IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 7, 2016, accepted August 22, 2016, date of publication September 7, 2016, date of current version October 6, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2606608

Some Connections Between Classical Coding and Network Coding Over Erroneous Cyclic Networks

VAHID SAMADI-KHAFTARI[1], MORTEZA ESMAEILI[1,2], AND THOMAS AARON GULLIVER[2]
[1]Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran
[2]Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 2Y2, Canada

Corresponding author: T. A. Gulliver (agullive@ece.uvic.ca)

ABSTRACT Recently, a framework was given for linear error-correcting network codes (LENCs) over cyclic networks on commutative rings. When the alphabet is considered as a rational power series ring, an LENC is referred to as a convolutional error-correcting network code (CENC). Recently, a metric was introduced for these codes based on the minimum rank distance. In this paper, a new metric is introduced for ring-based LENCs over cyclic networks based on the Hamming distance, which is referred to as the network Hamming distance. Then, some connections between maximum distance separable (MDS) LENCs and classical MDS codes are obtained. Finally, the network Hamming free distance is given for CENCs, which plays the role of the free distance for convolutional codes.

INDEX TERMS Linear error-correcting network code, commutative ring, network Hamming distance, ML decoder, free distance.

I. INTRODUCTION

The channels of a point-to-point communication network are not in general error-free, and in practice they can be affected by different types of errors. As a result, error-correction network coding was introduced. This was first introduced for acyclic networks in [1]–[3], and the Hamming, Singleton and Gilbert-Varshamov bounds were extended from classical coding theory to network codes. It was assumed that the sinks know the topology of the network, so these codes are referred to as coherent network codes. There are two well-known frameworks which have been proposed for coherent network codes [4], [5].

A framework based on extended coding vectors was presented in [4]. The minimum rank distance was also introduced which plays the same role as the minimum Hamming distance in classical coding theory. In [5], the concept of Hamming distance from classical coding was extended to network codes over acyclic networks, which is referred to as network Hamming distance. The error correction capability of these codes was characterized in terms of this distance. It was shown that the network Hamming distance of a code is equal to its minimum rank distance. In these papers, the refined version of the Singleton bound was independently derived. A code attaining this bound with equality is referred to as maximum distance separable (MDS). Algorithms to construct MDS codes were proposed in [5] and [6].

The frameworks in [4] and [5] are restricted to acyclic networks and cannot be directly applied to cyclic networks. By changing the symbol alphabet from a field to a commutative ring such as a principal ideal domain (PID) or a discrete valuation ring (DVR), the framework in [4] has recently been extended from acyclic networks to cyclic networks [7]. The refined version of the Singleton bound was also given for ring-based codes over cyclic networks, and the existence of MDS codes was confirmed.

In general, the concept of time does not exist in a commutative ring, but in a rational power series ring over a finite field F, denoted by $F[(D)]$, D can play the role of time. A linear error-correcting network code (LENC) with alphabet $F[(D)]$ is referred to as a convolutional error-correcting network code (CENC). Similar to classical convolutional codes, a semi-infinite formulation for these codes was given in [4] using the concept of time. Based on this, the free distance for classical convolutional codes was extended to CENCs and is referred to as the rank free distance. Subsequently, the generalized Singleton bound was extended to these codes from classical convolutional codes.

In this paper, we focus on ring-based codes over cyclic networks. We first extend the concept of network Hamming distance from field-based LENCs over acyclic networks [5] to ring-based LENCs. Then we generalize the refined Singleton bound and the refined Hamming bound from classical

coding theory. We also establish some connections between classical coding theory and network codes. The concept of network Hamming free distance for CENCs is introduced as a generalization of classical free distance. Finally, we show that the network Hamming free distance of a code is equal to its rank free distance given in [7].

The rest of this paper is organized as follows. In Section 2, we provide some necessary background information and notation. In Section 3, the concept of network Hamming distance is extended to ring-based LENCs over cyclic networks. Then, we derive some bounds and properties of codes over cyclic networks using results from classical coding theory. The concept of network Hamming free distance for CENCs over cyclic networks is introduced in Section 4, and some properties of this distance are presented. Finally, a summary of the paper is given in Section 5.

II. BACKGROUND AND NOTATION

In this section, we provide the necessary background, notation and definitions from [7] that will be used in the remainder of the paper.

A. RING-BASED LENC FORMULATION

LENCs on cyclic networks over commutative rings [7] are formulated as follows. A DVR is a PID with a unique maximal ideal. A rational power series ring over a finite field F, denoted by $F[(D)]$, is a DVR with a unique maximal ideal $< D >$, where $< r >$ denotes the ideal generated by the element r in $F[(D)]$. A finite field F is a DVR with a unique maximal ideal $< 0 >$. These facts imply that field-based linear network coding on acyclic networks and convolutional network coding on cyclic networks can be considered as special cases of ring-based linear network coding on cyclic networks.

