IEICE TRANS. FUNDAMENTALS, VOL.E91–A, NO.12 DECEMBER 2008

PAPER Special Section on Signal Design and its Application in Communications

Some Upper Bounds on the Inverse Relative Dimension/Length Profile*

Peisheng WANG[†a)], *Nonmember*, **Yuan LUO**[†], *Member*, *and* **A.J. Han VINCK**[††], *Nonmember*

SUMMARY The generalized Hamming weight played an important role in coding theory. In the study of the wiretap channel of type II, the generalized Hamming weight was extended to a two-code format. Two equivalent concepts of the generalized Hamming weight hierarchy and its two-code format, are the inverse dimension/length profile (IDLP) and the inverse relative dimension/length profile (IRDLP), respectively. In this paper, the Singleton upper bound on the IRDLP is improved by using a quotient subcode set and a subset with respect to a generator matrix, respectively. If these new upper bounds on the IRDLP are achieved, in the corresponding coordinated two-party wire-tap channel of type II, the adversary cannot learn more from the illegitimate party.

key words: *generalized Hamming weight, inverse relative dimension/length profile, quotient subcode set, wiretap channel of type II*

1. Introduction

The generalized Hamming weight provided by Wei [3] was widely used in communication theory and coding theory. It was extended to a two-code format by Luo, Mitrpant, Han Vinck, and Chen [2], in the study of the wiretap channel of type II which was invented by Wyner and Ozarow [4], [5].

Two equivalent concepts of the generalized Hamming weight hierarchy and its two-code format, are the inverse dimension/length profile (IDLP) [1] and the inverse relative dimension/length profile (IRDLP) [2], respectively.

In this paper, we consider some upper bounds on the IRDLP. Some preliminaries about the IDLP and the IRDLP are introduced in Sect. 2. Section 3 provides a definition of a quotient subcode set and calculates its cardinality.

The relations between the IDLP and the IRDLP are investigated in Sect. 4, see Theorem 2, etc. Then, by using the quotient subcode set, the only known upper bound on the IRDLP (the generalized Singleton bound [2]) is improved, see Corollary 1.

Since it is not easy to calculate the upper bound in Corollary 1, some other upper bounds are studied in Sect. 5, see Algorithm 1 and Corollary 4. In Sect. 6, These new bounds on the IRDLP are proved to be better than the Singleton bound.

Section 7 demonstrates that, if these bounds on the IRDLP are achieved, the adversary cannot learn more from the illegitimate party in the corresponding coordinated two-party wire-tap channel of type II, see Fig. 1. Conclusions are presented in Sect. 8.

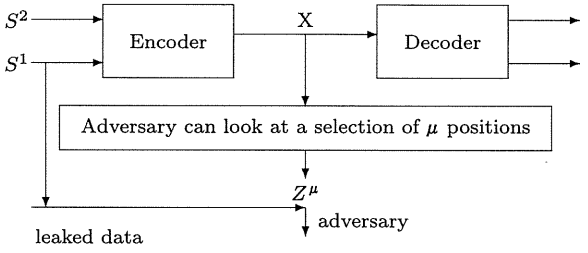


Fig. 1 A coordinated two-party wire-tap channel of type II when S^1 are leaked.

A summary of this paper was presented at IWSDA'07 [6]. All of the contents after Remark 1 are complementary materials with proofs for this full paper.

2. Preliminary

In the first part of this section, the IDLP and the IRDLP are introduced. Then, in the second part, we consider how to compare two sequences with each other in Definition 1 and Definition 2, which are useful for the establishment of some upper bounds on the IRDLP in Sect. 4 and Sect. 5.

In this paper, the linear codes are over $GF(2)$. 0^n denotes the all-zero vector of length n. Φ denotes the empty set. Let J be a subset of $I = \{1, 2, ..., n\}$. For an $[n, k]$ linear code C, its projection is denoted by

$$P_J(C) := \{P_J(\mathbf{c}) : \mathbf{c} = (c_1, c_2, ..., c_n) \in C\},$$

where $P_J(\mathbf{c})_j = c_j$ if $j \in J$, and $P_J(\mathbf{c})_j = 0$ if $j \in I - J$. For example, $P_{\{1,2,3\}}(1,0,1,0,1,0) = (1,0,1,0,0,0)$. The support of C is denoted by

$$supp(C) := \{j : \text{there exists } \mathbf{c} \in C \text{ such that } c_j \neq 0\}.$$

The inverse dimension/length profile (IDLP) of an $[n, k]$ linear code C, is a sequence (see [1])

$$\widetilde{\mathbf{k}}(C) = \{\widetilde{k}_i(C) : 0 \leq i \leq n\},$$

where

$$\widetilde{k}_i(C) = min\{\dim(P_J(C)) : |J| = i\}. \quad (1)$$

The inverse relative dimension/length profile (IRDLP)

Manuscript received January 16, 2008.
Manuscript revised June 30, 2008.
†The authors are with Computer Science and Engineering Department, Shanghai Jiao Tong University, Shanghai, China.
††The author is with Institute for Experimental Mathematics, Duisburg-Essen University, Germany.
*A summary of this paper was presented at IWSDA07.
a) E-mail: yuanluo@sjtu.edu.cn
DOI: 10.1093/ietfec/e91–a.12.1

of an $[n, k]$ linear code C and a linear subcode C^1, is a sequence (see [2])

$$\widetilde{\mathbf{k}}(C, C^1) = \{\widetilde{k}_i(C, C^1) : 0 \le i \le n)\},$$

where

$$\widetilde{k}_i(C, C^1) := min\{\dim[P_J(C)] - \dim[P_J(C^1)] : |J| = i\}. \quad (2)$$

The IDLP can be retrieved from the IRDLP if $\dim[C^1] = 0$.

