Refined Coding Bounds for Network Error Correction

Shenghao Yang
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
shyang5@ie.cuhk.edu.hk

Raymond W. Yeung
Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
whyeung@ie.cuhk.edu.hk

***Abstract*—With respect to a given set of local encoding kernels defining a linear network code, refined versions of the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound for network error correction are proved by the weight properties of network codes. This refined Singleton bound is also proved to be tight for linear message sets.**

***Index Terms*—Network error correction coding, network Hamming weight, Singleton bound, Gilbert-Varshamov bound.**

I. Introduction

The network error correction problem studied in [1]–[5] is to extend classical error correction coding theory to a general network setting. The concept of network error correction coding was first introduced by Cai and Yeung [1]–[3]. They generalized the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound in classical error correction coding to network coding. Zhang [4] introduced the minimum rank for linear network codes, which plays a role similar to that of the minimum distance in decoding classical error-correcting codes. Recently, network generalizations of the Hamming weight, the Hamming distance, and the minimum distance of network codes have been obtained by Yang and Yeung [5]. In terms of the minimum distance, the capability of a network code for error correction, error detection, and erasure correction can be fully characterized. The relation between network coding and maximum distance separation (MDS) codes in classical algebraic coding has been clarified in [6].

In this paper, we present stronger versions of the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound for network error correction compared with those bounds obtained in [1]–[3]. Our proofs of these bounds are based on the weight properties of network codes [5]. An algorithm that constructs a linear network codes achieving a refined Singleton bound from a classical linear block code has recently been presented in [9]. In this paper, we present a different constructive proof to the tightness of the Singleton bound with respect to a given sets of global encoding kernels defining a linear network code.

This paper is organized as follows. Section II formulates the network error correction problem. Section III reviews the weight properties of network codes. The coding bounds are proved in Section IV. In the last section we summarize our work.

II. Problem Formulation

We study network transmission in a directed acyclic communication network represented by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges in the network. We assume an order on the edge set $\mathcal{E}$ which is consistent with the associated partial order of the directed acyclic network $\mathcal{G}$. An edge from node a to node b, say edge e, represents a communication channel from node a to node b. We call node a (node b) the tail (head) of edge e, denoted by $tail(e)$ ($head(e)$). Let $In(a) = \{e \in \mathcal{E} : head(e) = a\}$ and $Out(a) = \{e \in \mathcal{E} : tail(e) = a\}$ be the sets of input edges and output edges of node a, respectively. There can be multiple edges between a pair of nodes, and each edge can transmit one symbol in a finite field $\mathbb{F}_q$.

A multicast on $\mathcal{G}$ transmits information from a source node s to a set of sink nodes $\mathcal{T}$. Let $n_s = |Out(s)|$. The source node s modulates the information to be multicast into a row vector $\mathbf{x} \in \mathbb{F}_q^{n_s}$ called the *message vector*. The set of all message vectors, a subset of $\mathbb{F}_q^{n_s}$, is called the *message set* and denoted by $\mathcal{C}$. The source node s transmits the message vector by mapping its n_s components onto the edges in $Out(s)$. Define an $n_s \times |\mathcal{E}|$ matrix $A = [A_{i,j}]$ as

$$A_{i,j} = \begin{cases} 1 & e_j \text{ is the } i\text{th edge in } Out(s), \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

By applying the order on $\mathcal{E}$ to $Out(s)$, the n_s non-zero columns of A form an identity matrix.

An *error vector* $\mathbf{z}$ is an $|\mathcal{E}|$-dimensional row vector with each component representing the error on the corresponding edge. An *error pattern* is a subset of $\mathcal{E}$. An error vector is said to match an error pattern if all the errors occur on the edges in the error pattern. The set of all error vectors that *match* error pattern ρ is denoted by ρ^*. Let $\rho_{\mathbf{z}}$ be the error pattern corresponding to the non-zero components of an error vector $\mathbf{z}$.

For network $\mathcal{G}$, a linear network error-correcting code, or a linear network code for brevity, is specified by a set of *local encoding kernels* $\{k_{e',e} : e', e \in \mathcal{E}\}$ and the message set $\mathcal{C}$. The local encoding kernel $k_{e',e}$ can be non-zero only if $e' \in In(tail(e))$. Define the $|\mathcal{E}| \times |\mathcal{E}|$ one-step transition matrix

$K = [K_{i,j}]$ for network $\mathcal{G}$ as

$$K_{i,j} = k_{e_i,e_j}. \tag{2}$$

For an acyclic network, $K^N = \mathbf{0}$ for some positive integer N. Define the transfer matrix of the network by $F = (I - K)^{-1}$ [7], so that the symbols transmitted on the edges are given by the components of $(\mathbf{x}A + \mathbf{z})F$.

