COMMUNICATIONS IN INFORMATION AND SYSTEMS
Vol. 6, No. 1, pp. 37-54, 2006
© 2006 International Press
003

# NETWORK ERROR CORRECTION, PART II: LOWER BOUNDS

NING CAI* AND RAYMOND W. YEUNG†

**Abstract.** In Part I of this paper, we introduced the paradigm of network error correction as a generalization of classical link-by-link error correction. We also obtained the network generalizations of the Hamming bound and the Singleton bound in classical algebraic coding theory. In Part II, we prove the network generalization of the Gilbert-Varshamov bound and its enhancement. With the latter, we show that the tightness of the Singleton bound is preserved in the network setting. We also discuss the implication of the results in this paper.

**Key words:** Network coding, multicast, error correction, algebraic coding, Gilbert bound, Varshamov bound, Singleton bound.

**1. Introduction.** In Part I of this paper [1], we introduced the paradigm of network error correction as a generalization of classical link-by-link error correction. We also obtained the network generalizations of the Hamming bound and the Singleton bound in classical algebraic coding theory.

To continue with our discussion, we first recall from [1] the definition of a network error-correcting code. The notations here and in the sequel are inherited from [1].

DEFINITION 1. *Let $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ be a network, and $r_{(a,b)} \leq R_{(a,b)}$ be positive integers for $(a,b) \in \mathcal{E}$. A network code for the network $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ is a family of local encoding functions $\{\phi_{(a,b)} : (a,b) \in \mathcal{E}\}$ such that $\phi_{(s,b)} : \mathcal{Z} \longrightarrow \mathcal{X}^{r_{(s,b)}}$ and $\phi_{(a,b)} : \prod_{(c,a)\in\Gamma_+(a)} \mathcal{X}^{r_{(c,a)}} \longrightarrow \mathcal{X}^{r_{(a,b)}}$ if $a$ is not the source node $s$.*

DEFINITION 2. *A network code is $t$-error-correcting if it can correct all $\tau$-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 $u \in \mathcal{U}$. A network code is $\Upsilon$-error-correcting if it can correct $E$-errors for all $E \in \Upsilon$.*

In Part I, we have proved the network generalizations of the Hamming bound and the Singleton bound. In this part, we will prove a network generalization of the Gilbert-Varshamov bound and its enhancement. With the latter, we will show that the tightness of the Singleton bound is preserved in the network setting.

The rest of Part II is organized as follows. In Section 2, we prove the Gilbert bound and the Varshamov bound for network error-correcting codes. In Section 3, we sharpen the Varshamov bound obtained in Section 2 to the strengthened Varshamov bound. By means of the latter, we prove the tightness of the Singleton bound for

*N. Cai is with The State Key Lab. of ISN, Xidian University, Xi'an, Shaanxi, 710071, China. He was with Department of Information Engineering, The Chinese University of Hong Kong, N.T., Hong Kong when this work was done. Email: caining@mail.xidian.edu.cn

†R. W. Yeung is with Department of Information Engineering, The Chinese University of Hong Kong, N.T., Hong Kong. Email: whyeung@ie.cuhk.edu.hk

network error-correcting codes obtained in Part I. Section 4 is a discussion of the implication of the results in this work. Section 5 contains the proof of the results, and the paper is concluded in Section 6.

**2. The Gilbert-Varshamov Bound.** In this and the next sections, we will prove sufficient conditions for the existence of error-correcting codes on an acyclic network $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ by constructing such codes. We will assume that the code alphabet $\mathcal{X}$ is $GF(q)$ for some sufficiently large prime power $q$ (called the *base field*), and we will work in an $n$-dimensional linear space $GF^n(q)$ spanned by a *linear-code multicast* (LCM) to be defined shortly. The source alphabet $\mathcal{Z}$ will be a subset of $GF^n(q)$ for a general code and a $k$-dimensional subspace of $GF^n(q)$ for some positive integer $k \leq n$ for a linear code. Boldfaced letters (e.g., $\mathbf{a}, \mathbf{b}, \ldots, \mathbf{z}$) stand for row vectors whose dimensions are understood from the context. The transpose operation on vectors and matrices will be denoted by "$\tau$". So, $\mathbf{v}^\tau, \mathbf{w}^\tau$, etc, are column vectors. Addition and subtraction of vectors are understood to be in the linear spaces over $GF(q)$. With a slight abuse of notation, we also use $GF^n(q)$ to denote the linear spaces of $n$-dimensional row vectors or column vectors in $GF(q)$.

In this section, we consider general $\Upsilon$-error-correcting codes and prove Gilbert-type and Varshamov-type lower bounds on the sizes of optimal $\Upsilon$-error-correcting codes. By applying these bounds to $t$-error-correcting codes, we obtain asymptotically optimal $t$-error-correcting codes for networks, i.e., codes that achieve the Singleton upper bound proved in Part I when the size of the code alphabet is sufficient large. For general $\Upsilon$-error-correcting codes, however, there is a "small gap" between the Varshamov-type lower bound and the Singleton upper bound asymptotically.

The definition of an LCM below has been simplified for acyclic networks and adopted for the discussion of linear network error-correcting codes in this paper.

DEFINITION 3. *[2] A linear code multicast (LCM) $V$ for an acyclic network $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ is an assignment of linear subspace $\mathcal{L}_V(a)$ of (column space) $GF^n(q)$ to a node $a \in \mathcal{V}$ and a column vector $\mathbf{v}_V^\tau((a,b))$ of dimension $n$ to a channel $(a,b) \in \mathcal{E}^*$ over a sufficiently large finite field $GF(q)$ for a positive integer $n$, such that*
*1)* $\mathcal{L}_V(s) \subset GF^n(q)$*;*
*2)* $\mathbf{v}_V^\tau((a,b)) \in \mathcal{L}_V(a)$ *if* $(a,b) \in \Gamma_-(a)$*;*
*3)* $\mathbf{v}_V^\tau((b,c))$ *is a linear combination of* $\mathbf{v}_V^\tau((a,b))$*,* $(a,b) \in \Gamma_+(b)$ *for all output channels* $(b,c) \in \Gamma_-(b)$*.*

In [2], an inactive channel (i.e., a channel that does not carry information) in an LCM is assigned a null vector ("all 0 vector"), but in the current paper, we simply delete it from the channel set. That is, a vector assigned to a channel in an LCM is always non-null. Denote by $M(a)$ the matrix whose columns are the vectors assigned to the input channels of node $a$. For any LCM $V$, by 3) in the above definition, there exists a column vector $\mathbf{c}^\tau$ such that $\mathbf{v}_V^\tau((a,b)) = M(a)\mathbf{c}^\tau$. Here, the column vector $\mathbf{c}^\tau$

depends on $(a, b)$, but we omit this dependence in order to keep the notation simple. For the time being, let $GF^n(q)$ plays the role of the source alphabet and call a row vector $\mathbf{w} \in GF^n(q)$ an input to the network. Let $\langle \cdot, \cdot \rangle$ denotes the inner product, i.e., for row vectors $\mathbf{a}$ and $\mathbf{b}$,

$$\langle \mathbf{a}, \mathbf{b} \rangle = \mathbf{a}\mathbf{b}^\tau = \mathbf{b}\mathbf{a}^\tau.$$

Then we can define a linear network code $\phi$ based on any LCM $V$ by

1. $\phi_{(s,a)}(\mathbf{w}) = \langle \mathbf{w}, \mathbf{v}_V((s, a)) \rangle$ for all $a \in \Gamma_-(s)$;
2. $\phi_{(a,b)}(\mathbf{u}(a)) = \mathbf{u}(a)\mathbf{c}^\tau$, where $\mathbf{u}(a)$ is the row vector whose $i$th component is the output of the $i$th channel in $\Gamma_+(a)$ in the same order as the columns of $M(a)$.

