}_1=\mathbf{y}_2+\mathbf{z}G_t\},$$

which means that there exists an error vector $\mathbf{z}\in\mathscr{Z}$ with $w_H(\mathbf{z})=0$ such that $\mathbf{y}_1=\mathbf{y}_2+\mathbf{z}G_t$. Subsequently, $w_H(\mathbf{z})=0$ only if $\mathbf{z}=\mathbf{0}$. Thus, $\mathbf{y}_1=\mathbf{y}_2$.

2. Assume that $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=d_1$, that is, there exists an error vector $\mathbf{z}\in\mathscr{F}^{|E|}$ with $w_H(\mathbf{z})=d_1$ such that $\mathbf{y}_1=\mathbf{y}_2+\mathbf{z}G_t$, which is equal to $\mathbf{y}_2=\mathbf{y}_1-\mathbf{z}G_t$. Together with the definition of the distance, this implies that

$$d^{(t)}(\mathbf{y}_2,\mathbf{y}_1)\le w_H(\mathbf{z})=d_1=d^{(t)}(\mathbf{y}_1,\mathbf{y}_2).$$

Similarly, we can also obtain

$$d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)\le d^{(t)}(\mathbf{y}_2,\mathbf{y}_1).$$

Therefore, it follows $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2)=d^{(t)}(\mathbf{y}_2,\mathbf{y}_1)$.

3. Let $d^{(t)}(\mathbf{y}_1,\mathbf{y}_2) = d_{1,2}$, $d^{(t)}(\mathbf{y}_2,\mathbf{y}_3) = d_{2,3}$, and $d^{(t)}(\mathbf{y}_1,\mathbf{y}_3) = d_{1,3}$. Correspondingly, there exist three error vectors $\mathbf{z}_{1,2},\mathbf{z}_{2,3},\mathbf{z}_{1,3} \in \mathscr{F}^{|E|}$ with Hamming weight $w_H(\mathbf{z}_{1,2}) = d_{1,2}$, $w_H(\mathbf{z}_{2,3}) = d_{2,3}$, and $w_H(\mathbf{z}_{1,2}) = d_{1,3}$ such that

$$\mathbf{y}_1 = \mathbf{y}_2 + \mathbf{z}_{1,2}G_t, \tag{2.3}$$
$$\mathbf{y}_2 = \mathbf{y}_3 + \mathbf{z}_{2,3}G_t, \tag{2.4}$$
$$\mathbf{y}_1 = \mathbf{y}_3 + \mathbf{z}_{1,3}G_t. \tag{2.5}$$

Combining the equalities (2.3) and (2.4), we have

$$\mathbf{y}_1 = \mathbf{y}_3 + (\mathbf{z}_{1,2} + \mathbf{z}_{2,3})G_t.$$

So it is shown that

$$\begin{aligned} d_{1,3} =& d^{(t)}(\mathbf{y}_1,\mathbf{y}_3) \\ =& w_H(\mathbf{z}_{1,3}) \\ \leq& w_H(\mathbf{z}_{1,2} + \mathbf{z}_{1,3}) \\ \leq& w_H(\mathbf{z}_{1,2}) + w_H(\mathbf{z}_{1,3}) \\ =& d_{1,2} + d_{2,3}. \end{aligned}$$

Combining the above (1), (2), and (3), the theorem is proved. □

Subsequently, we can define the minimum distance of a linear network error correction code at the sink node $t \in T$.

Definition 2.3. The minimum distance of a linear network error correction code at the sink node $t \in T$ is defined as:

$$\begin{aligned} d^{(t)}_{\min} &= \min\{d^{(t)}(\mathbf{x}_1F_t,\mathbf{x}_2F_t) : \text{ all distinct } \mathbf{x}_1,\mathbf{x}_2 \in \mathscr{F}^{\omega}\} \\ &= \min_{\substack{\mathbf{x}_1,\mathbf{x}_2 \in \mathscr{F}^{\omega} \\ \mathbf{x}_1 \neq \mathbf{x}_2}} d^{(t)}(\mathbf{x}_1F_t,\mathbf{x}_2F_t). \end{aligned}$$

Intuitively, the weight of an error vector should be a measure of seriousness of the error. So weight measure of an error vector should satisfy the following the conditions at least:

1. The weight measure $w(\cdot)$ for any error vector should be nonnegative, that is, it is a mapping:
$$w: \mathscr{Z} \to \mathbb{Z}^+ \cup \{0\},$$
where $\mathbb{Z}^+$ is the set of all positive integers.
2. For each message vector $\mathbf{x} \in \mathscr{X}$, when $\mathbf{x}$ is transmitted and two distinct error vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ happened respectively, if the two outputs are always the same, these two error vectors should have the same weight.

Actually, it is easy to see that the Hamming weight used in classical coding theory satisfies the two mentioned conditions. Further, recall that in the classical error-correcting coding theory, the Hamming weight can be induced by the Hamming distance, that is, for any $\mathbf{z} \in \mathscr{Z}$, $w_H(\mathbf{z}) = d_H(\mathbf{0}, \mathbf{z})$, where $d_H(\cdot,\cdot)$ represents the Hamming distance. Motivated by this idea, for linear network error correction codes, the distance defined as above should also induce a weight measure for error vectors with respect to each sink node $t \in T$. We state it below.