Consider a graph $G = (V, E)$, where V and E are the sets of nodes and edges, which represent the sets of nodes and channels of a network, respectively. Every edge is a transmission channel with capacity one and multiple channels between two nodes are allowed. The symbol alphabet is considered to be a PID P or DVR $\Re$. We assume that the network has only one source node denoted by s. The source node s has rate k which means it generates a message consisting of k symbols for transmission through the network per use of the network. The message is denoted by a vector $\mathbf{x}$ of size k. In general, the source node s has no incoming channels, but we use the concept of imaginary incoming channels for this node and assume that these imaginary channels send the message $\mathbf{x}$ to it. Hence, the source node s has imaginary incoming channels $d_1', d_2', \ldots, d_k'$, i.e. $In(s) = \{d_1', d_2', \ldots, d_k'\}$.

By a ring R, we mean a PID or a DVR. A k-dimensional R-based linear network code $C\left(k_{d,e}\right)$, or simply C, on a network is defined by $k_{d,e} \in R$ for each pair (d, e) of edges where $d \in E \cup In(s)$ and $e \in E$, with $k_{d,e} = 0$ if d and e are not adjacent, together with the assignment of a column vector $\mathbf{f}_e$ of size k over R to each edge e, called the *global encoding kernel* or *coding vector*, such that:

1. the set $\{\mathbf{f}_e, e \in In(s)\}$ forms a natural basis for the free module R^k, and
2. $\mathbf{f}_e = \sum_{d \in In(v)} k_{d,e}\mathbf{f}_d$ for every non-source node v and every edge $e \in Out(v)$ [8].

We refer to $k_{d,e}$ as the coding coefficient of pair (d, e). The matrix $\mathbf{K}_s = \left(k_{d,e}\right)_{d \in In(s), e \in E}$ is called the *local encoding matrix* at source s. The matrix $\mathbf{F}_C = \left(k_{d,e}\right)_{d,e \in E}$ is called the *transformation matrix* of the code $C\left(k_{d,e}\right)$. The two conditions can be combined as follows

$$(\mathbf{f}_e)_{e \in E} \det(\mathbf{I}_{|E|} - \mathbf{F}_C) = \mathbf{K}_s \mathrm{adj}(\mathbf{I}_{|E|} - \mathbf{F}_C). \tag{1}$$

The coding vectors for a given code are determined by solving the system of linear equations given by (1). The discriminant of the system is $\det(\mathbf{I}_{|E|} - \mathbf{F}_C)$. If the discriminant is zero, either no solution or multiple solutions exist. The code is said to be nonsingular if it has a nonzero discriminant. A nonsingular code is said to be normal if it has a unique set of coding vectors. In this case, matrices $\mathbf{G} := (\mathbf{f}_e)_{e \in E}$ and $\mathbf{G}_t := (\mathbf{f}_e)_{e \in In(t)}$ are referred to as the *information transformation matrix* and the *information transformation matrix* at sink t, respectively. For a message vector $\mathbf{x}$, the symbol y_e transmitted on an edge e and the received vector $\mathbf{y}_t$ at sink t are given by

$$y_e = \mathbf{x}\mathbf{f}_e, \quad \mathbf{y}_t = \mathbf{x}\mathbf{G}_t. \tag{2}$$

We can consider any nonsingular R-based linear network code as a normal Q-based linear network code, where Q denotes the quotient field of R. Further, any singular code can be normalized by multiplying the local encoding matrix $\mathbf{K}_s$ by $\det(\mathbf{I} - \mathbf{F}_C)$. By linear network code, we mean a normal linear network code.

Due to information looping, ring-based codes are not necessarily causal on cyclic networks. To solve this problem, causal DVR-based codes were introduced in [8]. Hereafter, let $\Re$ denote a DVR and q the uniformer in it, that is, the generator of the maximal ideal in $\Re$. The uniformer is unique up to a unit factor. In particular, when $\Re = F[(D)]$, we shall take q to be D. A delay function l on a network G is a nonnegative integer valued function defined over the set of adjacent pairs such that along every cycle there is at least one pair (d, e) with $l(d, e) > 0$. An $\Re$-based linear network code is said to be l-causal if the coding coefficient for every adjacent pair (d, e) is divisible by $q^{l(d,e)}$ [8, Definition 13].

A normal ring-based linear network code over a cyclic network is multicast when $\mathrm{rank}(\mathbf{G}_t) = k$ for every sink t with $\mathrm{maxflow}(t) \geq k$ [8]. An important property of these codes is that all components of a message vector transmitted through the network can be recovered from the received word at each sink. For a given multicast causal $\Re$-linear network code, the matrix $\mathbf{M}_t$ over $\Re$ is referred to as a *decoding matrix* at sink t with decoding delay δ_t when

$$\mathbf{G}_t \mathbf{M}_t = q^{\delta_t} \mathbf{I}_k, \tag{3}$$

where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix [8]. Let $\mathbf{x}$ be a message vector and $\mathbf{y}_t$ the corresponding received vector. Every sink t decodes $\mathbf{y}_t$ using $q^{\delta_t}\mathbf{x} = \mathbf{y}_t\mathbf{M}_t$.

Until now, the channels have been considered to be error free, but in practical networks, channels may create errors in the transmitted data. After transmission over a noisy channel e, the channel output is $\tilde{y}_e = y_e + z_e$, where y_e is the channel input and $z_e \in F$ is the channel error. However, when multiple channels create errors, the transmission model is not simple. Let $\mathbf{z} := (z_i : i \in E)$ be a row vector of size $|E|$ with $z_i \in R$ for all $i \in E$. The vector $\mathbf{z}$ is called the error vector. An erroneous symbol on edge e can be determined using the corresponding error coding vector which is denoted by $\mathbf{g}_e$ [7].