For a sink node $t \in \mathcal{T}$, write $n_t = |In(t)|$, and define an $|\mathcal{E}| \times n_t$ matrix $B_t = [B_{i,j}]$ for sink node t as

$$B_{i,j} = \begin{cases} 1 & e_i \text{ is the } j\text{th edge in } In(t), \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Again by applying the order on $\mathcal{E}$ to $In(t)$, the n_t nonzero rows of B_t form an identity matrix. The reception at a sink node t is given by

$$\begin{aligned} \mathbf{y}_t &= (\mathbf{x}A + \mathbf{z})FB_t, \\ &= \mathbf{x}F_{s,t} + \mathbf{z}F_t, \end{aligned} \tag{4}$$

where $F_{s,t} = AFB_t$ is the submatrix of F given by the intersection of the n_s rows corresponding to the edges in $Out(s)$ and the n_t columns corresponding to the edges in $In(t)$, and $F_t = FB_t$ is the submatrix of F formed by the columns of F corresponding to the input edges of sink node t. $F_{s,t}$ and F_t are the transfer matrices of message transmission and error transmission, respectively, for sink node t. Denote the rank of $F_{s,t}$ by m_t.

Equation (4) is the formulation of the multicast network error correction problem given in [4]. The classical error correction problem is a special case in which both of $F_{s,t}$ and F_t reduce to identity matrices. The message transmission capacity of the network code, in the absence of errors, is measured by the rank of the transfer matrix $F_{s,t}$. Denote the maximum flow between source node s and sink node t by maxflow(s,t). Evidently, for any linear network code on $\mathcal{G}$, the rank of $F_{s,t}$ is upper bounded by maxflow(s,t) [6]. When the network is error-free, the error correction problem is reduced to the usual network coding problem, for which the size of the message set $\mathcal{C}$ is bounded by $q^{\min_{t\in\mathcal{T}} \text{maxflow}(s,t)}$ [8].

III. Previous Results

A. Weight Properties of Network Codes

For any $t \in \mathcal{T}$, let $\Upsilon_t(\mathbf{y}) = \{\mathbf{z} \in \mathbb{F}_q^{|\mathcal{E}|} : \mathbf{z}F_t = \mathbf{y}\}$ for a received vector $\mathbf{y} \in Im(F_t) = \{\mathbf{z}'F_t : \mathbf{z}' \in \mathbb{F}_q^{|\mathcal{E}|}\}$.

Definition 1: For any sink node t, the *network Hamming weights* of a received vector $\mathbf{y}$, of an error vector $\mathbf{z}$, and of a message vector $\mathbf{x}$ are defined by

$$W_t^{rec}(\mathbf{y}) = \min_{\mathbf{z}\in\Upsilon_t(\mathbf{y})} w_H(\mathbf{z}), \tag{5}$$

$$W_t^{err}(\mathbf{z}) = W_t^{rec}(\mathbf{z}F_t), \tag{6}$$

and

$$W_t^{msg}(\mathbf{x}) = W_t^{rec}(\mathbf{x}F_{s,t}), \tag{7}$$

respectively.

Definition 2: For any sink node t, the *network Hamming distance* between two received vectors $\mathbf{y}_1$ and $\mathbf{y}_2$ is defined by

$$D_t^{rec}(\mathbf{y}_1, \mathbf{y}_2) = W_t^{rec}(\mathbf{y}_1 - \mathbf{y}_2); \tag{8}$$

the *network Hamming distance* between two message vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ is defined by

$$D_t^{msg}(\mathbf{x}_1, \mathbf{x}_2) = W_t^{msg}(\mathbf{x}_1 - \mathbf{x}_2). \tag{9}$$

Definition 3: The *unicast minimum distance* of a network code with message set $\mathcal{C}$ for sink node t is defined by

$$d_{\min,t} = \min\{D_t^{msg}(\mathbf{x}, \mathbf{x}') : \mathbf{x}, \mathbf{x}' \in \mathcal{C}, \mathbf{x} \neq \mathbf{x}'\}. \tag{10}$$

