Wuhan University
Journal of Natural Sciences

2013, Vol.18 No.6, 477-483

Article ID 1007-1202(2013)06-0477-07
DOI 10.1007/s11859-013-0960-6

Matroidal Error Correction Networks and Linear Network Error Correction MDS Codes

□ ZHOU Hang[1,2], LIU Guangjun[3]

1. The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, Shaanxi, China;
2. College of Science, Engineering University of the Chinese People's Armed Police Force, Xi'an 710086, Shaanxi, China;
3. School of Mathematics and Computer Engineering, Xi'an University of Arts and Science, Xi'an 710065, Shaanxi, China

Abstract: In this paper, we further study the connections between linear network error correction codes and representable matroids. We extend the concept of matroidal network introduced by Dougherty *et al.* to a generalized case when errors occur in multiple channels. Importantly, we show the necessary and sufficient conditions on the existence of linear network error correction multicast/broadcast/dispersion maximum distance separable (MDS) code on a matroidal error correction network.

Key words: network error correction code; error pattern; imaginary error channels; extended network; matroid
CLC number: TN 915.01; TN 919.3+1

Received date: 2013-04-27
Foundation item: Supported by the National Natural Science Foundation of China (61271174, 61272492)
Biography: ZHOU Hang, male, Associate professor, Ph.D. candidate, research direction: network coding and matroid theory. E-mail: zhouhang2010@163.com

0 Introduction

The theory of matroids was widely used in combinatorial optimization, integer programming, and network flow in the past. However, some new applications have been found in the field of network coding. The original idea of network error correction coding (NEC) was proposed by Yeung and Cai in Ref. [1]. In their subsequent papers [2] and [3], they generalized the Hamming bound, the Singleton bound, and the Gilbert-Varshamov bound in classical error correction coding to network coding. In Ref. [4], Zhang defined the minimum distance of linear network error correction code (LNEC) and proved that the minimum distance plays exactly the same role as it does in classical coding theory for the characterization of error correction/detection capabilities of the code. The existence and construction of network error correction maximum distance separable (MDS) code is also studied in Refs. [5-8].

In Ref. [9], Dougherty *et al* defined matroidal networks and used matroids to construct various networks systematically. They used matroidal networks to show the insufficiency of linear network coding and the inachievability of network coding capacity [10]. Kim and Medard [11] proved that a network is scalar-linearly solvable if and only if the network is a matroidal network associated with a representable matroid over some finite field. In this paper, we attempt to establish some connections between LNEC and representable matroids. We propose a definition of matroidal error correction network. Then, we show the conditions for the existence of linear network error correction multicast/broadcast/dispersion MDS codes on a matroidal error correction network.

1 Preliminaries

1.1 Network Error Correcting Problem

Let $\mathcal{F}$ be a finite field of sufficiently large cardinality. Unless otherwise specified, all the algebraic operations in this paper are over this field. A communication network is usually represented by a finite acyclic directed graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, where $\mathcal{V}$ is the vertex set consisting of nodes, and $\mathcal{E}$ is the edge set whose elements represent communication channels of the network. There is an upstream-to-downstream order on $\mathcal{E}$. A directed edge $e=(i,j)\in\mathcal{E}$ stands for a channel leading from node i to node j. Node i is called the tail of e, and j is called the head of e. We denote this as $i=\text{tail}(e)$ and $j=\text{head}(e)$. Correspondingly, the channel e is called an outgoing channel of i and an incoming channel of j. For a node i, we define $\text{In}(i)=\{e\in\mathcal{E}:\text{head}(e)=i\}$ and $\text{Out}(i)=\{e\in\mathcal{E}:\text{tail}(e)=i\}$. We allow multiple channels between two nodes and assume that one field symbol can be transmitted over a channel in a unit time.

In this paper, we only consider single source acyclic networks, and the unique source node is denoted by s. Let T be a collection of nonsource nodes. A cut between s and T is a set of channels whose removal disconnects s from any $t\in T$. For unit capacity channels, the capacity of a cut between s and T can be regarded as the number of channels in the cut, and the minimum of all capacities of cuts between s and T is called the minimum cut capacity, which is denoted by C_T. In particular, the minimum cut capacity between s and a nonsource node t is denoted as C_t.

Let the information rate be ω symbols per unit time. Then, the source node has ω imaginary incoming channels $d_1,d_2,\cdots,d_\omega$, and let $\text{In}(s)=\{d_1,d_2,\cdots,d_\omega\}$. The source messages are ω symbols arranged in a row vector $\underline{\boldsymbol{X}}=(X_1,X_2,\cdots,X_\omega)$, where each X_i is an element of base field $\mathcal{F}$. Assume they are transmitted to s through ω imaginary incoming channels in $\text{In}(s)$. By using network coding, source messages are transmitted to and decoded at each sink node.

Denote by U_e, the message is transmitted over the channel e. At the source node s, assume that the message transmitted over the i th imaginary channel is $U_{d_i}=X_i$. In general, the message U_e transmitted over channel e is calculated by $U_e=\underline{\boldsymbol{X}}f_e$, where f_e is an ω-dimensional $\mathcal{F}$-valued column vector, which is called the global encoding kernel vector of channel e.