It is easy to verify inductively that

$$\tilde{\phi}_{(a,b)}(\mathbf{w}) = \langle \mathbf{w}, \mathbf{v}_V((a, b)) \rangle \tag{1}$$

for all $(a, b) \in \mathcal{E}^*$.

We now define a *generic* LCM which we will use for code construction. The existence of a generic LCM is guaranteed by the theorem following the next definition.

DEFINITION 4. *[2] An LCM $V$ assigning $n$-dimensional column vectors to the channels in a network $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ is generic if for all $k \leq n$ and any subset of $k$ channels $\{(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)\}$, that $\mathcal{L}_V(a_j) \not\subset span[\mathbf{v}_V^\tau((a_i, b_i)),\ i \neq j]$ for all $j \in \{1, 2, \ldots, k\}$ implies that $\mathbf{v}_V^\tau((a_1, b_1)), \mathbf{v}_V^\tau((a_2, b_2)) \ldots, \mathbf{v}_V^\tau((a_k, b_k))$ are linearly independent.*

THEOREM 1. *[2]*
*i) For a given network with source node $s$, for all $n$ and sufficiently large $q$ (depending on the network and $n$), there exists a generic LCM assigning $n$-dimensional column vectors over $GF(q)$ to the channels in the network.*
*ii) For the generic LCM in i) and all nodes $a \in \mathcal{V} \setminus \{s\}$, $dim(\mathcal{L}_V(a))$ is equal to* $\min(\text{maxflow}(\text{s}, \text{a}), \text{n}) = \min(c(s, a), n)$.

To construct error correcting codes via a generic LCM, we need the following preparation. Consider the given network and let $n = \min_{u \in \mathcal{U}} c(s, u)$. Then we can obtain a subnetwork by deleting some channels if necessary, such that for all $u \in \mathcal{U}$,

$$cut(s, u) = d_+(u) = n. \tag{2}$$

For simplicity of notation, without loss of generality, we assume that (2) holds for the given network. Moreover, we may assume without loss of generality that for all $a \in \mathcal{V} \setminus \mathcal{U}$, $d_-(a) > 0$, because a non-sink node without an output channel is useless for communication and hence can be deleted from the node set. Obviously, for such a network, a coding order always ends at a sink node. Choose a coding order and denote it by $\preceq_*$. Then we order the channel according to $\preceq_*$ so that $(a, b)$ precedes

$(c,d)$ implies $a \preceq_* c$ (note that $a \preceq_* a$ so in this case $a$ may be equal to $c$), and denote this order by $\preceq_{*e}$.

Now by Theorem 1, we can find a generic LCM $V$ assigning $n$-dimensional column vectors to the channels in the network. This generic LCM $V$ induces a network code specified by $\phi$ and $\tilde{\phi}$ as described above. Since for any $u \in \mathcal{U}$,

$$dim(\mathcal{L}_V(u)) = cut(s,u) = n = dim(\mathcal{L}_V(s))$$

by Theorem 1 and (2), and since $\mathcal{L}_V(u) \subset \mathcal{L}_V(s)$, we see that

$$\mathcal{L}_V(u) = \mathcal{L}_V(s) = GF^n(q).$$

This implies that the matrix $M(u)$ is a full rank square matrix of size $n$.

Fix the coding order $\preceq_*$ and choose any generic LCM $V$ as prescribed above. We now consider the situation that the channels are not necessarily error-free. As in the previous sections, we regard the output of a channel $(a,b) \in \mathcal{E}^*$ as the sum of the input of the channel and an error symbol $e_{(a,b)} \in GF(q)$. Define $\mathbf{e} = (e_{(a,b)} : (a,b) \in \mathcal{E}^*)$, which we will refer to as an *error vector*, where the components of $\mathbf{e}$ are ordered according to $\preceq_{*e}$. Further, we denote the set of all edges leading to a node $c$ by $\mathbf{e}^c = (e_{(a,b)} : b \preceq c)$. Note that $a \preceq c$ implies that $a \preceq_* c$ since $\preceq_*$ is a linear extension of $\preceq$.

We remind the readers that if an error vector $\mathbf{e}$ occurs, its components are added to the channel inputs according to the coding order $\preceq_*$. Then the output of a channel $(a,b)$ is a function of both the input $\mathbf{w}$ to the network and the error vector $\mathbf{e}$ that occurs, and we denote it by $\psi_{(a,b)}(\mathbf{w},\mathbf{e})$. With this notation, a sink node $u \in \mathcal{U}$ cannot distinguish the case that $\mathbf{w}$ is the input to the network and error $\mathbf{e}$ occurs in the network from the case that $\mathbf{w}'$ is the input to the network and error $\mathbf{e}'$ occurs in the network if and only if

$$(\psi_{(a,u)}(\mathbf{w},\mathbf{e}) : (a,u) \in \Gamma_+(u)) = (\psi_{(a,u)}(\mathbf{w}',\mathbf{e}') : (a,u) \in \Gamma_+(u)). \tag{3}$$

Obviously, the value of $\psi_{(a,b)}(\mathbf{w},\mathbf{e})$ only depends on $\mathbf{w}$ and $\mathbf{e}^b$. By the definition of $\psi_{(a,b)}$, we have the recursive formula

$$\psi_{(a,b)}(\mathbf{w},\mathbf{e}) = \phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w},\mathbf{e}) : (c,a) \in \Gamma_+(a)) + e_{(a,b)}, \tag{4}$$

with the initial condition

$$\begin{aligned} \psi_{(s,g)}(\mathbf{w},\mathbf{e}) &= \phi_{(s,g)}(\mathbf{w}) + e_{(s,g)} \\ &= \tilde{\phi}_{(s,g)}(\mathbf{w}) + e_{(s,g)} \\ &= \mathbf{w}\mathbf{v}_V^\tau((s,g)) + e_{(s,g)} \end{aligned} \tag{5}$$

for all $g \in \Gamma_-(s)$.

