Network Generalized Hamming Weight

Chi-Kin Ngai
Chinese University of Hong Kong
Hong Kong SAR
China
Email: ckngai@alumni.cuhk.net

Raymond W. Yeung
Chinese University of Hong Kong
Hong Kong SAR
Hong Kong
Email: whyeung@ie.cuhk.edu.hk

Zhixue Zhang[1]
School of Information and
Communication Engineering
Beijing University of Posts and
Telcommunications
Beijing, China
Email: zxzhang@ie.cuhk.edu.hk

Abstract — **In this paper, we extend the notion of generalized Hamming weight for classical linear block code to linear network codes by introducing the *network generalized Hamming weight (NGHW)* of a linear block code with respect to a given linear network code. The basic properties of NGHW are studied. We further show that NGHW can be used as a tool to characterize the security performance of a linear network code on a wiretap network. We also introduce the idea of Network Maximum Distance Separation code (NMDS code) by extending the notion of Maximum Distance Separation code in classical algebraic coding theory. We prove that NMDS codes play an important role in minimizing the information that an eavesdropper can obtain from the network.**

I. Introduction

Motivated by the work of Wei on generalized Hamming weight for linear block codes [1] and the work of Cai and Yeung on secure network coding [5], we extend the definition of generalized Hamming weight for linear block codes to linear network codes. To be more specific, we will define the *network generalized Hamming weight (NGHW)* for a linear block code with respect to a given linear network code. Based on the NGHW for linear network codes, we will prove a network extension of the generalized Singleton bound in [1] and show that it is tight. Moreover, through the construction of a linear network code that can achieve this bound, we can recover the construction of a secure network code in [5, 6].

By extending the original definition of the generalized Hamming weight, our network generalized Hamming weight can completely characterize the performance of linear network codes on a wiretap network [5, 6], which includes secret sharing in classical cryptography [3,4] as a special case.[2] The details of this application are discussed in Section IV.

The remainder of the paper is organized as follows. In Section II, we define NGHW and prove some of its basic properties. In Section III, we define network generalized Singleton bound and show its tightness under two different conditions. In addition, *Network Maximum Distance Separable* (*NMDS*) code will be discussed. In Section IV, we show that NGHW can completely characterize the security performance of a linear block code when it is applied in conjunction with a linear network code on a wiretap network. In Section V, we show NGHW reduces to the generalized Hamming weight in [1] when the network being considered is the degenerated network representing the classical communication channel.

II. Definitions

Wei [1] introduced the notion of generalized Hamming weight for the classical point-to-point channel which is closely related to the security of data transmission in the wiretap channel II model [2], which can be regarded as a special case of secret sharing [3, 4]. They showed that the generalized Hamming weight can completely characterize the performance of coset coding on a wiretap channel II.

In this section, by integrating the generalized Hamming weight with network coding, we extend the notion of the generalized Hamming weight to point-to-point communication networks. We will first define NGHW and then prove some of its basic properties. In the following, $\langle\cdot\rangle$ denotes the span of a set of vectors.

Definition 1. An n-dimensional linear network code is said to be *full rank* if there exists a set of n linearly independent global encoding kernels.

Definition 2 (Network Generalized Hamming Weight)**.** Let $\mathcal{C}$ be an (n, k) linear block code. The rth generalized Hamming weight of $\mathcal{C}$, denoted by $d_r(\mathcal{C}, F)$, with respect to a given n-dimensional full-rank linear network code specified by the set of global encoding kernels $F = \{f_e, e \in \mathcal{E}\}$, is defined as

$$d_r(\mathcal{C}, F) = \min_{\mathrm{W}\subset\mathcal{E}}\{|\mathrm{W}| : \mathcal{L}_{\mathrm{W}} \text{ contains some subcode } D \text{ of } \mathcal{C} \text{ with dimension } r\}, \tag{1}$$

where $\mathcal{L}_{\mathrm{W}} = \langle\{f_e^T, e \in \mathrm{W}\}\rangle$.

Note that in (1), if $\mathcal{L}_{\mathrm{W}}$ contains some subcode D of $\mathcal{C}$ with dimension r, then $dim(\mathcal{C} \cap \mathcal{L}_{\mathrm{W}}) \geq r$.