Theorem 1 ([5]): For a sink node t, the following five properties of a network code are equivalent:

1) The code can correct any error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq d/2$;
2) The code can correct any error vector $\mathbf{z}$ with $W_t^{err}(\mathbf{z}) \leq d/2$;
3) The code can detect any error vector $\mathbf{z}$ with $0 < w_H(\mathbf{z}) \leq d$;
4) The code can detect any error vector $\mathbf{z}$ with $0 < W_t^{err}(\mathbf{z}) \leq d$;
5) The code has $d_{\min,t} \geq d + 1$;

where d is a nonnegative integer.

B. Coding Bounds

Let

$$d_{\min} = \min_{t\in\mathcal{T}} d_{\min,t}, \tag{11}$$

and

$$n = \min_{t\in\mathcal{T}} \text{maxflow}(s,t). \tag{12}$$

In terms of the notion of minimum distance, the Hamming bound and the Singleton bound for network codes obtained in [2] can be restated as

$$|\mathcal{C}| \leq \frac{q^n}{\sum_{i=0}^{r} \binom{n}{i}(q-1)^i}, \tag{13}$$

where $r = \lfloor \frac{d_{\min}-1}{2} \rfloor$, and

$$|\mathcal{C}| \leq q^{n-d_{\min}+1}. \tag{14}$$

The tightness of (14) has been proved in [3].

IV. Refined Coding Bounds

In this section, we employ the tools of network Hamming weight to prove refined versions of the coding bounds in [1]–[3]. The proofs presented here are considerably simpler and more transparent.

A. Hamming Bound and Singleton Bound

Theorem 2 (Hamming bound and Singleton bound): A network code with $rank(F_{s,t}) = m_t$, message set $\mathcal{C}$, and unicast minimum distance $d_{\min,t} > 0$ for any sink node t satisfies the

1) Hamming bound:

$$|\mathcal{C}| \leq \frac{q^{m_t}}{\sum_{i=0}^{r_t} \binom{m_t}{i}(q-1)^i}, \tag{15}$$

where $r_t = \lfloor \frac{d_{\min,t}-1}{2} \rfloor$, and the

2) Singleton bound:

$$|\mathcal{C}| \leq q^{m_t - d_{\min,t}+1} \tag{16}$$

for all sink node t.

Proof: Fix a sink node t. Find m_t linearly independent rows of $F_{s,t}$ and let ρ_t be the set of edges in $Out(s)$ that corresponds to these m_t linearly independent rows. Note that $\rho_t \subset Out(s) \subset \mathcal{E}$, so that ρ_t is an error pattern. Define the set

$$\mathcal{C}'_t = \{\mathbf{x}' \in \mathbb{F}_q^{n_s} : \mathbf{x}'A \in \rho_t^*,\ \mathbf{x}'F_{s,t} = \mathbf{x}F_{s,t} \text{ for some } \mathbf{x} \in \mathcal{C}\}, \tag{17}$$

where the matrix A is defined as (1). Define a mapping

$$\phi_t : \mathcal{C} \to \mathcal{C}'_t \tag{18}$$

by $\phi_t(\mathbf{x}) = \mathbf{x}'$ if $\mathbf{x}'F_{s,t} = \mathbf{x}F_{s,t}$. Since the rows of $F_{s,t}$ indexed by ρ_t form a basis for the row space of $F_{s,t}$, ϕ_t is well-defined. The mapping ϕ_t is onto by the definition of $\mathcal{C}'_t$. The mapping ϕ_t is also one-to-one because otherwise there exists $\mathbf{x}' \in \mathcal{C}'_t$ such that $\mathbf{x}'F_{s,t} = \mathbf{x}_1F_{s,t} = \mathbf{x}_2F_{s,t}$ for distinct $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}$, a contradiction to the assumption that $d_{\min,t} > 0$. Thus the mapping ϕ_t is a one-to-one and onto mapping, which implies that $|\mathcal{C}'_t| = |\mathcal{C}|$.

