Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9750-y

On the relative profiles of a linear code and a subcode

Zhuojun Zhuang · Bin Dai · Yuan Luo · A. J. Han Vinck

Received: 25 October 2011 / Revised: 5 June 2012 / Accepted: 11 September 2012
© Springer Science+Business Media New York 2012

Abstract Relative dimension/length profile (RDLP), inverse relative dimension/length profile (IRDLP) and relative length/dimension profile (RLDP) are equivalent sequences of a linear code and a subcode. The concepts were applied to protect messages from an adversary in the wiretap channel of type II with illegitimate parties. The equivocation to the adversary is described by IRDLP and upper-bounded by the generalized Singleton bound on IRDLP. Recently, RLDP was also extended in wiretap network II for secrecy control of network coding. In this paper, we introduce new relations and bounds about the sequences. They not only reveal new connections among known results but also find applications in trellis complexities of linear codes. The state complexity profile of a linear code and that of a subcode can be bounded from each other, which is particularly useful when a tradeoff among coding rate, error-correcting capability and decoding complexity is considered. Furthermore, a unified framework is proposed to derive bounds on RDLP and IRDLP from an upper bound on

Communicated by T. Helleseth.

Z. Zhuang · B. Dai · Y. Luo (✉)
Department of Computer Science and Engineering, Shanghai Jiao Tong University,
800 Dongchuan Road, Min Hang District, Shanghai 200240, China
e-mail: yuanluo@sjtu.edu.cn

Z. Zhuang
e-mail: zhuojunzzj@sjtu.edu.cnn

Z. Zhuang · Y. Luo
The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China

B. Dai
National Mobile Communications Research Laboratory, Southeast University, Nanjing, China
e-mail: daibin007@sjtu.edu.cn

A. J. Han Vinck
Institute for Experimental Mathematics, Duisburg-Essen University, Essen, Germany
e-mail: vinck@iem.uni-due.de

Published online: 23 October 2012

RLDP. We introduce three new upper bounds on RLDP and use some of them to tighten the generalized Singleton bounds by applying the framework. The approach is useful to improve equivocation estimation in the wiretap channel of type II with illegitimate parties.

Keywords Generalized Hamming weight (GHW) · Relative dimension/length profile (RDLP) · Trellis complexity · Wiretap channel · Wiretap network

Mathematics Subject Classification (2010) 94B05 · 94B65

1 Introduction

The dimension/length profile (DLP) [2] of an $[n, k]$ linear code is a sequence of length $n+1$. Two equivalent concepts are inverse dimension/length profile (IDLP) and length/dimension profile (LDP), which are sequences of length $n+1$ and $k+1$, respectively. The original idea of DLP came from [3]. LDP was named as support weight distribution [8] or effective length [19]. Wei [21] showed that LDP characterizes the secrecy of the wiretap channel of type II [17]. He called it generalized Hamming weight (GHW) hierarchy because one component is minimum Hamming weight.

Independently, many researches were made on trellis complexities of linear codes. Each linear code has a well-defined minimal trellis diagram. Wolf [22] devised the Viterbi decoding algorithm [10] on the diagram. The decoding efficiency is mainly measured by state and branch complexities. The Wolf bound was derived as an upper bound on state complexity. Muder [16] showed that the bound is achieved for maximum distance separable (MDS) codes and almost achieved for perfect codes. The application of DLP to trellis complexity was introduced by Forney [2]. He found the DLP bound on state complexity profile and showed its connection to MDS codes. Reuven and Be'ery [18] extended DLP to entropy/length profile (ELP) for studying trellis complexities of nonlinear codes.

Extending the work of [21], Luo et al. [12] proposed the wiretap channel of type II with illegitimate parties. The adversary is more powerful than that of [21], i.e. he can tap not only partial transmitted symbols but also some data symbols. The minimum uncertainty, i.e. equivocation, of the legitimate parties' data symbols to the more powerful adversary is described by the inverse relative dimension/length profile (IRDLP) of a linear code and a subcode, which is a two-code generalization of IDLP. Similarly, DLP and LDP are extended to the relative dimension/length profile (RDLP) and relative length/dimension profile (RLDP) of a linear code and a subcode, respectively. Luo et al. [12,14] found the generalized Singleton bounds on these three sequences and provided partial code constructions achieving the bounds. Complete constructions are based on the MDS conjecture [15, p. 265]. Later, Wang et al. [20] showed a tighter bound, but the calculation by a cumbersome algorithm is not acceptable when the dimensions of the two codes are large.

In this paper, we introduce new relations about relative profiles (i.e. RDLP, IRDLP and RLDP), and apply them to trellis complexity. Intuitively, in a minimum trellis diagram for a linear code, a subcode provides more information for decoding but no previous work involved the discussion. We also consider how to tighten the generalized Singleton bounds. The significance is from a lot of applications, e.g. to get better estimation of the equivocation in [12]. The idea is as follows: we first introduce new tighter upper bounds on RLDP and then translate them to RDLP and IRDLP.

The rest of the paper is organized as follows. Section 2 is for preliminaries. We first introduce basic notations. Then, the relative profiles and their properties are given. The generalized

Singleton bounds on the profiles are shown in Proposition 1. Finally, for RLDP in Definition 1, we provide two equivalent expressions (Propositions 2 and 4) and their relation (Proposition 3).

Section 3 defines the conjugates of RDLP, IRDLP and RLDP (or briefly cRDLP, cIRDLP and cRLDP) of a linear code C and a subcode C^1. They are determined from the relative profiles of dual codes $C^{1\perp}$ and $C^{\perp}$, and vice versa, see Proposition 5. By giving a code pair equivalence, generator matrices of C and C^1 are assumed in the form of (25). Using the structure, Theorems 1 and 2, mainly based on Lemma 6, show some new inequalities about RDLP, IRDLP, cRDLP and cIRDLP. Conditions for achieving the equalities are discussed. Furthermore, Theorem 1 implies that Luo's bounds can be derived from Forney's MDS bounds [2] though the former is a two-code generalization of the latter. By combining Proposition 5 and Theorem 2, Corollary 4 presents new bounds on RDLP and IRDLP which are useful to investigate bounds on state complexity profile of Sect. 5.

Section 4 has two subsections. Section 4.1 introduces three new upper bounds on RLDP. The first two are Theorems 3 and 4 which extend the generalized Plotkin and Griesmer bounds on LDP, respectively. Theorem 5 shows another bound which is not merely a natural generalization on LDP since the support weight of C^1 is involved. Relations among the bounds are discussed. Section 4.2 introduces a unified framework to derive bounds on RDLP and IRDLP from an upper bound on RLDP. It consists of two parts: bound refinement (Algorithm 1) and bound translation (Proposition 9). Note that the framework is adaptable for the generalized Singleton bounds. Applying Algorithm 1, we refine the bounds of Theorems 3 and 4, and compare them with the Singleton one, see Propositions 7 and 8. Then translating them by Proposition 9, Corollary 8 tightens the generalized Singleton bounds on RDLP and IRDLP, which provides better equivocation estimation than that of [12].

For given C and C^1, Sect. 5 defines ordered RDLP and ordered IRDLP to investigate relations between state complexity profiles $\mathbf{s}(C)$ and $\mathbf{s}(C^1)$, see Theorem 6. Particularly, the DLP and Wolf bounds [2,22] are obtained if C^1 is a zero code. On one hand, the relations show that the bounds are "duality" results from two-code perspectives, which are not revealed from previous researches. On the other hand, they also provide a method to estimate $\mathbf{s}(C^1)$ when $\mathbf{s}(C)$ is known, and vice versa. (However, in previous literature little was known about relations between $\mathbf{s}(C)$ and $\mathbf{s}(C^1)$.) The work of this section is particularly useful in some applications where a tradeoff among coding rate, error-correcting capability and decoding complexity has to be considered, e.g. [13]. Final conclusions are in Sect. 6.

2 Preliminaries

This section consists of three subsections. Section 2.1 introduces some notations. Section 2.2 defines relative profiles, discusses their properties and then shows the generalized Singleton bounds. Besides the definition of RLDP in Sect. 2.2, Sect. 2.3 presents another two equivalent forms and related properties. Note that the results of the section are mainly from [11,12].

2.1 Notations

- Let $\mathrm{GF}(q)$ be a finite field with q elements $0, \ldots, q-1$ and $\mathrm{GF}(q)^k$ be a k-dimensional vector space over $\mathrm{GF}(q)$. **Assume codes and matrices are over** $\mathrm{GF}(q)$ **unless otherwise specified.**
- Let $F_{n,k}$ denote the set of $[n, k]$ linear codes.
- Denote 0^n by an $[n, 0]$ linear code (i.e. a zero code).

– For a matrix $A_{k\times n}$ and a row vector $\mathbf{x} \in \mathrm{GF}(q)^k$, the occurrence of $\mathbf{x}$ in the columns of A is denoted by

$$m_A(\mathbf{x}) = |\{i : A^{(i)} = \mathbf{x}^T, 1 \le i \le n\}|,$$

where $A^{(i)}$ is the ith column of A and $\mathbf{x}^T$ is the transpose of $\mathbf{x}$. For $U \subseteq \mathrm{GF}(q)^k$, define

$$m_A(U) = \sum_{\mathbf{x}\in U} m_A(\mathbf{x}).$$

Adopt $m_A(\emptyset) = 0$ where $\emptyset$ is an empty set.

– For sets S_1 and S_2, $S_1 \subseteq S_2$ means S_1 is a subset of S_2 and $S_1 \subset S_2$ means S_1 is a **proper** subset of S_2.

– Let $\mathcal{N}_n$ be the set $\{1, \ldots, n\}$.

– For a linear code C of length n and $J \subseteq \mathcal{N}_n$, the **subcode of** C **on** J is defined as

$$C_J = \{(c_1, \ldots, c_n) \in C : c_i = 0 \quad \text{for } i \notin J\}. \tag{1}$$

The **projection of** C **on** J is defined as

$$P_J(C) = \{(P_J(\mathbf{c})_1, \ldots, P_J(\mathbf{c})_n) : \mathbf{c} = (c_1, \ldots, c_n) \in C\} \tag{2}$$

where

$$P_J(\mathbf{c})_j = \begin{cases} c_j & \text{if } j \in J, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

For example, assume C is a binary [7, 4] Hamming code with generator matrix

$$G = \begin{pmatrix} 1\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1\,0 \end{pmatrix}$$

and $J = \{1, 2, 5, 6, 7\}$. C_J is spanned by the first and the third rows of G. $P_J(C)$ is with generator matrix

$$\begin{pmatrix} 1\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,0\,0\,1\,1\,0 \end{pmatrix}.$$

Note that the restriction of $C_J(P_J(C))$ to J is a shortened(punctured) code [15, pp. 28–29].

– For an $[n, k]$ linear code C, its **support** is defined as

$$\mathrm{supp}(C) = \{i : \exists (c_1, \ldots, c_n) \in C, c_i \neq 0\}$$

and its **support weight** is defined as

$$w_S(C) = |\,\mathrm{supp}(C)|.$$

If $k = 1$, then $w_S(C) = \mathrm{wt}(\mathbf{c})$ for all nonzero $\mathbf{c} \in C$, where $\mathrm{wt}(\mathbf{c})$ is the Hamming weight of $\mathbf{c}$.

– Let $C^\perp$ denote the dual code of C.

– For integer sequences $\mathbf{s} = \{s_0, \ldots, s_n\}$ and $\mathbf{t} = \{t_0, \ldots, t_n\}$, $\mathbf{s}$ is said to be **upper-bounded (lower-bounded)** by $\mathbf{t}$ if $s_i \leq t_i (s_i \geq t_i)$ for $0 \leq i \leq n$, which is denoted by

$$\mathbf{s} \leq \mathbf{t} (\mathbf{s} \geq \mathbf{t}).$$

Denote $\mathbf{s} = \mathbf{t}$ if $\mathbf{s} \leq \mathbf{t}$ and $\mathbf{s} \geq \mathbf{t}$. Furthermore, an upper(a lower) bound $\mathbf{t}$ on $\mathbf{s}$ is said to be **achieved** if $\mathbf{s} = \mathbf{t}$, and said to be **tighter** than $\mathbf{t}'$ if $\mathbf{s} \leq \mathbf{t} \leq \mathbf{t}' (\mathbf{s} \geq \mathbf{t} \geq \mathbf{t}')$ where $\mathbf{t}'$ is an integer sequence of length $n + 1$.