LEMMA 1. *For all* $(a,b) \in \mathcal{E}^*$, *all network inputs* $\mathbf{w}$ *and* $\mathbf{w}'$, *error vectors* $\mathbf{e}$ *and* $\mathbf{e}'$, *and* $\mu \in GF(q)$,

$$\psi_{(a,b)}(\mathbf{w}+\mathbf{w}', \mathbf{e}+\mathbf{e}') = \psi_{(a,b)}(\mathbf{w},\mathbf{e}) + \psi_{(a,b)}(\mathbf{w}',\mathbf{e}') \tag{6}$$

*and*

$$\psi_{(a,b)}(\mu\mathbf{w}, \mu\mathbf{e}) = \mu\psi_{(a,b)}(\mathbf{w},\mathbf{e}). \tag{7}$$

Denote a null vector ("all 0 vector") by $\mathbf{0}$ whose dimension is understood from the context. By the above lemma, for any network input $\mathbf{w}$ and error vector $\mathbf{e}$, we have,

$$\psi_{(a,b)}((\mathbf{w},\mathbf{e}) = \psi_{(a,b)}(\mathbf{w},\mathbf{0}) + \psi_{(a,b)}(\mathbf{0},\mathbf{e}).$$

Note that the two null vectors on the RHS above have different dimensions. Upon observing that $\psi_{(a,b)}(\mathbf{w},\mathbf{0}) = \tilde{\phi}_{(a,b)}(\mathbf{w})$ and defining $\theta_{(a,b)}(\mathbf{e}) = \psi_{(a,b)}(\mathbf{0},\mathbf{e})$, we can write

$$\psi_{(a,b)}(\mathbf{w},\mathbf{e}) = \tilde{\phi}_{(a,b)}(\mathbf{w}) + \theta_{(a,b)}(\mathbf{e}). \tag{8}$$

In other words, $\psi_{(a,b)}(\mathbf{w},\mathbf{e})$ can be written as the sum of two linear functions of $\mathbf{w}$ and $\mathbf{e}$, respectively.

Our strategy for constructing a $t$-error-correcting code is to choose an appropriate subset $\mathcal{Z}$ of $GF^n(q)$ as the source alphabet. To facilitate the description of the codes that we will construct in the proof of the Gilbert-Varshamov bound (to be stated shortly), we first introduce a few notations. An error vector $\mathbf{e}$ is said to have *error pattern* $E$ for a subset $E$ of channels if its component $e_{(a,b)} \neq 0$ if only if $(a,b) \in E$. For an error pattern set $\Upsilon$, we denote by $\Upsilon*$ the set of error vectors with error pattern in $\Upsilon$, and for each $u \in \mathcal{U}$, define the set

$$\Xi(V,\Upsilon,u) = \{(\theta_{(a,u)}(\mathbf{e})M^{-1}(u), (a,u) \in \Gamma_+(u)) : \mathbf{e} \in \Upsilon*\}, \tag{9}$$

We further define the set

$$\Delta(V,\Upsilon) = \bigcup_{u\in\mathcal{U}} \{\mathbf{f} = \mathbf{g}' - \mathbf{g} : \mathbf{g},\mathbf{g}' \in \Xi(V,\Upsilon,u)\}. \tag{10}$$

For a vector $\mathbf{w} \in GF^n(q)$, we write the sum set

$$\mathbf{w} + \Delta(V,\Upsilon) := \{\mathbf{w}+\mathbf{f} : \mathbf{f} \in \Delta(V,\Upsilon)\} \tag{11}$$

so that for all $\mathbf{w}$, $\mathbf{w}+\Delta(V,\Upsilon)$ has the same cardinality as $\Delta(V,\Upsilon)$, i.e.,

$$|\mathbf{w} + \Delta(V,\Upsilon)| = |\Delta(V,\Upsilon)|. \tag{12}$$

In the case that $\Upsilon$ is the subset of channels with cardinality not larger than $t$, we write $\Xi(V, \Upsilon, u)$ as $\Xi(V, t, u)$ and $\Delta(V, \Upsilon)$ as $\Delta(V, t)$, i.e.,

$$\Xi(V, t, u) = \{(\theta_{(a,u)}(\mathbf{e})M^{-1}(u), (a, u) \in \Gamma_+(u)) : w_H(\mathbf{e}) \leq t\}, \tag{13}$$

where $w_H(\mathbf{e})$ denotes the Hamming weight of $\mathbf{e}$. We say that a pair of input vectors of the network $\mathbf{w}$ and $\mathbf{w}'$ are $\Upsilon$-*separable* at a sink node $u$ if (3) does not hold for all error vectors $\mathbf{e}$ and $\mathbf{e}'$ in $\Upsilon*$, and that $\mathbf{w}$ and $\mathbf{w}'$ are $\Upsilon$-separable if they are $\Upsilon$-separable for all sink nodes. The notion of $t$-separability is defined analogously.

LEMMA 2.
*i) For all* $\mathbf{w}, \mathbf{w}' \in GF^n(q)$,

$$\mathbf{w}' \in \mathbf{w} + \Delta(V, \Upsilon) \tag{14}$$

*if and only if* $\mathbf{w} \in \mathbf{w}' + \Delta(V, \Upsilon)$.
*ii)* $\mathbf{w}$ *and* $\mathbf{w}'$ *are* $\Upsilon$*-separable if and only if*

$$\mathbf{w}' \notin \mathbf{w} + \Delta(V, \Upsilon). \tag{15}$$

*iii) Let* $\mathcal{Z} \subset GF^n(q)$. *Then the restriction of the network code* $\{\phi_{(a,b)} : (a, b) \in \mathcal{E}^*\}$ *induced by* $\mathcal{Z}$ *and a generic LCM* $V$ *is a* $\Upsilon$*-error correcting code for the network if and only if the vectors in* $\mathcal{Z}$ *are pairwise* $\Upsilon$*-separable. Moreover, the code is linear if* $\mathcal{Z}$ *is a linear subspace of* $GF^n(q)$.

THEOREM 2 (Gilbert-Varshamov Bound). *For all positive integer* $A$ *with*

$$(A - 1)|\Delta(V, \Upsilon)| < q^n, \tag{16}$$

*one can construct an* $\Upsilon$*-error-correcting code with source alphabet size* $A$ *(i.e.,* $|\mathcal{Z}| = A$*). Moreover, for all positive integers* $k$ *such that*

$$|\Delta(V, \Upsilon)| < q^{n-k}, \tag{17}$$

*one can construct a linear code of at least* $k$ *dimensions (i.e.,* $|\mathcal{Z}| = q^k$*) via the given generic LCM* $V$.

The first and the second parts of this theorem are the network generalizations of the Gilbert bound and the Varshamov bound for classical error-correcting codes, respectively.

**Remark:** It can be seen from the proof of the Varshamov bound in Theorem 2 that instead of (17), the condition

$$\max_{1 \leq i \leq n} |\Delta_i(V, \Upsilon)| < q^{n-k} \tag{18}$$

is sufficient for the existence of a linear code of at least $k$ dimensions, where $\{\Delta_i(V, \Upsilon) : 1 \leq i \leq n\}$ is partition of $\Delta(V, \Upsilon)$ such that $\Delta_0(V, \Upsilon) = \{\mathbf{0}\}$ and for $1 \leq i \leq n$,

$\mathbf{w} \in \Delta_i(V, \Upsilon)$ if and only if $\mathbf{w} \in \Delta(V, \Upsilon)$ and the last non-zero component of $\mathbf{w}$ is the $i$th component.