Let

$$\mathcal{Z}_t = \{\mathbf{z} \in \rho_t^* : w_H(\mathbf{z}) \leq r_t\}. \tag{19}$$

By Theorem 1, the network code with $\mathcal{C}$ being the message set can correct all the errors in $\mathcal{Z}_t$ at sink node t. Since sink node t has the same reception for the transmission of either $\mathbf{x} \in \mathcal{C}$ or $\phi_t(\mathbf{x}) \in \mathcal{C}'_t$ for the same error vector, the network code with $\mathcal{C}'_t$ being the message set can also correct all the errors in $\mathcal{Z}_t$ at sink node t.

Consider the problem of finding a subset of ρ_t^* as an error-correcting code that can correct all the errors in $\mathcal{Z}_t$. This problem is equivalent to the problem in classical algebraic coding of finding a block code with codeword length m_t that can correct r_t errors. The vectors in the set $\mathcal{C}''_t = \{\mathbf{x}A : \mathbf{x} \in \mathcal{C}'_t\}$ must form such a code, otherwise the network code with $\mathcal{C}'_t$ being the message set cannot possibly correct all the error vectors in $\mathcal{Z}_t$ at sink node t. Applying the Hamming bound and the Singleton bound for classical error-correcting codes to $\mathcal{C}''_t$, we have

$$|\mathcal{C}''_t| \leq \frac{q^{m_t}}{\sum_{i=0}^{r_t} \binom{m_t}{i}(q-1)^i}, \tag{20}$$

and

$$|\mathcal{C}''_t| \leq q^{m_t - d_{\min,t}+1}. \tag{21}$$

The proof is completed by noting that $|\mathcal{C}| = |\mathcal{C}'_t| = |\mathcal{C}''_t|$. ■

The Hamming bound and the Singleton bound in Theorem 2 are more refined than those in [1], [2] because as we will show, they imply (13) and (14) but not vice versa. The Hamming bound in Theorem 2 implies

$$\begin{aligned} |\mathcal{C}| &\leq \frac{q^{m_t}}{\sum_{i=0}^{r_t} \binom{m_t}{i}(q-1)^i} && (22)\\ &\leq \frac{q^{m_t}}{\sum_{i=0}^{r} \binom{m_t}{i}(q-1)^i} && (23)\\ &\leq \frac{q^{\text{maxflow}(s,t)}}{\sum_{i=0}^{r} \binom{\text{maxflow}(s,t)}{i}(q-1)^i} && (24) \end{aligned}$$

for all sink nodes t, where (23) follows from $r \leq r_t$ and (24) follows from $m_t \leq \text{maxflow}(s,t)$ and the inequality proved in the Appendix. By the same inequality, upon minimizing over all sink nodes $t \in \mathcal{T}$, we obtain (13).

To verify that the condition for the inequality in the Appendix applies in the above, by considering the Singleton bound in (16), we obtain

$$\begin{aligned} 1 &\leq |\mathcal{C}| && (25)\\ &\leq q^{m_t - d_{\min,t}+1} && (26) \end{aligned}$$

or

$$d_{\min,t} - 1 \leq m_t \tag{27}$$

for all $t \in \mathcal{T}$. Then

$$\begin{aligned} r &= \lfloor \frac{d_{\min}-1}{2} \rfloor && (28)\\ &\leq \lfloor \frac{d_{\min,t}-1}{2} \rfloor && (29)\\ &\leq \frac{d_{\min,t}-1}{2} && (30)\\ &\leq \frac{m_t}{2} && (31) \end{aligned}$$

for all $t \in \mathcal{T}$.

For the Singleton bound in Theorem 2, we first note that it is maximized when $m_t = \text{maxflow}(s,t)$ for all $t \in \mathcal{T}$. This can be achieved by a linear broadcast whose existence was proved in [10], [6]. To show that the Singleton bound in Theorem 2 implies (14), consider

$$\begin{aligned} |\mathcal{C}| &\leq q^{m_t - d_{\min,t}+1} && (32)\\ &\leq q^{m_t - d_{\min}+1} && (33)\\ &\leq q^{\text{maxflow}(s,t) - d_{\min}+1} && (34) \end{aligned}$$

for all sink nodes t. Then (14) is obtained upon minimizing over all $t \in \mathcal{T}$.