– Let $\lfloor x \rfloor$ be the largest integer not greater than x and $\lceil x \rceil$ be the smallest integer not less than x.

– For integers a and $b \geq 0$, denote the q-ary **Gaussian binomial coefficient** [15, p. 443] by

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{cases} 1 & \text{if } b = 0, \\ \prod_{i=0}^{b-1} \frac{q^{a-i}-1}{q^{b-i}-1} & \text{otherwise.} \end{cases}$$

2.2 Relative profiles and generalized Singleton bounds

In this subsection, we introduce three character sequences of a linear code and a subcode. They are RDLP, IRDLP and RLDP, which extend the DLP, IDLP and LDP of a linear code, respectively. Three equivalent bounds on the sequences are shown in Proposition 1, and each bound is a generalized Singleton bound.

Definition 1 (*RDLP, IRDLP and RLDP [12]*) Let J be a subset of $\mathcal{N}_n$. For an $[n, k]$ linear code C and a subcode C^1 of dimension k_1, their RDLP is defined as a sequence $K(C, C^1) = \{K_i(C, C^1) : 0 \leq i \leq n\}$ where

$$K_i(C, C^1) = \max\{\dim(C_J) - \dim(C_J^1) : |J| = i\}.$$

Their IRDLP is defined as $\widetilde{K}(C, C^1) = \{\widetilde{K}_i(C, C^1) : 0 \leq i \leq n\}$ where

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

Their RLDP is defined as $M(C, C^1) = \{M_r(C, C^1) : 0 \leq r \leq k - k_1\}$ where

$$M_r(C, C^1) = \min\{|J| : \dim(C_J) - \dim(C_J^1) = r\}.$$

Particularly,

$$K(C) = K(C, 0^n), \ \widetilde{K}(C) = \widetilde{K}(C, 0^n), M(C) = M(C, 0^n)$$

are the DLP, IDLP and LDP of C [2], respectively. In addition, denote their components by $K_i(C)$, $\widetilde{K}_i(C)$ and $M_r(C)$, where $0 \leq i \leq n$ and $0 \leq r \leq k$.

Wei [21] called $M_r(C)$ the rth **GHW** of C in studying the wiretap channel of type II [17]. Forney [2] applied $K(C)$ and $\widetilde{K}(C)$ to trellis complexity. Luo et al. [12] introduced $M_r(C, C^1)$, called the rth **relative generalized Hamming weight (RGHW)** of C and C^1, in a more generalized wiretap channel. Lemma 1 shows that the character sequences can be determined from each other.

Lemma 1 ([12]) *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \leq i \leq n$, $K_i(C, C^1)$ and $\widetilde{K}_i(C, C^1)$ are both nondecreasing with i from $K_0(C, C^1) =$*

$\widetilde{K}_0(C, C^1) = 0$ *to* $K_n(C, C^1) = \widetilde{K}_n(C, C^1) = k - k_1$. *The increment at each step is at most 1, i.e. for* $0 \le j \le n-1$,

$$0 \le K_{j+1}(C, C^1) - K_j(C, C^1) \le 1, \tag{4}$$

$$0 \le \widetilde{K}_{j+1}(C, C^1) - \widetilde{K}_j(C, C^1) \le 1. \tag{5}$$

For $0 \le r \le k - k_1$, $M_r(C, C^1)$ *is strictly increasing with r from* $M_0(C, C^1) = 0$. *Furthermore, for* $0 \le i \le n$ *and* $0 \le r \le k - k_1$,

$$K_i(C, C^1) = k - k_1 - \widetilde{K}_{n-i}(C, C^1), \tag{6}$$

$$K_i(C, C^1) = \max\{r : M_r(C, C^1) \le i\}, \tag{7}$$

$$M_r(C, C^1) = \min\{i : K_i(C, C^1) \ge r\}. \tag{8}$$

Remark 1 From (7) and (8), $K_i(C, C^1) \ge r$ if and only if $M_r(C, C^1) \le i$ for $0 \le i \le n$ and $0 \le r \le k - k_1$.

Roughly speaking, by (6) and (7), smaller M leads to larger K and smaller $\widetilde{K}$, i.e. an upper bound on M derives a lower bound on K and an upper bound on $\widetilde{K}$. These properties will be refined in Proposition 9 of Sect. 4.

In the model of [12], the adversary is more powerful than that of [17], i.e. he can tap not only partial transmitted symbols but also the data symbols of illegitimate parties. The minimum uncertainty, i.e. equivocation, of the legitimate parties' data symbols to the more powerful adversary is described by IRDLP and upper-bounded by the following generalized Singleton bound on IRDLP, see Proposition 1. By using (6) and (8), the bound is translated to RDLP and RLDP.

Proposition 1 (Generalized Singleton Bounds [12]) *For an* $[n, k]$ *linear code C and a subcode* C^1 *of dimension* k_1, *their RDLP satisfies*

$$\begin{aligned} K(C, C^1) \ge LO(K) &\triangleq \{LO(K)_i : 0 \le i \le n\} \\ &= \{0, \ldots, 0, 1, \ldots, k - k_1, \ldots, k - k_1\} \end{aligned}$$

where $\max\{i : LO(K)_i = 0\} = n - k$. $LO(K)$ *is achieved if and only if* $K_{n-k}(C, C^1) = 0$. *Their IRDLP satisfies*

$$\begin{aligned} \widetilde{K}(C, C^1) \le UP(\widetilde{K}) &\triangleq \{UP(\widetilde{K})_i : 0 \le i \le n\} \\ &= \{0, \ldots, 0, 1, \ldots, k - k_1, \ldots, k - k_1\} \end{aligned}$$

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

$$\begin{aligned} M(C, C^1) \le UP(M) &\triangleq \{UP(M)_r : 0 \le r \le k - k_1\} \\ &= \{0, n - k + 1, n - k + 2, \ldots, n - k_1\}. \end{aligned}$$

$UP(M)$ *is achieved if and only if* $M_1(C, C^1) = n - k + 1$. *If* $C^1 = 0^n$, $LO(K)$, $UP(\widetilde{K})$ *and* $UP(M)$ *degenerate to those of [2,21]. Furthermore, if one of* $LO(K)$, $UP(\widetilde{K})$ *and* $UP(M)$ *is achieved, then so are the other two.*

Proposition 1 shows the equivalence of $LO(K)$, $UP(\widetilde{K})$ and $UP(M)$. Each bound is a generalized Singleton bound. **If $C^1 = 0^n$, the classic Singleton bound is retrieved from** $UP(M)_1$. Note that C is not necessary to be an MDS code for achieving the bounds, see [12]. In Sect. 4, we shall tighten the generalized Singleton bounds, which provides better equivocation estimation than that of [12].

2.3 Equivalent descriptions of RLDP

In this subsection, two equivalent forms of RLDP (in fact the rth component) are expressed in Propositions 2 and 4. A relation between them is given in Proposition 3 for studying Proposition 6 of Sect. 4.

Let C and C^1 be an $[n, k]$ linear code and a subcode of dimension k_1 with generator matrices G and G^1, respectively. **Without loss of generality, assume**

$$G = \begin{pmatrix} G^1 \\ G^2 \end{pmatrix}_{k \times n} \tag{9}$$

where G^2 is of size $(k - k_1) \times n$. A subcode D of C is called a **relative subcode** of C and C^1 if $D \cap C^1 = 0^n$, and denoted by

$$D \trianglerighteq (C, C^1).$$

For $0 \le r \le k - k_1$, let

$$\mathcal{D}_r(C, C^1) = \{D : D \trianglerighteq (C, C^1), \dim(D) = r\}$$

be the set of r-dimensional relative subcodes of C and C^1, and

$$\mathcal{U}_{k,k-r} = \{U : U \in F_{k,k-r}, \dim[P_{\mathcal{N}_{k_1}}(U)] = k_1\}$$

be the set of $[k, k-r]$ linear codes whose projection on the first k_1 components has dimension k_1. In particular, $\mathcal{D}_0(C, C^1) = \{0^n\}$ and $\mathcal{U}_{k,k} = \{\mathrm{GF}(q)^k\}$.

Proposition 2 (First Equivalent Form of RLDP [11]) *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \le r \le k - k_1$,*

$$\begin{aligned} M_r(C, C^1) &= \min\{w_S(D) : D \trianglerighteq (C, C^1), \dim(D) = r\} \\ &= \min\{w_S(D) : D \in \mathcal{D}_r(C, C^1)\}. \end{aligned} \tag{10}$$

If $C^1 = 0^n$, then (10) is the expression of the rth GHW in [21]. In particular,

$$M_1(C, C^1) = \min_{\boldsymbol{c} \in C - C^1} \mathrm{wt}(\boldsymbol{c}).$$

By Proposition 2, Liu et al. [11] showed the following proposition. Furthermore, by the idea of [1] we obtain Lemma 2 of which the proof is similar to the discussion after Lemma 6 of [1]. These results are to show Proposition 6.

Proposition 3 ([11]) *For a given $D \in \mathcal{D}_r(C, C^1)(1 \le r \le k - k_1)$, let $R_{r \times k}$ be any given full row-rank matrix such that RG is a generator matrix of D. Then the dual code U of the row space of R satisfies $U \in \mathcal{U}_{k,k-r}$. Furthermore, the mapping $\varphi : \mathcal{D}_r(C, C^1) \to \mathcal{U}_{k,k-r}$*

$$D \mapsto U$$

is a one-to-one correspondence and

$$w_S(D) = n - m_G[\varphi(D)] = n - m_G(U). \tag{11}$$

Lemma 2 *For $1 \le r_1 \le r_2 \le k - k_1$, let $D_1 \in \mathcal{D}_{r_1}(C, C^1)$ and $D_2 \in \mathcal{D}_{r_2}(C, C^1)$. Then $\varphi(D_1) \supseteq \varphi(D_2)$ if $D_1 \subseteq D_2$.*

By Propositions 2, 3 and Lemma 2, we have the following expression.

Proposition 4 (Second Equivalent Form of RLDP [11]) *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \le r \le k - k_1$,*

$$\begin{aligned} M_r(C, C^1) &= n - \max\{m_G(U) : U \in F_{k,k-r}, \dim[P_{\mathcal{N}_{k_1}}(U)] = k_1\} \\ &= n - \max\{m_G(U) : U \in \mathcal{U}_{k,k-r}\}, \end{aligned} \tag{12}$$

where G is specified by (9). If $C^1 = 0^n$, then (12) is the expression of the rth GHW in [4].

3 Conjugates of RDLP, IRDLP and RLDP

Conjugates of RDLP, IRDLP and RLDP (cRDLP, cIRDLP and cRLDP) are defined as sequences changing "max" with "min" or "min" with "max" in the concepts of Definition 1. They are determined by the RDLP, IRDLP and RLDP of dual codes (see Proposition 5), and also determined from each other (see Corollary 1). Theorems 1 and 2 show some connections about the bounds of [2,12,20], and derive new bounds on RDLP and IRDLP for studying trellis complexity in Sect. 5.

Definition 2 (*cRDLP, cIRDLP and cRLDP*) Let J be a subset of $\mathcal{N}_n$. For an $[n, k]$ linear code C and a subcode C^1 of dimension k_1, their cRDLP is defined as a sequence $\widehat{K}(C, C^1) = \{\widehat{K}_i(C, C^1) : 0 \le i \le n\}$ where

$$\widehat{K}_i(C, C^1) = \min\{\dim(C_J) - \dim(C^1_J) : |J| = i\}.$$

Their cIRDLP is defined as $\widehat{\widehat{K}}(C, C^1) = \{\widehat{\widehat{K}}_i(C, C^1) : 0 \le i \le n\}$ where

$$\widehat{\widehat{K}}_i(C, C^1) = \max\{\dim[P_J(C)] - \dim[P_J(C^1)] : |J| = i\}.$$

Their cRLDP is defined as $\widehat{M}(C, C^1) = \{\widehat{M}_r(C, C^1) : 0 \le r \le k - k_1\}$ where

$$\widehat{M}_r(C, C^1) = \max\{|J| : \dim(C_J) - \dim(C^1_J) = r\}.$$

Particularly,

$$\widehat{K}(C) = \widehat{K}(C, 0^n),\ \widehat{\widehat{K}}(C) = \widehat{\widehat{K}}(C, 0^n) \quad \text{and} \quad \widehat{M}(C) = \widehat{M}(C, 0^n)$$

are called the **cDLP**, **cIDLP** and **cLDP** of C, respectively. In addition, denote their components by $\widehat{K}_i(C)$, $\widehat{\widehat{K}}_i(C)$ and $\widehat{M}_r(C)$, where $0 \le i \le n$ and $0 \le r \le k$.