To obtain a lower bound on $|\mathcal{Z}|$ which does not depend on the particular choice of the LCM $V$, we observe that by the definitions of $\Delta(V, \Upsilon)$ and $\Xi(V, \Upsilon, u)$, $|\Delta(V, \Upsilon)|$ is upper bounded by

$$\begin{aligned} |\Delta(V,\Upsilon)| &\le \sum_{u\in\mathcal{U}} |\Xi(V,\Upsilon,u) - \Xi(V,\Upsilon,u)| \\ &\le \sum_{u\in\mathcal{U}} |\Xi(V,t,u)|^2 \\ &\le |\mathcal{U}|(|\Upsilon *|)^2, \end{aligned} \tag{19}$$

where

$$\Xi(V,\Upsilon,u) - \Xi(V,\Upsilon,u) = \{\mathbf{f} = \mathbf{g}' - \mathbf{g} : \mathbf{g}, \mathbf{g}' \in \Xi(V,\Upsilon,u)\}.$$

Let $K = |\mathcal{E}^*|$ and define

$$\Upsilon_j = \{E : |E| = j, E \in \Upsilon\}$$

for $j = 0, 1, \ldots, K$. Then by the definition of $\Upsilon *$, we have

$$|\Upsilon * | = \sum_{j=0}^{K} |\Upsilon_j|(q-1)^j. \tag{20}$$

By (19) and (20), the following corollary of Theorem 2 is immediate.

COROLLARY 1. *For any given error-pattern set $\Upsilon$ and all positive integer $A$ with*

$$(A-1)|\mathcal{U}| \left( \sum_{j=0}^{K} |\Upsilon_j|(q-1)^j \right)^2 < q^n, \tag{21}$$

*one can construct an $\Upsilon$-error-correcting code with source alphabet size $A$. Moreover, for all positive integers $k$ such that*

$$|\mathcal{U}| \left( \sum_{j=0}^{K} |\Upsilon_j|(q-1)^j \right)^2 < q^{n-k}, \tag{22}$$

*one can construct a linear code of at least $k$ dimensions.*

In particular, if $\Upsilon$ is the collection of subsets of channels with cardinality no larger than $t$, then

$$|\Upsilon_j| = \begin{cases} \binom{K}{j} & \text{if } j \le t \\ 0 & \text{otherwise.} \end{cases}$$

Thus for $t$-error-correcting codes, the bounds in Corollary 1 can be expressed explicitly as

$$|\Delta(V,t)| \le |\mathcal{U}| \left[\sum_{j=0}^{t} \binom{K}{j} (q-1)^j\right]^2. \tag{23}$$

COROLLARY 2. *For a network with $\min_{u\in\mathcal{U}} c(s,u) = n$, for all $\epsilon > 0$ and sufficiently large prime power $q$ (depending on the network and $\epsilon$), one can construct a $t$-error correcting code with source alphabet $\mathcal{Z}$ such that*

$$\log|\mathcal{Z}| \ge (n-2t)(1-\epsilon)\log q. \tag{24}$$

*Moreover, for all sufficiently large prime power $q$ and $k = n-2t-1$, one can construct a $k$-dimensional linear $t$-error correcting code for the network.*

**3. The Strengthened Varshamov Bound and the Singleton Bound.** In this section, we continue with our discussion on $t$-error correcting codes for networks. We first state the Singleton bound for network error-correcting codes proved in Part I [1]. The tightness of this bound will also be shown upon proving in Theorem 4 an enhancement of the Varshamov bound.

THEOREM 3 (Singleton Bound). *[1] Let $(\mathcal{G}, s, \mathcal{U}, \mathcal{R})$ be an acyclic network and $n = \min_{u\in\mathcal{U}} c(s,u)$. If there exists a $t$-error-correcting code for the network with source alphabet $\mathcal{Z}$, then*

$$\log|\mathcal{Z}| \le (n-2t)\log q, \tag{25}$$

*where $n - 2t > 0$.*

Comparing the Singleton bound (upper bound on $|\mathcal{Z}|$) and the bound in Corollary 2 (lower bound on $|\mathcal{Z}|$), which is a consequence of the Gilbert bound, we see that the two bounds differ only by the $\epsilon$ in the latter. However, the gap between the two bounds can be quite large because according to the proof of Corollary 2, $q \to \infty$ as $\epsilon \to 0$.

Closing this gap involves sharpening the Varshamov bound by making a more careful estimate on $|\Delta(V,t)|$, the size of the difference set. Toward this end, we rewrite (10) via (9) as

$$\begin{aligned}&\Delta(V,t)\\ &= \{(\theta_{(a,u)}(\mathbf{e}), (a,u)\in\Gamma_+(u))M^{-1}(u) - (\theta_{(a,u)}(\mathbf{e}'), (a,u)\in\Gamma_+(u))M^{-1}(u) :\\ &\quad u\in\mathcal{U} \text{ and } w_H(\mathbf{e}), w_H(\mathbf{e}') \le t\}.\end{aligned} \tag{26}$$

By the linearity of $\theta_{(a,u)}$, we have

$$\begin{aligned}&(\theta_{(a,u)}(\mathbf{e}), (a,u)\in\Gamma_+(u))M^{-1}(u) - (\theta_{(a,u)}(\mathbf{e}'), (a,u)\in\Gamma_+(u))M^{-1}(u)\\ &= (\theta_{(a,u)}(\mathbf{e}-\mathbf{e}'), (a,u)\in\Gamma_+(u))M^{-1}(u),\end{aligned} \tag{27}$$

and obviously

$$\{\mathbf{e}-\mathbf{e}' : w_H(\mathbf{e}), w_H(\mathbf{e}') \le t\} = \{\mathbf{d} : w_H(\mathbf{d}) \le 2t\}$$

since $n - 2t > 0$. So,

$$\Delta(V,t) = \{(\theta_{(a,u)}(\mathbf{d})\ (a,u) \in \Gamma_+(u))M^{-1}(u) : u \in \mathcal{U} \text{ and } w_H(\mathbf{d}) \le 2t\}. \tag{28}$$

Then we have the upper bound

$$|\Delta(V,t)| \le |\mathcal{U}| \sum_{i=0}^{2t} \binom{n}{i} (q-1)^i \tag{29}$$

which is tighter than (23) which was obtained from the more general upper bound in (19). However, by combining this bound and Theorem 2, we still can only obtain the same lower bound $(n-2t-1)$ on the dimension of optimal linear codes as in Corollary 2. Nevertheless, the bound in (29) will be instrumental in proving the strengthened Varshamov bound in the next theorem. In proving this theorem, we also need to employ a more elaborate technique for bounding $|\Delta(V,t)|$.

THEOREM 4 (Strengthened Varshamov Bound). *For a fixed arbitrary acyclic network with* $\min_{u\in\mathcal{U}} c(s,u) = n$ *and all sufficiently large* $q$*, there exists an* $(n-2t)$*-dimensional linear* $t$*-error-correcting code for the network.*

With the strengthened Varshamov bound, the tightness of the Singleton bound for all sufficiently large $q$ is readily seen. It is well-known that the Singleton bound for classical error-correcting codes on a sufficiently large field is tight. Thus not only that the Singleton bound can be generalized for network error-correcting codes, but also that the tightness of the bound is preserved.

**4. Discussion.** In this section, we discuss the implication of the results obtained in Part I and Part II of this paper.

Classical error-correcting codes are devised for correcting errors in point-to-point communications. Such errors may be due to noise in the channel, or they may be injected by adversaries such as a wiretapper. In either case, as long as the error-correcting code employed is sufficiently powerful, reliable communication can be achieved. The main idea of classical error correction is to spread redundancy over time.

