Network Coding, Algebraic Coding, and Network Error Correction

Raymond W. Yeung
Network Coding Research Centre
The Chinese University of Hong Kong
N.T., Hong Kong
Email: whyeung@ie.cuhk.edu.hk

Ning Cai
Department of Information Engineering
The Chinese University of Hong Kong
N.T., Hong Kong
Email: cai@mathematik.uni-bielefeld.de

***Abstract*— This paper discusses the relation between network coding, (classical) algebraic coding, and network error correction. In the first part, we clarify the relation between network coding and algebraic coding. By showing that the Singleton bound in algebraic coding theory is a special case of the Max-flow Min-cut bound in network coding theory, we formally establish that linear multicast and its stronger versions are network generalizations of a maximum distance separation (MDS) code. In the second part, we first give an overview of network error correction, a paradigm for error correction on networks which can be regarded as an extension of classical point-to-point error correction. Then by means of an example, we show that an upper bound in terms of classical error-correcting codes is not tight even for a simple class of networks called *regular networks*. This illustrates the complexity involved in the construction of network error-correcting codes.**

I. Introduction

The concept of *network coding* was introduced for satellite communication networks in [2] and fully developed in [3], where in the latter the term "network coding" was coined and the advantage of network coding over routing was demonstrated. The main result in [3], namely a characterization of the maximum rate at which information generated at a single source node can be multicast, can be regarded as the Max-flow Min-cut theorem for network information flow. An algorithm for constructing linear network codes that achieve the Max-flow Min-cut bound was devised in [5]. Subsequently, a more transparent proof for the existence of such linear network codes was given in [6]. For further references on the subject, we refer the reader to the Network Coding Homepage [10] and the tutorial [7].

Inspired by network coding, network error correction has been introduced in [4] as a paradigm for error correction on networks which can be regarded as an extension of classical point-to-point error correction. Specifically, the results in [4] [8] [9] are network generalizations of the fundamental bounds in classical algebraic coding theory. In this paper, we discuss the relation between network coding, algebraic coding, and network error correction.

The rest of the paper is organized as follows. In Section II, we first establish that a linear network code achieving the Max-flow Min-cut bound is a network generalization of a maximum distance separation (MDS) code in classical algebraic coding [1]. This clarifies the relation between network coding and classical algebraic coding. In Section III, upon giving an overview of network error correction, we illustrate the complexity involved in the construction of network error-correcting codes by means of an example. Concluding remarks are in Section IV.

II. The Singleton Bound and MDS Codes

Consider the network in Fig. 1. In this network, there are three layers of nodes. The top layer consists of the source node s, the middle layer consists of n nodes each connecting to node s, and the bottom layer consists of $\binom{n}{r}$ nodes each connecting to a distinct subset of r nodes on the middle layer. We call this network an $\binom{n}{r}$ *combination network*, or simply an $\binom{n}{r}$ network, where $1 \leq r \leq n$.

Assume that a message consisting of k information symbols taken from a finite field F is generated at the source node s, and each channel can transmit one symbol in F in the specified direction. A linear

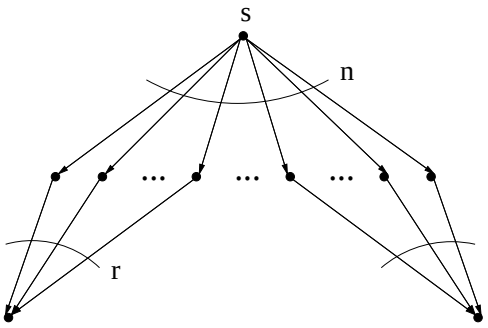

Fig. 1. An $\binom{n}{r}$ combination network.

network code on a given network is qualified as a *linear multicast* [7] if for all non-source node T in the network, if

$$\text{maxflow}(T) \geq k, \tag{1}$$

then node T can decode the source message. Note that by the Max-flow Min-cut theorem, (1) is a necessary condition for any node T to be able to decode the source message. In [7], linear broadcast, linear dispersion, and generic linear network code are also defined as linear network codes possessing stronger properties than linear multicast. These stronger linear network codes are useful for various applications.

Consider a classical (n, k) linear block code with *minimum distance* d and regard it as a linear network code on the $\binom{n}{n-d+1}$ network. Specifically, the code takes the source message as input and outputs n symbols, each being transmitted on one of the n outgoing channels of node s. For each node on the middle layer, since there is only one input channel, we assume without loss of generality that the symbol received is replicated and transmitted on each outgoing channel.