For $\mathrm{W} \subset \mathcal{E}$, let F_{W} be an $n\times|\mathrm{W}|$ matrix formed by the juxtaposition of $\{f_e, e \in \mathrm{W}\}$. When the network considered is reduced to the network with n channels connecting the source node s and the unique sink node t, with the

[1] This work was done when Z. Zhang was on leave at The Chinese University of Hong Kong.

[2] Secret sharing in turn includes wiretap channel II [2] as a special case.

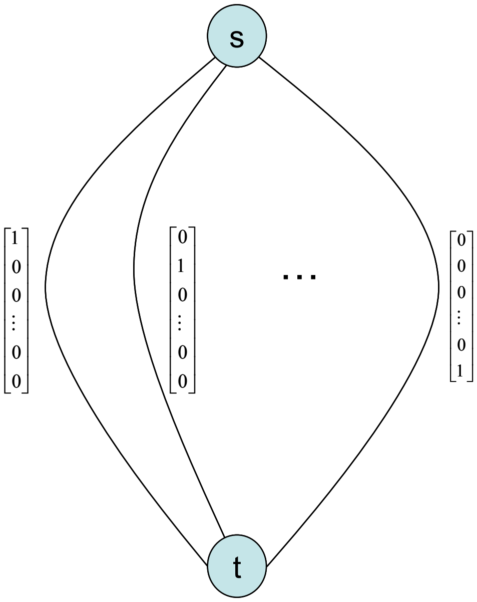

Figure 1: A degenerated network consisting of n-channels with $F_{\mathcal{E}} = I$.

global encoding kernels being the standard basis as indicated in Figure 1, the definition of $d_r(\mathcal{C}, F)$ reduces to the generalized Hamming weight in [1]. See Section V for a proof.

In the remainder of this section, we study several basic properties of NGHW. Whenever we refer to the NGHW of a linear block code $\mathcal{C}$, we always assume a given full-rank linear network code as prescribed in Definition 2.

Lemma 1 (Monotonicity)**.** *For an (n, k) linear block code $\mathcal{C}$ with $k > 0$,*

$$1 \le d_1(\mathcal{C}, F) < d_2(\mathcal{C}, F) < \cdots < d_k(\mathcal{C}, F) \le n. \tag{2}$$

Proof. See [9]. □

For an (n, k) linear block code $\mathcal{C}$, denote its $(n-k) \times n$ parity check matrix by $\mathbf{H}$, that is, for all $\mathbf{c} \in \mathcal{C}, \mathbf{H}\mathbf{c}^T = 0$. The following theorem gives a characterization of $d_r(\mathcal{C}, F)$ in terms of $\mathbf{H}$.

Theorem 1.

$$\begin{aligned} & d_r(\mathcal{C}, F) \\ &= \min_{W \subset \mathcal{E}} \{|W| : dim(\mathcal{L}_W) - \dim(\langle\{\mathbf{H}f_e, e \in W\}\rangle) \ge r\} \end{aligned} \tag{3}$$

Proof. See [9]. □

III. Network Generalized Singleton Bound and Network MDS codes

In this section, we define the generalized Singleton bound and show its tightness under two different settings. In addition, the class of *Network Maximum Distance Separable* (*NMDS*) codes will also be discussed.

In Section IV, we will see that NGHW has a very close relation with the security performance of a given linear network code. Moreover, achieving the generalized Singleton bound is in fact very closely related to achieving the maximum rate of secure linear multicast in the presence of an eavesdropper.

Theorem 2 (Generalized Singleton bound)**.** *For an (n, k) linear code $\mathcal{C}$, $d_r(\mathcal{C}, F) \le n - k + r$, for $1 \le r \le k$.*

Proof. From (2), we can see that $d_k(\mathcal{C}, F) \le n$. Assume that for $1 < r' \le k, d_{r'}(\mathcal{C}, F) \le n-k+r'$ is true. Then by the monotonicity of NGHW, $d_{r'-1}(\mathcal{C}, F) \le d_r'(\mathcal{C}, F) - 1 \le n - k + (r' - 1)$. The theorem is proved. □

In the rest of the paper, we write $d_1(\mathcal{C}, F)$ as d_1. Note that in the case of classical algebraic coding, d_1 is reduced to the minimum Hamming distance of $\mathcal{C}$.