In a communication network as modeled in this paper, suppose the errors are due to noise in the channels. Then a natural approach to achieving reliable and efficient end-to-end communication is to convert each noisy channel into a noiseless channel with rate equal to its own capacity by means of a channel code (e.g. a turbo code [5]) and then employ an optimal network code for the whole network. In other words, error correction is carried out on a link-by-link basis. This is called separation of network coding and channel coding and has been studied in [6] and [7]. Specifically,

separation theorems have been proved for general cyclic networks under the following conditions:

1. the channels in the network are independent;
2. all the channels are memoryless.

In [6], the separation theorem is established under the assumption that there is a unit delay in the transmission in every channel in the network, while in [7], the separation theorem is established under a more general setting.

For wired communication networks, while it may be valid to assume that the channels are independent, they are usually not memoryless. Thus, there is generally no guarantee that link-by-link error correction is asymptotically optimal.

If instead the errors in the network are injected by adversaries such as a wiretapper or a malicious node, the considerations would be very different. For example, if a particular node within the network is malicious, then that node is unreliable even over time. Since a classical error-correcting code only spreads redundancy over time, no link-by-link error correction scheme can correct the errors injected by that node. On the other hand, if a network error-correcting node is employed, as long as there are not an overwhelming number of errors, which may be due to noise in the channels or injected by adversaries, they can all be corrected because for a network error-correcting code, redundancy is spread not only over time but also over space. This is a feature of network correction which is not possessed by classical error correction.

For link-by-link error correction, a channel code is decoded at every intermediate node in the network. Since decoding involves nonlinear operations, it is computationally expensive. In the last section, we have proved the strengthened Varshamov bound which implies that when the base field is sufficiently large, the tightness of the Singleton bound established in Part I can be achieved by linear network error-correcting codes, i.e., linear network error-correcting codes are optimal (in the sense of $t$-error correcting). For linear network error correction, unlike link-by-link error correction, only linear operations is required at the intermediate nodes. Thus linear network error correction offers a significant computational advantage over link-by-link error correction.

As a remark, although we have established that linear network error-correcting codes are optimal for correcting $t$ errors when the base field is sufficiently large, it is possible that a nonlinear network error-correcting code can correct certain (but not all) error vectors $\mathbf{e}$ containing more than $t$ errors which are impossible for the best possible linear network code. This is a tradeoff between the computational efficiency and the error-correcting capability of the scheme.

## 5. Proof of Results.

**Proof of Lemma 1**

We prove the lemma by induction on the order $\preceq_{*e}$. The first channel in the order

$\preceq_{*e}$ is a channel with input node $s$, say $(s,g)$. Then by (5),

$$\begin{aligned}
&\psi_{(s,g)}(\mathbf{w}+\mathbf{w}',\mathbf{e}+\mathbf{e}')\\
&=(\mathbf{w}+\mathbf{w}')\mathbf{v}_V^\tau((s,g))+(e_{(s,g)}+e'_{(s,g)})\\
&=(\mathbf{w}\mathbf{v}_V^\tau((s,g))+e_{(s,g)})+(\mathbf{w}'\mathbf{v}_V^\tau((s,g))+e'_{(s,g)})\\
&=\psi_{(s,g)}(\mathbf{w},\mathbf{e})+\psi_{(s,g)}(\mathbf{w}',\mathbf{e}'), \qquad (30)
\end{aligned}$$

and

$$\begin{aligned}
\psi_{(s,g)}(\mu\mathbf{w},\mu\mathbf{e})&=(\mu\mathbf{w})\mathbf{v}_V^\tau((s,g))+\mu e_{(s,g)}\\
&=\mu[\mathbf{w}\mathbf{v}_V^\tau((s,g))+e_{(s,g)}]\\
&=\mu\psi_{(s,g)}(\mathbf{w},\mathbf{e}).
\end{aligned}$$

Assume that (6) and (7) hold for all the channels preceding channel $(a,b)$. Then by (4) and the induction hypothesis, we have

$$\begin{aligned}
&\psi_{(a,b)}(\mathbf{w}+\mathbf{w}',\mathbf{e}+\mathbf{e}')\\
&=\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w}+\mathbf{w}',\mathbf{e}+\mathbf{e}'):(c,a)\in\Gamma_+(a))+(e_{(a,b)}+e'_{(a,b)})\\
&=\phi_{(a,b)}((\psi_{(c,a)}(\mathbf{w},\mathbf{e})+\psi_{(c,a)}(\mathbf{w}',\mathbf{e}')):(c,a)\in\Gamma_+(a))+(e_{(a,b)}+e'_{(a,b)}). \qquad (31)
\end{aligned}$$

By the linearity of $\phi_{(a,b)}$, (31) yields

$$\begin{aligned}
&\psi_{(a,b)}(\mathbf{w}+\mathbf{w}',\mathbf{e}+\mathbf{e}')\\
&=\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w},\mathbf{e}):(c,a)\in\Gamma_+(a))\\
&\quad+\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w}',\mathbf{e}'):(c,a)\in\Gamma_+(a))+(e_{(a,b)}+e'_{(a,b)})\\
&=(\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w},\mathbf{e}):(c,a)\in\Gamma_+(a))+e_{(a,b)})\\
&\quad+(\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w}',\mathbf{e}'):(c,a)\in\Gamma_+(a))+e'_{(a,b)})\\
&=\psi_{(a,b)}(\mathbf{w},\mathbf{e})+\psi_{(a,b)}(\mathbf{w}',\mathbf{e}'), \qquad (32)
\end{aligned}$$

i.e., (6). Similarly, by (4), the induction hypothesis, and the linearity of $\phi_{(a,b)}$, we have

$$\begin{aligned}
&\psi_{(a,b)}(\mu\mathbf{w},\mu\mathbf{e})\\
&=\phi_{(a,b)}(\psi_{(c,a)}(\mu\mathbf{w},\mu\mathbf{e}):(c,a)\in\Gamma_+(a))+\mu e_{(a,b)}\\
&=\phi_{(a,b)}(\mu\psi_{(c,a)}(\mathbf{w},\mathbf{e}):(c,a)\in\Gamma_+(a))+\mu e_{(a,b)}\\
&=\mu\phi_{(a,b)}(\psi_{(c,a)}(\mathbf{w},\mathbf{e}):(c,a)\in\Gamma_+(a))+\mu e_{(a,b)}\\
&=\mu\psi_{(a,b)}(\mathbf{w},\mathbf{e}), \qquad (33)
\end{aligned}$$

i.e., (7) holds.

**Proof of Lemma 2**

i) If $\mathbf{w}'\in\mathbf{w}+\Delta(V,\Upsilon)$, then $\mathbf{w}'=\mathbf{w}+\mathbf{f}$, or $\mathbf{w}=\mathbf{w}'+(-\mathbf{f})$, for some $\mathbf{f}\in\Delta(V,\Upsilon)$.