In [7], it was shown that if C is a normal code, then the error coding vectors can be determined uniquely as $[\mathbf{g}_e]_{e\in E} = (\mathbf{I}_{|E|} - \mathbf{F}_C)^{-1}$. We call $\mathbf{E}_t := (\mathbf{g}_e : e \in \mathrm{In}(t))$ the *error transformation matrix at sink t*. If a message vector $\mathbf{x}$ is transmitted through the network and an error vector $\mathbf{z}$ occurs, then the corresponding received symbol over a channel e is $r_e(\mathbf{x}, \mathbf{z}) = \mathbf{x}\mathbf{f}_e + \mathbf{z}\mathbf{g}_e$. The received vector at sink t is then $\mathbf{r}_t(\mathbf{x}, \mathbf{z}) = \mathbf{x}\mathbf{G}_t + \mathbf{z}\mathbf{E}_t$. The reader is referred to [7] for details on linear error-correcting network codes.

III. NETWORK HAMMING DISTANCE OF LENCs OVER CYCLIC NETWORKS

The network version of the Hamming distance was given in [5] for field-based LENCs over acyclic networks. In this section, we first extend the network Hamming distance to ring-based LENCs over cyclic networks. Then, we derive some fundamental properties of these codes using results from classical coding theory.

A classical $[n, k]$ linear code of length n and dimension k over a field F is a k-dimensional subspace of F^n. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ be vectors of size n. The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is the number of positions in which they differ. The Hamming weight of $\mathbf{x}$ is the number of its nonzero components and is denoted by $w(x)$. The minimum Hamming distance of a classical $[n, k]$ linear code is the minimum Hamming weight among its nonzero codewords. An $[n, k]$ code of minimum distance d^H_{min} is denoted as $[n, k, d^H_{min}]$. It is well-known that $d^H_{min} \leq n - k + 1$. This is called the Singleton bound.

A. NETWORK HAMMING DISTANCE

Let C be a k-dimensional ring-based LENC over a network with information transformation matrix $\mathbf{G}_t$ at sink t. The codeword space at sink t is defined as $C_t = \{\mathbf{x}\mathbf{G}_t : \mathbf{x} \in R^k\}$. Let $\mathbf{r}_t$ denote a received word at sink t, and let $\phi_t(\mathbf{r}_t) = \{\mathbf{z} : \mathbf{z}\mathbf{E}_t = \mathbf{r}_t\}$. By a ring we mean a PID or a DVR.

Definition 1: For a given ring-based LENC over a network, we have the following.

1) The received network Hamming weight of a received word $\mathbf{r}_t$ at a sink t is defined as $w^R_t(\mathbf{r}_t) = \min_{\mathbf{z}\in\phi_t(\mathbf{r}_t)} w(\mathbf{z})$. The received network Hamming distance between two received words $\mathbf{r}_t$ and $\mathbf{r'}_t$ at a sink t is defined as $D^R_t(\mathbf{r}_t, \mathbf{r'}_t) = w^R_t(\mathbf{r}_t - \mathbf{r}'_t)$.
2) The message network Hamming weight of a message word $\mathbf{x}$ at a sink t is defined as $w^M_t(\mathbf{x}) = w^R_t(\mathbf{x}\mathbf{G}_t)$. The message network Hamming distance between two message words $\mathbf{x}$ and $\mathbf{x}'$ at a sink t is defined as $D^M_t(\mathbf{x}, \mathbf{x}') = w^M_t(\mathbf{x} - \mathbf{x}')$.

We now define the minimum Hamming distance of a ring-based LENC.

Definition 2: The minimum network Hamming distance of a ring-based LENC C at a sink t is defined as $d^N_{min,t} := \min_{\mathbf{x}_1\neq\mathbf{x}_2} D^M_t(\mathbf{x}_1, \mathbf{x}_2) := \min_{\mathbf{y}_1\neq\mathbf{y}_2\in C_t} D^R_t(\mathbf{y}_1, \mathbf{y}_2)$.

Since C_t, the codeword space of a LENC C at sink t, is a linear space, we always have that $d^N_{min,t} = \min_{\mathbf{0}\neq\mathbf{y}_t\in C_t} w^R_t(\mathbf{y}_t) = \min_{\mathbf{0}\neq\mathbf{x}} w^M_t(\mathbf{x})$. Similar to [5], we can define the minimum network Hamming distance decoder as follows. The decoder maps a received word $\mathbf{r}_t$ to codeword $\hat{\mathbf{y}}_t \in C_t$ by the function defined as $\hat{\mathbf{y}}_t := \arg\max_{\mathbf{y}_t\in C_t} D^R_t(\mathbf{r}_t, \mathbf{y}_t)$. The error correction capability of an LENC can be interpreted in terms of its minimum distance. In fact, an LENC at a sink t can correct any error vector z with $w^R_t(\mathbf{z}\mathbf{E}_t) \leq \frac{d^N_{min,t}-1}{2}$. The proof of this fact is similar to that in [5] and so is omitted.