Definitions 1 and 2 will be frequently used in the rest of the paper. We suggest the readers to look up them when evaluating results. Lemmas 3 and 4 present relations between C_J and $P_J(C)$.

Lemma 3 (First Duality Lemma [2]) *For an $[n, k]$ linear code C and a set $J \subseteq \mathcal{N}_n$,*

$$\dim[P_J(C)] + \dim(C_{\mathcal{N}_n - J}) = k.$$

Lemma 4 (Second Duality Lemma [2]) *For an $[n, k]$ linear code C and a set $J \subseteq \mathcal{N}_n$,*

$$\dim[P_J(C^\perp)] + \dim(C_J) = |J|.$$

By using Lemmas 3 and 4, Proposition 5 shows that the RDLP, IRDLP and RLDP of C and C^1 are determined by the cRDLP, cIRDLP and cRLDP of ${C^1}^\perp$ and $C^\perp$, and vice versa. The properties are useful in getting the new bounds of Corollary 4. In addition, we shall apply them to study trellis complexity in Sect. 5.

Proposition 5 *Let C be an $[n,k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \le i \le n$ and $0 \le r \le k-k_1$,*

$$\widehat{K}_i(C,C^1) = \widetilde{K}_i({C^1}^\perp, C^\perp), \tag{13}$$

$$\widehat{\widetilde{K}}_i(C,C^1) = K_i({C^1}^\perp, C^\perp), \tag{14}$$

$$\widehat{M}_r(C,C^1) = n - M_{k-k_1-r}({C^1}^\perp, C^\perp). \tag{15}$$

Proof First,

$$\begin{aligned}\widehat{K}_i(C,C^1) &= \min\{\dim(C_J) - \dim(C^1_J) : |J| = i\}\\ &= \min\{\dim[P_J({C^1}^\perp)] - \dim[P_J(C^\perp)] : |J| = i\}\\ &= \widetilde{K}_i({C^1}^\perp, C^\perp),\end{aligned}$$

where the second equation follows from Lemma 4. The proof of (14) is similar. Finally,

$$\begin{aligned}\widehat{M}_r(C,C^1) &= \max\{|J| : \dim(C_J) - \dim(C^1_J) = r\}\\ &\overset{(a)}{=} \max\{|J| : \dim[P_J({C^1}^\perp)] - \dim[P_J(C^\perp)] = r\}\\ &\overset{(b)}{=} \max\{|J| : \dim({C^1}^\perp)_{\mathcal{N}_n - J} - \dim(C^\perp)_{\mathcal{N}_n - J} = k - k_1 - r\}\\ &= \max\{|\mathcal{N}_n - J| : \dim({C^1}^\perp)_J - \dim(C^\perp)_J = k - k_1 - r\}\\ &= n - \min\{|J| : \dim({C^1}^\perp)_J - \dim(C^\perp)_J = k - k_1 - r\}\\ &= n - M_{k-k_1-r}({C^1}^\perp, C^\perp),\end{aligned}$$

where (a) and (b) follow from Lemmas 4 and 3, respectively.

Equation 13 implies that the equivocation to the adversary of Luo's wiretap channel is also described by cRDLP. By combining (6) and (14), cIRDLP can determine the equivocation when dual codes are applied to coset coding scheme. In addition, from Proposition 5, the conjugates can be determined from each other as follows, which is similar to Lemma 1.

Corollary 1 *Let C be an $[n,k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \le i \le n$ and $0 \le r \le k-k_1$,*

$$\widehat{K}_i(C,C^1) = k - k_1 - \widehat{\widetilde{K}}_{n-i}(C,C^1), \tag{16}$$

$$\widehat{K}_i(C,C^1) = \min\{r : \widehat{M}_r(C,C^1) \ge i\}, \tag{17}$$

$$\widehat{M}_r(C,C^1) = \max\{i : \widehat{K}_i(C,C^1) \le r\}. \tag{18}$$

Remark 2 It follows similarly to Remark 1 that $\widehat{K}_i(C,C^1) \le r$ if and only if $\widehat{M}_r(C,C^1) \ge i$ for $0 \le i \le n$ and $0 \le r \le k-k_1$.

The rest of the section will show some new relations about the sequences of Definitions 1 and 2, see Theorems 1 and 2. The relations deriving bounds on RDLP and IRDLP are based on the following Lemma 5 and Corollary 2.

Lemma 5 *Let C^1 and C^2 be two subcodes of an $[n,k]$ linear code C such that $C = C^1 \oplus C^2$, where $\oplus$ denotes the direct sum of vector spaces. Then*

$$C^1_J \oplus C^2_J \subseteq C_J, \tag{19}$$

$$P_J(C^1) + P_J(C^2) = P_J(C), \tag{20}$$

where $J \subseteq \mathcal{N}_n$. *Furthermore,*

$$\dim(C_J) - \dim(C_J^1) \geq \dim(C_J^2), \tag{21}$$
$$\dim[P_J(C)] - \dim[P_J(C^1)] \leq \dim[P_J(C^2)]. \tag{22}$$

Proof First, $C_J^1, C_J^2 \subseteq C_J$ and then $C_J^1 + C_J^2 \subseteq C_J$. In addition, $C_J^1 \cap C_J^2 = 0^n$ or otherwise contradicts $C^1 \cap C^2 = 0^n$, which proves (19). Second, we show $P_J(C^1) + P_J(C^2) \subseteq P_J(C)$ and $P_J(C^1) + P_J(C^2) \supseteq P_J(C)$. The former claim follows from $P_J(C^1)$, $P_J(C^2) \subseteq P_J(C)$. For the latter one, given $\mathbf{c} \in C$, there exist $\mathbf{c}^1 = (c_1^1, \ldots, c_n^1) \in C^1$ and $\mathbf{c}^2 = (c_1^2, \ldots, c_n^2) \in C^2$ such that $\mathbf{c} = \mathbf{c}^1 + \mathbf{c}^2$. By using (3), for $1 \leq j \leq n$,

$$P_J(\mathbf{c})_j = \begin{cases} c_j^1 + c_j^2 & \text{if } j \in J, \\ 0 & \text{otherwise.} \end{cases} = P_J(\mathbf{c}^1)_j + P_J(\mathbf{c}^2)_j.$$

Thus $P_J(C^1) + P_J(C^2) \supseteq P_J(C)$ and so (20) follows. Furthermore, (21) and (22) follow from

$$\dim(C_J) \geq \dim(C_J^1 \oplus C_J^2) = \dim(C_J^1) + \dim(C_J^2)$$

and

$$\begin{aligned} \dim[P_J(C)] &= \dim[P_J(C^1)] + \dim[P_J(C^2)] - \dim[P_J(C^1) \cap P_J(C^2)] \\ &\leq \dim[P_J(C^1)] + \dim[P_J(C^2)], \end{aligned}$$

respectively.

The equality in (19) does not always hold. For example, let C_J^1 and C_J^2 be the linear codes generated by (1011) and (0111), respectively. For $J = \{1, 2\}$, $\dim(C_J^1) = \dim(C_J^2) = 0$ but $\dim(C_J) = 1$. Lemma 5 immediately yields the following inequalities used to prove Theorems 1 and 2.

Corollary 2 *For a linear code* C, *let* C^1 *and* C^2 *be two subcodes such that* $C = C^1 \oplus C^2$, *where* $\oplus$ *denotes the direct sum of vector spaces. Then*

$$K(C, C^1) \geq K(C^2), \quad \widetilde{K}(C, C^1) \leq \widetilde{K}(C^2), \tag{23}$$
$$\widehat{K}(C, C^1) \geq \widehat{K}(C^2), \quad \widehat{\widetilde{K}}(C, C^1) \leq \widehat{\widetilde{K}}(C^2). \tag{24}$$

By (6) the inequalities in (23) are equivalent, and by (16) the inequalities in (24) are equivalent. Conditions for achieving the equalities are studied in Corollaries 3 and 4. Let C' be a linear code by permuting some coordinates of C, and C'^1 be the subcode of C' under the same operation on C^1. The RDLP, IRDLP, RLDP and their conjugates of C' and C'^1 are the same as those of C and C^1, since J traverses all subsets with size i of $\{1, \ldots, n\}$. Hence, code pairs (C, C^1) and (C', C'^1) can be seen as equivalent.

Definition 3 (*Code Pair Equivalence*) Let $C(C')$ be a linear code and $C^1(C'^1)$ be a subcode. Code pairs (C, C^1) and (C', C'^1) are called (permutation) equivalent if $C = \{\sigma(\mathbf{c}) : \mathbf{c} \in C'\}$ and $C^1 = \{\sigma(\mathbf{c}) : \mathbf{c} \in C'^1\}$, where $\sigma(\cdot)$ is any compound of coordinate permutations. If $C^1 = 0^n$, then the (permutation) equivalence of linear codes [6, p. 20] is retrieved.

Considering equivalence, we can always assume that C^1 has a standard generator matrix G^1. By appending $k - k_1$ rows to G^1, a generator matrix G of C is obtained. Then adding some rows of G^1 to the other $k - k_1$ rows of G,

$$\begin{aligned} G &= \begin{pmatrix} G^1 \\ G^2 \end{pmatrix}_{k\times n}, \\ G^1 &= \left(E_{k_1\times k_1}, D_{k_1\times(n-k_1)}\right), \\ G^2 &= \left(O_{(k-k_1)\times k_1}, G^*_{(k-k_1)\times(n-k_1)}\right), \end{aligned} \tag{25}$$

where E is an identity matrix and O is a zero matrix. Let C^2 and C^* be the $[n, k-k_1]$ and $[n-k_1, k-k_1]$ linear codes generated by G^2 and G^*, respectively. For $k = k_1$, G^2 and G^* vanish and we adopt $C^2 = 0^n$ and $C^* = 0^{n-k_1}$. Lemma 6 shows two key identities for proving Theorems 1 and 2.

Lemma 6 *Let C^2 and C^* be the linear codes generated by G^2 and G^* in (25), respectively. For $0 \le i \le n$,*

$$K_i(C^2) = \begin{cases} K_i(C^*) & \text{if } 0 \le i \le n-k_1, \\ k-k_1 & \text{if } n-k_1 < i \le n. \end{cases} \tag{26}$$

$$\widehat{\widehat{K}}_i(C^2) = \begin{cases} \widehat{\widehat{K}}_i(C^*) & \text{if } 0 \le i \le n-k_1, \\ k-k_1 & \text{if } n-k_1 < i \le n. \end{cases} \tag{27}$$

Proof The case $k = k_1$ is trivial. Consider $k > k_1$. For $k_1 = 0$, the theorem is obvious since $C^2 = C^*$. We discuss the case $k_1 \ge 1$ and only show (26). (27) can be similarly shown by using the "substituting" skill of (30) and details are omitted.

Case 1 $0 \le i \le n-k_1$. Clearly, $K_0(C^2) = K_0(C^*) = 0$. Consider the case $1 \le i \le n-k_1$. The idea is as follows: we first show (28) and use it to obtain (32); then, we prove (33) and finally derive the result by combining (32) and (33).