Since $\mathbf{f} \in \Delta(V,\Upsilon)$ implies $(-\mathbf{f}) \in \Delta(V,\Upsilon)$, we have $\mathbf{w} \in \mathbf{w}' + \Delta(V,\Upsilon)$. The converse is immediate by symmetry.

ii) Assume that $\mathbf{w}$ and $\mathbf{w}'$ are not $\Upsilon$-separable. Then there exists a sink node $u \in \mathcal{U}$ and error vectors $\mathbf{e}$ and $\mathbf{e}'$, both in $\Upsilon*$, such that (3) holds. Now substitute (8) into (3) to obtain

(34)
$$(\tilde{\phi}_{(a,u)}(\mathbf{w}) + \theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u)) = (\tilde{\phi}_{(a,u)}(\mathbf{w}') + \theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u)).$$

By (1) and the definition of the matrix $M(u)$, we have

$$\begin{aligned} &(\tilde{\phi}_{(a,u)}(\mathbf{w}) + \theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u)) \\ &= (\tilde{\phi}_{(a,u)}(\mathbf{w}) : (a,u) \in \Gamma_+(u)) + (\theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u)) \\ &= \mathbf{w}M(u) + (\theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u)), \end{aligned} \tag{35}$$

and similarly

(36)
$$(\tilde{\phi}_{(a,u)}(\mathbf{w}') + \theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u)) = \mathbf{w}'M(u) + (\theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u)).$$

Substituting (35) and (36) into (34), we have

$$\mathbf{w}M(u) + (\theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u)) = \mathbf{w}'M(u) + (\theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u)). \tag{37}$$

Multiplying $M^{-1}(u)$ to both sides, we obtain

$$\mathbf{w} + (\theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u))M^{-1}(u) = \mathbf{w}' + (\theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u))M^{-1}(u),$$

or equivalently,

(38)
$$\mathbf{w}' = \mathbf{w} + [(\theta_{(a,u)}(\mathbf{e}) : (a,u) \in \Gamma_+(u))M^{-1}(u) - (\theta_{(a,u)}(\mathbf{e}') : (a,u) \in \Gamma_+(u))M^{-1}(u)].$$

Thus we have shown that (3) is equivalent to (38). Since $[\Xi(V,\Upsilon,u) - \Xi(V,\Upsilon,u)] \subset \Delta(V,\Upsilon)$ by the definition in (10), (38) implies that (cf. (9))

$$\mathbf{w}' \in \mathbf{w} + [\Xi(V,\Upsilon,u) - \Xi(V,\Upsilon,u)] \subset \mathbf{w} + \Delta(V,\Upsilon). \tag{39}$$

Hence, (15) does not hold.

Conversely, assume that (15) does not hold. Then there exists by (10) a sink node $u \in \mathcal{U}$ such that (39) holds. Thus by the definition in (9), there is a pair of error vectors $\mathbf{e}$ and $\mathbf{e}'$ in $\Upsilon*$ such that (38) holds, which we have shown is equivalent to (3), i.e., $\mathbf{w}$ and $\mathbf{w}'$ are not $\Upsilon$-separable. This completes the proof of part ii).

iii) This part follows immediately from the definitions of $\Upsilon$-error-correcting codes for networks, $\Upsilon$-separability, and the linearity of $\{\phi_{(a,b)} : (a,b) \in \mathcal{E}^*\}$.

**Proof of Theorem 2**

To obtain (16), we employ the well-known greedy algorithm due to Gilbert [3] to

obtain a set $\mathcal{Z} \subset GF^n(q)$ such that for all $\mathbf{z}, \mathbf{z}' \in \mathcal{Z}$,

$$\mathbf{z}' \notin \mathbf{z} + \Delta(V, \Upsilon). \tag{40}$$

Then by ii) and iii) of Lemma 2 and (40), the restriction of $\{\phi_{(a,b)} : (a,b) \in \mathcal{E}^*\}$ is an $\Upsilon$-error correcting code for the network. The greedy algorithm works as follows. We begin with the initial ground set $\mathcal{W}_1 = GF^n(q)$. In each step, say the $i$th step, where $i \geq 1$, we add an arbitrary vector $\mathbf{z}_i$ taken from the ground set $\mathcal{W}_i$ to $\mathcal{Z}$, delete the vectors in the subset $(\mathbf{z}_i + \Delta(V, \Upsilon)) \cap \mathcal{W}_i$ from the ground set $\mathcal{W}_i$, and call the resulting set the $(i+1)$th ground set $\mathcal{W}_{i+1}$. That is, the new ground set becomes $\mathcal{W}_{i+1} = \mathcal{W}_i \setminus (\mathbf{z}_i + \Delta(V, \Upsilon))$. We repeat this procedure until we obtain a set $\mathcal{Z}$ with $|\mathcal{Z}| = A$. By (12), we delete at most $|\Delta(V, \Upsilon)|$ vectors from the ground set in each step. So for $i \leq A - 1$, by the condition (16), the ground set still has at least

$$\begin{aligned} &|GF^n(q)| - i|\Delta(V, \Upsilon)| \\ &= q^n - i|\Delta(V, \Upsilon)| \\ &\geq q^n - (A-1)|\Delta(V, \Upsilon)| \\ &> 0 \end{aligned}$$

vectors after the $i$th step, and therefore it is possible to choose the next vector $\mathbf{z}_{i+1}$ from the ground set. Obviously, the set $\mathcal{Z}$ obtained this way satisfies (40).

To obtain a linear code with dimension $k$ for $k$ satisfying (17), by ii) and iii) of Lemma 2, it is sufficient for us to find a $k$-dimensional subspace of $GF^n(q)$ such that (40) hold for all $\mathbf{z}, \mathbf{z}' \in \mathcal{Z}$, which by linearity is equivalent to

$$\Delta(V, \Upsilon) \cap \mathcal{Z} = \{\mathbf{0}\}. \tag{41}$$

This is done by a Varshamov-type approach as follows (cf. [4]). According to this approach, in order to obtain the linear $\Upsilon$-error-correcting code for the network, we will construct an $(n-k) \times n$ matrix $H$ analogous to the parity check matrix in classical coding theory. To this end, we need a few definitions. First, we partition $\Delta(V, \Upsilon)$ into

$$\{\Delta_i(V, \Upsilon) : 0 \leq i \leq n\}, \tag{42}$$

where $\Delta_0(V, \Upsilon) = \{\mathbf{0}\}$, and for $1 \leq i \leq n$, $\mathbf{w} \in \Delta_i(V, \Upsilon)$ if and only if $\mathbf{w} \in \Delta(V, \Upsilon)$ and the last non-zero component of $\mathbf{w}$ is the $i$th component. That is, for $i > 0$, for all $\mathbf{w} \in \Delta_i(V, \Upsilon)$,

$$\mathbf{w} = (w_1, w_2, \ldots, w_i, \mathbf{0}), \tag{43}$$

with $w_i \neq 0$. Next, we let $\mathcal{K}_1 = \{\mathbf{0}^\tau\} \subset GF^{n-k}(q)$, where $\mathbf{0}$ is the $(n-k)$-dimensional null row vector. For $2 \leq i \leq n$ and any fixed $(i-1)$ $(n-k)$-dimensional column

vectors $(\mathbf{h'}_1^\tau, \mathbf{h'}_2^\tau, \ldots \mathbf{h'}_{i-1}^\tau)$, let

$$\mathcal{K}_i(\mathbf{h'}_1^\tau, \mathbf{h'}_2^\tau, \ldots \mathbf{h'}_{i-1}^\tau) := \left\{ \mathbf{k}^\tau : w_i \mathbf{k}^\tau + \sum_{j=1}^{i-1} w_j \mathbf{h'}_j^\tau = \mathbf{0}^\tau \text{ for some } \mathbf{w} \in \Delta_i(V, \Upsilon) \text{ and } \mathbf{k}^\tau \in GF^{n-k}(q) \right\}. \tag{44}$$