B. UPPER BOUNDS FOR RING-BASED LENCs OVER CYCLIC NETWORKS

Let C be a normal k-dimensional R-based LENC over a network. Recall that the codeword space at sink t is $C_t = \{\mathbf{x}\mathbf{G}_t : \mathbf{x} \in R^k\}$. Since the code is normal, i.e. $rank_t(\mathbf{G}_t) = n_t$, we can also consider C_t as a classical $[n_t, k]$ linear error-correcting code. We denote the minimum network Hamming distance and the minimum Hamming distance of C_t by $d^N_{min,t}$ and $d^H_{min,t}$, respectively. If $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$, then we denote the vector $(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n)$ by $(\mathbf{x}, \mathbf{y})$. Hereafter by saying a LENC, we mean a normal LENC.

Theorem 1: Let P denote a PID. For a given k-dimensional multicast P-based LENC over a network, we have for every sink t

$$d^N_{min,t} \leq d^H_{min,t}. \tag{4}$$

Proof: It suffices to consider the statement for a field because every P-based linear network code can be considered as a Q-based linear network code. Assume that the incoming edges of a sink t are labelled from 1 to n_t and the other edges are labelled from n_t+1 to $|E|$. Hence, there exists a codeword $\mathbf{y}_t = (y_i : i \in In(t))$ of weight $d^H_{min,t}$ in C_t. Now suppose that the zero message vector is transmitted from the source and the error vector $\mathbf{z} = (\mathbf{y}_t, \mathbf{0})$ occurs, where $\mathbf{0}$ denotes the zero vector of length $|E| - n_t$. Then an edge $i \in In(t)$ may be affected by the error symbol y_i and the other edges are error-free. Since C is a linear network code and any edge which is not in $In(t)$ is error-free, the edge $i \in In(t)$ receives a zero symbol as the input. On the other hand, since there is no intermediate node between edge i and sink t, edge i transmits

the corresponding error symbol y_i to sink t. Hence, sink t receives the vector $\mathbf{y}_t = (y_i : i \in In(t))$, i.e. the effect of the error vector $\mathbf{z}$ at sink t is $\mathbf{y}_t$, so then $\mathbf{zE}_t = \mathbf{y}_t$ and therefore $\mathbf{z} \in \phi_t(\mathbf{y}_t)$. This implies that $d^N_{min,t} \leq w^R_t(\mathbf{y}_t) \leq w(\mathbf{z}) = d^H_{min,t}$. □

In the following, the refined Singleton bound for ring-based LENCs over cyclic networks is given. The proof is similar to that in [7] and so is omitted.

Theorem 2: For a given multicast PID-based LENC, $\mathrm{d}^N_{min,t} \leq n_t - k + 1$ for every sink t with maxflow$(t) \geq k$.

We refer to codes attaining the refined Singleton bound with equality as *maximum distance separable* (MDS). Ring-based MDS LENCs were characterized in [7]. It was also shown that a ring-based MDS LENC exists over a given cyclic network if the symbol alphabet is sufficiently large.

Theorem 3: Let C be a multicast PID-based LENC over a network. If C is an MDS LENC, then C_t is a classical MDS code for every sink t.

Proof: Since C is an MDS LENC, we have that $\mathrm{d}^N_{min,t} = n_t - k + 1$. Inequality (4) implies that $\mathrm{d}^H_{min,t} \geq n_t - k + 1$. On the other hand, we have $\mathrm{d}^H_{min,t} \leq n_t - k + 1$ from the Singleton bound. These facts imply that $\mathrm{d}^H_{min,t} = n_t - k + 1$. □

The following corollary follows from classical coding theory and Theorem 3.

Corollary 1: Let C be a multicast PID-based LENC over a network with information transformation matrix $\mathbf{G}_t$ at a sink t. If C is an MDS LENC, then every k columns of $\mathbf{G}_t$ are linearly independent for every sink t.

It can easily be shown that the converse of the above theorem is not true.

Example 1: Consider the field $F_4 = \{0, 1, \alpha, \alpha^2\}$ where α is a root of the primitive polynomial $p(x) = x^2 + x + 1$ over F_2. The $[3, 1, 3]$ code C over F_4 with generator polynomial $g(x) = (x + \alpha)(x + \alpha^2) = x^2 + x + 1$ is a Reed-Solomon (RS) code and the corresponding generator matrix is $\mathbf{G} = [1\ 1\ 1]$.

Let $\mathcal{C}$ be an F_4-LENC on the network $\mathcal{N}$ depicted in Figure 1, with all coding coefficients equal to 1. The corresponding information transformation matrix at sink t, $\mathbf{G}_t$, is equal to G. It can easily be determined that $\mathbf{g}_{e_6} = (10000000)$, $\mathbf{g}_{e_7} = (11011010)$, and $\mathbf{g}_{e_8} = (00100000)$. From Theorem 2, we have that $d^N_{min,t} \leq n_t - k + 1 = 3$. In the following, we show that there exists an error pattern of weight one which cannot be corrected by sink t. This implies that the code $\mathcal{C}$ is not MDS.

Suppose that the zero word $\mathbf{0}$ is transmitted through the network and the error vector $\mathbf{z} = (10000000)$ matching the error pattern $\rho = \{e_1\}$ occurs. The corresponding received word is $[1\ 1\ 0]$. Sink t decodes the received word using the minimum rank distance decoding algorithm given in [4]. For any error pattern, the decoder solves the corresponding decoding problem and then if all solvable error patterns correspond to the same message, the decoder claims that the received word is correctable and gives this message as the output.