When an error occurs on channel e, the output of the channel is $\tilde{U}_e=U_e+Z_e$, where U_e is the message that should be transmitted over e, and $Z_e\in\mathcal{F}$ is the error occurred in e. In the original network $\mathcal{G}=(\mathcal{V},\mathcal{E})$, for each channel $e\in\mathcal{E}$, an imaginary channel e' is introduced, which is connected with the tail of e to provide error message Z_e. Let $\mathcal{E}'=\{e':e\in\mathcal{E}\}$. This new network $\tilde{\mathcal{G}}=(\tilde{\mathcal{V}},\tilde{\mathcal{E}})$ with imaginary channels $\text{In}(s)\bigcup\mathcal{E}'$ is called the extended network of $\mathcal{G}=(\mathcal{V},\mathcal{E})$, where $\tilde{\mathcal{V}}=\mathcal{V}$ and $\tilde{\mathcal{E}}=\text{In}(s)\bigcup\mathcal{E}'\bigcup\mathcal{E}$. For each non source node i in the extended network, $\text{In}(i)$ only includes the real incoming channels of i, that is, the imaginary channel e' corresponding to $e\in\text{Out}(i)$ are not in $\text{In}(i)$. We can also define the global encoding kernel $\tilde{f}_e$ for each channel $e\in\tilde{\mathcal{E}}$ in the extended network. It is an $(\omega+|\mathcal{E}|)$-dimensional column vector, and the entries can be indexed by the elements of $\text{In}(s)\bigcup\mathcal{E}$. For each imaginary message channel $d_i\in\text{In}(s)$, let $\tilde{f}_{d_i}=1_{d_i}$, and for each imaginary error channel $e'\in\mathcal{E}'$, let $\tilde{f}_{e'}=1_e$ (1_e is an $(\omega+|\mathcal{E}|)$-dimensional column vector, which is the indicator function of e. Specifically, the entry indexed by e equals to 1, and the others are 0's). For a real channel $e\in\mathcal{E}$, the global encoding kernel is determined by the recursive formula:

$$\tilde{f}_e=\sum_{d\in\text{In}(\text{tail}(e))}k_{d,e}\tilde{f}_d+1_e \tag{1}$$

where $k_{d,e}$ is the local encoding coefficient for an adjacent pair (d,e) of channels.

Let $\underline{\boldsymbol{Z}}=(Z_e:e\in\mathcal{E})$ be an $|\mathcal{E}|$-dimensional row vector and call $\underline{\boldsymbol{Z}}$ the error message vector. An error pattern ρ is a set of channels of $\mathcal{G}$ in which errors occur. We call that $\underline{\boldsymbol{Z}}$ matches the error pattern ρ, if $Z_e=0$ for all $e\in\mathcal{E}\setminus\rho$. For an error pattern ρ, let $\rho'=\{e':e\in\rho\}$ represent the imaginary channel set corresponding to ρ. Zhang [4] defined a modified network $\mathcal{G}_\rho=(\mathcal{V}_\rho,\mathcal{E}_\rho)$ corresponding to ρ with $\mathcal{V}_\rho=\mathcal{V}$ and $\mathcal{E}_\rho=\text{In}(s)\bigcup\rho'\bigcup\mathcal{E}$.

For all messages including information messages and error messages, if they are considered as column vectors, the set $\{\tilde{f}_e:e\in\mathcal{E}\}$ of all extended global encoding kernels constitutes a global description of an ω-dimensional $\mathcal{F}$-value LNEC for the original network $\mathcal{G}=(\mathcal{V},\mathcal{E})$.

First, we need some definitions that either are quoted directly or are extended from Ref. [8].

Definition 1[8] For an LNEC on network $\mathcal{G}$, let T be a collection of nonsource nodes and $\text{In}(T)=$

$\bigcup_{t\in T}\text{In}(t)$. The matrix

$$\tilde{\boldsymbol{F}}_T=(\tilde{f}_e : e\in \text{In}(T))$$

is called the decoding matrix with respect to T.

Definition 2 For an error pattern ρ, the matrix

$$\tilde{\boldsymbol{F}}_T^{\rho}=(\tilde{f}_e^{\rho} : e\in \text{In}(T))$$

is called the decoding matrix restricted to ρ with respect to T, where $\tilde{f}_e^{\rho}$ is an $(\omega+|\rho|)$-dimensional column vector obtained from $\tilde{f}_e$ by removing all entries not in $\text{In}(s)\bigcup\rho$.

We denote the row vector of $\tilde{F}_T$ indexed by the channel $d\in \text{In}(s)\bigcup\mathcal{E}$ as $\text{row}_T(d)$. Let L be a collection of vectors in a linear space, and we use $\langle L\rangle$ to represent the subspace by vectors in L. At a collection T of nonsource nodes, the following vector spaces are important.

Definition 3 For an LNEC on network $\mathcal{G}$ and a collection T of nonsource nodes, let

$$\boldsymbol{\Phi}(T)=\langle\{\text{row}_T(d) : d\in \text{In}(s)\}\rangle$$

$$\Delta(T,\rho)=\langle\{\text{row}_T(e) : e\in \rho\}\rangle$$

We call $\boldsymbol{\Phi}(T)$ the message space of T and $\Delta(T,\rho)$ the error space of error pattern ρ with respect to T.

Definition 4[8] An ω-dimensional LNEC on an acyclic network $\mathcal{G}=(\mathcal{V},\mathcal{E})$ qualifies as a linear multicast, linear broadcast, and linear dispersion, respectively, if

1) $\dim(\boldsymbol{\Phi}(t))=\omega$ for any nonsource node $t\in\mathcal{V}$ with $C_t\geqslant\omega$;

2) $\dim(\boldsymbol{\Phi}(t))=\min\{\omega, C_t\}$ for every non-source node $t\in\mathcal{V}$;

3) $\dim(\boldsymbol{\Phi}(T))=\min\{\omega, C_T\}$ for every collection T of non-source nodes.