Definition 2.4. For any error vector $\mathbf{z}$ in $\mathscr{F}^{|E|}$, the weight measure of $\mathbf{z}$ induced by the distance $d^{(t)}(\cdot,\cdot)$ with respect to the sink $t \in T$ is defined as:

$$\begin{aligned} w^{(t)}(\mathbf{z}) &= d^{(t)}(\mathbf{0}, \mathbf{z}G_t) \\ &= \min\{w_H(\mathbf{z}') : \text{ all error vectors } \mathbf{z}' \in \mathscr{F}^{|E|} \text{ such that } \mathbf{0} = \mathbf{z}G_t + \mathbf{z}'G_t\} \\ &= \min\{w_H(\mathbf{z}') : \text{ all error vectors } \mathbf{z}' \in \mathscr{F}^{|E|} \text{ such that } \mathbf{z}G_t = \mathbf{z}'G_t\}, \end{aligned}$$

which is called *network Hamming weight* of the error vector $\mathbf{z}$ with respect to the sink node t.

Now, we will show that this weight of errors satisfies two conditions on weight measure as stated above. First, it is easily to be seen that $w^{(t)}(\mathbf{z})$ is nonnegative for any error vector $\mathbf{z} \in \mathscr{F}^{|E|}$. On the other hand, assume that $\mathbf{z}_1$ and $\mathbf{z}_2$ are arbitrary two error vectors in $\mathscr{F}^{|E|}$ satisfying that, for any message vector $\mathbf{x} \in \mathscr{X}$,

$$\mathbf{x}F_t + \mathbf{z}_1 G_t = \mathbf{x}F_t + \mathbf{z}_2 G_t,$$

or equivalently,

$$\mathbf{z}_1 G_t = \mathbf{z}_2 G_t.$$

Together with the definition:

$$w^{(t)}(\mathbf{z}_i) = \min\{w_H(\mathbf{z}') : \text{ all error vectors } \mathbf{z}' \in \mathscr{F}^{|E|} \text{ such that } \mathbf{z}_i G_t = \mathbf{z}'G_t\},\ i = 1,2,$$

it follows $w^{(t)}(\mathbf{z}_1) = w^{(t)}(\mathbf{z}_2)$.

Further, if any two error vectors $\mathbf{z}_1, \mathbf{z}_2 \in \mathscr{F}^{|E|}$ satisfy $\mathbf{z}_1 G_t = \mathbf{z}_2 G_t$, we denote this by $\mathbf{z}_1 \overset{w^{(t)}}{\sim} \mathbf{z}_2$, and then we can obtain the following result easily.

Proposition 2.2. *The relationship "$\overset{w^{(t)}}{\sim}$" is an equivalent relation, that is, for any three error vectors $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3 \in \mathscr{F}^{|E|}$, it has the following three properties:*

1. $\mathbf{z}_1 \overset{w^{(t)}}{\sim} \mathbf{z}_1$;
2. *if* $\mathbf{z}_1 \overset{w^{(t)}}{\sim} \mathbf{z}_2$, *then* $\mathbf{z}_2 \overset{w^{(t)}}{\sim} \mathbf{z}_1$;
3. *if* $\mathbf{z}_1 \overset{w^{(t)}}{\sim} \mathbf{z}_2$, $\mathbf{z}_2 \overset{w^{(t)}}{\sim} \mathbf{z}_3$, *then* $\mathbf{z}_1 \overset{w^{(t)}}{\sim} \mathbf{z}_3$.

In addition, the weight $w^{(t)}(\cdot)$ of error vectors at the sink node $t \in T$ also induces a weight measure for received vectors in vector space $\mathscr{Y}_t = \mathscr{F}^{|In(t)|}$ denoted by $W^{(t)}(\cdot)$. To be specific, let $\mathbf{y} \in \mathscr{Y}_t$ be a received vector at the sink node t, for any error vector $\mathbf{z} \in \mathscr{Z}$ such that $\mathbf{y} = \mathbf{z}G_t$, define:

$$W^{(t)}(\mathbf{y}) = w^{(t)}(\mathbf{z}).$$

It is easily seen that $W^{(t)}(\cdot)$ is a mapping from the received message space $\mathscr{Y}_t = \mathscr{F}^{|In(t)|}$ to $\mathbb{Z}^+ \cup \{0\}$. Further, $W^{(t)}(\cdot)$ is well-defined, because the values $w^{(t)}(\mathbf{z})$ for all $\mathbf{z} \in \mathscr{Z}$ satisfying $\mathbf{z}G_t = \mathbf{y}$ are the same from the definition of the weight of errors, and, for any $\mathbf{y} \in \mathscr{Y}_t$, there always exists an error vector $\mathbf{z} \in \mathscr{Z}$ such that $\mathbf{y} = \mathbf{z}G_t$ as G_t is full-rank, i.e., $\mathrm{Rank}(G_t) = |In(t)|$. In other words, for any $\mathbf{y} \in \mathscr{Y}_t$,

$$W^{(t)}(\mathbf{y}) = \min\{w_H(\mathbf{z}) :\ \mathbf{z} \in \mathscr{Z} \text{ such that } \mathbf{y} = \mathbf{z}G_t\}.$$

In particular, $W^{(t)}(\mathbf{z}G_t) = w^{(t)}(\mathbf{z})$ for any $\mathbf{z} \in \mathscr{Z}$. Then, for any two received vectors $\mathbf{y}_1, \mathbf{y}_2 \in \mathscr{Y}_t$,

$$\begin{aligned} d^{(t)}(\mathbf{y}_1, \mathbf{y}_2) &= \min\{w_H(\mathbf{z}) :\ \mathbf{z} \in \mathscr{Z} \text{ such that } \mathbf{y}_1 = \mathbf{y}_2 + \mathbf{z}G_t\} \\ &= \min\{w_H(\mathbf{z}) :\ \mathbf{z} \in \mathscr{Z} \text{ such that } \mathbf{y}_1 - \mathbf{y}_2 = \mathbf{z}G_t\} \\ &= W^{(t)}(\mathbf{z}G_t) \\ &= W^{(t)}(\mathbf{y}_1 - \mathbf{y}_2). \end{aligned} \tag{2.6}$$