Example 1: Let C be a $[7, 3]$ linear code with a generator matrix A, where

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Then $\widetilde{\mathbf{k}}(C) = \{0, 0, 1, 1, 2, 2, 3, 3\}$. Let C^1 be a $[7, 2]$ linear subcode with a generator matrix

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Then $\widetilde{\mathbf{k}}(C, C^1) = \{0, 0, 0, 0, 0, 1, 1, 1\}$.

Below we consider how to compare two sequences with each other by using two methods. In Definition 1, each component of the two sequences is investigated. Definition 2 depends on a dictionary order.

Definition 1: For any two integer sequences $\mathbf{s} := \{s_0, ..., s_n\}$ and $\mathbf{t} := \{t_0, ..., t_n\}$ with the same length, we say that $\mathbf{s}$ is upper-bounded (lower-bounded) by $\mathbf{t}$, if $s_i \le t_i (s_i \ge t_i)$ for $0 \le i \le n$.

Definition 2: For any two integer sequences $\mathbf{s} := \{s_0, ..., s_n\}$ and $\mathbf{t} := \{t_0, ..., t_n\}$ with the same length, we say that $\mathbf{s} \succ \mathbf{t}$, if there exists $j (0 \le j \le n)$ such that $s_j > t_j$ and $s_i = t_i$ for $0 \le i \le j - 1$. Denote that $\mathbf{s} \succeq \mathbf{t}$ if $\mathbf{s} \succ \mathbf{t}$ or $\mathbf{s} = \mathbf{t}$.

It is easy to verify that, any two integer sequences with the same length could be compared with each other by the dictionary order relation "$\succeq$." Therefore, if S is a finite set of sequences with the same length, we can define a minimum sequence

$$\min_{\succeq}\{\mathbf{s} : \mathbf{s} \in S\}$$

by the relation "$\succeq$," i.e., $\mathbf{t} \succeq \min_{\succeq}\{\mathbf{s} : \mathbf{s} \in S\}$ for any $\mathbf{t} \in S$. Note that, "$\mathbf{s} \succeq \mathbf{t}$" doesn't mean that $\mathbf{t}$ is upper-bounded by $\mathbf{s}$. For example, let $\mathbf{s} = \{0, 0, 1, 1, 1, 2, 3\}$ and $\mathbf{t} = \{0, 0, 0, 1, 2, 2, 3\}$. Then $\mathbf{s} \succ \mathbf{t}$, but $\mathbf{t}$ is not upper-bounded by $\mathbf{s}$.

3. Quotient Subcode Set

In order to study the relations between the IDLP and the IRDLP, we introduce a definition of a quotient subcode set in this section. The cardinality of the quotient subcode set is investigated in Theorem 1.

Definition 3: Let C be a linear code with length n, and C^1 be its subcode. A quotient subcode set of C to C^1, is denoted by

$$M_{C,C^1} := \{C^2 : C = C^1 \oplus C^2, \; C^2 \text{ is a linear subcode of C}\},$$

where $C^1 \oplus C^2$ is the direct sum of C^1 and C^2. The direct sum implies the condition $C^1 \cap C^2 = \{0^n\}$.

If $C^1 = C$, $M_{C,C^1} = \{\{0^n\}\}$. If $C^1 = \{0^n\}$, $M_{C,C^1} = \{C\}$.

For any $C^2 \in M_{C,C^1}$, C^2 and C/C^1 are isomorphic. An example is presented as follows.

Example 2: Let C and C^1 be linear codes of Example 1. Then, the quotient subcode set M_{C,C^1} is a set of four linear codes C^2, C^3, C^4, C^5 with generator matrices A_2, A_3, A_4, A_5, respectively, where

$$A_2 = (1\,0\,0\,0\,0\,1\,1), \quad A_3 = (1\,1\,0\,0\,1\,1\,0),$$
$$A_4 = (1\,0\,1\,0\,1\,1\,0), \quad A_5 = (1\,1\,1\,0\,0\,1\,1).$$

Generally, the number of elements in M_{C,C^1} is calculated in Theorem 1. Lemma 1 presents the number of all generator matrices of all of the linear codes in M_{C,C^1}.

Lemma 1: For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, let GM_{C,C^1} be a set

$$\{G : G \text{ is a generator matrix of any code in } M_{C,C^1}\}.$$

Then,

$$|GM_{C,C^1}| = (2^k - 2^{k_1})(2^k - 2^{k_1+1}) \cdots (2^k - 2^{k-1}).$$

Proof. Let $A_1 = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_{k_1} \end{pmatrix}$ be a generator matrix of C^1. Then a matrix $A_2 = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_{k-k_1} \end{pmatrix}$ is a generator matrix of any code in M_{C,C^1}, if and only if $\alpha_1, \alpha_2, ..., \alpha_{k_1}, \beta_1, \beta_2, ..., \beta_i$ are linearly independent for any $1 \le i \le k - k_1$, where $\beta_i \in C$. This lemma follows from the fact that, if we determine the matrix A_2 from β_1 to β_{k-k_1} one by one, the number of all possible β_i is $2^k - 2^{k_1+i-1}$. □

Theorem 1: For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, $|M_{C,C^1}| = 2^{k_1 k_2}$ where $k_2 = k - k_1$.