For any collection T of nonsource nodes with $C_T\geqslant\omega$, define $\delta_T=C_T-\omega$, which is called the redundancy of T. Let

$$R_T(\delta_T)=\{\rho\text{: } |\rho|=\text{rank}_T(\rho)=\delta_T\}$$

be the collection of error pattern of size δ_T.

Definition 5 The rank of an error pattern ρ with respect to T is defined by

$$\text{rank}_T(\rho)=\min\{|\rho_1| : \Delta(T,\rho)\subseteq\Delta(T,\rho_1)\}.$$

Definition 6[8] The minimum distance of an LNEC on network $\mathcal{G}$ with respect to T is defined as

$$d_{\min}^{(T)}=\min\{\text{ran}k_T(\rho) : \boldsymbol{\Phi}(T)\cap\Delta(T,\rho)\neq\{0\}\}.$$

Lemma 1[8] Let $d_{\min}^{(T)}$ be the minimum distance of a linear network error correction dispersion code with respect to T. Then,

$$d_{\min}^{(T)}\leqslant\begin{cases}C_T-\omega+1, & \text{if } C_T\geqslant\omega\\ 1 &, \text{ if } C_T<\omega\end{cases}\tag{2}$$

This is called the extended Singleton bound.

Lemma 2[8] Let $d_{\min}^{(t)}$ be the minimum distance of a linear network error correction broadcast code with respect to a nonsource node t. Then

$$d_{\min}^{(t)}\leqslant\begin{cases}C_t-\omega+1, & \text{if } C_t\geqslant\omega\\ 1 &, \text{ if } C_t<\omega\end{cases}\tag{3}$$

This is called the weakly extended Singleton bound.

Definition 7[8] An ω-dimensional linear network error correction multicast/broadcast/dispersion code is called multicast/broadcast/dispersion MDS code, if it satisfies the corresponding (weakly) extended Singleton bound with equality.

Definition 8 An LNEC is called α-error-correcting with respect to T if $d_{\min}^{(T)}\geqslant 2\alpha+1$ for every collection T of nonsource nodes.

Note 1. It is easy to see that $d_{\min}^{(T)}\geqslant 1$. Thus, for the case $C_T<\omega$, $d_{\min}^{(T)}=1$, which implies that the LNEC has no error-correcting capability with respect to T.

1.2 Matroid Fundamentals

We review here some definitions and results in matroid theory, as they are useful in the remainder of the paper.

Definition 9[12] Amatroid $\mathcal{M}$ is an ordered pair $(E,\mathcal{I})$, where E is a finite set, and $\mathcal{I}$ is a set of subsets of E satisfying the following conditions:

1) $\varnothing\in\mathcal{I}$;

2) If $I\in\mathcal{I}$ and $J\subseteq I$, then $J\in\mathcal{I}$;

3) If $I,J\in\mathcal{I}$ and $|J|<|I|$, then there exists an element $x\in I-J$ such that $J\bigcup x\in\mathcal{I}$.

The set E is called the ground set of $\mathcal{M}$. We often write $E(\mathcal{M})$ for E, particularly when several matroids are being considered. The members of $\mathcal{I}$ are called independent sets and any subset of E not in $\mathcal{I}$ is called a dependent set. A maximal independent set of E is called a base of $\mathcal{M}$, and the set of all bases of $\mathcal{M}$ is denoted by $\mathcal{B}(\mathcal{M})$.

Definition 10[12] Let $\mathcal{M}$ be a matroid $(E,\mathcal{I})$ and $X\subseteq E$. Let $\mathcal{I}|X=\{I\subseteq X, I\in\mathcal{I}\}$, $\mathcal{M}|X=(X,\mathcal{I}|X)$. Then, $\mathcal{M}|X$ is a matroid, which is called the restriction of $\mathcal{M}$ to X. The size of a base of $\mathcal{M}|X$ is called the rank of X, which is denoted by $r_{\mathcal{M}}(X)$. $r_{\mathcal{M}}(E)$ is called the rank of $\mathcal{M}$, which is denoted by $r(\mathcal{M})$.

Definition 11[12] Two matroids $\mathcal{M}_1=(E_1,\mathcal{I}_1)$ and $\mathcal{M}_2=(E_2,\mathcal{I}_2)$ are isomorphic if there is a bijection map φ from E_1 to E_2, such that for all $I\in\mathcal{I}_1$ if and only if $\varphi(I)\in\mathcal{I}_2$.

Definition 12[12] Let $\boldsymbol{A}$ be an $m\times n$ matrix over field $\mathcal{F}$. If $E=\{1,2,\cdots,n\}$ is the set of column indices of $\boldsymbol{A}$ and $\mathcal{I}$ is the set of all $X\subseteq E$ such that the multiset of columns of $\boldsymbol{A}$ indexed by the elements of X is linearly independent, then $(E,\mathcal{I})$ is a matroid, called the vector matroid of $\boldsymbol{A}$, which is denoted by $\mathcal{M}[\boldsymbol{A}]$.

A matroid $\mathcal{M}$ that is isomorphic to $\mathcal{M}[\boldsymbol{A}]$ is called $\mathcal{F}$-representable, and $\boldsymbol{A}$ is called an $\mathcal{F}$-representation of $\mathcal{M}$.