Particularly, for any two codewords $\mathbf{x}_1 F_t$ and $\mathbf{x}_2 F_t$ at the sink node $t \in T$, we deduce

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) = W^{(t)}(\mathbf{x}_1 F_t - \mathbf{x}_2 F_t) = W^{(t)}((\mathbf{x}_1 - \mathbf{x}_2)F_t),$$

which further implies that

$$\begin{aligned} d^{(t)}_{\min} &= \min\{d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) :\ \mathbf{x}_1, \mathbf{x}_2 \in \mathscr{X} = \mathscr{F}^{\omega} \text{ with } \mathbf{x}_1 \neq \mathbf{x}_2\} \\ &= \min\{W^{(t)}((\mathbf{x}_1 - \mathbf{x}_2)F_t) :\ \mathbf{x}_1, \mathbf{x}_2 \in \mathscr{X} = \mathscr{F}^{\omega} \text{ with } \mathbf{x}_1 \neq \mathbf{x}_2\} \\ &= \min\{W^{(t)}(\mathbf{x}F_t) :\ \mathbf{0} \neq \mathbf{x} \in \mathscr{X} = \mathscr{F}^{\omega}\} \\ &= \min_{\mathbf{x} \in \mathscr{F}^{\omega} \setminus \{\mathbf{0}\}} W^{(t)}(\mathbf{x}F_t) \qquad (2.7) \\ &= \min_{c \in \mathscr{C}_t \setminus \{\mathbf{0}\}} W^{(t)}(c) \triangleq W^{(t)}(\mathscr{C}_t). \qquad (2.8) \end{aligned}$$

We say $W^{(t)}(\mathscr{C}_t)$ the weight of the codebook $\mathscr{C}_t$ with respect to the sink node $t \in T$, which is defined as the minimum weight of all nonzero codewords in $\mathscr{C}_t$.

2.3 Error Correction and Detection Capabilities

In the last section, we have established network error correction model over linear network coding. In this section, we will discuss the error correction and detection capabilities.

Similar to the minimum distance decoding principle for classical error-correcting codes, we can also apply the minimum distance decoding principle to linear network error correction codes at each sink node.

Definition 2.5 (Minimum Distance Decoding Principle). When a vector $\mathbf{y} \in \mathscr{Y}_t$ is received at a sink node $t \in T$, choose a codeword $c \in \mathscr{C}_t$ (or equivalently, $\mathbf{x}F_t \in \mathscr{C}_t$) that is closest to the received vector $\mathbf{y}$. To be specific, choose a codeword $c \in \mathscr{C}_t$ (or equivalently, $\mathbf{x}F_t \in \mathscr{C}_t$) such that

$$\begin{aligned} d^{(t)}(\mathbf{y}, c) &= \min_{c' \in \mathscr{C}_t} d^{(t)}(\mathbf{y}, c') \\ &= \min_{\mathbf{x} \in \mathscr{F}^{\omega}} d^{(t)}(\mathbf{y}, \mathbf{x}F_t). \end{aligned}$$

And refer to this as the *minimum distance decoding principle* at the sink node $t \in T$.

Definition 2.6 (d-Error-Detecting). Let d be a positive integer. A linear network error correction code is d-error-detecting at the sink node $t \in T$, if, whichever error vector $\mathbf{z} \in \mathscr{Z}$ with weight $w^{(t)}(\mathbf{z})$ no more than d but at least one happens, when any source message vector in $\mathscr{X}$ is transmitted by this linear network error correction code, the received vector at the sink node t is not a codeword. A linear network error correction code is exactly d-error-detecting at the sink node $t \in T$, if it is d-error-detecting but not $(d+1)$-error-detecting at t.

Definition 2.7 (d-Error-Correcting). Let d be a positive integer. A linear network error correction code is d-error-correcting at the sink node $t \in T$, if the minimum distance decoding principle at the sink node t is able to correct any error vector in $\mathscr{Z}$ with weight no more than d, assuming that the incomplete decoding[1] rule is used. A linear network error correction code is exactly d-error-correcting at the sink node t if it is d-error-correcting but not $(d+1)$-error-correcting at t.

In the following two theorems, it is shown that, similar to classical coding theory, the error detection and error correction capabilities of linear network error correction codes at each sink node are characterized by its corresponding minimum distance.

Theorem 2.2. *A linear network error correction code is exactly d-error-detecting at sink node t, if and only if $d^{(t)}_{\min} = d+1$.*

Proof. First, assume that $d^{(t)}_{\min} = d+1$. Then we claim that this linear network error correction code is d-error-detecting at the sink node t, that is, for any message vector $\mathbf{x}_1 \in \mathscr{F}^{\omega}$ and any error vector $\mathbf{z} \in \mathscr{F}^{|E|}$ with $1 \le w^{(t)}(\mathbf{z}) \le d$,

$$\mathbf{x}_1 F_t + \mathbf{z} G_t \notin \mathscr{C}_t = \{\mathbf{x}F_t : \ \text{all } \mathbf{x} \in \mathscr{F}^{\omega}\}.$$