Corollary 1. *An (n, k) linear code $\mathcal{C}$ satisfies*

$$|\mathcal{C}| \le q^{n-d_1+1}. \tag{4}$$

In Theorem 3 and 4, we will show that the generalized Singleton bound is tight for a linear multicast [8]. The result can easily be extended to a general linear network code. Here the tightness of the generalized Singleton bound has two meanings. The first one is, for a given set of global encoding kernels, we can find a linear code that achieves the tightness of the generalized Singleton bound. The second one is, for a given linear code, we can find a set of global encoding kernels that achieves the generalized Singleton bound.

Theorem 3. *Given any n-dimensional linear multicast over a finite field $\mathbb{F}$, when $|\mathbb{F}| = q$ is sufficiently large, there exists a linear code $\mathcal{C}$ with $|\mathcal{C}| = q^k$ such that*

$$d_1 = n - k + 1. \tag{5}$$

Proof. We start with any given set of global encoding kernels which defines a linear multicast, which is an n-dimensional full-rank linear network code. Let $\mathcal{W}' = \{\mathrm{W} \subset \mathcal{E} : |\mathrm{W}| = n - k\}$.

Now we construct the linear code $\mathcal{C}$. Let $\mathbf{g}_1, \cdots, \mathbf{g}_k \in \mathbb{F}_q^n$ be a sequence of row vectors obtained as follows. For each $i, 1 \le i \le k$, choose $\mathbf{g}_i$ such that

$$\mathbf{g}_i \notin \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{i-1} \rangle. \tag{6}$$

We first prove that $\mathbf{g}_i$ satisfying (6) exists if the field size q is sufficiently large. We observe that for all $i \le k$,

$$\begin{aligned}
&\left|\bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{i-1}\rangle\right| \\
&\le |\bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}| q^{i-1} && (7)\\
&\le \binom{|\mathcal{E}|}{n-k} q^{n-k} q^{i-1} && (8)\\
&= \binom{|\mathcal{E}|}{n-k} q^{n-k+i-1} && (9)\\
&\le \binom{|\mathcal{E}|}{n-k} q^{n-1} && (10)
\end{aligned}$$

which does not depend on i.
If

$$q > \binom{|\mathcal{E}|}{n-k}, \tag{11}$$

then there exists a vector that can be chosen as $\mathbf{g}_i$ for $i = 1, \cdots, k$. Note that by virtue of (6), $\mathbf{g}_i \ne 0$ for all i.

Fix $\mathbf{g}_1, \cdots, \mathbf{g}_k$ that satisfy (6). We prove by induction that

$$\left(\bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}\right) \cap \langle \mathbf{g}_1, \cdots, \mathbf{g}_i\rangle = \{0\} \tag{12}$$

holds for $1 \le i \le k$. If (12) does not hold for $i = 1$, then there exists a non-zero vector $\alpha\mathbf{g}_1 \in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}$, where $\alpha \in \mathbb{F}\backslash\{0\}$. Since $\bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}$ is closed under scalar multiplication and $\alpha \ne 0$, we have $\mathbf{g}_1 \in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}$, a contradiction to (6) for $i = 1$. Assume (12) holds for $i \le k-1$. If (12) does not hold for $i = k$, then there exists a non-zero vector

$$\sum_{i=1}^{k} \alpha_i \mathbf{g}_i \in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}, \tag{13}$$

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

$$\sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i \in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}, \tag{14}$$

a contradiction to the assumption that (12) holds for $i = k-1$. Thus $\alpha_k \ne 0$. Again, by $\bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}}$ being closed under scalar multiplication, we have

$$\begin{aligned}
\mathbf{g}_k &\in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}} - \left\{\alpha_k^{-1} \sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i\right\} && (15)\\
&\subset \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}\rangle, && (16)
\end{aligned}$$

a contradiction to (6) for $i = k$. Therefore, $\mathbf{g}_1, \cdots, \mathbf{g}_k$ satisfy (12), and we let $\mathcal{C} = \langle \mathbf{g}_1, \cdots, \mathbf{g}_k\rangle$.