Lemma 3[12] Suppose $\boldsymbol{A}$ is a matrix over field $\mathcal{F}$. Then, the vector matroid $\mathcal{M}[\boldsymbol{A}]$ remains unaltered by performing any of the following operations on $\boldsymbol{A}$:

1) Interchange two rows.

2) Multiply a row by a non-zero member of $\mathcal{F}$.

3) Replace a row by the sum of that row and another.

4) Delete a zero row (unless it is the only row).

5) Interchange two columns (moving the labels with the columns).

6) Multiply a column by a nonzero member of $\mathcal{F}$.

Definition 13 Let $\mathcal{M}$ be a matroid $(E,\mathcal{I})$ and $X\subseteq E$. Let $\mathcal{I}'=\{I\subseteq E-X: I\cup B_X\in\mathcal{I}\}$, where $B_X\subseteq X$ is a maximal independent subset within X. Then, $(E-X,\mathcal{I}')$ is a matroid, called the contraction of X from $\mathcal{M}$ and denoted by $\mathcal{M}/X$.

Lemma 4[12] Let $\mathcal{M}[A]$ be the vector matroid represented by A. If x labels a nonzero column of $\boldsymbol{A}$, by operations (1) to (6) in Lemma 3, we can transform $\boldsymbol{A}$ into a matrix $\boldsymbol{A}'$, which has a unique nonzero entry in the column labeled by x. Let $\boldsymbol{A}'/\{x\}$ denotes the matrix that is obtained by deleting the row and column containing the nonzero entry. Then

$$\mathcal{M}/x=\mathcal{M}[\boldsymbol{A}'/\{x\}].$$

2 Matroidal Error Correction Networks and Linear Multicast/ Broadcast/Dispersion MDS Codes

2.1 Matroidal Error Correction Networks

Doughter *et al.* defined matroidal networks and presented a method for constructing matroidal networks [9]. The network appropriately reflects the data dependency relationship among the elements in the given matroid.

Definition 14 (Ref. [9], Definition V.1) Let $\mathcal{G}$ be a network with message set μ, node set $\mathcal{V}$, and edge set $\mathcal{E}$, and let $\mathcal{M}=(E,\mathcal{I})$ be a matroid with rank r. The network $\mathcal{G}$ is a matroidal network associated with $\mathcal{M}$ if a function exists, such that the following conditions are satisfied:

1) f is one to one on μ;

2) $f(\mu)\in\mathcal{I}$;

3) $r_M(f(\mathrm{In}(i)))=r_M(f(\mathrm{In}(i)\cup\mathrm{Out}(i)))$, for every $i\in\mathcal{V}$.

Next, we extend the concept of matroidal networks to a more general case as follows.

Definition 15 Let $\mathcal{G}=(\mathcal{V},\mathcal{E})$ be a single source acyclic network with information rate ω and a given topological order on $\mathcal{E}$. Let $\mathcal{M}=(E,\mathcal{I})$ be an $\mathcal{F}$-representable matroid with $|E(\mathcal{M})|=\omega+2|\mathcal{E}|$ and $r(\mathcal{M})=\omega+|\mathcal{E}|$. The network $\mathcal{G}$ is said to be a matroidal $\left\lfloor\frac{1}{2}d_{\min}^{(T)}-1\right\rfloor$ error correction network associated with $\mathcal{M}$ if the following conditions are satisfied:

(A) There exists a function

$$f:\mathrm{In}(s)\cup\mathcal{E}'\cup\mathcal{E}\to E(\mathcal{M})$$

from the extended network $\tilde{\mathcal{G}}=(\tilde{\mathcal{V}},\tilde{\mathcal{E}})$ to the matroid $\mathcal{M}$ such that

(A1) f is one to one on $\mathrm{In}(s)\cup\mathcal{E}'$.

(A2) $f(\mathrm{In}(s)\cup\mathcal{E}')\in\mathcal{B}(M)$.

(A3) For every $i\in\tilde{\mathcal{V}}$ and $e_j\in\mathrm{Out}(i)$,

$$r_{\mathcal{M}}(f(\mathrm{In}(i))\cup f(e_j))=r_{\mathcal{M}}(f(\mathrm{In}(i))\cup f(e_j')).$$

(B) For any collection T of nonsource nodes with $C_T\geqslant\omega$ and each error pattern $\rho\in R_T(\delta_T)$, let $\bar{\rho}=\mathcal{E}'\setminus\rho'$, $B_{\bar{\rho}}=f(\mathcal{E}'\setminus\rho')$ and $\mathcal{M}^{\rho}=\mathcal{M}/B_{\bar{\rho}}$. The network-matroid mapping

$$f^{\rho}:\mathrm{In}(s)\cup\rho'\cup\mathcal{E}\to E(\mathcal{M}^{\rho})$$

from $\mathcal{G}_\rho=(\mathcal{V}_\rho,\mathcal{E}_\rho)$ to $\mathcal{M}^{\rho}$ is determined by

$$f^{\rho}(x)=f(x),\qquad \forall x\in\mathrm{In}(s)\cup\rho'\cup\mathcal{E},$$

such that

$$r_{\mathcal{M}_T^{\rho}}(f^{\rho}(\mathrm{In}(T)))=C_T,$$

where $\mathcal{M}_T^{\rho}=\mathcal{M}^{\rho}\big|f^{\rho}(\mathrm{In}(T))$.