Then

$$|\Delta_0(V, \Upsilon)| = |\mathcal{K}_1| = 1, \tag{45}$$

and for $2 \le i \le n$ and all $\mathbf{h'}_1^\tau, \mathbf{h'}_2^\tau, \ldots \mathbf{h'}_{i-1}^\tau$,

$$|\mathcal{K}_i(\mathbf{h'}_1^\tau, \mathbf{h'}_2^\tau, \ldots \mathbf{h'}_{i-1}^\tau)| \le |\Delta_i(V, \Upsilon)|. \tag{46}$$

To construct an $(n-k) \times n$ matrix $H = (\mathbf{h}_1^\tau, \mathbf{h}_2^\tau \ldots, \mathbf{h}_n^\tau)$, we will choose the $n$ $(n-k)$-dimensional column vectors $\mathbf{h}_1^\tau, \mathbf{h}_2^\tau, \ldots, \mathbf{h}_n^\tau$ recursively as follows:

Step 1: Begin with $GF^{n-k}(q) \setminus \mathcal{K}_1$ and choose an arbitrary $\mathbf{h}_1$ in it.

Step 2: Choose an arbitrary vector $\mathbf{h}_2^\tau \in GF^{n-k}(q) \setminus \mathcal{K}_2(\mathbf{h}_1^\tau)$.

For $i \ge 2$,

Step $i$: Choose an arbitrary $\mathbf{h}_i^\tau \in GF^{n-k}(q) \setminus \mathcal{K}_i(\mathbf{h}_1^\tau, \mathbf{h}_2^\tau \ldots, \mathbf{h}_{i-1}^\tau)$.

This procedure can be continued until $i = n$ so that we can obtain all the columns of $H$, i.e., $\mathbf{h}_1^\tau, \mathbf{h}_2^\tau \ldots, \mathbf{h}_n^\tau$, because for all $i \le n$, by the conditions in (17), (45) and (46), the size of the set of candidates for $\mathbf{h}_i^\tau$ is at least

$$\begin{aligned} &|GF^{n-k}(q)| - |\mathcal{K}_i(\mathbf{h'}_1^\tau, \mathbf{h'}_2^\tau, \ldots \mathbf{h'}_{i-1}^\tau)| \\ &\ge q^{n-k} - |\Delta_i(V, \Upsilon)| \\ &\ge q^{n-k} - |\Delta(V, \Upsilon)| \\ &> 0. \end{aligned}$$

Next we let

$$\mathcal{Z} = \{\mathbf{z} : \mathbf{z} \in GF^n(q) \text{ and } H\mathbf{z}^\tau = 0\}. \tag{47}$$

Obviously, $\mathcal{Z}$ is a linear subspace having dimension $n - \text{rank}(H) \ge n - (n-k) = k$. To complete the proof, we have to show that $\mathcal{Z}$ satisfies the condition (41). Indeed, if (41) does not hold for $\mathcal{Z}$, there must exist a $\mathbf{z} \in \mathcal{Z} \cap \Delta_i(V, \Upsilon)$ for some $i$ with $0 < i \le n$. Now we write $\mathbf{z} = (z_1, z_2, \ldots, z_i, \mathbf{0})$ as in (43), and then by (47), we have

$$0 = H\mathbf{z}^\tau = z_i \mathbf{h}_i^\tau + \sum_{j=1}^{i-1} z_j \mathbf{h}_j^\tau,$$

which by (44) yields

$$\mathbf{h}_i^\tau \in \mathcal{K}_i(\mathbf{h}_1^\tau, \mathbf{h}_2^\tau \ldots, \mathbf{h}_{i-1}^\tau).$$

So we have arrived at a contradiction to Step $i$ in the construction of $H$, completing our proof.

**Proof of Corollary 2**

We assume that $n - 2t > 0$, otherwise both parts of the corollary are trivial. Then $t < n \leq K(= |\mathcal{E}^*|)$. From (23), we have

$$\begin{aligned} |\Delta(V,t)| &\leq |\mathcal{U}| \left[ \sum_{j=0}^{K} \binom{K}{j} \right]^2 q^{2t} \\ &= |\mathcal{U}| 2^{2K} q^{2t}. \end{aligned}$$

Thus

$$\log |\Delta(V,t)| < 2t \log q + 2K + \log |\mathcal{U}|. \tag{48}$$

Now choose

$$(|\mathcal{Z}| =)\ A = \lceil \frac{q^n}{|\Delta(V,t)|} \rceil \tag{49}$$

so that (16) is satisfied, and for any fixed $\epsilon > 0$, choose

$$q \geq 2^{\frac{2K + \log |\mathcal{U}|}{(n-2t)\epsilon}},$$

so that

$$\log |\mathcal{U}| \leq (n-2t)\epsilon \log q - 2K.$$

Then from (48), we have

$$\log |\Delta(V,t)| < 2t \log q + (n-2t)\epsilon \log q. \tag{50}$$

Hence, it follows from (49) that

$$\begin{aligned} \log |\mathcal{Z}| &\geq n \log q - \log |\Delta(V,t)| \\ &> n \log q - 2t \log q - (n-2t)\epsilon \log q \\ &= (n-2t)(1-\epsilon) \log q. \end{aligned}$$

This proves the first part of the corollary upon invoking the Gilbert bound in Theorem 2.

In (50), by choosing $\epsilon = (n-2t)^{-1}$, we have

$$\begin{aligned} \log |\Delta(V,t)| &< 2t \log q + \log q \\ &= (2t+1) \log q, \end{aligned}$$

or

$$|\Delta(V,t)| < q^{2t+1} = q^{n-(n-2t-1)} = q^{n-k}.$$

Then the second part of the corollary is proved upon invoking the Varshamov bound in Theorem 2.

**Proof of Theorem 4**

To enhance the Varshamov bound, we proceed as follows. Let

$$\Delta^*(V,t) = \Delta(V,t) \setminus \{\mathbf{0}\}, \tag{51}$$

and write

$$\mathcal{Z} = \{\mathbf{z} : H\mathbf{z}^\tau = 0\}, \tag{52}$$

where $H$ is an $(n-k) \times n$ matrix. Then (41) holds if and only if for all $\mathbf{w} \in \Delta^*(V,t)$,

$$H\mathbf{w}^\tau \neq 0. \tag{53}$$

By (51), the partition in (42) partitions $\Delta^*(V,t)$ into

$$\{\Delta_i(V,t) : 1 \leq i \leq n\}. \tag{54}$$

The set $\mathcal{Z}$ in (52) is a subspace of $GF^n(q)$ of at least $k$ dimensions, and the matrix $H$ is to be chosen such that the restriction of the network code $\{\phi_{(a,b)} : (a,b) \in \mathcal{E}^*\}$ induced by $\mathcal{Z}$ is a $t$-error-correcting code for the network.