B. Gilbert Bound and Varshamov Bound

Let

$$\Delta_t(\mathbf{x}, d) = \{\mathbf{x}' \in \mathbb{F}_q^{n_s} : D_t^{msg}(\mathbf{x}', \mathbf{x}) \leq d\}. \tag{35}$$

For $\mathbf{x} = \mathbf{0}$, we can write

$$\Delta_t(\mathbf{0}, d) = \{\mathbf{x}' \in \mathbb{F}_q^{n_s} : W_t^{msg}(\mathbf{x}') \leq d\}. \tag{36}$$

Then it is readily seen that $\Delta_t(\mathbf{0}, d)$ is closed under scalar multiplication, i.e.,

$$\alpha\Delta_t(\mathbf{0}, d) = \{\alpha\mathbf{x} : \mathbf{x} \in \Delta_t(\mathbf{0}, d)\} = \Delta_t(\mathbf{0}, d), \tag{37}$$

where $\alpha \in \mathbb{F}_q$ and $\alpha \neq 0$.

For two subsets $V_1, V_2 \subset \mathbb{F}_q^{n_s}$, their sum is the set defined by

$$V_1 + V_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2\}. \tag{38}$$

For $\mathbf{v} \in \mathbb{F}_q^{n_s}$ and $V \subset \mathbb{F}_q^{n_s}$, we also write $\{\mathbf{v}\} + V$ as $\mathbf{v} + V$.

Theorem 3 (Gilbert bound): Given a set of local encoding kernels, let $|\mathcal{C}|_{\max}$ be the maximum possible size of the message set such that the network code has unicast minimum distance greater than or equal to $d_t > 0$ for each sink node t. Then,

$$|\mathcal{C}|_{\max} \geq \frac{q^{n_s}}{|\Delta(\mathbf{0})|}, \tag{39}$$

where

$$\Delta(\mathbf{0}) = \cup_{t\in\mathcal{T}}\Delta_t(\mathbf{0}, d_t - 1). \tag{40}$$

Proof: Let $\mathcal{C}$ be the message set with the maximum possible size. Then for any $\mathbf{x} \in \mathbb{F}_q^{n_s}$, there exists a codeword $\mathbf{c} \in \mathcal{C}$ and a sink node t such that

$$D_t^{msg}(\mathbf{x}, \mathbf{c}) \leq d_t - 1, \tag{41}$$

since otherwise we could add $\mathbf{x}$ to the message set while keeping the minimum distance larger than or equal to d_t for each sink node t, which is a contradiction on the maximality of $|\mathcal{C}|$.

Let

$$\Delta(\mathbf{c}) = \cup_{t\in\mathcal{T}}\Delta_t(\mathbf{c}, d_t - 1). \tag{42}$$

Hence, the whole space $\mathbb{F}_q^{n_s}$ is contained in the union of $\Delta(\mathbf{c})$ over all messages $\mathbf{c} \in \mathcal{C}$, i.e.,

$$\mathbb{F}_q^{n_s} \subset \cup_{\mathbf{c}\in\mathcal{C}}\Delta(\mathbf{c}). \tag{43}$$

Since $\Delta(\mathbf{c}) = \mathbf{c} + \Delta(\mathbf{0})$, we have $|\Delta(\mathbf{c})| = |\Delta(\mathbf{0})|$. So we deduce that $q^{n_s} \leq |\mathcal{C}||\Delta(\mathbf{0})|$, that is

$$|\mathcal{C}| \geq \frac{q^{n_s}}{|\Delta(\mathbf{0})|}. \tag{44}$$

■

Theorem 4 (Varshamov bound): Given a set of local encoding kernels, let $\omega_{\max}$ be the maximum possible dimension of the *linear* message set such that the network code has unicast minimum distance larger than or equal to $d_t > 0$ for each sink node t. Then,

$$\omega_{\max} \geq n_s - \log_q |\Delta(\mathbf{0})|, \tag{45}$$

where $\Delta(\mathbf{0})$ is defined in (40).

Proof: Let $\mathcal{C}$ be the linear message set with the maximum possible dimension. We claim that

$$\mathbb{F}_q^{n_s} \subset \Delta(\mathbf{0}) + \mathcal{C}. \tag{46}$$

If the claim is true, then

$$\begin{aligned} q^{n_s} &= |\Delta(\mathbf{0}) + \mathcal{C}| && (47)\\ &\leq |\Delta(\mathbf{0})||\mathcal{C}| && (48)\\ &= |\Delta(\mathbf{0})|q^{\omega_{\max}}, && (49) \end{aligned}$$

proving (45).