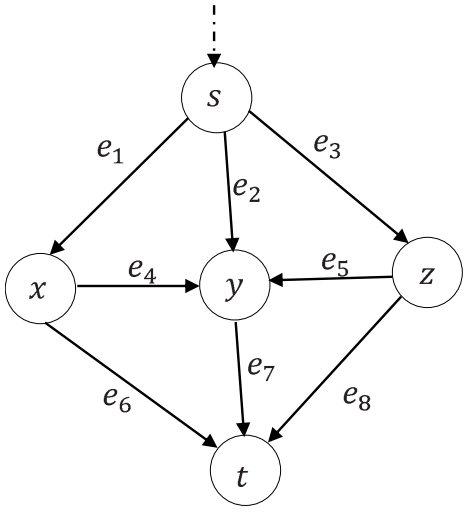

FIGURE 1. An acyclic network $\mathcal{N}$ with sink t.

Now, suppose that the decoder has selected the error pattern $\rho_1 = \{e_3\}$. The corresponding decoding equation is $(x, z_3)\mathbf{G}^{\rho_1}_t = (1\ 1\ 0)$, where $\mathbf{G}^{\rho_1}_t = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. The solution of this equation is $(1, 1)$, while the correct message is 0, so the error pattern is $\rho_1 = \{e_1\}$, or equivalently the received word $(1\ 1\ 0)$ cannot be corrected by the decoder at sink t, which implies that the code $\mathcal{C}$ at sink t is not an MDS LENC.

In [5], an algorithm was proposed to construct MDS LENCs over acyclic networks from classical MDS codes. Extending this algorithm to cyclic networks is left as an open problem. We now give the refined version of the Hamming bound for cyclic networks. Recall that if C denotes a k-dimensional LENC, then the codeword space at sink t is $C_t = \{\mathbf{xG}_t : \mathbf{x} \in R^k\}$. Let $|C_t|$ denote the cardinality of the set C_t.

Theorem 4: Let C be a multicast k-dimensional LENC over a cyclic network on the finite field F of size q. For every sink t, we have

$$|C_t| \leq \frac{q^{n_t}}{\sum_{i=0}^{r^N_{min,t}} \binom{n_t}{i} (q-1)^i},$$

where $r^N_{min,t} = \left\lfloor \frac{d^N_{min,t} - 1}{2} \right\rfloor$.

Proof: Since C_t is a multicast code, it can be considered as an $\left[n_t, k, d^H_{min,t}\right]$ classical code. Then from the classical Hamming bound we have

$$|C_t| \leq \frac{q^{n_t}}{\sum_{i=0}^{r^H_{min,t}} \binom{n_t}{i} (q-1)^i},$$

where $r^H_{min,t} = \left\lfloor \frac{d^H_{min,t} - 1}{2} \right\rfloor$. On the other hand, from Theorem 4 we have $d^N_{min,t} \leq d^H_{min,t}$, so that $r^N_{min,t} \leq r^H_{min,t}$,

which implies

$$|C_t| \leq \frac{q^{n_t}}{\sum_{i=0}^{r^H_{min,t}} \binom{n_t}{i}(q-1)^i} \leq \frac{q^{n_t}}{\sum_{i=0}^{r^N_{min,t}} \binom{n_t}{i}(q-1)^i}.$$

□

A PID which is not a field has infinite size, so in this case Theorem 4 clearly holds for PIDs.

IV. NETWORK HAMMING DISTANCE FOR CONVOLUTIONAL ERROR-CORRECTING NETWORK CODES

When rational power series rings are considered as symbol alphabets, LENCs are referred to as convolutional error-correcting network codes (CENCs). The rational power series ring over a finite field F, denoted by $F[(D)]$, is the set of all rational functions of the form $\frac{p(D)}{1+q(D)}$ where $p(D)$ and $q(D)$ are finite polynomials over F. In general, there is no concept of time in commutative rings, but in a ring $F[(D)]$, D is a dummy variable which can be used to denote a unit delay. In [7], a semi-infinite formulation was presented for CENCs using the concept of time. With this formulation, the concept of rank free distance was introduced for CENCs which plays the role of the free distance in classical convolutional codes. In this section, the concept of network Hamming free distance for CENCs is derived as a generalization of the free distance. We then obtain some properties of this distance. In particular, we show that the rank free distance of a code is equal to its network Hamming free distance.

A. NETWORK HAMMING FREE DISTANCE AND ITS PROPERTIES

The coding coefficients of a CENC are generally of the form $\frac{p[D]}{q[D]}$, but one can assume they have a polynomial form, as without loss of generality, all coding coefficients can be multiplied by their least common multiple. By a CENC C, we mean a normal code with polynomial information transformation matrices for all sinks.

We can write $\mathbf{G}_t = (g_{i,j}(D))_{k\times n_t}$, where $g_{i,j}(D)$ is a finite polynomial. Then $\mathbf{G}_t(D) = \sum_{j=0}^{j=m} \mathbf{G}_{t,j}D^j$, where $\mathbf{G}_{t,j}$ is called the information transformation matrix of sink t at time index j. Any element of the rational power series $F[(D)]$ can be expressed as $\sum_{j\geq 0} a_j D^j$, where $a_j \in F$ [7]. Then the error transform matrix at sink t can be written as $\mathbf{E}_t(D) = \sum_{j\geq 0} \mathbf{E}_{t,j}D^j$, where $\mathbf{E}_{t,j}$ is the error transformation matrix of sink t at time index j.