Proof. It follows from Lemma 1 that,

$$|GM_{C,C^1}| = (2^k - 2^{k_1})(2^k - 2^{k_1+1})...(2^k - 2^{k_1+k_2-1}),$$

and

$$|GM_{C^2}| = (2^{k_2} - 2^0)(2^{k_2} - 2^1)...(2^{k_2} - 2^{k_2-1}),$$

where C^2 is any fixed code with dimension k_2 in M_{C,C^1}, and GM_{C^2} is a set of all generator matrices of the code C^2. Therefore,

$$|M_{C,C^1}| = \frac{|GM_{C,C^1}|}{|GM_{C^2}|} = 2^{k_1 k_2}.$$

□

In Example 2, we have $|M_{C,C^1}| = 4$.

4. Relations between the IDLP and the IRDLP

In this section, a relation between the IDLP and the IRDLP is studied in Theorem 2. Then, an upper bound on the IRDLP is obtained in Corollary 1 by using the quotient subcode set. A necessary and sufficient condition for achieving the bound is provided. This bound is proved to be better than the generalized Singleton bound [2] in Sect. 6. Corollary 1 follows from Lemma 2 and Theorem 2.

For the proofs of Lemma 2, Theorem 2 and Corollary 1, please refer to our summary paper [6].

Lemma 2: For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, we have

$$\dim[P_J(C)] - \dim[P_J(C^1)] \leq \dim[P_J(C^2)], \tag{3}$$

where $C^2 \in M_{C,C^1}$ and $J \subseteq I = \{1, 2, ..., n\}$. For a given $J \subseteq I$, the equality (3) holds if and only if $\dim[P_J(C^1) \cap P_J(C^2)] = 0$. The equality (3) holds for any subset J if and only if $supp(C^1) \cap supp(C^2) = \Phi$.

By using Lemma 2, a relation between the components of the IRDLP and the IDLP is investigated in Theorem 2.

Theorem 2: Let C be an $[n, k]$ linear code and C^1 be an $[n, k_1]$ subcode. Then for any $C^2 \in M_{C,C^1}$,

$$\widetilde{k}_i(C, C^1) \leq \widetilde{k}_i(C^2), \tag{4}$$

where $0 \leq i \leq n$. The equality (4) holds if $supp(C^1) \cap supp(C^2) = \Phi$.

Example 3: The first part of Theorem 2 can be verified by Example 2 as follows, where C^2 is replaced with the subcodes C^2, C^3, C^4 and C^5 in Example 2, respectively.

$$\widetilde{\mathbf{k}}(C, C^1) = \{0, 0, 0, 0, 0, 1, 1, 1\},$$
$$\widetilde{\mathbf{k}}(C^2) = \{0, 0, 0, 0, 0, 1, 1, 1\},$$
$$\widetilde{\mathbf{k}}(C^3) = \{0, 0, 0, 0, 1, 1, 1, 1\},$$
$$\widetilde{\mathbf{k}}(C^4) = \{0, 0, 0, 0, 1, 1, 1, 1\},$$
$$\widetilde{\mathbf{k}}(C^5) = \{0, 0, 0, 1, 1, 1, 1, 1\}.$$

It is easy to see from Theorem 2 that, $\widetilde{\mathbf{k}}(C, C^1)$ is upper-bounded by $\widetilde{\mathbf{k}}(C^2)$ if $C^2 \in M_{C,C^1}$, see Corollary 1.

Corollary 1: For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, $\widetilde{\mathbf{k}}(C, C^1)$ is upper-bounded by

$$UP(\widetilde{\mathbf{k}}(C, C^1)) := \min_{\geq}\{\widetilde{\mathbf{k}}(C^2) : C^2 \in M_{C,C^1}\}.$$

Furthermore, $UP(\widetilde{\mathbf{k}}(C, C^1))$ is achieved if and only if there exists a code $C^{2*} \in M_{C,C^1}$ such that $\widetilde{\mathbf{k}}(C^{2*}) = \widetilde{\mathbf{k}}(C, C^1)$.

Remark 1: It follows from Theorem 2 and Corollary 1 that, if there exists $C^2 \in M_{C,C^1}$ such that $supp(C^1) \cap supp(C^2) = \Phi$, then the upper bound $UP(\widetilde{\mathbf{k}}(C, C^1))$ is achieved.

In Example 3, $\widetilde{\mathbf{k}}(C, C^1) = \{0, 0, 0, 0, 0, 1, 1, 1\} = UP(\widetilde{\mathbf{k}}(C, C^1))$, i.e. $UP(\widetilde{\mathbf{k}}(C, C^1))$ is achieved, but $supp(C^1) \cap supp(C^2) \neq \Phi$. Therefore, $supp(C^1) \cap supp(C^2) = \Phi$ in Remark 1 is only a sufficient but not necessary condition for achieving the bound $UP(\widetilde{\mathbf{k}}(C, C^1))$.

Furthermore, $UP(\widetilde{\mathbf{k}}(C, C^1))$ is clarified in the case of $\dim[C^2] = 1$, see Corollary 2.