To show the existence of an $(n-k) \times n$ matrix $H$ as in the proof of Theorem 2 with $k = n - 2t$ (instead of $k = n - 2t - 1$), we further partition $\Delta_i(V,t)$ in (54) by defining a relation $\sim$ among the vectors in $GF^n(q) \setminus \{\mathbf{0}\}$ such that for $\mathbf{w}, \mathbf{w}' \in GF^n(q) \setminus \{\mathbf{0}\}$, $\mathbf{w} \sim \mathbf{w}'$ if and only if there exists a $\mu \in GF(q) \setminus \{0\}$ such that $\mathbf{w}' = \mu\mathbf{w}$. Obviously, the relation $\sim$ is an equivalence relation and therefore induces a partition of $GF^n(q) \setminus \{\mathbf{0}\}$. For all $\mathbf{w} \in \Delta^*(V,t)$, by (28), there exists $\mathbf{d} \in GF^K(q)$ ($K = |\mathcal{E}^*|$) such that $w_H(\mathbf{d}) \leq 2t$ and

$$\mathbf{w} = (\theta_{(a,u)}(\mathbf{d}), (a,u) \in \Gamma_+(u))M^{-1}(u). \tag{55}$$

It is clear that $\mathbf{d} \neq \mathbf{0}$ since by the linearity of $\theta_{(a,u)}$,

$$(\theta_{(a,u)}(\mathbf{0}), (a,u) \in \Gamma_+(u))M^{-1}(u) = \mathbf{0} \notin \Delta^*(V,t)$$

(note that the two $\mathbf{0}$'s have different dimensions). Again by the linearity of $\theta_{(a,u)}$, for all $\mu \in GF(q) \setminus \{0\}$ and for all $\mathbf{w} \in \Delta^*(V,t)$, from (55), we have

$$\mu\mathbf{w} = \mu(\theta_{(a,u)}(\mathbf{d}), (a,u) \in \Gamma_+(u))M^{-1}(u) = (\theta_{(a,u)}(\mu\mathbf{d}), (a,u) \in \Gamma_+(u))M^{-1}(u),$$

where $\mu\mathbf{d} \neq 0$ and $w_H(\mu\mathbf{d}) \leq 2t$. Thus, if $\mathbf{w} \in \Delta^*(V,t)$, then $\mu\mathbf{w} \in \Delta^*(V,t)$. Further, it is easy to see from the definition of $\Delta_i^*(V,t)$ that if $\mathbf{w} \in \Delta_i^*(V,t)$, then $\mu\mathbf{w} \in \Delta_i^*(V,t)$. Then the relation $\sim$ partitions $\Delta_i(V,t)$ for $i = 1, 2, \ldots n$ into equivalence classes each with $(q-1)$ vectors, implying a total of $(q-1)^{-1}|\Delta_i(V,t)|$ equivalence classes in $\Delta_i(V,t)$.

We now prove that for any fixed equivalence class $\mathcal{Q}$ of $\Delta_i(V,t)$, there are exactly $q^{2t(n-1)}$ $2t \times n$ matrices $H := (\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n)$ such that there exists $\mathbf{w} \in \mathcal{Q}$ satisfying

$$H\mathbf{w}^\tau = \mathbf{0}. \tag{56}$$

Since the vectors in $\mathcal{Q}$ are multiples of each other, a matrix $H$ satisfies (56) for all $\mathbf{w} \in \mathcal{Q}$ if and only if it satisfies (56) for $\mathbf{w} = (w_1, w_2, \ldots, w_{i-1}, 1, \mathbf{0}) \in \mathcal{Q} \subset \Delta_i(V,t)$. Now $H\mathbf{w}_1^\tau = 0$ if and only if

$$\mathbf{h}_i = -\sum_{j=1}^{i-1} w_j \mathbf{h}_j.$$

Thus $\mathbf{h}_i$ is fixed once $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{i-1}, \mathbf{h}_{i+1}, \ldots, \mathbf{h}_n$ are arbitrarily chosen ($\mathbf{h}_i$ actually depends only on $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{i-1}$). This proves our claim that there are exactly $q^{2t(n-1)}$ matrices $H$ such that there exists $\mathbf{w} \in \mathcal{Q}$ satisfying (56). Together with (29) and (51), this implies that the number of $2t \times n$ matrices $H$ such that there exists $\mathbf{w} \in \Delta^*(V,t)$ satisfying (56) is upper bounded by

$$\begin{aligned}
&\sum_{i=1}^{n} (q-1)^{-1} |\Delta_i(V,t)| q^{2t(n-1)} \\
&= q^{2t(n-1)} (q-1)^{-1} |\Delta^*(V,t)| \\
&= q^{2t(n-1)} (q-1)^{-1} (|\Delta(V,t)| - 1) \\
&\leq q^{2t(n-1)} (q-1)^{-1} |\mathcal{U}| \sum_{i=1}^{2t} \binom{n}{i} (q-1)^i \\
&\leq 2^K |\mathcal{U}| q^{2t(n-1)} (q-1)^{2t-1} \\
&< (2^K |\mathcal{U}| q^{-1}) q^{2tn},
\end{aligned}$$

where the second last inequality above follows because $2t < n \leq K$. On the other hand there are totally $q^{2tn}$ $2t \times n$ matrices over $GF(q)$. So if $q$ is a prime power such that

$$q \geq 2^K |\mathcal{U}|,$$

then there must exist a $2t \times n$ matrix $H$ such that (53) holds for all $\mathbf{w} \in \Delta^*(V,t)$, which defines a subspace $\mathcal{Z}$ via (52) of at least $(n-2t)$ dimensions that induces a $t$-error-correcting code. This completes the proof.

**6. Conclusion.** In this two-part paper, we introduce network error correction as a generalization of classical link-by-link error correction. We have obtained network generalizations of the fundamental bounds in classical algebraic coding theory on the size of the source alphabet, namely the Hamming bound, the Singleton bound, and the Gilbert-Varshamov bound. In particular, we have shown that the tightness of the Singleton bound is preserved in the network setting. The results in this paper have set a new direction for both network coding theory and algebraic coding theory.

## 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. W. Yeung and N. Cai, *Network Error Correction, Part I: Basic concepts and upper bounds*, submitted.

[2] S.-Y. R. Li, R. W. Yeung and N. Cai, *Linear network coding*, IEEE Trans. Inform. Theory, IT-49(2003), pp. 371–381.

[3] E. N. Gilbert, *A comparison of signaling alphabets*, Bell System Tech. J., 31(1952), pp. 504–522.

[4] R. R. Varshamov, *Estimate of the number of signals in error correcting codes*, Dokl. Akad. Nauk SSSR, 117(1957), pp. 739–741.

[5] C. Berrou, A. Glavieux, and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: Turbo codes*, Proceedings of the 1993 International Conferences on Communications, 1064–1070, 1993.

[6] S. Borade, *Network information flow: Limits and achievability*, 2002 IEEE International Symposium on Information Theory, Lausanne, Switzerland, Jun 30-Jul 5, 2002.

[7] L. Song and R. W. Yeung and N. Cai, *A separation theorem for single source network coding*, IEEE Transactions on Information Theory, 52:5(2006), pp. 1861–1871.