For any subspace D of $\mathcal{C}$ and any $\mathrm{W} \subset \mathcal{E}$ with $|\mathrm{W}| \le n-k$, it follows from (12) for $i = k$ that

$$\mathcal{L}_{\mathrm{W}} \cap D = \{0\}. \tag{17}$$

In particular, (17) holds when the dimension of D is equal to 1. Therefore, by Definition 2, $d_1 \ge n-k+1$. Together with Theorem 2, we obtain

$$d_1 = n-k+1 \tag{18}$$

The proof is completed. □

Theorem 4. *Given an (n,k) linear code $\mathcal{C}$ with $|\mathcal{C}| = q^k$, we can construct a linear multicast over a finite field $\mathbb{F}$, when q is sufficiently large, such that*

$$d_1 = n-k+1 \tag{19}$$

Proof. We first use the Jaggi-Sanders algorithm in [7] to construct an n-dimensional deterministic linear multicast, whose global encoding kernels are denoted by $F' = \{f'_e, e \in \mathcal{E}\}$. Then we use the method in the proof of Theorem 3 to find an (n,k) linear code $\mathcal{C}'$ that achieves the upper bound in (4), i.e., $d_1(\mathcal{C}', F') = n-k+1$. We will show that $\mathcal{C}$ can be obtained from $\mathcal{C}'$ by taking an invertible linear transformation T, i.e., $T(c') = c'M$ for all $c' \in \mathcal{C}'$, where M is an $n \times n$ invertible matrix. Let $f_e = M^{-1} f'_e$ for $e \in \mathcal{E}$. We will further show that the set of global encoding kernel $F = \{f_e : e \in \mathcal{E}\}$ achieves the upper bound in (4).

i) Let G_0 be a $k \times n$ matrix formed by the first k rows of the $n \times n$ identity matrix I, and G and G' be the generator matrix of $\mathcal{C}$ and $\mathcal{C}'$, respectively. We form two invertible $n \times n$ matrices M_1 and M_2, such that the first k columns of M_1 and M_2 are G^T and G'^T respectively. Then $G_0 M_1^T = G$ and $G_0 M_2^T = G'$. Hence $G(M_2 M_1^{-1})^T = G'$ and M can be taken to be $M_2 M_1^{-1}$.

ii) The sink nodes in the network can still decode successfully with the new network code specified by the global encoding kernels $\{f_e : e \in \mathcal{E}\}$ since M is invertible. We now prove that the linear code $\mathcal{C}$ achieves the upper bound in (4) with respect to $F = \{f_e : e \in \mathcal{E}\}$. Assume that $\mathcal{C}$ does not achieve the upper bound, i.e., $d_1 \le n-k$ or $k < n - d_1 + 1$. Then according to the definition of the generalized Hamming weight, there exists $\mathbf{c} \in \mathcal{C}, \mathbf{c} \ne 0$ and $n-k$ global encoding kernels, say $f_1, f_2, \cdots, f_{n-k}$, such that $\mathbf{c} = a_1 f_1^T + \cdots + a_{n-k} f_{n-k}^T$ and $a_i, i = 1, \cdots, n-k$ are not all zero.

Therefore,

$$\mathbf{c} = (a_1 f_1'^T + a_2 f_2'^T + \cdots + a_{n-k} f_{n-k}'^T)(M^T)^{-1} \tag{20}$$

or

$$\mathbf{c} M^T = a_1 f_1'^T + a_2 f_2'^T + \cdots + a_{n-k} f_{n-k}'^T. \tag{21}$$

Let $c' = cM^{-1}$. Since $\langle c'\rangle$ is a 1-dimensional subcode of $\mathcal{C}'$, in light of (21) and Definition 2, $d_1(\mathcal{C}', F')$ is less than $n-k+1$. This is contradictory to that $\mathcal{C}'$ achieves the upper bound in (4).

The proof is completed. □

Theorem 5. *Given a linear code $\mathcal{C}$ (a linear multicast specified by $F = \{f_e, e \in \mathcal{E}\}$), we can find a corresponding linear multicast specified by $F = \{f_e, e \in \mathcal{E}\}$(linear code $\mathcal{C}$), such that the tightness of the generalized Singleton bound of $\mathcal{C}$ can be achieved, that is, $d_r(\mathcal{C}, F) = n - k + r$ for all $1 \le r \le k$.*

Proof. $d_1(\mathcal{C}, F) = n - k + 1$ is obtained by Theorem 3 (Theorem 4). Together with the monotonicity proved in Lemma 1 and the fact that $d_k(\mathcal{C}, F) \le n$, we see that $d_r(\mathcal{C}, F) = n - k + r$ for all $1 \le r \le k$. □

We will refer to those linear codes that achieve the generalized Singleton bound based on a given linear network code as *Network Maximum Distance Separable* (*NMDS*) codes. This terminology is motivated by the fact that in the classical channel, MDS codes are the only linear codes that can achieve the generalized Singleton bound induced by the generalized Hamming weight.