Corollary 2: For an $[n, k]$ linear code C and an $[n, k-1]$ subcode C^1, $UP(\widetilde{\mathbf{k}}(C, C^1)) = \widetilde{\mathbf{k}}(C^{2*})$, where C^{2*} is a one-dimension subcode of C and the only nonzero codeword $\mathbf{c}$ in C^{2*} is the one with the smallest Hamming weight in $C \setminus C^1$.

Proof. Denoted by $w_H(C^{2*})$ the Hamming weight of the codeword $\mathbf{c}$. Then $\widetilde{\mathbf{k}}(C^2) = \{\pi_i : 0 \leq i \leq n\} = \{0, ..., 0, 1, ..., 1\}$, where $min\{i : \pi_i = 1\} = n - w_H(C^2) + 1$. Furthermore, $C^{2*} \in M_{C,C^1}$. Therefore $\min_{\geq}\{\widetilde{\mathbf{k}}(C^2) : C^2 \in M_{C,C^1}\} = \widetilde{\mathbf{k}}(C^{2*})$, and

$$UP(\widetilde{\mathbf{k}}(C, C^1)) = \widetilde{\mathbf{k}}(C^{2*}).$$

□

5. Some Other Upper Bounds on the IRDLP

An upper bound $UP(\widetilde{\mathbf{k}}(C, C^1))$ on the IRDLP is introduced in Corollary 1. But it is unrealistic to calculate the bound through exhaustive search in M_{C,C^1} when k is large.

In this section, by using Algorithm 1, some new upper bounds on the IRDLP are introduced in Remark 2 and Corollary 4, which are also better than the generalized Singleton bound (see Sect. 6). Compared with Corollary 1, the new bounds can be calculated more easily, see Remark 2. But the bounds of Corollaries 1 and 4 cannot be compared with each other by Definition.1.

In order to get some new bounds on the IRDLP in polynomial time, Algorithm 1 is provided in the following to select a code $C^2 \in M_{C,C^1}$.

Algorithm 1: Given a generator matrix G of an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, where $G = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_k \end{pmatrix}_{k \times n}$. There are four steps to find k_2 row vectors of G, where $k_2 = k - k_1$, which span a linear code of M_{C,C^1}:

1. Let $G_1 = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_{k_1} \end{pmatrix}_{k_1 \times n}$ be a generator matrix of C^1, which is not necessarily a part of G. Since C^1 is a subcode of C, there exists a matrix $P = \begin{pmatrix} p_1 \\ p_2 \\ \cdots \\ p_{k_1} \end{pmatrix}_{k_1 \times k}$ satisfying

$$G_1 = PG, \tag{5}$$

where p_i is obtained by solving a system of linear equations $\beta_i = p_i G$. P is unique and has rank k_1.

2. Let $Q = \begin{pmatrix} q_1 \\ q_2 \\ \cdots \\ q_{k_1} \end{pmatrix}_{k_1 \times k}$ be the row reduced echelon (RRE) form of P. It can be proved that Q only depends on G and C^1 later. Assume that the positions of the first non-zero elements (**leading 1**) of its row vectors are $a_1 < a_2 < \cdots < a_{k_1}$, respectively.
3. Denote

$$I_i = supp(q_i) \cap \{1, 2, ..., a_{i+1} - 1\} \subseteq \{a_i, ..., a_{i+1} - 1\}, \tag{6}$$

where $1 \le i \le k_1$ and $a_{k_1+1} = k + 1$. It's easy to see that $a_i \in I_i$ and $I_i \cap I_j = \Phi$ if $i \ne j$.
4. Let

$$J = \{j_1, ..., j_{k_1}\} \subseteq L = \{1, 2, ..., k\}, \tag{7}$$

where j_i is any element of I_i. Then the sequence $j_1, ..., j_{k_1}$ is strictly increasing and

$$I_i \cap J = \{j_i\}. \tag{8}$$

Denote $L - J$ by $\{l_1, l_2, ..., l_{k_2}\}$. It follows that $\alpha_{l_1}, .., \alpha_{l_{k_2}}, \beta_1, \beta_2, ..., \beta_{k_1}$ are linearly independent. Let C^2 be the code spanned by $\alpha_{l_1}, .., \alpha_{l_{k_2}}$. Then, C^2 is a linear code of M_{C,C^1}.

Remark 2:

- For given G and G_1, Algorithm 1 can be completed in polynomial time. Then it is easy to construct a code $C^2 \in M_{C,C^1}$ such that $\widetilde{\mathbf{k}}(C^2)$ is an upper bound on $\widetilde{\mathbf{k}}(C, C^1)$.
- The matrix Q only depends on G and C^1,see Corollary 3. For given G and C^1, the set J of (7) is not unique, and therefore the code C^2 is not unique too. Denote by M_{G,C^1} the set of all possible C^2 in Algorithm 1 for given G and C^1. Then

$$M_{G,C^1} \subseteq M_{C,C^1} \quad \text{and} \quad |M_{G,C^1}| \ll |M_{C,C^1}|.$$

- Theorem 2 implies that $\widetilde{\mathbf{k}}(C, C^1)$ is upper-bounded by $\widetilde{\mathbf{k}}(C^2)$. In the proof of Theorem 4, it is shown that, if G is RRE and $C^2 \in M_{G,C^1}$, then the bound $\widetilde{\mathbf{k}}(C^2)$ is better than the generalized Singleton bound on $\widetilde{\mathbf{k}}(C, C^1)$.

The correctness of Algorithm 1 is presented in Lemma 3.