First, for any $J' \nsubseteq \mathcal{N}_n - \mathcal{N}_{k_1}$ with $|J'| = i$, we show

$$\dim(C^2_{J'}) \le \max\{\dim(C^2_J) : J \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}, |J| = i\} \tag{28}$$

by constructing $J'' \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}$ with $|J''| = i$ such that $C^2_{J'} \subseteq C^2_{J''}$. Without loss of generality, assume that $J' = \{j_1, \ldots, j_i\}$ such that $j_1, \ldots, j_l \in \mathcal{N}_{k_1}$ and $j_{l+1}, \ldots, j_i \in \mathcal{N}_n - \mathcal{N}_{k_1}$, where $1 \le l \le i$. By using (1),

$$\begin{aligned} C^2_{J'} &= \{(c_1, c_2, \ldots, c_n) \in C^2 : c_t = 0, t \notin J'\} \\ &= \left\{(c_1, c_2, \ldots, c_n) \in C^2 : c_t = 0, t \notin \{j_{l+1}, \ldots, j_i\}\right\}, \end{aligned} \tag{29}$$

where the second equation follows since the first k_1 components of C^2 are all zero (see (25)). Since $i \le n-k_1$, there exist $j'_1, \ldots, j'_l \in \mathcal{N}_n - \mathcal{N}_{k_1}$ such that $\{j'_1, \ldots, j'_l\} \cap \{j_{l+1}, \ldots, j_i\} = \emptyset$. Let

$$J'' = \{j'_1, \ldots, j'_l\} \cup \{j_{l+1}, \ldots, j_i\}. \tag{30}$$

Then $J'' \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}$ and therefore $C^2_{J'} \subseteq C^2_{J''}$ by combining (1), (29) and (30). This leads to

$$\dim(C^2_{J'}) \le \dim(C^2_{J''}) \le \max\{\dim(C^2_J) : J \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}, |J| = i\}. \tag{31}$$

Second, from (28),

$$\max\{\dim(C^2_J) : J \subseteq \mathcal{N}_n, |J| = i\} \le \max\{\dim(C^2_J) : J \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}, |J| = i\}$$

and furthermore

$$\max\{\dim(C_J^2) : J \subseteq \mathcal{N}_n, |J| = i\} = \max\{\dim(C_J^2) : J \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}, |J| = i\}. \quad (32)$$

For $J_1 \subseteq \mathcal{N}_{k_1}$[1] with $|J_1| = i$ and $J = \{j + k_1 : j \in J_1\} \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}$, $\dim(C_{J_1}^*) = \dim(C_J^2)$ since the first k_1 components of C^2 are all zero. Then

$$\max\{\dim(C_{J_1}^*) : J_1 \subseteq \mathcal{N}_{k_1}, |J_1| = i\} = \max\{\dim(C_J^2) : J \subseteq \mathcal{N}_n - \mathcal{N}_{k_1}, |J| = i\}. \quad (33)$$

Finally, $K_i(C^2) = K_i(C^*)$ follows by combining (32), (33) and Definition 1.

Case 2 $n - k_1 < i \leq n$. It follows that

$$\begin{aligned} K_i(C^2) &= \max\{\dim(C_J^2) : J \subseteq \mathcal{N}_n, |J| = i\} \\ &\overset{(a)}{=} k - k_1 - \min\{\dim[P_{\mathcal{N}_n - J}(C^2)] : J \subseteq \mathcal{N}_n, |J| = i\} \\ &= k - k_1 - \min\{\dim[P_J(C^2)] : J \subseteq \mathcal{N}_n, |J| = n - i\}, \\ &\overset{(b)}{=} k - k_1, \end{aligned}$$

where (a) follows from Lemma 3 and (b) follows since $n - i < k_1$ and the first k_1 components of C^2 are all zero.

By combining Corollary 2, Lemma 6 and Forney's MDS bounds [2], we obtain the following relations about RDLP and IRDLP.

Theorem 1 *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. Considering equivalence, assume that their generator matrices are in the form of (25). Let C^2 and C^* be the linear codes generated by G^2 and G^* in (25), respectively. For $0 \leq i \leq n$,*

$$\begin{aligned} K_i(C, C^1) &\overset{(a)}{\geq} K_i(C^2) \overset{(b)}{=} \begin{cases} K_i(C^*) & \text{if } 0 \leq i \leq n - k_1, \\ k - k_1 & \text{if } n - k_1 < i \leq n. \end{cases} \\ &\overset{(c)}{\geq} \begin{cases} 0 & \text{if } 0 \leq i \leq n - k, \\ i - (n - k) & \text{if } n - k < i \leq n - k_1, \\ k - k_1 & \text{if } n - k_1 < i \leq n. \end{cases} \end{aligned} \quad (34)$$

$$\begin{aligned} \widetilde{K}_i(C, C^1) &\overset{(a)}{\leq} \widetilde{K}_i(C^2) \overset{(b)}{=} \begin{cases} 0 & \text{if } 0 \leq i \leq k_1, \\ \widetilde{K}_{i-k_1}(C^*) & \text{if } k_1 < i \leq n. \end{cases} \\ &\overset{(c)}{\leq} \begin{cases} 0 & \text{if } 0 \leq i \leq k_1, \\ i - k_1 & \text{if } k_1 < i \leq k, \\ k - k_1 & \text{if } k < i \leq n. \end{cases} \end{aligned} \quad (35)$$

Proof The case $k = k_1$ is trivial because $C = C^1$, $C^2 = 0^n$ and $C^* = 0^{n-k_1}$. Consider $k > k_1$. In (34), (a) follows from Corollary 2; (b) follows from Lemma 6; (c) follows from [2, Theorem 5]. In (35), (a) follows from Corollary 2 and (c) follows [2, Theorem 5]; (b) follows from

[1] The coordinates of C^* are labeled by $1, \ldots, n - k_1$ corresponding, respectively, to the coordinates $k_1 + 1, \ldots, n$ of C^2.

$$\widetilde{K}_i(C^2) \overset{(1)}{=} k - k_1 - K_{n-i}(C^2)$$
$$\overset{(2)}{=} \begin{cases} k - k_1 - K_{n-i}(C^*) & \text{if } 0 \le n-i \le n-k_1, \\ 0 & \text{if } n-k_1 < n-i \le n. \end{cases}$$
$$\overset{(3)}{=} \begin{cases} 0 & \text{if } 0 \le i \le k_1, \\ \widetilde{K}_{i-k_1}(C^*) & \text{if } k_1 < i \le n. \end{cases}$$

The above (1) and (3) follow from the special case of (6) and (2) follows from Lemma 6.

Remark 3 (*c*) of (34) and (*c*) of (35) are $LO(K)$ and $UP(\widetilde{K})$ of Proposition 1, respectively.

Theorem 1 shows that $LO(K)$ and $UP(\widetilde{K})$ can be obtained by applying Forney's bounds to C^*. In addition, (*a*) and (*c*) of (35) imply that Wang's bound [20] is tighter than $UP(\widetilde{K})$. Corollary 3 shows that the conditions on the equalities of Theorem 1 characterize linear codes and subcodes achieving the generalized Singleton bounds.

Corollary 3 *Considering equivalence, any of $LO(K)$, $UP(\widetilde{K})$ and $UP(M)$ is achieved by an $[n, k]$ linear code C and a subcode C^1 of dimension k_1, if and only if the following two conditions hold:*

- $K(C, C^1) = K(C^2)$ *or* $\widetilde{K}(C, C^1) = \widetilde{K}(C^2)$,
- C^* *is an MDS code,*

where C^2 and C^* are the linear codes generated by G^2 and G^* in (25), respectively.

Proof The case $k = k_1$ is trivial because $C = C^1$, $C^2 = 0^n$ and $C^* = 0^{n-k_1}$. Consider $k > k_1$. By Proposition 1, any of $LO(K)$, $UP(\widetilde{K})$ and $UP(M)$ is achieved if and only if $LO(K)$ is achieved. In addition, by using (6), $K(C, C^1) = K(C^2)$ is equivalent to $\widetilde{K}(C, C^1) = \widetilde{K}(C^2)$. Thus it suffices to show that $LO(K)$ is achieved, if and only if $K(C, C^1) = K(C^2)$ and C^* is an MDS code. By Theorem 1, $LO(K)$ is achieved if and only if the equalities in (*a*) and (*c*) of (34) hold. Moreover, by using [2, Theorem 5], the equality in (*c*) of (34) holds if and only if C^* is an MDS code.

The following example illustrates the property of Corollary 3.

Example 1 Let $n = 9$, $k = 5$, $k_1 = 2$ and $q = 8$. In (25), let

$$G^* = \begin{pmatrix} \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 & 0 & 0 \\ 0 & \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 & 0 \\ 0 & 0 & \omega^6 & \omega^5 & \omega^5 & \omega^2 & 1 \end{pmatrix}_{3\times 7} \quad \text{and} \quad D = O_{2\times 7}$$

be matrices over $GF(8) = F_2[x]_{x^3+x+1}$, where ω is the primitive element x. In fact, G^* generates a [7, 3] Reed–Solomon code C^* [15] which is an MDS code. Let C, C^1 and C^2 be the linear codes generated by G, G^1 and G^2 in (25), respectively. It is easy to see that $\dim[P_J(C)] = \dim[P_J(C^1)] + \dim[P_J(C^2)]$ for $J \subseteq \{1, \ldots, 9\}$. Thus $\widetilde{K}(C, C^1) = \widetilde{K}(C^2)$. Specifically,

$$K(C, C^1) = LO(K) = \{0, 0, 0, 0, 0, 1, 2, 3, 3, 3\},$$
$$\widetilde{K}(C, C^1) = UP(\widetilde{K}) = \{0, 0, 0, 1, 2, 3, 3, 3, 3, 3\},$$
$$M(C, C^1) = UP(M) = \{0, 5, 6, 7\}.$$

Lemma 7 determines the cDLP and cIDLP of a linear code, which is for proving the following Theorem 2.

Lemma 7 *For an $[n, k]$ linear code C,*

$$\widehat{K}(C) = \{0, \ldots, 0, 1, \ldots, k\}, \tag{36}$$

$$\widehat{\widehat{K}}(C) = \{0, 1, \ldots, k, \ldots, k\}. \tag{37}$$

Proof From the special case of (16), it is clear that (36) and (37) are equivalent. We only give a proof of (37). From Definition 2, for $0 \leq i \leq n$,

$$\widehat{\widehat{K}}_i(C) = \max\{\dim[P_J(C)] : |J| = i\}$$

where $J \subseteq \{1, \ldots, n\}$. Let G be a generator matrix of C. For any set J with $|J| = i$, it is easy to see that $\dim[P_J(C)] = \operatorname{rank}(G_{\mathrm{col}(J)})$, where $G_{\mathrm{col}(J)}$ is a matrix consisting of the columns of G indexed by J. For $0 \leq i < k$,

$$\widehat{\widehat{K}}_i(C) = \max\{\operatorname{rank}(G_{\mathrm{col}(J)}) : |J| = i\} = i$$

since $\operatorname{rank}(G) = k$. For $k \leq i \leq n$, it can be shown similarly that $\widehat{\widehat{K}}_i(C) = \operatorname{rank}(G) = k$.

By combining Corollary 2, Lemmas 6 and 7, we get the following relations about cRDLP and cIRDLP. Using Corollary 1, the proof is similar to that of Theorem 1.

Theorem 2 *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. Considering equivalence, assume that their generator matrices are in the form of (25). Let C^2 and C^* be the linear codes generated by G^2 and G^* in (25), respectively. For $0 \leq i \leq n$,*

$$\begin{aligned}\widehat{K}_i(C, C^1) \geq \widehat{K}_i(C^2) &= \begin{cases} 0 & \text{if } 0 \leq i \leq k_1, \\ \widehat{K}_{i-k_1}(C^*) & \text{if } k_1 < i \leq n. \end{cases} \\ &= \begin{cases} 0 & \text{if } 0 \leq i \leq n - (k - k_1), \\ i - [n - (k - k_1)] & \text{if } n - (k - k_1) < i \leq n. \end{cases} \end{aligned} \tag{38}$$

$$\begin{aligned}\widehat{\widehat{K}}_i(C, C^1) \leq \widehat{\widehat{K}}_i(C^2) &= \begin{cases} \widehat{\widehat{K}}_i(C^*) & \text{if } 0 \leq i \leq n - k_1, \\ k - k_1 & \text{if } n - k_1 < i \leq n. \end{cases} \\ &= \begin{cases} i & \text{if } 0 \leq i \leq k - k_1, \\ k - k_1 & \text{if } k - k_1 < i \leq n. \end{cases} \end{aligned} \tag{39}$$

By using Proposition 5, Corollary 4 shows two new bounds on RDLP and IRDLP. Note that by (6) the bounds are equivalent.