The claim is proved by contradiction. Let

$$\mathbf{g} \in \mathbb{F}_q^{n_s} \setminus (\Delta(\mathbf{0}) + \mathcal{C}), \tag{50}$$

and

$$\mathcal{C}' = \mathcal{C} + \langle\mathbf{g}\rangle.$$

Then $\mathcal{C}'$ is a subspace with dimension $\omega_{\max}+1$. If $\mathcal{C}'\cap\Delta(\mathbf{0}) \neq \{\mathbf{0}\}$, then there exists a non-zero vector

$$\mathbf{c} + \alpha\mathbf{g} \in \Delta(\mathbf{0}), \tag{51}$$

where $\mathbf{c} \in \mathcal{C}$ and $\alpha \in \mathbb{F}$. Here, $\alpha \neq 0$, otherwise we have $\mathbf{c} = \mathbf{0}$ because $\mathcal{C} \cap \Delta(\mathbf{0}) = \{\mathbf{0}\}$. Since $\Delta_t(\mathbf{0}, d_t - 1)$ is closed under scalar multiplication for all $t \in \mathcal{T}$, see from (40) that the same holds for $\Delta(\mathbf{0})$. Thus from (51),

$$\begin{aligned} \mathbf{g} &\in \Delta(\mathbf{0}) - \alpha^{-1}\mathbf{c} && (52)\\ &\subset \Delta(\mathbf{0}) + \mathcal{C}, && (53) \end{aligned}$$

which is a contradiction to (50). Therefore, $\mathcal{C}' \cap \Delta(\mathbf{0}) = \{\mathbf{0}\}$, i.e., $\mathcal{C}'$ is a message set such that the network code has unicast minimum distance larger than or equal to d_t, which is a contradiction on the maximality of $\mathcal{C}$. The proof is completed.

■

C. Tightness of the Singleton Bound

Theorem 5: Given a set of local encoding kernels over a finite field with size q where q is sufficiently large, for every

$$0 \leq \omega \leq \min_{t\in\mathcal{T}} m_t, \tag{54}$$

there exists a message set $\mathcal{C}$ with $|\mathcal{C}| = q^\omega$ such that

$$d_{\min,t} = m_t - \omega + 1 \tag{55}$$

for all sink nodes t.

Proof: we start with any given set of local encoding kernels which defines a linear network code. This determines m_t for all sink nodes t. Fix an ω which satisfies (54). We will then construct an ω-dimensional linear message set which together with the given linear network code constitute a linear network error-correcting code that satisfy (55) for all t. Note that (54) and (55) imply

$$d_{\min,t} \geq 1. \tag{56}$$

We now construct the message set $\mathcal{C}$. Let $\mathbf{g}_1, \cdots, \mathbf{g}_\omega \in \mathbb{F}_q^{n_s}$ be a sequence of vectors obtained as follows. For each i, $1 \leq i \leq \omega$, choose $\mathbf{g}_i$ such that

$$\mathbf{g}_i \notin \Delta_t(\mathbf{0}, m_t - \omega) + \langle\mathbf{g}_1, \cdots, \mathbf{g}_{i-1}\rangle, \tag{57}$$

and

$$\Delta_t(\mathbf{0}, m_t - \omega) \cap \langle\mathbf{g}_1, \cdots, \mathbf{g}_i\rangle = \{\mathbf{0}\}, \tag{58}$$

for each sink node t. If such $\mathbf{g}_1, \cdots, \mathbf{g}_\omega$ exist, then $\mathcal{C} = \langle \mathbf{g}_1, \cdots, \mathbf{g}_\omega \rangle$ is the desired message set since (58) holding for $i = \omega$ means $d_{\min,t} \geq m_t - \omega + 1$ for any sink node t.

We first prove that $\mathbf{g}_i$ satisfying (57) exists if the field size q is sufficiently large. Observe that

$$\begin{aligned} & |\Delta_t(\mathbf{0}, m_t - \omega) + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{i-1} \rangle| \\ \leq \; & |\Delta_t(\mathbf{0}, m_t - \omega)| q^{i-1} && (59) \\ \leq \; & \binom{|E|}{m_t - \omega} q^{m_t - \omega} q^{n_s - m_t} q^{i-1} && (60) \\ = \; & \binom{|E|}{m_t - \omega} q^{n_s - \omega + i - 1}. && (61) \end{aligned}$$

Thus, when considering all the sink nodes, we have at most

$$\sum_{t \in \mathcal{T}} \binom{|E|}{m_t - \omega} q^{n_s - \omega + i - 1} \tag{62}$$

vectors that cannot be chosen as $\mathbf{g}_i$. If

$$q > \sum_{t \in \mathcal{T}} \binom{|E|}{m_t - \omega}, \tag{63}$$

then there exists a vector that can be chosen as $\mathbf{g}_i$ for $i = 1, \cdots, \omega$.