Since the (n, k) code has minimum distance d, by accessing a subset of $n - d + 1$ of the nodes on the middle layer (corresponding to $d - 1$ erasures), each node T on the bottom layer can decode the source message. From the foregoing, by the Max-flow Min-cut theorem,

$$\text{maxflow}(T) \geq k. \tag{2}$$

Since

$$\text{maxflow}(T) = n - d + 1,$$

it follows that

$$k \leq n - d + 1,$$

or

$$d \leq n - k + 1, \tag{3}$$

which is precisely the Singleton bound for classical linear block code [1]. Thus the Singleton bound is a special case of the Max-flow Min-cut theorem. Moreover, by (2), the non-source nodes in the network with maximum flow at least equal to k are simply all the nodes on the bottom layer, and each of them can decode the source message. Hence, we conclude that an (n, k) classical linear block code with minimum distance d is a k-dimensional linear multicast on the $\binom{n}{n-d+1}$ network.

More generally, an (n, k) classical linear block code with minimum distance d is a k-dimensional linear multicast on the $\binom{n}{r}$ network for all $r \geq n - d + 1$. The proof is straightforward (we already have shown it for $r = n-d+1$). On the other hand, it is readily seen that a k-dimensional linear multicast on the $\binom{n}{r}$ network, where $r \geq k$, is an (n, k) classical linear block code with minimum distance d satisfying

$$d \geq n - r + 1.$$

A classical linear block code achieving tightness in the Singleton bound is called a *maximum distance separation* (MDS) code [1]. From the foregoing, the Singleton bound is a special case of the Max-flow Min-cut theorem. Since a linear multicast, broadcast, or dispersion achieves tightness in the Max-flow Min-cut theorem to different extents, they can all be regarded as network generalizations of an MDS code. The existence of MDS codes corresponds, in the more general paradigm of network coding, to the existence of linear multicasts and their stronger versions. This has been discussed in great detail in [7].

III. Network Error Correction

Inspired by network coding, network error-correcting codes has been introduced in [4] for multicasting a source message to a set of nodes on a network when the communication channels are not error-free. The usual approach in existing networks, namely link-by-link error correction, is a special case of network error correction. Network

generalizations of the Hamming bound, the Singleton bound, and the Gilbert-Varshamov bound in classical algebraic coding have been obtained. In particular, the tightness of the Singleton bound in the network setting is preserved, meaning that linear network codes are asymptotically optimal. We refer the reader to [8] [9] for the details.

In this section, we discuss an upper bound obtained in [8] which is given in terms of bounds defined for classical error-correcting codes. By means of an example, we will show that this bound is not tight even for a simple class of networks called *regular networks*. This illustrates the complexity involved in the construction of network error-correcting codes.

Let us first describe the setup of network error correction. An acylic communication network is represented by a directed acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the node set and $\mathcal{E}$ is the channel set, in which multiple channels between a pair of nodes is allowed. On each channel, one symbol from a certain code alphabet $\mathcal{X}$ can be transmitted in the specified direction. A message taken from a source alphabet $\mathcal{Z}$ is generated at the source node s, which is to be multicast to a set of sink nodes $\mathcal{U}$. A network code on $\mathcal{G}$ is defined in the usual way (see for example [8]), and for a network code ϕ, the symbol transmitted on channel e when the message is z is denoted by $\tilde{\phi}_e(z)$.

Definition 1: A network code on $\mathcal{G}$ is t-error-correcting if it can correct all τ-errors for $\tau \leq t$, i.e., if the total number of errors in the network is at most t, then the source message can be recovered by all the sink nodes $u \in \mathcal{U}$.

Since $\mathcal{G}$ is acyclic, it naturally defines a partial order $\preceq$ on the channel set $\mathcal{E}$. Two channels $e, e' \in \mathcal{E}$ are said to be incompatible if neither $e \preceq e'$ nor $e' \preceq e$. A set of channels $\mathcal{A} \subset \mathcal{E}$ is called an antichain if the channels in $\mathcal{A}$ are pairwise incompatible.

Definition 2: For a partition (A, B) of the node set $\mathcal{V}$, $cut(A, B)$ is a regular cut if its members form an antichain, i.e., if $e, e' \in cut(A, B)$, then there exists no path either from e to e' or from e' to e.

Definition 3: An acyclic network is regular if $\min_u \text{maxflow}(s, u) = \min_u rg(s, u)$, where $rg(s, u)$ is the minimum volume of a regular cut between s and u.

For a t-error-correcting network code on a given network $\mathcal{G}$, we are naturally interested in the maximum possible value of $|\mathcal{Z}|$, the size of the source alphabet. The following theorem renders an upper bound on $|\mathcal{Z}|$.