Corollary 4 *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For dual codes ${C^1}^\perp$ and $C^\perp$,*

$$K({C^1}^\perp, C^\perp) \leq UP(K) = \{0, 1, \ldots, k - k_1, \ldots, k - k_1\}, \tag{40}$$

$$\widetilde{K}({C^1}^\perp, C^\perp) \geq LO(\widetilde{K}) = \{0, \ldots, 0, 1, \ldots, k - k_1\}. \tag{41}$$

Considering equivalence, the following statements are equivalent:

- *$UP(K)$ is achieved by ${C^1}^\perp$ and $C^\perp$;*
- *$LO(\widetilde{K})$ is achieved by ${C^1}^\perp$ and $C^\perp$;*
- *$\widehat{K}(C, C^1) = \widehat{K}(C^2)$;*
- *$\widehat{\widehat{K}}(C, C^1) = \widehat{\widehat{K}}(C^2)$.*

The above C^2 is the linear code generated by G^2 in (25).

Proof The case $k = k_1$ is trivial because $C = C^1$, $C^2 = 0^n$ and $C^* = 0^{n-k_1}$. Consider $k > k_1$. By Propositions 5, (40) and (41) follow from (39) and (38), respectively. From (6), $UP(K)$ is achieved by $C^{1\perp}$ and $C^\perp$ if and only if $LO(\widetilde{K})$ is achieved by them. By Theorem 2, $UP(K)$ is achieved by $C^{1\perp}$ and $C^\perp$ if and only if $\widehat{\widetilde{K}}(C, C^1) = \widehat{\widetilde{K}}(C^2)$; $LO(\widetilde{K})$ is achieved by $C^{1\perp}$ and $C^\perp$ if and only if $\widehat{K}(C, C^1) = \widehat{K}(C^2)$. This proves the equivalence of four statements.

Remark 4 Clearly, $\widehat{K}(C, C^1) = \widehat{K}(C^2)$ and $\widehat{\widetilde{K}}(C, C^1) = \widehat{\widetilde{K}}(C^2)$ if $C^1 = 0^n$. Therefore, both $UP(K)$ and $LO(\widetilde{K})$ are achieved by $GF(q)^n$ and $C^\perp$. The observation will be used to study the Wolf bound of Sect. 5.

Though $UP(K)$ and $LO(\widetilde{K})$ can also be obtained from (4) and (5), Theorem 2 and Corollary 4 provide more useful properties, especially including conditions with the bounds achieved. In addition, by replacing $C^{1\perp}$ and $C^\perp$ with C and C^1 in (40) and (41), we still have

$$K(C, C^1) \le UP(K) \quad \text{and} \quad \widetilde{K}(C, C^1) \ge LO(\widetilde{K}) \tag{42}$$

corresponding to $LO(K)$ and $UP(\widetilde{K})$ of Proposition 1, respectively. The following paragraph shows a nontrivial example in which both $UP(K)$ and $LO(\widetilde{K})$ are achieved.

Example 2 Let $n = 4$, $k = 2$, $k_1 = 1$ and $q = 2$. In (25), let $G^* = (101)$ and $D = (010)$ be matrices over $GF(2)$. Let C, C^1 and C^2 be the linear codes generated by G, G^1 and G^2, respectively. Then $\dim[P_J(C)] = \dim[P_J(C^1)] + \dim[P_J(C^2)]$ for $J \subseteq \{1, \ldots, 4\}$. Therefore, $\widehat{\widetilde{K}}(C, C^1) = \widehat{\widetilde{K}}(C^2)$ and so $UP(K)$ and $LO(\widetilde{K})$ are both achieved.

4 Bounds on relative profiles

This section is mainly about how to tighten the generalized Singleton bounds in Proposition 1. The significance is from a lot of applications, e.g. to get better estimation of the equivocation in [12]. The approach is composed of two parts:

- first, we tighten the generalized Singleton bound on RLDP by introducing new upper bounds;
- second, general refinement and translation are proposed to derive bounds on RDLP and IRDLP from an upper bound on RLDP (in particular the versions for the new bounds are tighter).

4.1 Upper bounds on RLDP

The first upper bound on RLDP is the generalized Singleton bound, see Proposition 1. In this subsection, we show three new upper bounds. The first two are Theorems 3 and 4 which are shown by using an important inequality in Proposition 6. The third one in Theorem 5 cannot be obtained from previous researches on LDP since it involves $w_S(C^1)$. Relations among the bounds are discussed in Example 3, Corollaries 6 and 7. Note that we only consider $1 \le r \le k - k_1$ because $M_0(C, C^1) = 0$.

We begin with the following lemma about the number of subcodes.

Lemma 8 ([7, p. 19]) *The number of* $[n, k]$ *linear codes including a subcode of dimension* r *is* $\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q$.

By Lemma 2, Lemma 8, Propositions 3 and 4, we have the following inequality.

Proposition 6 *For* $1 \le r \le s \le k - k_1$,

$$(1 - q^{-s})M_r(C, C^1) \le (1 - q^{-r})M_s(C, C^1). \tag{43}$$

The equality holds if and only if there exists an s-dimensional relative subcode D of C and C^1 *such that*

- *Condition 1.* $w_S(D) = M_s(C, C^1)$*;*
- *Condition 2. for all t-dimensional*$(r \le t \le s)$ *subcodes* D' *of D,*

$$w_S(D') = M_t(C, C^1).$$

For $r = s - 1$ *and* $q = 2$*, (43) is Theorem 1 of [4] if* $C^1 = 0^n$.

Proof Denote $M_r(C, C^1)$ briefly by M_r. The theorem is obvious for $r = s$. Consider $r < s$. In the following, the first part shows (43) and the second part shows the condition for the equality.

First, we show (50) and then prove (43) by (51). Distinguish the following steps.

- By Proposition 4, for $r < i \le s$ there exists $U \in \mathcal{U}_{k,k-i}$ such that

$$m_G(U) = n - M_i. \tag{44}$$

- Consider the set of $[k, k - i + 1]$ linear codes including U, i.e.

$$\{V_j : V_j \in F_{k,k-i+1}, U \subset V_j, j = 1, \ldots, l(i)\}$$

where $l(i) = \begin{bmatrix} i \\ 1 \end{bmatrix}_q = \frac{q^i - 1}{q - 1}$ (by Lemma 8). Note that $\dim[P_{\mathcal{N}_{k_1}}(V_j)] = k_1$ for all V_j since $\dim[P_{\mathcal{N}_{k_1}}(U)] = k_1$. By Proposition 4,

$$M_{i-1} \le n - m_G(V_j). \tag{45}$$

Then for all V_j

$$m_G(V_j - U) \overset{(a)}{=} m_G(V_j) - m_G(U) \overset{(b)}{\le} M_i - M_{i-1}, \tag{46}$$

where (a) follows from $U \subset V_j$ and (b) follows from (44) and (45). Clearly,

$$\text{the equality in } (b) \text{ of (46) holds} \Leftrightarrow \text{the equality in (45) holds.} \tag{47}$$

- Summing up the left-hand side of (46) over all j,

$$\begin{aligned} \sum_{j=1}^{l(i)} m_G(V_j - U) &\overset{(a)}{=} m_G\left[\bigcup_{j=1}^{l(i)}(V_j - U)\right] \\ &= m_G\left(\bigcup_{j=1}^{l(i)} V_j - U\right) \\ &\overset{(b)}{=} m_G[\mathrm{GF}(q)^k - U] \\ &\overset{(c)}{=} n - m_G(U) \\ &\overset{(d)}{=} M_i, \end{aligned} \tag{48}$$

where

(*a*) follows from $(V_{j_1} - U) \cap (V_{j_2} - U) = \emptyset$ for $j_1 \neq j_2$ (both V_{j_1} and V_{j_2} are of 1 dimension greater than U);
(*b*) follows from $\mathrm{GF}(q)^k - U \subseteq \bigcup_{j=1}^{l(i)} V_j - U$;
(*c*) follows from $m_G[\mathrm{GF}(q)^k] = n$ and $U \cap [\mathrm{GF}(q)^k - U] = \emptyset$;
(*d*) follows from (44).

Combining (46) with (48), for $r < i \leq s$

$$M_i = \sum_{j=1}^{l(i)} m_G(V_j - U) \leq \frac{q^i - 1}{q - 1}(M_i - M_{i-1}) \tag{49}$$

or

$$(1 - q^{-i})M_{i-1} \leq (1 - q^{-(i-1)})M_i. \tag{50}$$

– Using iterations of (50),

$$M_r \leq \frac{1 - q^{-r}}{1 - q^{-(r+1)}} M_{r+1} \leq \cdots \leq \frac{1 - q^{-r}}{1 - q^{-s}} M_s \tag{51}$$

which proves (43).

Second, we use Proposition 3 to show the condition for the equality in (43).

Only if part. Assume the equality in (43) holds. By Proposition 2, there exists an s-dimensional relative subcode D of C and C^1 such that $w_S(D) = M_s$ which satisfies Condition 1. The following paragraph shows D satisfies Condition 2.

By Proposition 3, $\varphi(D) \in \mathcal{U}_{k,k-s}$ and $m_G[\varphi(D)] = n - M_s$. Since D' is a subcode of D, $\varphi(D) \subseteq \varphi(D') \in \mathcal{U}_{k,k-t}$ by Lemma 2. For any $t (r \leq t \leq s)$ and any W satisfying $\varphi(D) \subseteq W \in \mathcal{U}_{k,k-t}$, we show $m_G(W) = n - M_t$ by induction on t (in a decreasing manner).

– The case $t = s$ is obvious since $D' = D$.
– For $t = i (r < i \leq s)$, assume $m_G(W) = n - M_i$ for any W satisfying $\varphi(D) \subseteq W \in \mathcal{U}_{k,k-i}$.
– Consider $t = i - 1$. For any W' satisfying $\varphi(D) \subset W' \in \mathcal{U}_{k,k-i+1}$, there exists $W_0 \in \mathcal{U}_{k,k-i}$ such that $\varphi(D) \subseteq W_0 \subset W'$. Then $m_G(W_0) = n - M_i$ by the hypothesis. Because the equality in (43) holds, all the equalities in (51) hold. Hence the equality in (49) holds and then the equality in (*b*) of (46) holds. Thus $m_G(W') = n - M_{i-1}$ by (47).

In particular, $m_G[\varphi(D')] = n - M_t$ since $\varphi(D) \subseteq \varphi(D') \in \mathcal{U}_{k,k-t}$. By (11), $w_S(D') = n - m_G[\varphi(D')] = M_t$ which proves Condition 2.

If part. Assume D is an s-dimensional relative subcode of C and C^1, and also satisfies the two conditions. It suffices to show all the equalities in (51) hold, or $M_{i-1} = n - m_G(V_j)$ for any $i (r < i \leq s)$ and any V_j.

For any given i and j, we have $V_j \in \mathcal{U}_{k,k-i+1}$ by $\dim[P_{\mathcal{N}_{k_1}}(V_j)] = k_1$. Then $w_S[\varphi^{-1}(V_j)] = n - m_G(V_j)$ by (11), where φ^{-1} is the inverse of φ and $\varphi^{-1}(V_j)$ is an $(i-1)$-dimensional relative subcode of C and C^1. On the other hand, $w_S[\varphi^{-1}(V_j)] = M_{i-1}$ by Condition 2 and thus $M_{i-1} = n - m_G(V_j)$.

Generally, the generalized Singleton bound on RLDP is not tight and conditions for achieving it is strict. Thus we consider tighter bounds. One possible improvement is from the Plotkin bound [15, pp. 41–42] which is strongly linked with equidistant codes. For linear cases, this bound is achieved by linear constant-weight codes [23]. The generalized Plotkin bound on LDP was given in [5]. We extend it to RLDP by Proposition 6. Note that the classic Plotkin bound is on the size of a code while the following is on a parameter like minimum distance.