Definition 3. Given a full-rank linear network code, a *Network Maximum Distance Separable* (*NMDS*) code is a linear block code that achieves the tightness of the generalized Singleton bound.

By Theorem 4, for any full-rank block code, we can find a corresponding full-rank linear network code such that the generalized Singleton bound is achieved. In other words, any full-rank block code is an NMDS code for some full-rank linear network code. However, such a block code is not necessarily an MDS code.

On the other hand, with respect to the full-rank network code depicted in Figure 1, a linear block code is an NMDS code if and only if it is an MDS code.

IV. Security Performance of Linear Network Codes

The generalized Hamming weight in [1] can completely characterize the performance of a linear code $\mathcal{C}$ on wiretap channel II. The network generalized Hamming weight introduced in this paper can also fully characterize the performance of a linear code on the wiretap network.

In the model of wiretap network studied here, we assume that there is an eavesdropper in the network who can arbitrarily choose and fully access μ edges in the network. We define $\mathcal{W} := \{\mathrm{W} \subset \mathcal{E} : |\mathrm{W}| = \mu\}$ and say an eavesdropper is characterized by $\mathcal{W}$ if the eavesdropper can arbitrarily choose and access one and only one set in $\mathcal{W}$.

We denote the message that the source node wants to transmit securely by a k-dimensional row vector $\mathbf{s} \in \mathbb{F}_q^k$ and let $\mathcal{C}$ be an $(n, n-k)$ linear code and $\mathbf{H}$ be the $k \times n$ parity check matrix of $\mathcal{C}$. In order to protect the messages from the eavesdropper, we apply coset coding [2] based on $\mathcal{C}$ at the source node as follows: The encoded message that is transmitted in the network is denoted by an n-dimensional row vector $\mathbf{x} \in \mathbb{F}_q^n$. The source selects one of the q^k cosets to represent $\mathbf{s}$, and transmits a vector $\mathbf{x}$ chosen from that coset according to the uniform distribution. Equivalently, we can write

$$\mathbf{x} = [\ \mathbf{s} \quad \mathbf{r}\ ] \begin{bmatrix} G_M \\ G_C \end{bmatrix}, \tag{22}$$

where G_C is the $(n-k) \times n$ generator matrix of $\mathcal{C}$, G_M is any $k \times n$ full-rank matrix such that G_M and G_C together forms an $n \times n$ full-rank matrix, and $\mathbf{r}$ is chosen from $\mathbb{F}_q^{n-k}$ uniformly. The proof is omitted here due to limited space.

Let S be the random variable denoting the information source, X be the random variable denoting the source of the encoded message to be transmitted by the source node, and Y be the random variable denoting the message received by the eavesdropper.

We denote the symbols that the eavesdropper obtains by a $|\mathrm{W}|$-dimensional row vector $\mathbf{y} \in \mathbb{F}_q^{|\mathrm{W}|}$. Write $\mathbf{s} = (s_1, s_2, \cdots, s_k), \mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_{|\mathrm{W}|})$. The symbols in $\mathbf{s}$ and $\mathbf{x}$ are i.i.d. and chosen uniformly from $\mathbb{F}_q$. Since G_M and G_C together form an $n \times n$ full-rank matrix, for all $\mathbf{s} \in \mathbb{F}_q^k$ such that $\mathbf{s} \ne 0, \mathbf{s}G_M\mathbf{H}^T \ne 0$, otherwise, there exists a non-zero vector $R \in \mathbb{F}_q^{n-k}$ such that $\mathbf{s}G_M = \mathbf{r}G_C$. This contradicts the fact that G_M and G_R together forms a $n \times n$ full-rank matrix. Therefore, $G_M\mathbf{H}^T$ is invertible. Then letting $\mathbf{H}' = (G_M\mathbf{H}^T)^{-1}$, we have

$$\mathbf{x}\mathbf{H}^T\mathbf{H}' = [\ \mathbf{s} \quad \mathbf{r}\ ] \begin{bmatrix} G_M \\ G_C \end{bmatrix} \mathbf{H}^T\mathbf{H}' \tag{23}$$

$$= \mathbf{s}G_M\mathbf{H}^T\mathbf{H}' \tag{24}$$

$$= \mathbf{s}, \tag{25}$$

giving the formula for recovering the information source $\mathbf{s}$ from the encoded message $\mathbf{x}$.