Lemma 3: The vectors $\alpha_{l_1}, ..., \alpha_{l_{k_2}}$ obtained in step 4 of Algorithm 1 satisfy that $\alpha_{l_1}, ..., \alpha_{l_{k_2}}, \beta_1, ..., \beta_{k_1}$ are linearly independent.

Proof. There are 3 steps to prove the lemma, using the arguments of Algorithm 1.

1. The proof of this lemma is converted to the prove that the matrix (10) is reversible.

Assume that $G_2 = \begin{pmatrix} \alpha_{l_1} \\ \alpha_{l_2} \\ \cdots \\ \alpha_{l_{k_2}} \end{pmatrix}_{k_2 \times n}$, where l_i is given in step 4 of Algorithm 1. Denote $R = \begin{pmatrix} r_1 \\ r_2 \\ \cdots \\ r_{k_2} \end{pmatrix}_{k_2 \times k}$ such that

$$G_2 = RG. \tag{9}$$

Note that, R has full row rank and is unique, G_2 is a submatrix of G and $supp(r_i) = \{l_i\}$ for $1 \le i \le k_2$. It follows from (5) and (9) that

$$\begin{pmatrix} G_1 \\ G_2 \end{pmatrix}_{k \times n} = \begin{pmatrix} P \\ R \end{pmatrix}_{k \times k} G.$$

Therefore, to prove "$\alpha_{l_1}, ..., \alpha_{l_{k_2}}, \beta_1, ..., \beta_{k_1}$ are linearly independent" in Algorithm 1, we only need to prove that

$$\begin{pmatrix} P \\ R \end{pmatrix}_{k \times k} \tag{10}$$

is reversible.

2. To prove that matrix (10) is reversible, we only need to prove that matrix (11) is reversible.

Since Q is the RRE matrix of P, $\begin{pmatrix} Q \\ R \end{pmatrix}_{k \times k}$ can be retrieved from $\begin{pmatrix} P \\ R \end{pmatrix}_{k \times k}$ through elementary linear transformation. It follows from $supp(r_i) = \{l_i\}$ and $supp(R) = \{l_1, l_2, ..., l_{k_2}\} = L - J$ that, $\begin{pmatrix} Q \\ R \end{pmatrix}$ can be transformed into

$$\begin{pmatrix} Q' \\ R \end{pmatrix} \tag{11}$$

through elementary linear transformation, where

$$supp(Q') \cap supp(R) = \Phi. \tag{12}$$

Denote that $Q' = \begin{pmatrix} q_1' \\ q_2 \\ \cdots \\ q_{k_1}' \end{pmatrix}_{k_1 \times k}$, then

$$\begin{aligned} supp(q_i') &= supp(q_i) - supp(R) \\ &= supp(q_i) - (L - J) \\ &= supp(q_i) \cap \overline{L - J} \\ &= supp(q_i) \cap J, \end{aligned} \tag{13}$$

where q_i is given in step 3 of Algorithm 1.

3. It will be shown that matrix (11) is reversible.

It follows from (13), (6), (8) that,

$$\begin{aligned} &\{1, ..., a_{i+1} - 1\} \cap supp(q_i') \\ &= \{1, ..., a_{i+1} - 1\} \cap supp(q_i) \cap J \\ &= I_i \cap J \\ &= \{j_i\}. \end{aligned} \tag{14}$$

Then, for $1 \le i \le k_1$, j_i is the position of the leading 1

in q_i', i.e. the leading 1 positions in the rows of Q' are $\{j_1, ..., j_{k_1}\}$, which implies that Q' has full row rank and $\dim[Q'] = k_1$. Then it follows from (12) that

$$\dim[\begin{pmatrix} Q \\ R \end{pmatrix}] = \dim[Q'] + \dim[R] = k_1 + k_2 = k.$$

Then matrix $\begin{pmatrix} Q' \\ R \end{pmatrix}$ is reversible, so are $\begin{pmatrix} P \\ R \end{pmatrix}_{k\times k}$ and $\begin{pmatrix} Q \\ R \end{pmatrix}_{k\times k}$, i.e., the rows of G_2 are linearly independent to the rows of G_1. □

Remark 3: To conduct Algorithm 1, we need to determine the generator matrices G of C and the subcode C^1 in advance. But the result of Algorithm 1 is independent on G^1 after step 2 of Algorithm 1. Moreover Corollary 3 demonstrates that Q is only dependent on G and C^1. Thus Algorithm 1 is independent on the form of the generator matrix of C^1, i.e., if the generator matrix G of C and the subcode C^1 are given, then the result of Algorithm 1 is fixed.

Corollary 3: For a given generator matrix G of a linear code C and a subcode C^1, G_{10} and G_{11} are assumed as any two generator matrices of C^1. Denote matrices P_{10} and P_{11} such that $G_{10} = P_{10}G$ and $G_{11} = P_{11}G$, where the corresponding RRE generator matrices of P_{10} and P_{11} are Q_{10} and Q_{11} respectively, then $Q_{10} = Q_{11}$.