On the contrary, suppose that there exists some message vector $\mathbf{x}_1 \in \mathscr{F}^{\omega}$ and some error vector $\mathbf{z} \in \mathscr{F}^{|E|}$ with $1 \le w^{(t)}(\mathbf{z}) \le d$ such that

$$\mathbf{x}_1 F_t + \mathbf{z} G_t \in \mathscr{C}_t,$$

[1] Incomplete decoding refers to the case that if a word is received, find the closest codeword. If there are more than one such codewords, request a retransmission. The counterpart is complete decoding which means that if there are more than one such codewords, select one of them arbitrarily.

which means that there exists another message vector $\mathbf{x}_2 \in \mathscr{F}^{\omega}$ such that

$$\mathbf{x}_1 F_t + \mathbf{z} G_t = \mathbf{x}_2 F_t.$$

Together with the equality (2.6), this implies that

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) = W^{(t)}(\mathbf{x}_1 F_t - \mathbf{x}_2 F_t) = W^{(t)}(\mathbf{z} G_t) = w^{(t)}(\mathbf{z}) \leq d,$$

which contradicts to $d_{\min}^{(t)} = d+1 > d$.

In the following, we will show that this linear network error correction code is not $(d+1)$-error-detecting at t. Since $d_{\min}^{(t)} = d+1$, then there exist two codewords $\mathbf{x}_1 F_t$ and $\mathbf{x}_2 F_t$ satisfying

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) = d+1.$$

That is, there exists an error vector $\mathbf{z}$ with $w^{(t)}(\mathbf{z}) = d+1$ such that $\mathbf{x}_1 F_t = \mathbf{x}_2 F_t + \mathbf{z} G_t$, which indicates that this linear network error correction code is not $(d+1)$-error-detecting code at the sink node $t \in T$.

On the other hand, let this linear network error correction code be exactly d-error-detecting at the sink node $t \in T$. To be specific, it is d-error-detecting and not $(d+1)$-error-detecting at t. The d-error-detecting property shows $\mathbf{x} F_t + \mathbf{z} G_t \notin \mathscr{C}_t$ for any codeword $\mathbf{x} F_t \in \mathscr{C}_t$ and any error vector $\mathbf{z} \in \mathscr{Z}$ with $1 \leq w^{(t)}(\mathbf{z}) \leq d$. Thus, it follows $d_{\min}^{(t)} \geq d+1$.

Conversely, assume that $d_{\min}^{(t)} < d+1$. Notice that $d_{\min}^{(t)} = \min_{\mathbf{x} \in \mathscr{F}^{\omega} \setminus \{\mathbf{0}\}} W^{(t)}(\mathbf{x} F_t)$ from (2.7), which implies that there is a codeword $\mathbf{x}_1 F_t \in \mathscr{C}_t$ satisfying $W^{(t)}(\mathbf{x}_1 F_t) = d_{\min}^{(t)} < d+1$. Further, let $\mathbf{z} \in \mathscr{Z}$ be an error vector satisfying $\mathbf{x}_1 F_t = \mathbf{z} G_t$, and thus one has

$$1 \leq w^{(t)}(\mathbf{z}) = W^{(t)}(\mathbf{z} G_t) = W^{(t)}(\mathbf{x}_1 F_t) = d_{\min}^{(t)} < d+1.$$

Thus, for any codeword $\mathbf{x}_2 F_t \in \mathscr{C}_t$, we have

$$\mathbf{x}_2 F_t + \mathbf{z} G_t = \mathbf{x}_2 F_t + \mathbf{x}_1 F_t = (\mathbf{x}_1 + \mathbf{x}_2) F_t \in \mathscr{C}_t,$$

which, together with $1 \leq w^{(t)}(\mathbf{z}) \leq d$, violates the d-error-detecting property at the sink node t. In addition, this LNEC code is not $(d+1)$-error-detecting at the sink node t, that is, there exists a codeword $\mathbf{x} F_t \in \mathscr{C}_t$ and an error vector $\mathbf{z} \in \mathscr{F}^{|E|}$ with $w^{(t)}(\mathbf{z}) = d+1$ such that $\mathbf{x} F_t + \mathbf{z} G_t \in \mathscr{C}_t$. Let $\mathbf{x}_1 F_t = \mathbf{x} F_t + \mathbf{z} G_t$ for some $\mathbf{x}_1 \in \mathscr{F}^{\omega}$, and then

$$d_{\min}^{(t)} \leq d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x} F_t) = W^{(t)}(\mathbf{x}_1 F_t - \mathbf{x} F_t) = W^{(t)}(\mathbf{z} G_t) = w^{(t)}(\mathbf{z}) = d+1.$$

Combining the above, it is shown $d_{\min}^{(t)} = d+1$. This completes the proof. □

Theorem 2.3. *A linear network error correction code is exactly d-error-correcting at sink node t if and only if $d_{\min}^{(t)} = 2d+1$ or $d_{\min}^{(t)} = 2d+2$.*

Proof. First, we assume that a linear network error correction code is d-error-correcting at the sink node $t \in T$, which means that, for any codeword $\mathbf{x}F_t \in \mathscr{C}_t$ and any error vector $\mathbf{z} \in \mathscr{Z}$ with weight no more than d, it follows

$$d^{(t)}(\mathbf{x}F_t, \mathbf{x}F_t + \mathbf{z}G_t) < d^{(t)}(\mathbf{x}'F_t, \mathbf{x}F_t + \mathbf{z}G_t),$$

for any other codeword $\mathbf{x}'F_t \in \mathscr{C}_t$.