We assume that the eavesdropper knows the $(n, n-k)$ linear code $\mathcal{C}$ and its parity check matrix $\mathbf{H}$ used in the coset coding scheme as well as the matrix $F_{\mathcal{E}}$. We define the uncertainty of the eavesdropper about the source as $\Delta = \min_{\mathrm{W} \in \mathcal{W}} H(S|Y)$, and say the network is perfectly secured if $\Delta = H(S) = k$. Here $H(\cdot)$ denotes entropy in the base q, and $H(\cdot|\cdot)$ denotes conditional entropy.

In [6], Rouayheb and Soljanin treated the secure network coding problem as a network generalization of wiretap channel II in [2], and coined the term "wiretap network." They gave a construction based on coset coding, which is equivalent to the approach in [5] with the exception that in [6] the linear block code at the source node must be an MDS code.

Theorem 6. *Given an acyclic directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, a linear multicast, and an eavesdropper characterized by $\mathcal{W} = \{W \subset \mathcal{E} : |W| \le \mu\}$, if we apply coset coding at the source node using an $(n, n-k)$ linear code $\mathcal{C}$, then*

i) the eavesdropper cannot obtain any information about the source, i.e., $\Delta = k$, if and only if $d_1(\mathcal{C}^\perp, F) > \mu$.

ii) *the eavesdropper can obtain r units of information about the source, i.e., $\Delta \leq k - r$, if and only if $\mu \geq d_r(\mathcal{C}^\perp, F)$.*

Proof. We first compute the uncertainty of the eavesdropper about the source. Let $\mathbf{H}$ be the parity check matrix of $\mathcal{C}$. Then

$$(\mathbf{H}')^T \mathbf{H} \mathbf{x}^T = \mathbf{s}^T \tag{26}$$

according to (25) and

$$\mathbf{x} F_{\mathrm{W}} = \mathbf{y}. \tag{27}$$

The uncertainty we seek is given by

$$\begin{aligned} \Delta &= \min_{\mathrm{W} \in \mathcal{W}} H(S|Y) & (28)\\ &= \min_{\mathrm{W} \in \mathcal{W}} \left\{ H(S|X,Y) + H(X|Y) - H(X|S,Y) \right\}. & (29) \end{aligned}$$

Writing (26) and (27) together in matrix form, we have

$$\begin{bmatrix} \mathbf{H'}^T \mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix} \mathbf{x}^T = \begin{bmatrix} \mathbf{s}^T \\ \mathbf{y}^T \end{bmatrix}. \tag{30}$$

The dimension of solution space of (30) is $n - rank\left(\begin{bmatrix} \mathbf{H'}^T \mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix} \right)$.

Since we assumed $\mathbf{x}$ is uniformly distributed,

$$\begin{aligned} &H(X|S,Y)\\ &= n - rank\left(\begin{bmatrix} \mathbf{H'}^T \mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix} \right) & (31)\\ &= n - rank(\mathbf{H'}^T \mathbf{H}) - rank(F_{\mathrm{W}}^T) + \dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}} \right) & (32)\\ &= n - k - rank(F_{\mathrm{W}}^T) + \dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}} \right), & (33) \end{aligned}$$

where (32) follows from the fact $\mathbf{H}'$ is a full-rank matrix and (33) follows from (25). Together with $H(S|X,Y) = 0$ and $H(X|Y) = n - rank(F_{\mathrm{W}})$, we have from (29)

$$\Delta = k - \max_{\mathrm{W} \in \mathcal{W}} \dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}} \right). \tag{34}$$

From (34), the proof for i) and ii) follows immediately:

i) $d_1(\mathcal{C}^\perp, F) > \mu$, i.e., for all $\mathrm{W} \in \mathcal{W}$, $\dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}} \right) = 0$, is equivalent to $\Delta = k$.

ii) $\mu \geq d_r(\mathcal{C}^\perp, F)$, i.e., there exists $\mathrm{W} \in \mathcal{W}$ s.t. $\dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}} \right) = r$, is equivalent to $\Delta \leq k - r$.