The semi-infinite matrix representation of $\mathbf{G}_t(D)$ is given by

$$\bar{\mathbf{G}}_t := \begin{pmatrix} \mathbf{G}_{t,0} & \mathbf{G}_{t,1} & \cdots & \mathbf{G}_{t,m} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_{t,0} & \mathbf{G}_{t,1} & \cdots & \mathbf{G}_{t,m} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{G}_{t,0} & \mathbf{G}_{t,1} & \cdots & \mathbf{G}_{t,m} & \mathbf{0} \\ & & & \ddots & \ddots & & \ddots \end{pmatrix}, \tag{5}$$

and the semi-infinite representation of $\mathbf{E}_t(D)$ is

$$\bar{\mathbf{E}}_t := \begin{pmatrix} \mathbf{E}_{t,0} & \mathbf{E}_{t,1} & \cdots & \mathbf{E}_{t,n} & \mathbf{E}_{t,n+1} & \cdots \\ \mathbf{0} & \mathbf{E}_{t,0} & \cdots & \mathbf{E}_{t,n-1} & \mathbf{E}_{t,n} & \cdots \\ \mathbf{0} & \mathbf{0} & & \mathbf{E}_{t,n-2} & \mathbf{E}_{t,n-1} & \\ \vdots & & \ddots & \vdots & & \ddots \end{pmatrix}.$$

Let $\bar{\mathbf{x}} := (\mathbf{x}_0, \mathbf{x}_1, \ldots)$ and $\bar{\mathbf{z}} := (\mathbf{z}_0, \mathbf{z}_1, \ldots)$, where $\mathbf{x}_j = (x_{1,j}, \ldots, x_{k,j})$ and $\mathbf{z}_j = (z_{1,j}, \ldots, z_{|E|+k,j})$ are the message and error vectors at time index j, respectively. The received word at sink t is $\bar{\mathbf{r}}_t(\bar{\mathbf{x}}, \bar{\mathbf{z}}) = \bar{\mathbf{x}}\bar{\mathbf{G}}_t + \bar{\mathbf{z}}\bar{\mathbf{E}}_t$, where $\bar{\mathbf{r}}_t$ is the semi-infinite representation of the received word.

In theory, the coded sequences of CENCs have infinite length, but in practical applications finite sequences are employed. In the following, we formulate the truncated form of CENCs over cyclic networks. Corresponding to $\bar{\mathbf{x}}$ and $\bar{\mathbf{z}}$, we have $\bar{\mathbf{x}}[n] := (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ and $\bar{\mathbf{z}}[n] := (\mathbf{z}_1, \ldots, \mathbf{z}_n)$, and for $\bar{\mathbf{G}}_t$ and $\bar{\mathbf{E}}_t$ define

$$\bar{\mathbf{G}}[n] := \begin{pmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \ldots & \mathbf{G}_n \\ \mathbf{0} & \mathbf{G}_0 & \ddots & \mathbf{G}_{n-1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{G}_0 \end{pmatrix}, \tag{6}$$

$$\bar{\mathbf{E}}[n] := \begin{pmatrix} \mathbf{E}_0 & \mathbf{E}_1 & \ldots & \mathbf{E}_n \\ \mathbf{0} & \mathbf{E}_0 & \ddots & \mathbf{E}_{n-1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{E}_0 \end{pmatrix}. \tag{7}$$

A received word from time index 0 to time index n is given by $\bar{\mathbf{r}}_t(\bar{\mathbf{x}}[n], \bar{\mathbf{z}}[n]) = \bar{\mathbf{x}}[n]\bar{\mathbf{G}}_t[n] + \bar{\mathbf{z}}[n]\bar{\mathbf{E}}_t[n]$.

Define $\phi_t(\bar{\mathbf{r}}_t) := \{\bar{\mathbf{z}} : \bar{\mathbf{z}}\bar{\mathbf{E}}_t = \bar{\mathbf{r}}_t\}$ and $\phi_t(\bar{\mathbf{r}}_t[n]) := \{\bar{\mathbf{z}}[n] := \bar{\mathbf{z}}[n]\bar{\mathbf{E}}_t[n] = \bar{\mathbf{r}}_t[n]\}$, where $\bar{\mathbf{r}}_t$ is the received word at sink t. The generalized received Hamming weight of a received word $\bar{\mathbf{r}}_t$ at sink t is defined as $w_t^{GR}(\bar{\mathbf{r}}_t) = \min_{\bar{\mathbf{z}}\in\phi_t(\bar{\mathbf{r}}_t)} w(\bar{\mathbf{z}})$. Similarly, we can define the generalized message network Hamming weight, the generalized message network Hamming distance, and the generalized received network Hamming distance at sink t by $w_t^{GM}(.)$, $D_t^{GM}(.,.)$, and $D_t^{GR}(.,.)$, respectively.

Definition 3: For a CENC over a network we have the following.