Proof. Since both G_{10} and G_{10} are the generator matrices of C^1, it can be assumed that $G_{10} = AG_{11}$, where A is a basic elementary transformation matrix. Then we have $(P_{10} - AP_{11})G = O$(zero matrix). In addition, G has full row rank. Therefore $P_{10} = AP_{11}$. Moreover, it is easy to know that both P_{10} and P_{11} have full row rank, then the linear space generated by P_{10} and P_{11} are the same. Therefore the RRE form matrices of P_{10} and P_{11} are identical, i.e. $Q_{10} = Q_{11}$. □

Corollary 4: For a given generator matrix G of an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, $\widetilde{\mathbf{k}}(C, C^1)$ is upper-bounded by $\widetilde{\mathbf{k}}(C^2)$ where $C^2 \in M_{G,C^1}$. Furthermore, $\widetilde{\mathbf{k}}(C, C^1)$ is upper-bounded by

$$UP^G(\widetilde{\mathbf{k}}(C, C^1)) := \min_{\geq}\{\widetilde{\mathbf{k}}(C^2) : C^2 \in M_{G,C^1}\}.$$

If G is RRE, $UP^G(\widetilde{\mathbf{k}}(C, C^1))$ is denoted by

$$UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1)).$$

In Example 1, the RRE generator matrix of C is

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Then by using Algorithm 1,

$$Q = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore, $I_1 = \{2\}, I_2 = \{3\}, J = \{2, 3\}, L - J = \{1\}$ and $\alpha_{l_1} = \alpha_1$. It follows that $|M_{G,C^1}| = 1$. The linear code C^2 is generated by $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$. Thus,

$$UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1)) = \widetilde{\mathbf{k}}(C^2) = \{0, 0, 0, 0, 0, 1, 1, 1\},$$

which is the true value of $\mathbf{k}(C, C^1)$, i.e. the upper bounds $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ and $\widetilde{\mathbf{k}}(C^2)$ are both achieved.

6. Comparison with the Generalized Singleton Bound

In this section, the upper bounds in Sect. 4 and Sect. 5, are compared with the generalized Singleton bound on the IRDLP. Theorem 4 shows that $UP(\widetilde{\mathbf{k}}(C, C^1))$ and $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are both upper-bounded by the generalized Singleton bound.

Lemma 4: ([2]) Let $\{\pi_i : 0 \leq i \leq n\}$ be an integer sequence with length n. If π_i is nondecreasing with i from $\pi_0 = 0$ to $\pi_n = k$ where $k < n$, and the increment of each step is at most 1, then $\{\pi_0, ..., \pi_n\}$ is upper-bounded by

$$\{0, 1, 2, ..., k, .., k\}$$

and lower-bounded by

$$\{0, .., 0, 1, 2, .., k\}.$$

The generalized Singleton bound on the IRDLP was introduced in [2], see Theorem 3.

Theorem 3: ([2]) For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, their IRDLP is upper-bounded by $UP(\widetilde{\mathbf{k}})$:

$$\{UP(\widetilde{\mathbf{k}})_i : 0 \leq i \leq n\} := \{0, ..., 0, 1, 2, ..., k_2, ..., k_2\},$$

where $max\{i : UP(\widetilde{\mathbf{k}})_i = 0\} = k_1$ and $k_2 = k - k_1$. $UP(\widetilde{\mathbf{k}})$ is achieved if and only if $\widetilde{\mathbf{k}}_k(C, C^1) = k - k_1$.

Theorem 4: For an $[n, k]$ linear code C and an $[n, k_1]$ subcode C^1, $UP(\widetilde{\mathbf{k}}(C, C^1))$ and $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are both upper-bounded by the generalized Singleton bound $UP(\widetilde{\mathbf{k}})$.

Proof. $UP_i(\widetilde{\mathbf{k}}(C, C^1))$ and $UP_i^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are both nondecreasing with i from

$$UP_0(\widetilde{\mathbf{k}}(C, C^1)) = UP_0^{RRE}(\widetilde{\mathbf{k}}(C, C^1)) = 0$$

to

$$UP_n(\widetilde{\mathbf{k}}(C, C^1)) = UP_n^{RRE}(\widetilde{\mathbf{k}}(C, C^1)) = k_2,$$

and the increment at each step is at most 1, where $k_2 = k - k_1$. Then it follows from Lemma 4 and Theorem 3 that, $UP(\widetilde{\mathbf{k}}(C, C^1))$ and $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are upper-bounded by $UP(\widetilde{\mathbf{k}})$ if

$$UP_{k_1}(\widetilde{\mathbf{k}}(C, C^1)) = UP_{k_1}^{RRE}(\widetilde{\mathbf{k}}(C, C^1)) = 0. \quad (15)$$

Let C^2 be the code obtained by Algorithm 1, i.e.,

$$C^2 \in M_{G,C^1} \subseteq M_{C,C^1},$$

where G is the RRE generator matrix of C. It will be shown

in the next paragraph that

$$\widetilde{\mathbf{k}}_{k_1}(C^2) = 0. \tag{16}$$

According to Algorithm 1, denote $G = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_k \end{pmatrix}$ be the RRE generator matrix of the code C, and denote $G_2 = \begin{pmatrix} \alpha_{l_1} \\ \alpha_{l_2} \\ \cdots \\ \alpha_{l_{k_2}} \end{pmatrix}$ be the generator matrix of the code C^2. Let $T = \{j_1, ..., j_k\}$ be the index set of the leading 1s in the row vectors of G. Let $T_2 = \{j_{l_1}, ..., j_{l_{k_2}}\} \subseteq T$ be the index set of the leading 1s in the row vectors of G_2. Then, for $1 \le i \le k$,

$$supp(\alpha_i) \cap T = \{j_i\}.$$

Therefore, for $1 \le i \le k_2$,

$$\begin{aligned} supp(\alpha_{l_i}) \cap (T - T_2) &= supp(\alpha_{l_i}) \cap T \cap (T - T_2) \\ &= \{j_{l_i}\} \cap (T - T_2) \\ &= \Phi, \end{aligned}$$

which implies that $supp(C^2) \cap (T - T_2) = \Phi$, i.e.