Theorem 3 (Generalized Plotkin Bound on RLDP) *For* $1 \le r \le k - k_1$,

$$M_r(C, C^1) \le \left\lfloor \frac{1 - q^{-r}}{1 - q^{-(k-k_1)}}(n - k_1) \right\rfloor. \tag{52}$$

If $C^1 = 0^n$, *then (52) is the generalized Plotkin bound on LDP [5]. Furthermore,*

$$M_r(C, C^1) = \frac{1 - q^{-r}}{1 - q^{-(k-k_1)}}(n - k_1) \quad \text{for all } r \tag{53}$$

if and only if it holds for $r = 1$.

Proof For the first part, (52) follows since for all r

$$M_r(C, C^1) \overset{(a)}{\le} \frac{1 - q^{-r}}{1 - q^{-(k-k_1)}} M_{k-k_1}(C, C^1) \overset{(b)}{\le} \frac{1 - q^{-r}}{1 - q^{-(k-k_1)}}(n - k_1), \tag{54}$$

where (a) and (b) follow from Propositions 6 and 1, respectively. For the second part, it suffices to show the "if" part. Note that

$$\frac{1 - q^{-r}}{1 - q^{-1}} M_1(C, C^1) \overset{(a)}{\le} M_r(C, C^1) \overset{(b)}{\le} \frac{1 - q^{-r}}{1 - q^{-(k-k_1)}}(n - k_1), \tag{55}$$

where (a) and (b) follow from Proposition 6 and (54), respectively. If

$$M_1(C, C^1) = \frac{1 - q^{-1}}{1 - q^{-(k-k_1)}}(n - k_1),$$

then all the equalities in (55) hold for all r.

Remark 5 If $(1 - q^{-r})(n - k_1) < M_r(C, C^1)$, then by (52)

$$q^{k-k_1} \le \left\lfloor \frac{M_r(C, C^1)}{M_r(C, C^1) - (1 - q^{-r})(n - k_1)} \right\rfloor.$$

Letting $k_1 = 0$ and $r = 1$, the classic Plotkin bound for linear codes is derived.

We say (C, C^1) satisfying (53) achieves the **weak Plotkin bound**. Theorem 3 describes a sufficient and necessary condition for achieving it. By Proposition 6, Corollary 5 shows another condition from the perspective of equal support weights of subcodes.

Corollary 5 *Code pair* (C, C^1) *achieves the weak Plotkin bound if and only if there exists a* $(k - k_1)$*-dimensional relative subcode* D *of* C *and* C^1 *such that*

- $w_S(D) = n - k_1$;
- *for all* t*-dimensional*$(1 \le t \le k - k_1)$ *subcodes* D' *of* D, $w_S(D') = M_t(C, C^1)$.

Clearly, subcode D *satisfying the above conditions is a linear constant-weight code.*

The generalized Plotkin bound on RLDP is tighter than the Singleton one in most cases. Moreover, we shall show in Sect. 4.2 that the refined Plotkin one is always tighter, see Proposition 8.

Example 3 (Plotkin and Singleton) Let C be a binary $[10, 3]$ linear code with generator matrix G and C^1 be a subcode of dimension 1 with generator matrix G^1 such that

$$G = \begin{pmatrix} 1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,0\,1 \\ 0\,1\,0\,1\,0\,1\,1\,0\,1\,1 \end{pmatrix}$$

and G^1 is the first row of G. The generalized Plotkin bound on RLDP is achieved, while the generalized Singleton bound on RLDP which suggests $M_1(C, C^1) \leq 8$ is not tight.

Another idea of improving Proposition 1 is from the Griesmer bound [15, pp. 546–547], which is tighter than the Plotkin bound in many cases. The generalized Griesmer bound on LDP was given in [5]. Theorem 4 provides its extension on RLDP. We first show some preliminaries. For $1 \leq r \leq j \leq k - k_1$, let

$$L_r(j, d) = \begin{cases} d & \text{if } j = r, \\ \left\lceil \frac{q^j - 1}{q^j - q} L_r(j-1, d) \right\rceil & \text{if } j > r. \end{cases}$$

Similar to Theorem 2 of [4], by Proposition 6

$$M_j(C, C^1) \geq L_r(j, M_r(C, C^1)). \tag{56}$$

Then similar to Theorem 3 of [4],

$$L_r(j, d) = d + \sum_{i=1}^{j-r} \left\lceil \frac{(q-1)d}{q^i(q^r - 1)} \right\rceil. \tag{57}$$

Note that the approach of [4] based on GF(2) can be easily generalized to GF(q).

Theorem 4 (Generalized Griesmer Bound on RLDP) *For* $1 \leq r \leq k - k_1$,

$$n \geq k_1 + M_r(C, C^1) + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{(q-1)M_r(C, C^1)}{q^i(q^r - 1)} \right\rceil. \tag{58}$$

If $C^1 = 0^n$, *then (58) is the generalized Griesmer bound on LDP [5]. The equality in (58) holds for all* r *if and only if it holds for* $r = 1$. *Furthermore, if the equality in (58) holds for all* r, *then*

$$M_r(C, C^1) = \sum_{i=0}^{r-1} \left\lceil \frac{M_1(C, C^1)}{q^i} \right\rceil. \tag{59}$$

Proof Denote $M_r(C, C^1)$ briefly by M_r. The proof consists of three parts: the first part proves (58) by (60); the second part shows the fact that the right-hand side of (58) is increasing with r and then proves the condition for the equality of (58), see (61) and (63); the third part proves (59) by (64).

First, (58) follows because for all r

$$M_r + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{(q-1)M_r}{q^i(q^r - 1)} \right\rceil \overset{(a)}{\leq} M_{k-k_1} \overset{(b)}{\leq} n - k_1, \tag{60}$$

where (a) follows by combining (56) with (57), and (b) follows from Proposition 1.

Second, we show the equality in (58) holds for all r if and only if it holds for $r = 1$. It suffices to prove the "if" part. Assume the equality in (58) holds for $r = 1$. For $1 \leq j < k - k_1$,

$$\begin{aligned} n &\overset{(a)}{\geq} k_1 + M_{j+1} + \sum_{i=1}^{k-k_1-(j+1)} \left\lceil \frac{(q-1)M_{j+1}}{q^i(q^{j+1} - 1)} \right\rceil \\ &\overset{(b)}{\geq} k_1 + \left\lceil \frac{q^{j+1} - 1}{q^{j+1} - q} M_j \right\rceil + \sum_{i=1}^{k-k_1-(j+1)} \left\lceil \frac{q-1}{q^i(q^{j+1} - 1)} \times \frac{q^{j+1} - 1}{q^{j+1} - q} M_j \right\rceil \end{aligned} \tag{61}$$

$$= k_1 + \left(M_j + \left\lceil \frac{q-1}{q^{j+1}-q} M_j \right\rceil \right) + \sum_{i=1}^{k-k_1-(j+1)} \left\lceil \frac{(q-1)M_j}{q^{i+1}(q^j-1)} \right\rceil \tag{62}$$

$$= k_1 + M_j + \left\lceil \frac{q-1}{q(q^j-1)} M_j \right\rceil + \sum_{i=2}^{k-k_1-j} \left\lceil \frac{(q-1)M_j}{q^i(q^j-1)} \right\rceil$$

$$= k_1 + M_j + \sum_{i=1}^{k-k_1-j} \left\lceil \frac{(q-1)M_j}{q^i(q^j-1)} \right\rceil, \tag{63}$$

where (a) and (b) follow from (60) and Proposition 6, respectively. If j is replaced by $j+1$, then (63) becomes (61). Therefore the right-hand side of (58) is increasing with r, which proves the second part.

Finally, we show (59). If the equality in (58) holds for all r, then all the equalities between (61) and (62) hold. Comparing the last items in the right-hand sides of (61) and (62), for $1 \le i \le k - k_1 - r$

$$\left\lceil \frac{(q-1)M_r}{q^i(q^r-1)} \right\rceil = \left\lceil \frac{(q-1)M_{r-1}}{q^{i+1}(q^{r-1}-1)} \right\rceil = \cdots = \left\lceil \frac{M_1}{q^{i+r-1}} \right\rceil. \tag{64}$$

Therefore

$$\begin{aligned} n &= k_1 + M_r + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{(q-1)M_r}{q^i(q^r-1)} \right\rceil \\ &\overset{(a)}{=} k_1 + M_r + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{M_1}{q^{i+r-1}} \right\rceil \\ &= k_1 + M_r + \sum_{i=r}^{k-k_1-1} \left\lceil \frac{M_1}{q^i} \right\rceil \\ &\overset{(b)}{=} M_r + n - \sum_{i=0}^{r-1} \left\lceil \frac{M_1}{q^i} \right\rceil, \end{aligned}$$

where (a) follows from (64) and (b) follows from the equality in (58) for $r = 1$. This proves the third part.

Example 4 Let C be a binary $[6, 3]$ linear code with generator matrix G and C^1 be a subcode of dimension 1 with generator matrix G^1 such that

$$G = \begin{pmatrix} 1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,1 \end{pmatrix}$$

and G^1 is the first row of G. It is easy to see that the generalized Griesmer bound on RLDP is achieved and (59) holds.

Theorem 4 yields the following two relations.

Corollary 6 (Griesmer and Plotkin) *If (C, C^1) achieves the weak Plotkin bound, then it achieves the generalized Griesmer bound on RLDP.*

Proof By using (53),

$$\begin{aligned} & k_1 + M_r(C, C^1) + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{(q-1)M_r(C, C^1)}{q^i(q^r-1)} \right\rceil \\ & \geq k_1 + \frac{1-q^{-r}}{1-q^{-(k-k_1)}}(n-k_1) + \sum_{i=1}^{k-k_1-r} \left[\frac{q-1}{q^i(q^r-1)} \times \frac{1-q^{-r}}{1-q^{-(k-k_1)}}(n-k_1) \right] \\ & = n. \end{aligned}$$

Then it follows by combining the above formula with (58).

Corollary 7 (Griesmer and Singleton) *The generalized Griesmer bound on RLDP is tighter than the generalized Singleton bound on RLDP.*

Proof For $1 \leq r \leq k - k_1$,

$$\begin{aligned} n & \overset{(a)}{\geq} k_1 + M_r(C, C^1) + \sum_{i=1}^{k-k_1-r} \left\lceil \frac{(q-1)M_r(C, C^1)}{q^i(q^r-1)} \right\rceil \\ & \overset{(b)}{\geq} k_1 + M_r(C, C^1) + (k - k_1 - r) \\ & = k - r + M_r(C, C^1), \end{aligned}$$

where (a) follows from (58), and (b) follows since $M_r(C, C^1) \geq 1$ for $r \geq 1$ (by Lemma 1).

Theorem 5 shows another upper bound which is sometimes tighter than the generalized Plotkin and Griesmer bounds on RLDP (e.g. see Example 6). A linear code C is called a **relative constant-weight (RCW) code** to subcode C^1 if all codewords in $C - C^1$ have the same weight. Note that C is an equidistant code if it is an RCW code to a zero code.

Theorem 5 (RCW Bound on RLDP [27]) *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For $1 \leq r \leq k - k_1$,*

$$M_r(C, C^1) \leq \left\lfloor \frac{1-q^{-r}}{1-q^{-(k-k_1)}} \left(n - \frac{w_S(C^1)}{q^{k-k_1}} \right) \right\rfloor. \tag{65}$$

If $C^1 = 0^n$, then (65) is the generalized Plotkin bound on LDP [5]. Furthermore,

$$M_r(C, C^1) = \frac{1-q^{-r}}{1-q^{-(k-k_1)}} \left(n - \frac{w_S(C^1)}{q^{k-k_1}} \right) \quad \text{for } 1 \leq r \leq k - k_1,$$

if and only if C is an RCW code to C^1 with $w_S(C) = n$.

4.2 Bound refinement and translation

For applications, we are sometimes more interested in bounds on RDLP and IRDLP. The first example is that the equivocation of [12] can be expressed by IRDLP. Therefore, bounds on IRDLP describe the secrecy of that model. Another example will be motivated by Theorem 6 of Sect. 5. When bounds on RDLP and IRDLP are obtained, trellis complexities of a linear code and any subcode can be evaluated.