1) The network Hamming free distance of the code at a sink t is defined as
$$d^{GN}_{free,t} := \min_{\bar{\mathbf{y}}_1\neq\bar{\mathbf{y}}_2\in\bar{C}_t} D_t^{GR}(\bar{\mathbf{y}}_1, \bar{\mathbf{y}}_2) := \min_{\bar{\mathbf{0}}\neq\bar{\mathbf{y}}_t\in\bar{C}_t} w_t^{GR}(\bar{\mathbf{y}}_t).$$

2) The minimum generalized network Hamming distance of the code at a sink t of order n is defined as
$$d^{GN}_{min,t}[n] := \min_{\bar{\mathbf{y}}_1[n]\neq\bar{\mathbf{y}}_2[n]\in\bar{C}} D_t^{GR}(\bar{\mathbf{y}}_1[n], \bar{\mathbf{y}}_2[n]) := \min_{\bar{\mathbf{0}}\neq\bar{\mathbf{y}}_t[n]\in\bar{C}_t[n]} w_t^{GR}(\bar{\mathbf{y}}_t[n]).$$

The minimum Hamming distance decoder at a sink t maps a received word $\bar{\mathbf{r}}_t$ to the codeword $\hat{\bar{\mathbf{y}}}_t \in \bar{C}_t$ defined

as $\hat{\bar{y}}_t := \arg\max_{\bar{\mathbf{y}}_t \in \bar{C}_t} D_t^{GR}(\bar{\mathbf{r}}_t, \bar{\mathbf{y}}_t)$. Similarly, we can define the minimum distance decoder of order n at sink t as $\hat{\bar{\mathbf{y}}}_t[n] := \arg\max_{\bar{\mathbf{y}}_t[n] \in \bar{C}_t[n]} D_t^{GR}(\bar{\mathbf{r}}_t[n], \bar{\mathbf{y}}_t[n])$. The error correction capability of a code can be interpreted in terms of its free distance. In fact, a code at sink t can correct any error vector $\bar{\mathbf{z}}$ with $w_t^{GR}(\bar{\mathbf{z}}\bar{\mathbf{E}}_t) \leq \frac{d_{free,t}^{GN}-1}{2}$. The proof is similar to that in [5] and so is omitted.

Let $d_{min,t}^{H}[n]$ denote the minimum Hamming distance of the code at a sink t of order n. We then have the following theorem.

Theorem 5: For a given CENC over a cyclic network we have:

1) $d_{min,t}^{GN}[n] \leq d_{min,t}^{GN}[n+1]$,
2) $d_{min,t}^{GN}[n] \leq d_{min,t}^{H}[n]$,
3) the sequence $d_{min,t}^{GN}[n]$ is upper bounded, and
4) $d_{min,t}^{GN}[n]$ does not change when n is increased.

Proof:

1) It follows from Definition 3 that there exists a codeword $\bar{\mathbf{y}}_t$ such that $w_t^{GR}(\bar{\mathbf{y}}_t[n+1]) = d_{min,t}^{GN}[n+1]$. Hence, there exists an error vector $\bar{\mathbf{z}}$ such that $w(\bar{\mathbf{z}}[n+1]) = d_{min,t}^{GN}[n+1]$ and $\bar{\mathbf{z}}[n+1]\bar{\mathbf{E}}_t[n+1] = \bar{\mathbf{y}}_t[n+1]$. It is obvious that $\bar{\mathbf{z}}[n]\bar{\mathbf{E}}_t[n] = \bar{\mathbf{y}}_t[n]$, so $w_t^{GR}(\bar{\mathbf{y}}_t[n]) \leq w(\bar{\mathbf{z}}[n]) \leq d_{min,t}^{GN}[n+1]$. Therefore, $d_{min,t}^{GN}[n] \leq d_{min,t}^{GN}[n+1]$.
2) The proof is similar to that of Theorem 1 and so is omitted.
3) The proof follows from 2) and the fact that $d_{min,t}^{H}[n]$ is upper bounded [9, Th. 3.2].
4) This follows from 1) and 3). □

In [7], the concept of minimum rank free distance was introduced for CENCs over cyclic networks. Let $\bar{\rho}_j$ denote the set of all erroneous edges e_j at time index j. The set $\bar{\rho} = \cup_{j\geq 1}\rho^j$ is called the generalized error pattern. Define $W_t(\bar{\rho}) = \{\bar{\mathbf{r}}_t(\bar{\mathbf{0}}, \bar{\mathbf{z}}) : \bar{\mathbf{z}} \in \bar{\rho}^*\}$ where $\bar{\rho}^*$ is the set of all error vectors matching error pattern $\bar{\rho}$, and define $\bar{rank}_t(\bar{\rho}) = rank(W_t(\bar{\rho}))$. The rank free distance of a CENC at a sink t is defined as $d_{free,t} = \min\{|\bar{\rho}| : W_t(\bar{\rho}) \cap \bar{C}_t \neq \emptyset\}$. These definitions can be extended to truncated CENCs. Denote the minimum generalized rank distance of a code at a sink t of order n by $d_{min,t}[n]$.

Theorem 6: Let C be a CENC over a network G. Then $d_{free,t}^{GN} = d_{free,t}$ for every sink t, and $d_{min,t}^{GN}[n] = d_{min,t}[n]$ for every sink t.