$$\dim[P_{T-T_2}(C^2)] = 0. \tag{17}$$

Thus the formula (16) follows from (17) since $|T - T_2| = k - k_2 = k_1$. Furthermore, the formula (15) follows from (16). □

Remark 4: Theorem 4 shows that, if $\widetilde{\mathbf{k}}(C, C^1)$ achieves the generalized Singleton bound, then the upper bounds $UP(\widetilde{\mathbf{k}}(C, C^1))$ and $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are both achieved. In Example 1,

$$\begin{aligned} &UP(\widetilde{\mathbf{k}}) = \{0, 0, 0, 1, 1, 1, 1, 1\}, \\ &UP(\widetilde{\mathbf{k}}(C, C^1)) = UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1)) \\ &\qquad = \{0, 0, 0, 0, 0, 1, 1, 1\}. \end{aligned}$$

It is easy to see that $UP(\widetilde{\mathbf{k}}(C, C^1))$ and $UP^{RRE}(\widetilde{\mathbf{k}}(C, C^1))$ are better than the generalized Singleton bound $UP(\widetilde{\mathbf{k}})$.

7. The Coordinated Two-Party Wire-Tap Channel of Type II

In this section, we will apply above results to the model of the coordinated two-party wire-tap channel of type II in Fig. 1.

In the coordinated two-party wire-tap channel of type II, let $S = (S_1, S_2)$ be the data bits of the senders, where S^1 is the data bits of the first sender, and S^2 is the data bits of the second sender. Let $A = \begin{pmatrix} A^1 \\ A^2 \end{pmatrix}$ be the matrix of the coset coding scheme of [2], [4]. The transmitted bits are one of the solutions X in the equations $A^1 X^T = S_1^T$ and $A^2 X^T = S_2^T$. An adversary Z_τ has full knowledge about A and has ability to tap any μ transmitted bits of X, where τ is the index set of the μ tapped bits. The index set of the components of X is $\{1, 2, \ldots, n\}$.

Assume that the first sender is illegitimate, i.e. S^1 is leaked to the adversary. Then the equivocation of the legitimate party's data bits S^2 to the adversary is (see [2])

$$\Delta_{2|1:\mu} := \min_{\tau:|\tau|=\mu} H(S^2|Z_\tau, S^1) = \widetilde{\mathbf{k}}_{n-\mu}(C, C^1). \tag{18}$$

In addition, if S^1 is not leaked to the adversary, the equivocation is

$$\Delta_{2|\mu} := \min_{\tau:|\tau|=\mu} H(S^2|Z_\tau) = \widetilde{\mathbf{k}}_{n-\mu}(C^2), \tag{19}$$

where C, C^1 and C^2 are the linear codes with generator matrices A, A^1 and A^2, respectively.

If $\widetilde{\mathbf{k}}(C^2) = \widetilde{\mathbf{k}}(C, C^1)$, i.e. the upper bound $UP(\widetilde{\mathbf{k}}(C, C^1))$ is achieved, then for any μ, in the corresponding model of Fig. 1 with the encoder (with respect to C, C^1 and C^2), the adversary Z_τ cannot learn more about the legitimate party S^2 from the illegitimate party S^1, see Corollary 5.

Corollary 5: In the coordinated two-party wire-tap channel of type II, if $\Delta_{2|1:\mu} = \Delta_{2|\mu}$, i.e., $\widetilde{\mathbf{k}}_{n-\mu}(C, C^1) = \widetilde{\mathbf{k}}_{n-\mu}(C^2)$, there exists a set $\tau_0 (|\tau_0| = \mu)$ such that

$$\begin{aligned} \min_{\tau:|\tau|=\mu} H(S^2|Z_\tau, S^1) &= H(S^2|Z_{\tau_0}, S^1) = H(S^2|Z_{\tau_0}) \\ &= \min_{\tau:|\tau|=\mu} H(S^2|Z_\tau). \end{aligned}$$

Proof. Assume that τ_1 and $\tau_2 (|\tau_1| = |\tau_1| = \mu)$ are two subsets of $\{1, 2, \cdots, n\}$ such that,

$$\begin{aligned} &\min_{\tau:|\tau|=\mu} H(S^2|Z_\tau, S^1) = H(S^2|Z_{\tau_1}, S^1), \\ &\min_{\tau:|\tau|=\mu} H(S^2|Z_\tau) = H(S^1|Z_{\tau_2}). \end{aligned}$$

Since $\Delta_{2|1:\mu} = \Delta_{2|\mu}$, we have

$$\begin{aligned} H(S^2|Z_{\tau_1}, S^1) &\le H(S^2|Z_{\tau_2}, S^1) \le H(S^2|Z_{\tau_2}) \\ &= \Delta_{2|\mu} = \Delta_{2|1:\mu} = H(S^2|Z_{\tau_1}, S^1). \end{aligned}$$

Therefore,

$$\begin{aligned} &H(S^2|Z_{\tau_1}, S^1) = H(S^2|Z_{\tau_2}, S^1) = H(S^2|Z_{\tau_2}), \text{ i.e.} \\ &\min_{\tau:|\tau|=\mu} H(S^2|Z_\tau, S^1) = H(S^2|Z_{\tau_2}, S^1) \\ &\qquad = H(S^2|Z_{\tau_2}) = \min_{\tau:|\tau|=\mu} H(S^2|Z_\tau). \end{aligned}$$

Denotes $\tau_0 = \tau_2$, then this corollary follows.