□

In other words, similar to the role of the generalized Hamming weight in [1] for the classical point-to-point channel, our network generalized Hamming weight can also be used to measure the security performance of a linear code $\mathcal{C}$ for a given linear network code on a given network.

We will see that applying coset coding using a code $\mathcal{C}$ whose dual is an NMDS code is in fact a linear network code with optimal security performance. The following theorem gives a lower bound on the information of the source that the eavesdropper can obtain regardless of the coding scheme being used to multicast information.

Theorem 7. *Given an acyclic directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with maxflow n, and a linear multicast transmitting information at rate k from the source node s to the set of sink nodes $\mathcal{T}$, the information that the eavesdropper, who can wiretap any set of τ channels, where $n - k \leq \tau \leq n$, can obtain at least $k + \tau - n$ units of information.*

Proof. See [9]. □

By Definition 3, an NMDS code achieves the tightness of the generalized Singleton bound, i.e.,

$$d_r(\mathcal{C}^\perp, F) = n - k + r. \tag{35}$$

Let r' be the maximum amount of information the eavesdropper can obtain by wiretapping τ channels. Then by ii) of Theorem 6,

$$\tau \geq d'_r(\mathcal{C}^\perp, F) = n - k + r' \tag{36}$$

which implies

$$r' \leq k + \tau - n. \tag{37}$$

Therefore, the maximum amount of information that the eavesdropper can obtain is $k + \tau - n$ which is also minimal according to Theorem 7. Therefore, we see that applying coset coding using a code $\mathcal{C}$ whose dual is an NMDS code is in fact constructing a linear network code which guarantees that the information obtained by the eavesdropper is minimal, that is, the security performance of the overall linear network code is optimal.

According to [1], if we apply coset coding based on an $(n, n-k)$ linear code $\mathcal{C}$ in the wiretap channel II problem, the eavesdropper who can access at most $(n-k)$ channels gains no information about the source (we say the system achieves the best security performance) if and only if the dual code of $\mathcal{C}$ is an MDS code. In our problem, the network achieves the best security performance if and only if the dual code of $\mathcal{C}$ is an NMDS code.

Corollary 2. *Given an acyclic directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ and a linear multicast achieving the maxflow bound n, if we apply coset coding at the source based on an $(n, n-k)$ linear code $\mathcal{C}$, such that $\mathcal{C}^\perp$ is an NMDS code, then the network is perfectly secure against any eavesdropper with $\mathcal{W}' = \{W \subset \mathcal{E} : |W| \leq n - k\}$ while information can be multicast to the sink nodes at the rate of k.*

In [6], Rouayheb and Soljanin gave a coding scheme, which is a construction of linear secure network code based on an MDS code. According to our analysis of the NMDS code, one can construct a linear secure network code based on any full-rank linear block code.

V. Reduction to the Classical Communication Channel

In this section, we show that our network generalized Hamming weight reduces to the generalized Hamming weight in [1] when the network being considered is the degenerated network representing the classical communication channel. In such a network, there are only one source node and one sink node. The source node is connected directly to the sink node by n channels. Let the global encoding kernels of the channels be $\delta_i, 1 \leq i \leq n$, respectively, where δ_i is the unit n-dimensional column vector whose components are all equal to zero except that the ith component is equal to 1.

According to our definition,

$$\begin{aligned} d_r(\mathcal{C}, F) = \min \big\{ |\mathrm{W}| : \big\langle \big\{ \delta_i^T, i \in \mathrm{W} \big\} \big\rangle & \text{ contains} \\ \text{some subcode } D \text{ of } \mathcal{C} \text{ with dimension } r \big\}, & \end{aligned} \tag{38}$$

where $F = \{\delta_i, 1 \leq i \leq n\}$. We will show that (38) is equivalent to the definition of the generalized Hamming weight for the classical point-to-point channel.