Remark 1 Condition (A1) assigns unique ground set element of the matroid $\mathcal{M}$ to each imaginary incoming channel in $\mathrm{In}(s)$ and each imaginary error message channel in $\mathcal{E}'$. Condition (A2) assures the set of the imaginary channels to be mapped to a base of $\mathcal{M}$. Condition (A3) reflects the fact that for every $i\in\tilde{\mathcal{V}}$ and $e_j\in\mathrm{Out}(i)$, the symbol flow through e_j is a linear combination of the symbols flow through $\mathrm{In}(i)$ and the imaginary error channel e_j'.

Condition (B) assigns unique ground set element of $\mathcal{M}^{\rho}$ to each channel in the modified network $\mathcal{G}_\rho$ and assures that $r_{\mathcal{M}_T^{\rho}}(\tilde{F}_T^{\rho})=C_T$ for any collection T of nonsource nodes with $C_T\geqslant\omega$.

Remark 2 Definition V.1 in Ref. [9] can be regarded as a special case of Definition 15 under the assumption that channels are error-free. Specifically, conditions (A1), (A2), and (A3) of Definition 15 include conditions ($\mathcal{M}1$), ($\mathcal{M}2$), and ($\mathcal{M}3$) of Definition 14, respectively.

2.2 Existence of Linear Multicast/Broadcast/Dispersion MDS Codes on a Matroidal Error Correction Network

Theorem 1 Let $\mathcal{G}=(\mathcal{V},\mathcal{E})$ be a single source acyclic network with information rate ω. Let $\mathcal{M}=(E,\mathcal{I})$ be an $\mathcal{F}$-representable matroid with $|E(\mathcal{M})|=\omega+2|\mathcal{E}|$ and $r(\mathcal{M})=\omega+|\mathcal{E}|$. $\mathcal{G}$ is a matroidal $\left\lfloor \frac{1}{2}d_{\min}^{(T)}-1 \right\rfloor$ error correction network associated with $\mathcal{M}$ for any collection T of nonsource nodes if and only if there exists a scalar linear network error correction dispersion MDS code over $\mathcal{F}$ on $\mathcal{G}$.

Proof If part: Suppose the given linear network error correction dispersion MDS code on $\mathcal{G}=(\mathcal{V},\mathcal{E})$ is characterized by the set $\{\tilde{f}_e : e\in\mathcal{E}\}$. Similar to the Koetter-Médard Formula[13], there exists the following formula in Ref. [4]:

$$\left(\tilde{f}_e, e\in\mathcal{E}\right)=\begin{pmatrix}\boldsymbol{B}\\ \boldsymbol{I}\end{pmatrix}(\boldsymbol{I}-\boldsymbol{F})^{-1}$$

where $\boldsymbol{B}=\left(k_{d,e}\right)_{d\in\mathrm{In}(s),e\in\mathcal{E}}$ is an $\omega\times|\mathcal{E}|$ matrix with $k_{d,e}=0$ for $e\notin\mathrm{Out}(s)$, $k_{d,e}$ is the local encoding coefficient for $e\in\mathrm{Out}(s)$, $\boldsymbol{F}=\left(k_{d,e}\right)_{d\in\mathcal{E},e\in\mathcal{E}}$ is an $|\mathcal{E}|\times|\mathcal{E}|$ matrix with $k_{d,e}$ being the local encoding coefficient for $\mathrm{head}(d)=\mathrm{tail}(e)$ and $k_{d,e}=0$ for $\mathrm{head}(d)\neq\mathrm{tail}(e)$, and I denotes the $|\mathcal{E}|\times|\mathcal{E}|$ identity matrix. Let

$$\boldsymbol{A}=\begin{pmatrix}\boldsymbol{I}_{\omega\times\omega} & 0_{\omega\times|\mathcal{E}|} & \boldsymbol{B}(\boldsymbol{I}-\boldsymbol{F})^{-1}\\ 0_{|\mathcal{E}|\times\omega} & \boldsymbol{I}_{|\mathcal{E}|\times|\mathcal{E}|} & (\boldsymbol{I}-\boldsymbol{F})^{-1}\end{pmatrix}$$

and $\mathcal{M}[A]=(E,\mathcal{I})$ be the vector matroid of $\boldsymbol{A}$. Obviously, $r(\mathcal{M})=\omega+|\mathcal{E}|$. Define a network-matroid mapping as follows:

$$f:\mathrm{In}(s)\cup\mathcal{E}'\cup\mathcal{E}\rightarrow E(\mathcal{M})$$

For each $d_i\in\mathrm{In}(s)$, $1\leqslant i\leqslant\omega$, let $f(d_i)=i$. For each $e_j'\in\mathcal{E}'$, $1\leqslant j\leqslant|\mathcal{E}|$, let $f(e_j')=\ \omega+j$ and for every real channel $e_j\in\mathcal{E}$, let $f(e_j)=\omega+|\mathcal{E}|+j$.