In this subsection, we mainly focus on how to translate any upper bound on RLDP into a corresponding lower bound on RDLP and an upper bound on IRDLP, which was not mentioned by previous work. A unified framework consisting of the following parts is introduced:

– **bound refinement**, i.e. tightening an upper bound $\mathbf{u}$ on RLDP to a strictly increasing one $\mathbf{u}'$ by Algorithm 1;
– **bound translation**, i.e. translating $\mathbf{u}'$ to bounds on RDLP and IRDLP by Proposition 9.

Particularly, the refined generalized Plotkin and Griesmer bounds on RLDP by Algorithm 1 are tighter than the Singleton one, see Propositions 7 and 8. By combining them with Proposition 9, the generalized Singleton bounds on RDLP and IRDLP are tightened, see Corollary 8.

Assume that $M(C, C^1)$ is upper-bounded by an integer sequence

$$\mathbf{u} = \{u_0 = 0, u_1, \ldots, u_{k-k_1} \leq n\}.$$

(Here, $u_0 = 0$ and $u_{k-k_1} \leq n$ follow from $M_0(C, C^1) = 0$ and $M_{k-k_1}(C, C^1) \leq n$, respectively.) Generally, $\mathbf{u}$ is not necessarily strictly increasing and even not nondecreasing. On the other hand, since $M_r(C, C^1)$ is strictly increasing with r, we can always refine $\mathbf{u}$ to a tighter integer upper bound

$$\mathbf{u}' = \{u'_0 = u_0, u'_1, \ldots, u'_{k-k_1} = u_{k-k_1}\}$$

such that u'_r is strictly increasing with r, see Algorithm 1. (Clearly, $u'_0 = 0$ or otherwise $\mathbf{u}$ is invalid.) The procedure works from "tail" u_{k-k_1} to "head" u_0 step by step. If $u_{r-1} \geq u_r$, adjust u_{r-1} to $u_r - 1 (< u_r)$ for meeting the strictly increasing requirement. For example, $\mathbf{u}' = \{0, 1, 2, 3, 5\}$ if $\mathbf{u} = \{0, 3, 4, 3, 5\}$.

Input: an integer upper bound $\mathbf{u} = \{u_0 = 0, u_1, \ldots, u_{k-k_1} \leq n\}$
Output: a tighter integer upper bound $\mathbf{u}' = \{u'_0 = u_0, u'_1, \ldots, u'_{k-k_1} = u_{k-k_1}\}$ where u'_r is strictly increasing with r
$r \leftarrow k - k_1$;
while $r \geq 0$ **do**
  $u'_r \leftarrow u_r$;
  if $r \geq 1$ *and* $u_{r-1} \geq u_r$ **then**
    $u_{r-1} \leftarrow u_r - 1$;
  end
  $r \leftarrow r - 1$;
end

Algorithm 1: Refinement of an upper bound on RLDP

By Proposition 1, the generalized Singleton bound on RLDP does not need to be refined because it is strictly increasing. Even without Algorithm 1, the generalized Griesmer bound on RLDP is tighter than the Singleton one, which immediately yields Proposition 7.

Proposition 7 *The refined generalized Griesmer bound on RLDP by Algorithm 1 is tighter than the generalized Singleton bound on RLDP.*

The generalized Plotkin bound on RLDP is not always tighter than the Singleton one, but fortunately the refined one is.

Proposition 8 *The refined generalized Plotkin bound on RLDP by Algorithm 1 is tighter than the generalized Singleton bound on RLDP.*

Proof Note that $UP(M)_{k-k_1} = n - k_1$ (see Proposition 1) coincides with the right-hand side of (52) for $r = k - k_1$. Then the result follows since the refined sequence is strictly increasing, i.e. the increment at each step is at least 1.

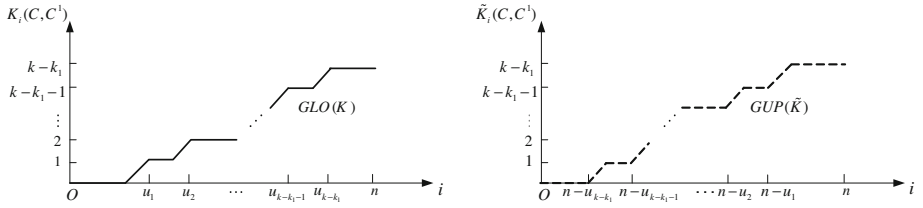

Fig. 1 Universal bounds on $K(C, C^1)$ and $\widetilde{K}(C, C^1)$

The refined RCW bound on RLDP is not always tighter than the Singleton one, especially when $q > 2$, see the following example.

Example 5 (Example 1 cont.*)* Consider the upper bounds on RLDP:

- **Singleton.** $M(C, C^1) \leq \mathbf{u}^s = \{0, 5, 6, 7\}$,
- **Plotkin.** $M(C, C^1) \leq \mathbf{u}^p = \{0, 6, 6, 7\}$,
- **Griesmer.** $M(C, C^1) \leq \mathbf{u}^g = \{0, 5, 6, 7\}$,
- **RCW.** $M(C, C^1) \leq \mathbf{u}^r = \{0, 7, 8, 8\}$.

Clearly, $\mathbf{u}^s$ and $\mathbf{u}^g$ is the tightest and achieved by C and C^1; $\mathbf{u}^p$ is only a bit looser at $M_1(C, C^1)$; $\mathbf{u}^r$ is the worst one. By applying Algorithm 1, the refined bound $\mathbf{u}'^p$ from $\mathbf{u}^p$ equals to $\{0, 5, 6, 7\}$ which is achieved; however, the refined bound $\mathbf{u}'^r$ from $\mathbf{u}^r$ equals to $\{0, 6, 7, 8\}$ which is still not achieved.

Since an upper bound $\mathbf{u}$ on RLDP can always be refined to $\mathbf{u}'$ by Algorithm 1, **assume in the following that u is already strictly increasing.** Then it can be translated to the following bounds on RDLP and IRDLP depicted in Fig. 1.

Proposition 9 (Universal Bounds on RDLP and IRDLP) *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. Assume their RLDP satisfies*

$$M(C, C^1) \leq \mathbf{u} = \{u_0 = 0, u_1, \ldots, u_{k-k_1} \leq n\} \tag{66}$$

where $\mathbf{u}$ is a strictly increasing integer sequence. Then their RDLP satisfies

$$\begin{aligned} K(C, C^1) \geq GLO(K) &\triangleq \{GLO(K)_i : 0 \leq i \leq n\} \\ &= \{0, \ldots, 0, 1, \ldots, 1, \ldots, k-k_1, \ldots, k-k_1\} \end{aligned}$$

where $\max\{i : GLO(K)_i = r\} = u_{r+1} - 1$ *for* $0 \leq r < k - k_1$. *Their IRDLP satisfies*

$$\begin{aligned} \widetilde{K}(C, C^1) \leq GUP(\widetilde{K}) &\triangleq \{GUP(\widetilde{K})_i : 0 \leq i \leq n\} \\ &= \{0, \ldots, 0, 1, \ldots, 1, \ldots, k-k_1, \ldots, k-k_1\} \end{aligned}$$

where $\max\{i : GUP(\widetilde{K})_i = r\} = n - u_{k-k_1-r}$ *for* $0 \leq r < k - k_1$. *Furthermore, $GLO(K)$ and $GUP(\widetilde{K})$ are both achieved if and only if (66) is achieved.*

Proof We first show $K(C, C^1) \geq GLO(K)$ by using the monotonicity of RDLP and Remark 1 (see (68) and (69)), and then prove $\widetilde{K}(C, C^1) \leq GUP(\widetilde{K})$ by using (6) (see (71)). Since $M_{r'}(C, C^1) \leq u_{r'}$ for $0 \leq r' \leq k - k_1$, it follows from Remark 1 that for all r'

$$K_{u_{r'}}(C, C^1) \geq r'. \tag{67}$$

Combining (4) and (67),

$$K_{u_{r+1}-1}(C, C^1) \geq K_{u_{r+1}}(C, C^1) - 1 \geq r$$

where $0 \le r < k - k_1$. Since $K_{u_r}(C, C^1) \ge r$ and $K_i(C, C^1)$ is nondecreasing with i,

$$K_i(C, C^1) \ge r \quad \text{for } u_r \le i \le u_{r+1} - 1 < u_{r+1} \quad \text{and} \quad 0 \le r < k - k_1. \tag{68}$$

In addition, since $K_{u_{k-k_1}} \ge k - k_1$ and $K_i(C, C^1) \le k - k_1$ (see Lemma 1),

$$K_i(C, C^1) = k - k_1 \quad \text{for } u_{k-k_1} \le i \le n. \tag{69}$$

Then

$$K(C, C^1) \ge GLO(K) \tag{70}$$

is obtained from (68) and (69). For the second part, it is easy to verify that

$$GUP(\widetilde{K})_i = k - k_1 - GLO(K)_{n-i} \quad \text{for } 0 \le i \le n. \tag{71}$$

Then $\widetilde{K}(C, C^1) \le GUP(\widetilde{K})$ follows from (6), (70) and (71). The last statement follows immediately from (6) through (8).

Remark 6 If $u_r = n - k + r$ for $1 \le r \le k - k_1$, then $GLO(K) = LO(K)$ and $GUP(\widetilde{K}) = UP(\widetilde{K})$, i.e. the generalized Singleton bounds of Proposition 1 are derived.

By combining Propositions 7 through 9, the generalized Singleton bounds on RDLP and IRDLP are tightened as follows.

Corollary 8 *If* $\mathbf{u}$ *of (66) is the refined generalized Plotkin or Griesmer bound on RLDP, then* $GLO(K)$ *and* $GUP(\widetilde{K})$ *are tighter than* $LO(K)$ *and* $UP(\widetilde{K})$ *of Proposition 1, respectively.*

As to the wiretap channel of [12], the equivocation of the legitimate parties' data symbols to the adversary is upper-bounded by $UP(\widetilde{K})$. Corollary 8 implies that the estimation of equivocation can be improved. The following paragraph provides an example to perform the bound translation of Proposition 9.

Example 6 Let C be a binary $[18, 4]$ linear code with generator matrix G and C^1 be a subcode of dimension 2 with generator matrix G^1 such that

$$G = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1 \\ 0\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,0\,0\,1 \\ 0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0 \end{pmatrix}$$

and G^1 is composed of the first two rows of G. Consider the following upper bounds on RLDP:

- **Singleton.** $M(C, C^1) \le \mathbf{u}^s = \{0, 15, 16\}$.
- **Plotkin.** $M(C, C^1) \le \mathbf{u}^p = \{0, 10, 16\}$.
- **Griesmer.** $M(C, C^1) \le \mathbf{u}^g = \{0, 10, 16\}$.
- **RCW.** $M(C, C^1) \le \mathbf{u}^r = \{0, 10, 15\}$.

It is easy to verify that the RCW bound is achieved by C and C^1. Since each $\mathbf{u}$-sequence is strictly increasing, the corresponding $GLO(K)$ and $GUP(\widetilde{K})$ can be obtained from Proposition 9. The results are depicted in Fig. 2. Clearly, $GLO(K)$ and $GUP(\widetilde{K})$ derived from the generalized Singleton bound on RLDP are the worst. Those derived from the Plotkin and Griesmer ones are the same since $\mathbf{u}^p = \mathbf{u}^g$. Those derived from the RCW one are the tightest and achieved.