We will show that $d_{\min}^{(t)} > 2d$ below. Assume the contrary that $d_{\min}^{(t)} \leq 2d$, that is, there exist two distinct codewords $\mathbf{x}_1F_t, \mathbf{x}_2F_t \in \mathscr{C}_t$ satisfying

$$d^{(t)}(\mathbf{x}_1F_t, \mathbf{x}_2F_t) \leq 2d.$$

Subsequently, we can always choose an error vector $\mathbf{z} \in \mathscr{Z}$ such that $\mathbf{x}_1F_t - \mathbf{x}_2F_t = \mathbf{z}G_t$ from $A_{In(t)}G_t = I_{|In(t)|}$ where again $I_{|In(t)|}$ is an $|In(t)| \times |In(t)|$ identity matrix. Thus, one has

$$2d \geq d^{(t)}(\mathbf{x}_1F_t, \mathbf{x}_2F_t) = W^{(t)}(\mathbf{x}_1F_t - \mathbf{x}_2F_t) = W^{(t)}(\mathbf{z}G_t) = w^{(t)}(\mathbf{z}) \triangleq \hat{d}.$$

Note that $w^{(t)}(\mathbf{z}) = \min\{w_H(\mathbf{z}') : \text{ all } \mathbf{z}' \in \mathscr{Z} \text{ such that } \mathbf{z}G_t = \mathbf{z}'G_t\}$. Thus, without loss of generality, we assume that

$$w^{(t)}(\mathbf{z}) = w_H(\mathbf{z}).$$

Further, let $d_1 = \lceil \frac{\hat{d}-1}{2} \rceil$ and $d_2 = \lfloor \frac{\hat{d}+1}{2} \rfloor$. And it is not difficult to see that

$$d_1 \leq d_2 \leq d \text{ and } d_1 + d_2 = \hat{d}.$$

Thus, we can claim that, there exist two error vectors $\mathbf{z}_1, \mathbf{z}_2 \in \mathscr{Z}$ satisfying:

- $w_H(\mathbf{z}_1) = d_1$ and $w_H(\mathbf{z}_2) = d_2$, respectively;
- $\rho_{\mathbf{z}_1} \cap \rho_{\mathbf{z}_2} = \emptyset$ and $\rho_{\mathbf{z}_1} \cup \rho_{\mathbf{z}_2} = \rho_{\mathbf{z}}$;
- $\mathbf{z} = \mathbf{z}_1 + \mathbf{z}_2$;

where $\rho_{\mathbf{z}'}$ is called an error pattern induced by an error vector $\mathbf{z}' \in \mathscr{Z}$, defined as the set of the channels on which the corresponding coordinates of $\mathbf{z}'$ are nonzero. Below, we will indicate that

$$w_H(\mathbf{z}_i) = w^{(t)}(\mathbf{z}_i), \ i = 1, 2.$$

Clearly, we know $w^{(t)}(\mathbf{z}_1) \leq w_H(\mathbf{z}_1)$. Further, if $w^{(t)}(\mathbf{z}_1) < w_H(\mathbf{z}_1)$, there exists an error vector $\mathbf{z}_1' \in \mathscr{Z}$ satisfying $\mathbf{z}_1'G_t = \mathbf{z}_1G_t$ and

$$w_H(\mathbf{z}_1') = w^{(t)}(\mathbf{z}_1') = w^{(t)}(\mathbf{z}_1) < w_H(\mathbf{z}_1). \tag{2.9}$$

Thus, we have

$$(\mathbf{z}_1' + \mathbf{z}_2)G_t = \mathbf{z}_1'G_t + \mathbf{z}_2G_t = \mathbf{z}_1G_t + \mathbf{z}_2G_t = (\mathbf{z}_1 + \mathbf{z}_2)G_t = \mathbf{z}G_t,$$

which leads to

$$\begin{aligned} w_H(\mathbf{z}_1' + \mathbf{z}_2) &\le w_H(\mathbf{z}_1') + w_H(\mathbf{z}_2) \\ &< w_H(\mathbf{z}_1) + w_H(\mathbf{z}_2) \qquad (2.10) \\ &= w_H(\mathbf{z}_1 + \mathbf{z}_2) \qquad (2.11) \\ &= w_H(\mathbf{z}) \\ &= w^{(t)}(\mathbf{z}), \end{aligned}$$

where the inequality (2.10) follows from (2.9) and the equality (2.11) follows from $\rho_{\mathbf{z}_1} \cap \rho_{\mathbf{z}_2} = \emptyset$. This means that there exists an error vector $\mathbf{z}_1' + \mathbf{z}_2 \in \mathscr{Z}$ satisfying $(\mathbf{z}_1' + \mathbf{z}_2)G_t = \mathbf{z}G_t$ and $w_H(\mathbf{z}_1' + \mathbf{z}_2) < w^{(t)}(\mathbf{z})$, which evidently violates the fact that

$$w^{(t)}(\mathbf{z}) = \min\{w_H(\mathbf{z}') : \text{ all } \mathbf{z}' \in \mathscr{Z} \text{ such that } \mathbf{z}'G_t = \mathbf{z}G_t\}.$$

Therefore, one obtains $w_H(\mathbf{z}_1) = w^{(t)}(\mathbf{z}_1)$. Similarly, we can also deduce $w_H(\mathbf{z}_2) = w^{(t)}(\mathbf{z}_2)$.