We show that f satisfies condition (A) of Definition 15. Clearly, f is one to one on $\mathrm{In}(s)\cup\mathcal{E}'$, giving condition (A1). Since the extended global kernels $\tilde{f}_e : e\in\ \mathrm{In}(s)\cup\mathcal{E}'$ correspond to the first $\omega+|\mathcal{E}|$ columns of $\boldsymbol{A}$, which are linearly independent, thus $f(\mathrm{In}(s)\cup\mathcal{E}')\in\mathcal{B}(M)$. Condition (A2) is held. For every $i\in\mathcal{V}$ and for any channel $e_j\in\mathrm{Out}(i)$, by the recursive formulas

$$\tilde{f}_{e_j}=\sum_{d\in\mathrm{In}(i)}k_{d,e_j}\tilde{f}_d+1_{e_j}$$

we have

$$r_{\mathcal{M}}(f(\mathrm{In}(i))\cup f(e_j))=r_{\mathcal{M}}(f(\mathrm{In}(i))\cup f\left(e_j{}'\right))$$

Condition (A3) is held.

For any collection T of nonsource nodes with $C_T\geqslant\omega$ and each $\rho\in R\left(\delta_T\right)$, let

$$\boldsymbol{A}(\rho)=\begin{pmatrix}\boldsymbol{I}_{\omega\times\omega} & 0_{\omega\times|\rho|} & \boldsymbol{B}(\boldsymbol{I}-\boldsymbol{F})^{-1}\\ 0_{|\rho|\times\omega} & \boldsymbol{I}_{|\rho|\times|\rho|} & ((\boldsymbol{I}-\boldsymbol{F})^{-1})_{\rho}\end{pmatrix}$$

where $((\boldsymbol{I}-\boldsymbol{F})^{-1})_{\rho}$ represents the submatrix of $(\boldsymbol{I}-\boldsymbol{F})^{-1}$ with the rows indexed by ρ. Precisely, $A(\rho)$ is a matrix modified from A by deleting the rows and columns indexed by $\bar{\rho}\in\mathcal{E}'\setminus\rho'$. Let $\mathcal{M}^{\rho}$ be the vector matroid of matrix $\boldsymbol{A}(\rho)$ and $\boldsymbol{B}_{\bar{\rho}}=f(\mathcal{E}'\setminus\rho')$. By Lemma 4, we get $\mathcal{M}^{\rho}=\mathcal{M}/B_{\bar{\rho}}$. Since f^{ρ} satisfies

$$f^{\rho}(x)=f(x),\quad \forall x\in\mathrm{In}(s)\cup\rho'\cup\mathcal{E}$$

then the extended global encoding kernel of channel e restricted to ρ can be expressed as the corresponding column vector of matrix:

$$\left(\tilde{f}_e^{\rho}:e\in\mathcal{E}\right)=\begin{pmatrix}\boldsymbol{B}(\boldsymbol{I}-\boldsymbol{F})^{-1}\\ \left((\boldsymbol{I}-\boldsymbol{F})^{-1}\right)_{\rho}\end{pmatrix}$$

Because $\mathrm{rank}_T(\rho)=\delta_T<d_{\min}^{(T)}=C_T-\omega+1$, we know that, for the fixed error pattern ρ, $\Phi(T)\cap\Delta(T,\rho)\ =\{0\}$. Then,

$$\begin{aligned}\mathrm{rank}(\tilde{f}_{\mathrm{e}}^{\rho}:e\in\mathrm{In}(T))&=\dim(\langle\Phi(T)\cup\Delta(T,\rho)\rangle)\\ &=\dim(\Phi(T))+\dim(\Delta(T,\rho))\\ &=\omega+\mathrm{rank}_T(\rho)\\ &=C_T\end{aligned}$$

Therefore,

$$r_{\mathcal{M}_T^{\rho}}(f^{\rho}(\mathrm{In}(T)))=\mathrm{rank}(\tilde{f}_{\mathrm{e}}^{\rho}:e\in\mathrm{In}(T))=C_T$$

Condition (B) of Definition 15 is satisfied.

In summary, $\mathcal{G}$ is a matroidal $\left\lfloor\frac{1}{2}d_{\min}^{(T)}-1\right\rfloor$ error correction network associated with the $\mathcal{F}$-representable matroid $\mathcal{M}[A]$.

Only if part: suppose $\mathcal{G}$ is a matroidal $\left\lfloor\frac{1}{2}d_{\min}^{(T)}-1\right\rfloor$ error correction network associated with the $\mathcal{F}$-representable matroid $\mathcal{M}$. Let matrix $\boldsymbol{A}_1$ be a representation of $\mathcal{M}$ over field $\mathcal{F}$. Since $r(\mathcal{M})=\omega+|\mathcal{E}|$, without loss of generality, we assume that $\boldsymbol{A}_1$ has the form:

$$A_1=\begin{pmatrix} \boldsymbol{I}_{\omega\times\omega} & 0_{\omega\times|\mathcal{E}|} & \boldsymbol{B}_1\\ 0_{|\mathcal{E}|\times\omega} & \boldsymbol{I}_{|\mathcal{E}|\times|\mathcal{E}|} & \boldsymbol{C}_1\end{pmatrix}$$

where $\boldsymbol{B}_1$ is an $\omega\times|\mathcal{E}|$ matrix, and C_1 is a $|\mathcal{E}|\times|\mathcal{E}|$ matrix.

According to the given topological order on $\tilde{\mathcal{E}}$, the network-matroid mapping

$$f:\mathrm{In}(s)\cup\mathcal{E}'\cup\mathcal{E}\to E(\mathcal{M}[A_1])$$

is determined. Precisely, $f(d_i)=i$ for each $d_i\in\mathrm{In}(s)$, $1\leqslant i\leqslant\omega$. For each $e_j'\in\mathcal{E}'$, $1\leqslant j\leqslant|\mathcal{E}|$, $f(e_j')=\omega+j$, and for every $e_j\in\mathcal{E}$, $f(e_j)=\omega+|\mathcal{E}|+j$.