□

8. Conclusions

The known results about the upper bounds on the IRDLP are very few. In this paper, the generalized Singleton bound is improved in Corollaries 1 and 4, and Remark 2, respectively. Some conditions for achieving the bounds are considered. If

these bounds on the IRDLP are achieved, in the corresponding coordinated two-party wire-tap channel of type II, the adversary cannot learn more from the illegitimate party. In addition, by using the quotient subcode sets, a relation between the IDLP and the IRDLP is investigated in Theorem 2, which are useful for the study of the generalized Hamming weight, the wiretap channel of type II and the trellis complexity, etc.

Acknowledgments

This work was supported by the German Science Foundation DFG, the National Natural Science Foundation of China (Grant no. 60402022), the Development Plan of the State Key Fundamental Research (Grant no. 2007CB310900), and the National High Technology Research and Development Program of China (Grant no. 2006AA01Z125).

The authors would like to thank the anonymous reviewers and the Associate Editor for their comments and suggestions that helped to improve this paper.

References

[1] G.D. Forney, "Dimension/length profiles and trellis complexity of linear block codes," IEEE Trans. Inf. Theory, vol.40, no.6, pp.1741–1752, Nov. 1994.

[2] Y. Luo, C. Mitrpant, A.J. Han Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," IEEE Trans. Inf. Theory, vol.51, no.3, pp.1222–1229, March 2005.

[3] V.K. Wei, "Generalized Hamming weights for linear codes," IEEE Trans. Inf. Theory, vol.37, pp.1412–1418, Sept. 1991.

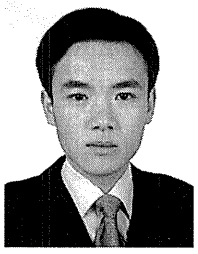
[4] L.H. Ozarow and A.D. Wyner, "Wire-tap channel II," AT&T Bell Labs. Tech. J., vol.63, no.10, pp.2135–2157, Dec. 1984.

[5] A.D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, Oct. 1975.

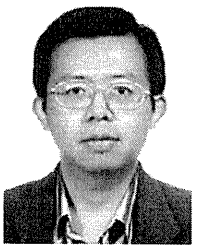
[6] P. Wang, Y. Luo, and A.J. Han Vink, "Quotient subcode set and inverse relative dimension/length profile," the Third International Workshop on Signal Design and Applications in Communications (IWSDA'07), Proc. IWSDA'07, pp.128–132, Sept. 2007.

no. 入れて下さい

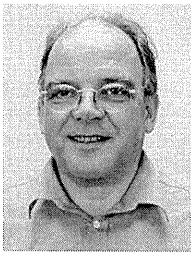
Please show the no. ○ of Ref. 3.



Peisheng Wang was born in 1983. He received his first Bachelor Degree in Material Science and Engineering, and received his second Bachelor Degree in Mathematics in Shanghai Jiao Tong University, China, in July 2005. In March 2008, he received his Master Degree in Cryptology. His interests include coding theory and cryptology.



Yuan Luo was born in Hebei, China, in 1971; and received the B.S., M.S. and Ph.D. degrees in applied mathematics from Nankai University, Tianjin, China, in 1993, 1996, and 1999, respectively. From July 1999 to April 2001, he got a postdoctoral position in the Institute of Systems Science, Chinese Academy of Sciences. And then he got another postdoctoral position supported by German Research Foundation-DFG from May 2001 to April 2003, in the Institute for Experimental Mathematics, Duisburg-Essen University, Germany. From 2003, he has been with the Computer Science and Engineering Department in Shanghai Jiao Tong University, Shanghai, China. In September 2006, he became a full professor in the department. His current research interests include coding theory and information theory. Now, he is an IEEE member and also a reviewer of Mathematical Reviews.



A.J. Han Vinck is a full professor in Digital Communications at the University of Duisburg-Essen, Essen, Germany, since 1990. He studied electrical engineering at the University of Eindhoven, the Netherlands, where he obtained his Ph.D. in 1980. In 2003 he was an adjoint professor at the Sun Yat-Sen University in Kaohsiung, Taiwan. His interest is in Information and Communication theory, Coding and Network aspects in digital communications. IEEE elected him as a fellow for his "Contributions to Coding Techniques." From 1991–1993, 1998–2000, 2006–2008, he was the director of the Institute for Experimental Mathematics in Essen. Professor Vinck serves on the Board of Governors of the IEEE Information Theory Society since 1997 (until 2006). In 2003 he was elected president of the IEEE Information theory Society. Professor Vinck is the initiator of the Japan-Benelux workshops on Information theory (now Asia-Europe) and the International winter-meeting on Coding, Cryptography and Information theory. He started (Essen, 1997) and still supports the organization of the series of conferences on Power Line Communications and its Applications. In 2006 he received the IEEE ISPLC2006 Achievement award in Olando (FL, USA) for his contributions to Powerline Communications. He is co-founder and president of the Shannon and the Gauss foundations. These foundations stimulate research and help young scientists in the field of Information theory and Digital Communications.