Combining the above, we have

$$\mathbf{x}_1F_t - \mathbf{x}_2F_t = \mathbf{z}G_t = \mathbf{z}_1G_t + \mathbf{z}_2G_t,$$

subsequently,

$$\mathbf{x}_1F_t - \mathbf{z}_1G_t = \mathbf{x}_2F_t + \mathbf{z}_2G_t.$$

This implies that

$$\begin{aligned} d^{(t)}(\mathbf{x}_1F_t, \mathbf{x}_2F_t + \mathbf{z}_2G_t) &= d^{(t)}(\mathbf{x}_1F_t, \mathbf{x}_1F_t - \mathbf{z}_1G_t) \\ &= W^{(t)}(\mathbf{z}_1G_t) = w^{(t)}(\mathbf{z}_1) = w_H(\mathbf{z}_1) = d_1 \\ &\le d_2 = w_H(\mathbf{z}_2) = w^{(t)}(\mathbf{z}_2) = W^{(t)}(\mathbf{z}_2G_t) \\ &= d^{(t)}(\mathbf{x}_2F_t, \mathbf{x}_2F_t + \mathbf{z}_2G_t), \end{aligned}$$

which further implies that when the message vector $\mathbf{x}_2$ is transmitted and the error vector $\mathbf{z}_2$ happens, the minimum distance decoding principle can not decode $\mathbf{x}_2$ successfully at the sink node t. This is a contradiction to d-error-correcting property at the sink node $t \in T$. So the hypothesis is not true, which indicates $d_{\min}^{(t)} \ge 2d + 1$.

On the other hand, if this LNEC code is not $(d+1)$-error-correcting, then $d_{\min}^{(t)} \le 2d + 2$. Conversely, suppose that $d_{\min}^{(t)} \ge 2d + 3$. We know that the fact that this LNEC code is not $(d+1)$-error-correcting at the sink node $t \in T$ means that there exists a codeword $\mathbf{x}_1F_t \in \mathscr{C}_t$ and an error vector $\mathbf{z}_1 \in \mathscr{Z}$ with $w^{(t)}(\mathbf{z}_1) = d + 1$ such that when the message vector $\mathbf{x}_1$ is transmitted and the error vector $\mathbf{z}_1$ happens, the minimum distance decoding principle cannot decode $\mathbf{x}_1$ successfully at the sink node t. To be specific, there exists another message $\mathbf{x}_2 \in \mathscr{X}$ satisfying:

$$d^{(t)}(\mathbf{x}_2F_t, \mathbf{x}_1F_t + \mathbf{z}_1G_t) \le d^{(t)}(\mathbf{x}_1F_t, \mathbf{x}_1F_t + \mathbf{z}_1G_t),$$

that is, there exists an error vector $\mathbf{z}_2 \in \mathscr{Z}$ with $w^{(t)}(\mathbf{z}_2) \le d+1$ satisfying

$$\mathbf{x}_2 F_t + \mathbf{z}_2 G_t = \mathbf{x}_1 F_t + \mathbf{z}_1 G_t.$$

Therefore,

$$\begin{aligned} d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) &\le d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_1 F_t + \mathbf{z}_1 G_t) + d^{(t)}(\mathbf{x}_2 F_t, \mathbf{x}_2 F_t + \mathbf{z}_2 G_t) \\ &= W^{(t)}(\mathbf{z}_1 G_t) + W^{(t)}(\mathbf{z}_2 G_t) \\ &= w^{(t)}(\mathbf{z}_1) + w^{(t)}(\mathbf{z}_2) \\ &\le 2d+2, \end{aligned}$$

which violates $d^{(t)}_{\min} \ge 2d+3$. Therefore, combining two cases $d^{(t)}_{\min} \ge 2d+1$ and $d^{(t)}_{\min} \le 2d+2$, we obtain $d^{(t)}_{\min} = 2d+1$, or $2d+2$.

In the following, we prove the sufficiency of the theorem. First, we consider the case $d^{(t)}_{\min} = 2d+1$. For this case, this LNEC code is d-error-correcting at the sink node $t \in T$, that is, for any codeword $\mathbf{x}F_t \in \mathscr{C}_t$ and any error vector $\mathbf{z} \in \mathscr{Z}$ with weight no more than d, it follows

$$d^{(t)}(\mathbf{x}F_t, \mathbf{x}F_t + \mathbf{z}G_t) < d^{(t)}(\mathbf{x}' F_t, \mathbf{x}F_t + \mathbf{z}G_t),$$

for any other codeword $\mathbf{x}' F_t \in \mathscr{C}_t$.

Assume the contrary that there are two distinct codewords $\mathbf{x}_1 F_t, \mathbf{x}_2 F_t \in \mathscr{C}_t$ and an error vector $\mathbf{z} \in \mathscr{Z}$ with weight no more than d such that

$$d^{(t)}(\mathbf{x}_2 F_t, \mathbf{x}_1 F_t + \mathbf{z}G_t) \le d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_1 F_t + \mathbf{z}G_t).$$

Therefore, we have

$$\begin{aligned} d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) &\le d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_1 F_t + \mathbf{z}G_t) + d^{(t)}(\mathbf{x}_2 F_t, \mathbf{x}_1 F_t + \mathbf{z}G_t) \\ &\le 2d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_1 F_t + \mathbf{z}G_t) \\ &= 2W^{(t)}(\mathbf{z}G_t) \\ &= 2w^{(t)}(\mathbf{z}) \\ &\le 2d, \end{aligned}$$

which contradicts to $d^{(t)}_{\min} = 2d+1$.