Theorem 1: [8] Let ϕ be a t-error-correcting code for an acyclic network $\mathcal{G}$ with source alphabet $\mathcal{Z}$ and code alphabet $\mathcal{X}$, and let $n = \min_{u \in \mathcal{U}} rg(s, u)$.

i) If $cut(A, B)$ is a regular cut between the source node s and a sink node u, then the set of all possible vectors transmitted across $cut(A, B)$, i.e.,

$$\{(\tilde{\phi}_e(z), e \in cut(A, B)) : z \in \mathcal{Z}\},$$

form a classical t-error correcting code with alphabet $\mathcal{X}$, and consequently

ii)

$$|\mathcal{Z}| \leq A(n, t, q),$$

and in the case that the code is linear,

$$|\mathcal{Z}| \leq L(n, t, q),$$

where $q = |\mathcal{X}|$, and $A(n, t, q)$ and $L(n, t, q)$ are the size of an optimal classical q-ary t-error-correcting code of length n and the size of an optimal classical linear q-ary t-error-correcting code of length n, respectively.

The upper bound on $|\mathcal{Z}|$ rendered in the above theorem is in terms of bounds defined for classical error-correcting codes. Since the errors occurring at the channels across any cut in a regular network do not interfere with each other (because the set of channels form an antichain), one may conjecture that this upper bound on $\mathcal{Z}$ is generally tight for regular networks. The following example, however, shows the contrary.

Example 1: Consider the network in Fig. 2 which is specified by

$$\mathcal{U} = \{u_1, u_2\}$$

$$\mathcal{V} = \{s\} \cup \{a, b, c, d, e, f, g\} \cup \mathcal{U}$$

and

$$\begin{aligned} \mathcal{E} \quad = \quad & \{(s, a), (s, b), (s, c), (a, d), (a, u_1), (b, f), \\ & (b, u_1), (c, d), (c, u_2), (d, e), (e, f), (e, u_2), \\ & (f, g), (g, u_1), (g, u_2)\}. \end{aligned}$$

Let us consider binary codes for this network, i.e.,

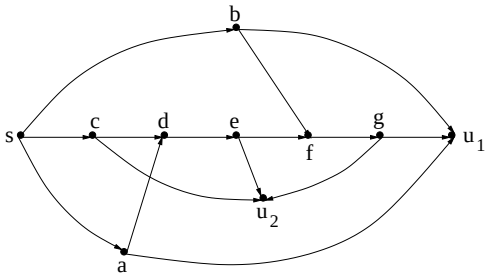

Fig. 2. The network for Example 1.

the encoding alphabet is given by $\mathcal{X} = \{0, 1\}$.

It is easy to verify for this network that $\text{maxflow}(s, u_i) = rg(u, u_i) = 3$ for $i = 1, 2$, so it is regular. In light of the existence of a classical binary 1-error-correcting (3,1) code, if the bounds in Theorem 1 are tight, then there would exist a binary 1-error-correcting network code

$$\phi = \{\phi_{(s,a)}, \phi_{(s,b)}, \phi_{(s,c)}, \ldots, \phi_{(g,u_1)}, \phi_{(g,u_2)}\}, \tag{4}$$

where $\phi_{(s,a)}$ denotes the encoding function of ϕ for channel (s, a), etc, that multicasts a message from the binary source alphabet $\mathcal{Z} = \{0, 1\}$.

Assume that the network code ϕ in (4) is 1-error-correcting. We will show that this leads to a contradiction. Without loss of generality, we let

$$\phi_{(s,a)}(0) = \phi_{(s,b)}(0) = \phi_{(s,c)}(0) = 0$$

and

$$\phi_{(s,a)}(1) = \phi_{(s,b)}(1) = \phi_{(s,c)}(1) = 1,$$

since by symmetry one can exchange the roles of 0 and 1 componentwise. We observe that for a particular network code, a channel can be removed if its encoding function can only take one value because such a channel does not convey any information. For the network in Fig. 2, if the encoding function of any channel can take only one value, then by removing that channel from the network, we will find a sink node such that the minimum cut between the source node and this sink node is reduced to 2. This contradicts Theorem 1 because of the nonexistence of a (2,1) code that can correct 1 error. This means that the encoding functions of all the channels must take two values. In particular, an encoding function of a channel whose input-nodes has in-degree one must be a bijection, so we may assume with loss of generality that it is the identity function.

Let us consider the encoding function $\phi_{(d,e)}$ with the first and the second arguments being the outputs of channels (a, d) and (c, d), respectively. We will show that there is no way to choose the function $\phi_{(d,e)}$ such that the code is able to correct 1 error.