We use A_1^l to denote the lth column of A_1. In the extended network $\tilde{\mathcal{G}}=(\tilde{\mathcal{V}},\tilde{\mathcal{E}})$, for every $i\in\tilde{\mathcal{V}}$, we consider any edge $e_j\in\mathrm{Out}(i)$. Because the imaginary channel e_j' corresponding to e_j is not in $\mathrm{In}(i)$ and $\boldsymbol{A}^{f(e_j')}=1_{e_j}$, from condition (A3) of Definition 15, we have

$$A_1^{f(e_j)}=\sum_{d\in\mathrm{In}(i)}k_{d,e_j}A_1^{f(d)}+c_{jj}A_1^{f(e_j')}$$

Moreover, if we suppose $\boldsymbol{B}_1=(b_{ij})_{1\leqslant i\leqslant\omega,1\leqslant j\leqslant|\mathcal{E}|}$ and $\boldsymbol{C}_1=(c_{ij})_{1\leqslant i\leqslant|\mathcal{E}|,1\leqslant j\leqslant|\mathcal{E}|}$, then

$$A_1^{f(e_j)}=(b_{1j},b_{2j},\cdots,b_{\omega j},c_{1j},c_{2j},\cdots,c_{jj},0,\cdots,0)^{\mathrm{T}}$$

and $c_{jj}\neq 0$. Furthermore, $\boldsymbol{C}_1$ is an upper-triangular matrix, i.e.,

$$\boldsymbol{C}_1=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1|\mathcal{E}|}\\ 0 & c_{22} & \cdots & c_{2|\mathcal{E}|}\\ 0 & 0 & \cdots & c_{3|\mathcal{E}|}\\ \vdots & \vdots & \cdots & \vdots\\ 0 & 0 & \cdots & c_{|\mathcal{E}||\mathcal{E}|}\end{pmatrix}$$

Multiplying $A_1^{f(e_j)}$ by c_{jj}^{-1} for every $1\leqslant j\leqslant|\mathcal{E}|$, A_1 can be transformed into matrix:

$$\boldsymbol{A}=\begin{pmatrix} \boldsymbol{I}_{\omega\times\omega} & 0_{\omega\times|\mathcal{E}|} & \boldsymbol{B}\\ 0_{|\mathcal{E}|\times\omega} & \boldsymbol{I}_{|\mathcal{E}|\times|\mathcal{E}|} & \boldsymbol{C}\end{pmatrix}$$

where

$$\boldsymbol{C}=\begin{pmatrix} 1 & c_{22}^{-1}c_{12} & \cdots & c_{|\mathcal{E}||\mathcal{E}|}^{-1}c_{1|\mathcal{E}|}\\ 0 & 1 & \cdots & c_{|\mathcal{E}||\mathcal{E}|}^{-1}c_{2|\mathcal{E}|}\\ 0 & 0 & \cdots & \vdots\\ \vdots & \vdots & \cdots & \vdots\\ 0 & 0 & \cdots & 1\end{pmatrix}$$

We know that $M[\boldsymbol{A}]=M[A_1]$ from Lemma 3.

We use $\boldsymbol{A}^l$ to denote the lth column of $\boldsymbol{A}$ and assign the global coding vectors on the extended network $\tilde{\mathcal{G}}$ as follows. For each $d_i\in\mathrm{In}(s)$, let $\tilde{f}_{d_i}=\boldsymbol{A}^{f(d_i)}$. For each $e_j'\in\mathcal{E}'$, let $\tilde{f}_{e_j'}=\boldsymbol{A}^{f(e_j')}$, and for every real channel $e_j\in\mathcal{E}$, $\tilde{f}_{e_j}=\boldsymbol{A}^{f(e_j)}$. By condition (A3) of Definition 15, we obtain that for each edge $e_j\in\mathrm{Out}(i)$, there exist some scalar $k_{d,e_j}\in\mathcal{F}$ such that

$$\tilde{f}_{e_j}=\sum_{d\in\mathrm{In}(i)}k_{d,e_j}\tilde{f}_d+1_{e_j}$$

For any collection T of nonsource nodes with $C_T\geqslant\omega$ and each error pattern $\rho\in R(\delta_T)$, by condition (B) of Definition 15, the modified network $\mathcal{G}_\rho$ is a matroidal network associated with $\mathcal{M}^\rho=\mathcal{M}/\boldsymbol{B}_{\bar{\rho}}$. We know from Lemma 4 that $\mathcal{M}^\rho$ can be represented by matrix

$$\boldsymbol{A}(\rho)=\begin{pmatrix} \boldsymbol{I}_{\omega\times\omega} & 0_{\omega\times|\rho|} & \boldsymbol{B}\\ 0_{|\rho|\times\omega} & \boldsymbol{I}_{|\rho|\times|\rho|} & \boldsymbol{C}_\rho\end{pmatrix}$$