On the other hand, this LNEC code is not $(d+1)$-error-correcting at the sink node $t \in T$. As $d^{(t)}_{\min} = 2d+1$, there exist two codewords $\mathbf{x}_1 F_t, \mathbf{x}_2 F_t \in \mathscr{C}_t$ such that

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) = 2d+1,$$

which further shows that there exists an error vector $\mathbf{z} \in \mathscr{Z}$ with $w^{(t)}(\mathbf{z}) = 2d+1$ such that

$$\mathbf{x}_1 F_t = \mathbf{x}_2 F_t + \mathbf{z}G_t. \tag{2.12}$$

Together with the definition of weight

$$w^{(t)}(\mathbf{z}) = \min\{w_H(\mathbf{z}') : \text{ all } \mathbf{z}' \in \mathscr{Z} \text{ such that } \mathbf{z}'G_t = \mathbf{z}G_t\},$$

without loss of generality, we assume $\mathbf{z} \in \mathscr{Z}$ satisfying $w_H(\mathbf{z}) = w^{(t)}(\mathbf{z}) = 2d+1$.

Subsequently, let $\mathbf{z}_1, \mathbf{z}_2 \in \mathscr{Z}$ be two error vectors satisfying $\mathbf{z} = \mathbf{z}_1 + \mathbf{z}_2$ with the following two conditions:

- $\rho_{\mathbf{z}_1} \cap \rho_{\mathbf{z}_2} = \emptyset$ and $\rho_{\mathbf{z}_1} \cup \rho_{\mathbf{z}_2} = \rho_{\mathbf{z}}$;
- $|\rho_{\mathbf{z}_1}| = d$, and $|\rho_{\mathbf{z}_2}| = d+1$.

Now, we can claim that $w_H(\mathbf{z}_1) = w^{(t)}(\mathbf{z}_1) = d$ and $w_H(\mathbf{z}_2) = w^{(t)}(\mathbf{z}_2) = d+1$. On the contrary, assume that $w_H(\mathbf{z}_1) \neq w^{(t)}(\mathbf{z}_1)$, which, together with $w_H(\mathbf{z}_1) \geq w^{(t)}(\mathbf{z}_1)$, indicates $w_H(\mathbf{z}_1) > w^{(t)}(\mathbf{z}_1)$. Again notice that

$$w^{(t)}(\mathbf{z}_1) = \min\{w_H(\mathbf{z}_1') : \text{ all } \mathbf{z}_1' \in \mathscr{Z} \text{ such that } \mathbf{z}_1'G_t = \mathbf{z}_1G_t\}.$$

It follows that there must exist an error vector $\mathbf{z}_1' \in \mathscr{Z}$ such that $w_H(\mathbf{z}_1') = w^{(t)}(\mathbf{z}_1)$ and $\mathbf{z}_1'G_t = \mathbf{z}_1G_t$. Thus, it is shown that

$$(\mathbf{z}_1' + \mathbf{z}_2)G_t = \mathbf{z}_1'G_t + \mathbf{z}_2G_t = \mathbf{z}_1G_t + \mathbf{z}_2G_t = \mathbf{z}G_t,$$

which implies that $w^{(t)}(\mathbf{z}_1' + \mathbf{z}_2) = w^{(t)}(\mathbf{z})$. However,

$$\begin{aligned} w_H(\mathbf{z}_1' + \mathbf{z}_2) &\leq w_H(\mathbf{z}_1') + w_H(\mathbf{z}_2) \\ &= w^{(t)}(\mathbf{z}_1) + w_H(\mathbf{z}_2) \\ &< w_H(\mathbf{z}_1) + w_H(\mathbf{z}_2) \\ &= w_H(\mathbf{z}_1 + \mathbf{z}_2) \\ &= w_H(\mathbf{z}) \\ &= w^{(t)}(\mathbf{z}) \\ &= w^{(t)}(\mathbf{z}_1' + \mathbf{z}_2), \end{aligned}$$

which is impossible. Similarly, we can also obtain $w_H(\mathbf{z}_2) = w^{(t)}(\mathbf{z}_2) = d+1$. Therefore, from (2.12), one has

$$\mathbf{x}_1F_t = \mathbf{x}_2F_t + \mathbf{z}G_t = \mathbf{x}_2F_t + \mathbf{z}_1G_t + \mathbf{z}_2G_t,$$

that is,

$$\mathbf{x}_1F_t - \mathbf{z}_1G_t = \mathbf{x}_2F_t + \mathbf{z}_2G_t.$$

So when the message vector $\mathbf{x}_2$ is transmitted and the error vector $\mathbf{z}_2$ happens, the minimum distance decoding principle cannot decode $\mathbf{x}_2$ successfully at the sink node t, that is, it is not $(d+1)$-error-correcting at the sink node $t \in T$.

Combining the above, this LNEC code is exactly d-error-correcting at the sink node $t \in T$. Similarly, we can show that $d_{\min}^{(t)} = 2d+2$ also implies exactly d-error-correcting at the sink node $t \in T$. The proof is completed. □

Corollary 2.1. *For a linear network error correction code, $d_{\min}^{(t)} = d$ if and only if it is exactly $\lfloor \frac{d-1}{2} \rfloor$-error-correcting at the sink node $t \in T$.*

Remark 2.1. In [51], the authors indicated an interesting discovery that, for nonlinear network error correction codes, the number of the correctable errors can be more than half of the number of the detectable errors, which is contrast to the linear cases as stated above.

In classical coding theory, if the positions of errors occurred are known by the decoder, the errors are called erasure errors. When network coding is under consideration, this scheme can be extended to linear network error correction codes. To be specific, we assume that the collection of channels on which errors may be occurred during the network transmission is known by sink nodes. For this case, we will characterize the capability for correcting erasure errors with respect to sink nodes, that is called *erasure error correction capability*. This characterization is a generalization of the corresponding result in classical coding theory.