Proof: It follows from Definition 3 that there exists a codeword $\bar{\mathbf{y}}_t$ such that $w_t^{GR}H(\bar{\mathbf{y}}_t) = d_{free,t}^{GN}$, so there exists an error vector $\bar{\mathbf{z}}$ with $w(\bar{\mathbf{z}}) = d_{free,t}^{GN}$ such that $\bar{\mathbf{z}}\bar{\mathbf{E}}_t = \bar{\mathbf{y}}_t$. Let $\bar{\rho}$ be the error pattern of weight $d_{free,t}^{GN}$ matching the error vector $\bar{\mathbf{z}}$. It is obvious that $\bar{W}_t(\bar{\rho}) \cap \bar{C}_t \neq \emptyset$, so $d_{free,t} \leq |\bar{rank}_t(\bar{\rho})|$. We have $\bar{rank}_t(\bar{\rho}) \leq d_{free,t}^{GN}$, and therefore $d_{free,t} \leq d_{free,t}^{GN}$. Then there exists an error pattern $\bar{\rho}$ with $\bar{rank}_t(\bar{\rho}) = |\bar{\rho}| = d_{free,t}$ such that $\bar{W}_t(\rho) \cap \bar{C}_t \neq \emptyset$. Hence, there exist a codeword $\bar{\mathbf{y}}_t \in \bar{C}_t$ and an error vector $\bar{\mathbf{z}}$ matching the error pattern $\bar{\rho}$ such that $\bar{\mathbf{y}}_t = \bar{\mathbf{z}}\bar{\mathbf{E}}_t$. Thus, $d_{free,t}^{GN} \leq w_t^{GR}(\bar{\mathbf{y}}_t) \leq w(\bar{\mathbf{z}}) = d_{free,t}$, which completes the proof of the first part. The proof of the second part is similar to that of the first, and so is omitted. □

V. SUMMARY

The focus of this paper was on ring-based LENCs over cyclic networks. In [7], a metric was introduced for these codes based on the minimum rank distance given in [4]. The network Hamming distance for field-based codes over acyclic networks given in [5] was extended to ring-based codes over cyclic networks. Further, the Hamming bound was extended from classical codes to field-based codes over cyclic networks. It was shown that if C is an MDS network code, then C_t is a classical MDS code at each sink. The Hamming free distance for CENCs was presented as a generalization of the free distance of classical convolutional codes. Finally, it was proven that the rank free distance of a code is equal to its network Hamming free distance.

REFERENCES

[1] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. IEEE Int. Theory Workshop*, Oct. 2002, pp. 119–122.
[2] R. W. Yeung and N. Cai, "Network error-correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.
[3] N. Cai and R. W. Yeung, "Network error-correcting, part II: Lower bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.
[4] Z. Zhang, "Linear network error correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 209–218, Jan. 2008.
[5] S. Yang, R. W. Yeung, and C. K. Ngai, "Refined coding bounds and code constructions for coherent network error correction," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1409–1424, Mar. 2011.
[6] X. Guang, F.-W. Fu, and Z. Zhang, "Construction of network error-correction codes in packet networks," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1030–1047, Feb. 2011.
[7] V. Samadi and M. Esmaeili, "Ring-based linear network coding on erroneous cyclic networks," *IET Commun.*, doi: 10.1049/iet-com.2015.1224
[8] S.-Y. R. Li and Q. T. Sun, "Network coding via commutative algebra," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 403–415, Jan. 2011.
[9] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*, 2nd ed. New York, NY, USA: Wiley, Jun. 2015.

VAHID SAMADI-KHAFTARI received the B.E. degree in pure mathematics from Shiraz University, Shiraz, Iran, in 2008, and the M.Sc. degree in applied mathematics from Amirkabir University of Technology, Tehran, Iran, in 2010. He is currently pursuing the Ph.D. degree at Isfahan University of Technology, Isfahan, Iran. His research interests are in the areas of error-correcting network coding, space time coding, and commutative algebra.

MORTEZA ESMAEILI received the M.S. degree in mathematics from the Teacher Training University of Tehran, Iran, in 1988, and the Ph.D. degree in mathematics (coding theory) from Carleton University, Ottawa, Canada, in 1996. He was a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. Since 1998, he has been with the Department of Mathematical Sciences at Isfahan University of Technology, Isfahan, Iran, where he is currently a Professor. He joined the Department of Electrical and Computer Engineering, University of Victoria, Victoria, B.C., Canada, as an Adjunct Professor in 2009. His current research interests include coding and information theory, cryptography, and combinatorics and its application to communication theory.

THOMAS AARON GULLIVER received the Ph.D. degree in electrical engineering from the University of Victoria, Victoria, BC, Canada, in 1989. From 1989 to 1991, he was employed at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic appointments at Carleton University, Ottawa, ON, Canada, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999, where he is currently a Professor with the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada. In 2012, he was elected a Fellow of the Canadian Academy of Engineering. From 2000 to 2003 he was a Secretary and a member of the Board of Governors of the IEEE Information Theory Society. He is currently an Area Editor of the IEEE TRANSACTIONS on WIRELESS COMMUNICATIONS. His research interests include information theory and communication theory, algebraic coding theory, multicarrier systems, smart grid, and security.