Fix $\mathbf{g}_1, \cdots, \mathbf{g}_\omega$ that satisfy (57). We proof by induction that (58) holds for these $\mathbf{g}_i$ and any sink node t. If (58) does not hold for $i = 1$, then there exists a non-zero vector $\alpha \mathbf{g}_1 \in \Delta_t(\mathbf{0}, m_t - \omega)$, where $\alpha \in \mathbb{F}$. Since $\Delta_t(\mathbf{0}, m_t - \omega)$ is closed under scalar multiplication and $\alpha \neq 0$, we have $\mathbf{g}_1 \in \Delta_t(\mathbf{0}, m_t - \omega)$, a contradiction to (57) holding for $\mathbf{g}_1$. Assume (58) holds for $i \leq k - 1$. If (58) does not hold for $i = k$, then there exists a non-zero vector

$$\sum_{i=1}^{k} \alpha_i \mathbf{g}_i \in \Delta_t(\mathbf{0}, m_t - \omega), \tag{64}$$

where $\alpha_i \in \mathbb{F}_q$. If $\alpha_k = 0$,

$$\sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i \in \Delta_t(\mathbf{0}, m_t - \omega), \tag{65}$$

a contradiction to the assumption that (58) holds for $i = k-1$. Thus $\alpha_k \neq 0$. Again, by $\Delta_t(\mathbf{0}, m_t - \omega)$ being closed under scalar multiplication, we have

$$\begin{aligned} \mathbf{g}_k \; & \in \; \Delta_t(\mathbf{0}, m_t - \omega) - \alpha_k^{-1} \sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i && (66) \\ & \subset \; \Delta_t(\mathbf{0}, m_t - \omega) + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{k-1} \rangle, && (67) \end{aligned}$$

a contradiction to $\mathbf{g}_k$ satisfying (57). The proof is completed. ■

V. Concluding Remarks

Refined versions of the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound for network error correction in [1]–[3] are obtained. This refined Singleton bound is also shown to be tight for linear message sets. By employing the tools of network Hamming weight, the proofs presented here are considerably simpler and more transparent.

Appendix
Proof of an inequality

The inequality

$$\frac{q^m}{\sum_{i=0}^{r} \binom{m}{i} (q-1)^i} < \frac{q^{m+1}}{\sum_{i=0}^{r} \binom{m+1}{i} (q-1)^i} \tag{68}$$

for $r \leq m/2$ can be established by considering

$$\begin{aligned} \frac{q^m}{\sum_{i=0}^{r} \binom{m}{i} (q-1)^i} \; & = \; \frac{q^{m+1}}{\sum_{i=0}^{r} \frac{q(m-i+1)}{m+1} \binom{m+1}{i} (q-1)^i} && (69) \\ & < \; \frac{q^{m+1}}{\sum_{i=0}^{r} \binom{m+1}{i} (q-1)^i}, && (70) \end{aligned}$$

where (70) holds because $\frac{q(m-i+1)}{m+1} > 1$ given that $q \geq 2$ and $i \leq r \leq m/2$.

References

[1] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. IEEE ITW'02*, 2002.

[2] R. W. Yeung and N. Cai, "Network error correction, part I: basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19 – 36, 2006.

[3] N. Cai and R. W. Yeung, "Network error correction, part II: lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37 – 54, 2006.

[4] Z. Zhang, "Network error correction coding in packetized networks," in *Proc. IEEE ITW'06*, Oct. 2006.

[5] S. Yang and R. W. Yeung, "Characterizations of network error correction/detection and erasure correction," in *Proc. NetCod'07*, Jan. 2007.

[6] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory," *Foundation and Trends in Communications and Information Theory*, vol. 2, no. 4 and 5, pp. 241–381, 2005.

[7] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[8] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[9] S. Yang, C. K. Ngai, and R. W. Yeung, "Construction of linear network codes that achieve a refined Singleton bound," submitted to *ISIT'07*.

[10] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[11] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 1973 – 1982, June 2005.