Let ρ be an error pattern consisting of the channels on which errors may happen, and we say that an error message vector $\mathbf{z} = [z_e : \ e \in E]$ matches an error pattern ρ, if $z_e = 0$ for all $e \in E \backslash \rho$. Since the error pattern ρ is known by the sink nodes, a weight measure $w^{(t)}$ of the error pattern ρ with respect to the weight measure $w^{(t)}$ of error vectors at the sink node t is defined as:

$$w^{(t)}(\rho) \triangleq \max_{\mathbf{z} \in \mathscr{Z}_\rho} w^{(t)}(\mathbf{z}),$$

where $\mathscr{Z}_\rho$ represents the collection of all error vectors matching the error pattern ρ, i.e.,

$$\mathscr{Z}_\rho = \{\mathbf{z} : \ \mathbf{z} \in \mathscr{F}^{|E|} \text{ and } \mathbf{z} \text{ matches } \rho\}.$$

Naturally, we still use the minimum distance decoding principle to correct erasure errors at sink nodes. First, we give the following definition.

Definition 2.8 (d-Erasure-Error-Correcting). Let d be a positive integer. A linear network error correction code is d-erasure-error-correcting at the sink node $t \in T$, if the minimum distance decoding principle at the sink node t is able to correct all error vectors in $\mathscr{Z}$ matching any error pattern ρ with weight no more than d, assuming that ρ is known by t and the incomplete decoding rule is used.

The following result characterizes the erasure error correction capability of linear network error correction codes.

Theorem 2.4. *A linear network error correction code is d-erasure-error-correcting at the sink node $t \in T$ if and only if $d_{\min}^{(t)} \geq d+1$.*

Proof. First, we prove that $d_{\min}^{(t)} \geq d+1$ is a sufficient condition. Assume that $d_{\min}^{(t)} \geq d+1$, and the contrary that this linear network error correction code is not d-erasure-error-correcting at the sink node t. That is, for some error pattern ρ with weight no more than d with respect to t, there are two distinct message vectors $\mathbf{x}_1, \mathbf{x}_2 \in \mathscr{F}^{\omega}$ and two distinct error vectors $\mathbf{z}_1, \mathbf{z}_2$ matching the error pattern ρ (or equivalently, $\mathbf{z}_1, \mathbf{z}_2 \in \mathscr{Z}_\rho$) such that

$$\mathbf{x}_1 F_t + \mathbf{z}_1 G_t = \mathbf{x}_2 F_t + \mathbf{z}_2 G_t.$$

Subsequently,

$$\mathbf{x}_1 F_t - \mathbf{x}_2 F_t = \mathbf{z}_2 G_t - \mathbf{z}_1 G_t,$$

which further shows

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) = W^{(t)}((\mathbf{z}_2 - \mathbf{z}_1) G_t) = w^{(t)}(\mathbf{z}_2 - \mathbf{z}_1) \leq w^{(t)}(\rho) \leq d, \qquad (2.13)$$

where the first inequality in (2.13) follows from both $\mathbf{z}_1$ and $\mathbf{z}_2$ matching ρ. This violates $d_{\min}^{(t)} \geq d+1$.

On the other hand, we will prove the necessary condition of this theorem by contradiction. Assume a linear network error correction code has $d_{\min}^{(t)} \leq d$ for some sink node t. We will find an error pattern ρ with weight $w^{(t)}(\rho) \leq d$ which can not be corrected.

Since $d_{\min}^{(t)} \leq d$, there exist two codewords $\mathbf{x}_1 F_t, \mathbf{x}_2 F_t \in \mathscr{C}_t$ such that

$$d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) \leq d.$$

Further, there exists an error vector $\mathbf{z} \in \mathscr{Z}$ such that $\mathbf{x}_1 F_t - \mathbf{x}_2 F_t = \mathbf{z} G_t$ and

$$w^{(t)}(\mathbf{z}) = W^{(t)}(\mathbf{z} G_t) = W^{(t)}(\mathbf{x}_1 F_t - \mathbf{x}_2 F_t) = d^{(t)}(\mathbf{x}_1 F_t, \mathbf{x}_2 F_t) \leq d.$$

Note that

$$w^{(t)}(\mathbf{z}) = \min\{w_H(\mathbf{z}') : \mathbf{z}' \in \mathscr{Z} \text{ such that } \mathbf{z}' G_t = \mathbf{z} G_t\}.$$

Without loss of generality, assume the error vector $\mathbf{z}$ satisfying $w_H(\mathbf{z}) = w^{(t)}(\mathbf{z}) \leq d$. Let $\rho_{\mathbf{z}}$ further be the error pattern induced by the error vector $\mathbf{z}$, that is the collection of channels on which the corresponding coordinates of $\mathbf{z}$ are nonzero. Hence,

$$w^{(t)}(\rho_{\mathbf{z}}) \leq |\rho_{\mathbf{z}}| = w_H(\mathbf{z}) \leq d.$$

This shows that when the message vector $\mathbf{x}_2$ is transmitted and the erasure error vector $\mathbf{z}$ matching ρ with $w^{(t)}(\rho) \leq d$ happens, the minimum distance decoding principle at the sink node t will decode $\mathbf{x}_1$ instead of $\mathbf{x}_2$, that is, $\mathbf{x}_2$ can not be decoded successfully at the sink node t, although ρ is known. This leads to a contradiction.

Combining the above, we complete the proof. □

http://www.springer.com/978-1-4939-0587-4

Linear Network Error Correction Coding
Guang, X.; Zhang, Z.
2014, VI, 107 p. 9 illus., Softcover
ISBN: 978-1-4939-0587-4