First, without loss of generality, let

$$\phi_{(d,e)}(0, 1) = 0. \tag{5}$$

Let us consider the case that the source message is 1 and an error occurs at channel (s, a). It is easy to see that the outputs of channels (a, d) and (c, d) are 0 and 1, respectively, so that by (5), channel (d, e) outputs a 0. Then across the cut

$$\begin{aligned} &cut(\{s, c, d, u_2\}, \mathcal{V} \setminus \{s, c, d, u_2\}) \\ &\quad = \quad \{(s, a), (s, b), (d, e)\} \end{aligned}$$

between s and u_1, the outputs of the channels are $(0, 1, 0)$ if the source message is 1 and an error occurs at channel (s, a).

Next, consider the case that the source message is 0 and an error occurs at channel (s, b). Then we must have

$$\phi_{(d,e)}(0, 0) = 1, \tag{6}$$

otherwise the outputs of the channels across the cut in (6) would again be $(0, 1, 0)$ so that the sink node u_1 cannot distinguish the source messages 0 and 1.

We now consider the cut

$$\begin{aligned} &cut(\{s, a, d, u_1\}, \mathcal{V} \setminus \{s, a, d, u_1\}) \\ &\quad = \quad \{(s, b), (s, c), (d, e)\} \end{aligned} \tag{7}$$

between s and u_2. It is easy to verify that if $\phi_{(d,e)}(1, 1) = 0$, then the outputs of the channels across the cut in (7) is $(0, 1, 0)$ if the source message is 0 and an error occurs at channel (s, c), or if the source message is 1 and an error occurs at channel (s, b). Thus we must have

$$\phi_{(d,e)}(1, 1) = 1. \tag{8}$$

Now again consider the cut in (6). With (5), (6), and (8), it can readily be verified that

$$\begin{aligned} &d_H((\tilde{\phi}_{(s,a)}(0), \tilde{\phi}_{(s,b)}(0), \tilde{\phi}_{(d,e)}(0)), \\ &(\tilde{\phi}_{(s,a)}(1), \tilde{\phi}_{(s,b)}(1), \tilde{\phi}_{(d,e)}(1))) \\ &\quad = \quad d_H((0, 0, 1), (1, 1, 1)) \\ &\quad = \quad 2. \end{aligned} \tag{9}$$

By Theorem 1,

$$\{(\tilde{\phi}_{(s,a)}(z), \tilde{\phi}_{(s,b)}(z), \tilde{\phi}_{(d,e)}(z)) : z \in \{0,1\}\}$$

is a classical 1-error-correcting code so that its minimum distance is at least 3, a contradiction to (9). Therefore, the assumption that the code in (4) is 1-error-correcting is incorrect, and we conclude that there exists no binary 1-error-correcting network code that can transmit 1 bit. This in turn shows that the upper bound in Theorem 1 is not tight.

IV. Concluding Remarks

We have clarified the relation between network coding and algebraic coding. We have also have given an overview of network error correction, a paradigm for error correction on networks and an extension of classical point-to-point error correction, and discussed the complexity involved in the construction of network error correction codes.

Acknowledgment

The work of Raymond W. Yeung was partially supported by a grant from the Research Grant Council of the Hong Kong Special Administrative Region, China (RGC Ref. No. CUHK4214/03E).

References

[1] R. C. Singleton, "Maximum distance Q-nary codes," *IEEE Trans. Inform. Theory*, IT-10: 116-118, 1964.

[2] R. W. Yeung and Z. Zhang, "Distributed source coding for satellite communications," *IEEE Trans. Inform. Theory*, IT-45: 1111-1120, 1999.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, IT-46: 1204-1216, 2000.

[4] N. Cai and R. W. Yeung, "Network Coding and Error Correction," IEEE Information Theory Workshop, Bangalore, India, Oct 20-25, 2002.

[5] S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, IT-49: 371-381, 2003.

[6] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on network coding*, vol. 11, 782-795, 2003.

[7] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Theory of network coding," to appear in *Foundation and Trends in Communications and Information Theory.*

[8] R. W. Yeung and N. Cai, "Network error correction, Part I: Basic concepts and upper bounds," submitted to *Communications in Information and Systems*, `http://www.ims.cuhk.edu.hk/~cis`

[9] N. Cai and R. W. Yeung, "Network error correction, Part II: Lower bounds," submitted to *Communications in Information and Systems*, `http://www.ims.cuhk.edu.hk/~cis`

[10] Network coding homepage, `http://www.networkcoding.info`