Here, $\boldsymbol{C}_\rho$ is the submatrix of $\boldsymbol{C}$ with the rows indexed by the elements of ρ'. Since the network-matroid mapping $f^\rho:\mathrm{In}(s)\cup\rho'\cup\mathcal{E}\to E(\mathcal{M}^\rho)$ is determined by

$$f^\rho(x)=f(x),\qquad \forall x\in\mathrm{In}(s)\cup\rho'\cup\mathcal{E},$$

then, for any channel e in $\mathcal{G}_\rho$, $\tilde{f}_e^\rho$ is the $f^\rho(e)$-th column of matrix $\boldsymbol{A}(\rho)$. According to the fact that

$$r_{\mathcal{M}_T^\rho}(f^\rho(\mathrm{In}(T)))=C_T$$

we get

$$\begin{aligned} r_{\mathcal{M}_T^\rho}(\tilde{F}_T^\rho)&=\dim(\langle\boldsymbol{\Phi}(T)\cup\Delta(T,\rho)\rangle)=C_T\\ &=\dim(\boldsymbol{\Phi}(T))+\dim(\Delta(T,\rho))\end{aligned}$$

Therefore,

$$\dim(\boldsymbol{\Phi}(T)\cap\Delta(T,\rho))=0.$$

Furthermore,

$$\boldsymbol{\Phi}(T)\cap\Delta(T,\rho)=\{0\},$$

and we obtain $d_{\min}^{(T)}>\delta_T=C_T-\omega$. By Lemma 1, we have

$$d_{\min}^{(T)}=C_T-\omega+1$$

Thus, the set $\{\tilde{f}_e:e\in\mathcal{E}\}$ is a scalar linear network error correction dispersion MDS code over $\mathcal{F}$.

Theorem 2 Let $\mathcal{G}=(\mathcal{V},\mathcal{E})$ be a single source acyclic network with information rate ω. Let $\mathcal{M}=(E,\mathcal{I})$ be an $\mathcal{F}$-representable matroid with $|E(\mathcal{M})|=\omega+2|\mathcal{E}|$ and $r(\mathcal{M})=\omega+|\mathcal{E}|$. $\mathcal{G}$ is a matroidal $\left\lfloor\frac{1}{2}d_{\min}^{(t)}-1\right\rfloor$ error correction network associated with $\mathcal{M}$ for every nonsource node t if and only if there exists a scalar linear network error correction broadcast MDS code over $\mathcal{F}$ on $\mathcal{G}$.

Theorem 3 Let $\mathcal{G}=(\mathcal{V},\mathcal{E})$ be a single source acyclic network with information rate ω. Let $\mathcal{M}=(E,\mathcal{I})$ be an $\mathcal{F}$-representable matroid with $|E(\mathcal{M})|=\omega+2|\mathcal{E}|$

and $r(\mathcal{M})=\omega+|\mathcal{E}|$. $\mathcal{G}$ is a matroidal $\left\lfloor \frac{1}{2} d_{\min}^{(t)} - 1 \right\rfloor$ error correction network associated with $\mathcal{M}$ for any nonsource node t with $C_t \geqslant \omega$ if and only if there exists a scalar linear network error correction multicast MDS code over $\mathcal{F}$ on $\mathcal{G}$.

Note 2. The proof of Theorem 2 and Theorem 3 is the same as Theorem 1 so long as replace the collection T of nonsource nodes by a nonsource node t, so the details are omitted.

3 Conclusion

In this paper, we establish the connections between LNEC and representable matroid. Exploiting the analogy between LNEC and representable matroid shown in the present paper, one might construct the demanded matroidal error correction network and the corresponding LNEC.

References

[1] Cai N, Yeung R W. Network coding and error correction [C] //*Proc IEEE Information Theory Workshop*. Bangalore: IEEE Press, 2002: 119-122.

[2] Yeung R W, Cai N. Network error correction, part Ⅰ: Basic concepts and upper bounds [J]. *Communications in Infomation and Systems*, 2006, **6**: 19-36.

[3] Cai N, Yeung R W. Network error correction, part Ⅱ: Lower bounds [J]. *Communications in Infomation and Systems*, 2006, **6**: 37- 54.

[4] Zhang Z. Linear network error correction codes in packet networks [J]. *IEEE TransInf Theory*, 2008, **54**(1): 209-218.

[5] Matsumoto R. Construction algorithm for network error -correcting codes attaining the singleton bound [J]. *IEICE Trans Fund*, E90-A, 2007, **9**: 1729-1735.

[6] Yang S, Yeung R W, Ngai C K. Refined coding bounds and code constructions for coherent network error correction [J]. *IEEE Trans Inf Theory*, 2011, **57**(3): 1409-1424.

[7] Guang X, Fu F W, Zhang Z. Construction of network error correction codes in packet networks [J]. *IEEE Trans Inf Theory*, 2013, **59**(2): 1030-1047.

[8] Guang X, Fu F W. Linear network error correction multicast/broadcast/dispersion codes [EB/OL]. [2013-02-18]. *http: //arXiv*: 1302.4146.

[9] Dougherty R, Freiling C, Zeger K. Networks, matroids, and non-shannon information inequalities [J]. *IEEE Trans Inf Theory*, 2007, **53**(6): 1949-1969.

[10] Dougherty R, Freiling C, Zeger K. Insufficiency of linear coding in networks information flow [J]. *IEEE Trans Inf Theory*, 2005, **51**(8): 2745-2759.

[11] Kim A, Medard M. Scalar-linear solvability of matroidal networks Associated with representable matroids [C]//*International Symposium on Turbo Codes and Iterative Information Processing*. Brest: IEEE Press, 2010: 452-456.

[12] Oxley J G. *Matroid Theory* [M]. New York: Oxford University Press, 1992.

[13] Koetter R, Medard M. An algebraic approach to network coding [J]. *IEEE/ACM Transon Networking*, 2003, **11**: 782- 795.

□