The support of a subcode D of C, denoted $\mathcal{X}(D)$, is the set of "not-always-zero" element positions of D, that is,

$$\mathcal{X}(C) \triangleq \{i : \exists\ (x_1, x_2, \ldots, x_n) \in C, x_i \neq 0\}. \tag{39}$$

Definition 4. (Generalized Hamming Weight [1])

$$d'_r(\mathcal{C}) \triangleq \min\{|\mathcal{X}(D)| : D \text{ is a subcode of} \tag{40}$$

$$C \text{ with dimension } r\}. \tag{41}$$

Let D be a subcode of C with dimension r such that $|\mathcal{X}(D)| = d'_r(\mathcal{C})$. Without loss of generality, assume $\mathcal{X}(D) = \{1, 2, \ldots, d'_r(\mathcal{C})\}$. This implies that for all $\mathbf{x} \in D, x_i = 0$ for $d'_r(\mathcal{C}) + 1 \leq i \leq n$. This further implies that for all $\mathbf{x} \in D, x \in \big\langle \big\{ \delta_i^T, 1 \leq i \leq d'_r(\mathcal{C}) \big\} \big\rangle$. Therefore,

$$d_r(\mathcal{C}, F) \leq d'_r(\mathcal{C}). \tag{42}$$

On the other hand, let $\mathrm{W} \subset \{1, 2, \ldots, n\}$ and $|\mathrm{W}| = d_r(\mathcal{C}, F)$ such that $\langle \{\delta_i, i \in \mathrm{W}\} \rangle$ contains some subcode D of C with dimension r. Without loss of generality, assume $\mathrm{W} = \{1, 2, \ldots, d_r(\mathcal{C}, F)\}$. This implies for all $\mathbf{x} \in D, x_i = 0$ where $d_r(\mathcal{C}, F) + 1 \leq i \leq n$. This further implies $\mathcal{X}(D) \subset \{1, 2, \ldots, d_r(\mathcal{C}, F)\}$ and $|\mathcal{X}(D)| \leq d_r(\mathcal{C}, F)$. Therefore,

$$d'_r(\mathcal{C}) \leq d_r(\mathcal{C}, F). \tag{43}$$

VI. Conclusion

In this paper, we have introduced the network generalized Hamming weight of a linear block code with respect to the set of global encoding kernels of a given linear network code. We have obtained the network generalized Singleton bound and proved its achievability. In addition, the network generalized Hamming weight can completely characterize the security performance of a linear block code when it is applied in conjunction with a linear network code on a wiretap network. Moreover, the previous constructions of secure network codes in [5] and [6] can be regarded as a construction of an NMDS code for any given linear network code.

Acknowledgment

The work of R. Yeung was supported in part by a grant from the Research Grant Committee of the Hong Kong Special Administrative Region, China (RGC Ref. No. CUHK 418006), a grant from the European Community (FP7-INFSO-ICT-215252, N-Crave Project), and a research grant from Qualcomm China, and a gift from Cisco, Inc.

References

[1] V. K. Wei,"Generalized Hamming Weight for Linear Codes," *IEEE Trans. Inform. Theory*,vol. 37 , no. 5, pp 1412-1418, Sep.1991.

[2] L. H. Ozarow and A. D. Wyner,"Wire-tap-channel II," AT& T Bell Labs Technical Journal, Vol63, pp.2135-2157, 1984.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc.* the National Computer Conference, 48: 313-317, 1979.

[4] A. Shamir, "How to share a secret," *Comm.* ACM, 22: 612-613, 1979.

[5] N. Cai and R. W. Yeung,"Secure Network Coding", in *Proc.* 2002 IEEE International Symposium on Information Theory, June 2002. Journal version submitted to *IEEE Trans. Inform. Theory*.

[6] S. Y. E. Rouayheb and E. Soljanin, "On Wiretap Networks II," in *Proc.* 2007 IEEE International Symposium on Information Theory, June 2007.

[7] S. Jaggi et al., "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inform. Theory*, vol.51, no. 6, pp.1973-1982, June 2005.

[8] R. W. Yeung, *A First Course in Information Theory,* Kluwer Academic/Plenum Publishers, 2002.

[9] C. K. Ngai, *Network Coding for Security and Error Correction*, Ph.D. Thesis, 2008.