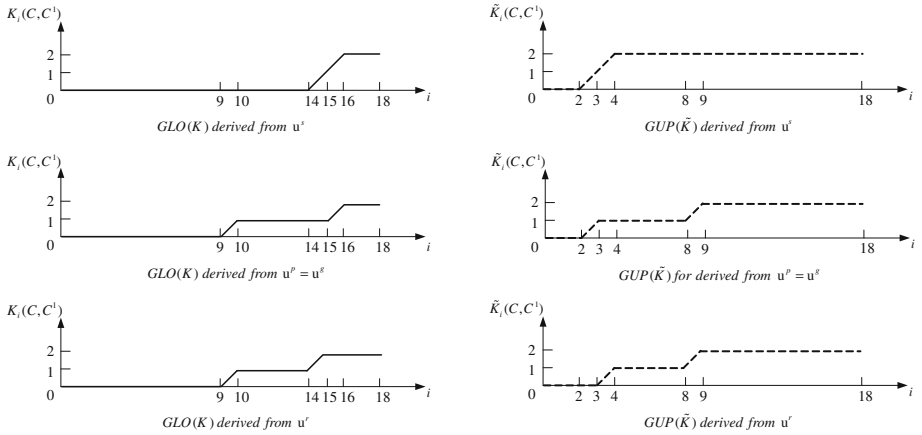

Fig. 2 $GLO(K)$ and $GUP(\widetilde{K})$ derived from upper bounds on RLDP of Example 6

5 Application of RDLP to trellis complexity

The trellis [10] for a linear code C is a directed graph with an initial vertex σ_0 and a final vertex σ_n. The vertices (or called states) of the graph are partitioned into subsets $\Sigma_0(C) = \{\sigma_0\}$, $\Sigma_1(C), \ldots, \Sigma_n(C) = \{\sigma_n\}$. Each edge from a state in $\Sigma_{i-1}(C)$ terminates at a state in $\Sigma_i(C)$ for $1 \le i \le n$, and is labeled by an element in $GF(q)$. A codeword of C is uniquely represented by a path from σ_0 to σ_n, and vice versa. Note that $\Sigma_i(C)$ is a vector space. For trellis construction, we refer the readers to [10, Chaps. 4.1, 4.2 and 9.4].

By applying the Viterbi algorithm [10,22], we can devise the maximum-likelihood soft-decision decoding based on trellises. The **state complexity profile** [2] of an $[n, k]$ linear code C is defined as $\mathbf{s}(C) = \{s_i(C) : 0 \le i \le n\}$ where

$$s_i(C) = \dim[\Sigma_i(C)].$$

The **state complexity**

$$s_{max}(C) = \max\{s_i(C)\}$$

is the key to measure the decoding efficiency. Forney [2] introduced the ordered DLP and ordered IDLP of C to describe $\mathbf{s}(C)$, and showed a lower bound on it (DLP bound). An earlier research of Wolf [22] provided an upper bound on $s_{max}(C)$ (Wolf bound). More notable results were shown in [9,16,24], etc.

In trellis-based decoding, sometimes we only need to decode codewords in a subcode C^1 when coding rate varies. Typically, the attempt is to enhance error-correcting capability when fewer users are involved, e.g., in wireless communications [13]. Unfortunately, relations between $\mathbf{s}(C^1)$ and $\mathbf{s}(C)$ were not known from previous work. In this section, we generalize Forney's approach and introduce the ordered RDLP and ordered IRDLP of C and C^1. By using the concepts, Theorem 6 shows a relation between $\mathbf{s}(C^1)$ and $\mathbf{s}(C)$, which reveals connections between the DLP and Wolf bounds. For $0 \le i \le n$, define

$$i^- = \{1, \ldots, i\} \quad \text{and} \quad i^+ = \{i+1, \ldots, n\}.$$

Note that $0^- = n^+ = \emptyset$. **The following paragraphs use the notations of [2].**

Definition 4 (*Ordered RDLP and Ordered IRDLP*) For an $[n, k]$ linear code C and a subcode C^1 of dimension k_1, their ordered RDLP is defined as a sequence $\overrightarrow{K}(C, C^1) = \{\overrightarrow{K}_i(C, C^1) : 0 \le i \le n\}$ where

$$\overrightarrow{K}_i(C, C^1) = \dim(C_{i^-}) - \dim(C^1_{i^-}).$$

Their ordered IRDLP is defined as $\overrightarrow{\widetilde{K}}(C, C^1) = \{\overrightarrow{\widetilde{K}}_i(C, C^1) : 0 \le i \le n\}$ where

$$\overrightarrow{\widetilde{K}}_i(C, C^1) = \dim[P_{i^-}(C)] - \dim[P_{i^-}(C^1)].$$

Particularly,

$$\overrightarrow{K}(C) = \overrightarrow{K}(C, 0^n) \quad \text{and} \quad \overrightarrow{\widetilde{K}}(C) = \overrightarrow{\widetilde{K}}(C, 0^n)$$

are the ordered DLP and ordered IDLP of C [2]. In addition, denote their components by $\overrightarrow{K}_i(C)$ and $\overrightarrow{\widetilde{K}}_i(C)$, where $0 \le i \le n$.

Lemma 9 shows that the state complexity profile of a linear code C is the difference between the ordered DLP and ordered IDLP of C.

Lemma 9 ([2]) *Let C be an $[n, k]$ linear code. For $0 \le i \le n$,*

$$s_i(C) = k - \dim(C_{i^-}) - \dim(C_{i^+}) = \overrightarrow{\widetilde{K}}_i(C) - \overrightarrow{K}_i(C).$$

By Lemma 9, Proposition 5 and Remark 4, we get the main result.

Theorem 6 *Let C be an $[n, k]$ linear code and C^1 be a subcode of dimension k_1. For $0 \le i \le n$,*

$$\widetilde{K}_i(C, C^1) - K_i(C, C^1) \overset{(a)}{\le} s_i(C) - s_i(C^1) \overset{(b)}{\le} K_i(C^{1^\perp}, C^\perp) - \widetilde{K}_i(C^{1^\perp}, C^\perp). \quad (72)$$

Furthermore, if $C^1 = 0^n$, (a) and (b) are the DLP bound [2] on $\mathbf{s}(C)$ and the Wolf bound [22] on $s_{max}(C)$, respectively.

Proof We first show (72). On one hand,

$$\begin{aligned} s_i(C) - s_i(C^1) &\overset{(a)}{=} [\overrightarrow{\widetilde{K}}_i(C) - \overrightarrow{\widetilde{K}}_i(C^1)] - [\overrightarrow{K}_i(C) - \overrightarrow{K}_i(C^1)] \\ &= \overrightarrow{\widetilde{K}}_i(C, C^1) - \overrightarrow{K}_i(C, C^1) \\ &\overset{(b)}{\ge} \widetilde{K}_i(C, C^1) - K_i(C, C^1), \end{aligned}$$

where (a) and (b) follow from Lemma 9 and $|i^-| = i$, respectively. On the other hand,

$$\begin{aligned} s_i(C) - s_i(C^1) &= \overrightarrow{\widetilde{K}}_i(C, C^1) - \overrightarrow{K}_i(C, C^1) \\ &\le \widehat{\widetilde{K}}_i(C, C^1) - \widehat{K}_i(C, C^1) \\ &= K_i(C^{1^\perp}, C^\perp) - \widetilde{K}_i(C^{1^\perp}, C^\perp), \end{aligned}$$

where the last equation follows from Proposition 5. For the second claim, it is clear that (a) of (72) yields the DLP bound on $\mathbf{s}(C)$ if $C^1 = 0^n$. For (b) of (72), if $C^1 = 0^n$,

$$s_i(C) = s_i(C) - s_i(0^n) \le K_i(GF(q)^n, C^\perp) - \widetilde{K}_i(GF(q)^n, C^\perp) \quad (73)$$

for $0 \leq i \leq n$. By using Remark 4,

$$K(GF(q)^n, C^{\perp}) = UP(K) = \{0, 1, \ldots, k-k_1, \ldots, k-k_1\}, \tag{74}$$
$$\widetilde{K}(GF(q)^n, C^{\perp}) = LO(\widetilde{K}) = \{0, \ldots, 0, 1, \ldots, k-k_1\}. \tag{75}$$

Combining (73) through (75),

– if $k \leq n-k$, then

$$s_i(C) \leq \begin{cases} i & \text{if } 0 \leq i \leq k, \\ k & \text{if } k < i \leq n-k, \\ n-i & \text{if } n-k < i \leq n; \end{cases}$$

– if $k \geq n-k$, then

$$s_i(C) \leq \begin{cases} i & \text{if } 0 \leq i \leq n-k, \\ n-k & \text{if } n-k < i \leq k, \\ n-i & \text{if } k < i \leq n. \end{cases}$$

Both of the cases yield $s_{max}(C) = \max\{s_i(C)\} \leq \max\{k, n-k\}$, i.e. the Wolf bound.

Remark 7 If C is an MDS code and $C^1 = 0^n$, then the equalities in (72) hold, see [2]. In addition, (b) of (72) can also be derived by combining (a) of (72) and $\mathbf{s}(C) = \mathbf{s}(C^{\perp})$ proved in [2].

Theorem 6 provides a method to estimate $\mathbf{s}(C^1)$ when $\mathbf{s}(C)$ is known, and vice versa. This method is particularly useful in choosing a suitable C^1 from C (or expanding C^1 to a "bigger" linear code C) when a tradeoff among coding rate, error-correcting capability and decoding complexity is considered. The result also implies that the DLP and Wolf bounds are "duality" results, which is seen from two-code perspectives but cannot be revealed from previous researches on trellises. Similar to Forney's approach, our result can be easily generalized to estimate the branch and section complexities of C^1 [2,10] when those of C are known. The details are omitted here.

6 Conclusions

The relative profiles (i.e. RDLP, IRDLP and RLDP) of a linear code and a subcode were applied to the wiretap channel of type II with illegitimate parties. Recently, RLDP was extended in network coding for secrecy control purpose [25,26]. Some bounds on RLDP and IRDLP were given in [12,20].

In this paper, we introduce new relations which not only reveal connections among some known results from two-code perspectives (see Theorems 1 and 2) but also facilitate researches of trellis complexity (see Theorem 6). Specifically,

– Theorem 1 implies that, considering equivalence, the generalized Singleton bounds on RDLP and IRDLP can be obtained by applying Forney's MDS bounds to linear code C^* generated by G^* of (25).
– Theorem 2 provides new bounds $UP(K)$ on RDLP and $LO(\widetilde{K})$ on IRDLP corresponding, respectively, to $LO(K)$ and $UP(\widetilde{K})$ of Proposition 1.
– Theorem 6 shows that the DLP and Wolf bounds are "duality" results from two-code perspectives. By using this theorem, the state complexity profile of a linear code and that of a subcode are bounded from each other.

In addition, a unified framework is proposed to derive bounds on RDLP and IRDLP from an upper bound on RLDP, see Algorithm 1 and Proposition 9. We introduce three new upper bounds on RLDP (Theorems 3, 4 and 5) and use the first two to tighten the generalized Singleton bounds by applying the framework, which provides better equivocation estimation than that of [12].

Acknowledgments The authors would like to thank Professor Tor Helleseth and the anonymous reviewers for their comments and suggestions that helped to improve this paper considerably. This work is supported in part by the National Key Basic Research and Development Plan (973 Plan) of China under Grant 2012CB316106, the National Natural Science Foundation of China under Grants 60972033 and 60832001, the open research fund of National Mobile Communications Research Laboratory of Southeast University under Grant 2010D04, the Research Fund for the Doctoral Program of Higher Education of China under Grant 20100073110016 and the Shanghai Jiao Tong University Innovation Fund For Postgraduates.

References

1. Encheva S., Kløve T.: Codes satisfying the chain condition. IEEE Trans. Inf. Theory **40**(1), 175–180 (1994).
2. Forney G.D.: Dimension/length profiles and trellis complexity of linear block codes. IEEE Trans. Inf. Theory **40**(6), 1741–1752 (1994).
3. Helleseth T., Kløve T., Mykkelveit J.: The weight distribution of irreducible cyclic codes with block length $n_1((q^l-1)/N)^n$. Discret. Math. **18**, 179–211 (1977).
4. Helleseth T., Kløve T., Ytrehus Ø.: Generalized Hamming weights of linear codes. IEEE Trans. Inf. Theory **38**(3), 1133–1140 (1992).
5. Helleseth T., Kløve T., Levenshtein V.I., Ytrehus Ø.: Bounds on the minimum support weights. IEEE Trans. Inf. Theory **41**(2), 432–440 (1995).
6. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University, Cambridge (2003).
7. Hughes D.R., Piper F.C.: Design Theory. Cambridge University, Cambridge (1998).
8. Kløve T.: Support weight distribution of linear codes. Discret. Math. **107**, 311–316 (1992).
9. Lafourcade A., Vardy A.: Lower bounds on trellis complexity of block codes. IEEE Trans. Inf. Theory **41**(6), 1938–1954 (1995).
10. Lin S., Kasami T., Fujiwara T., Fossorier M.: Trellises and Trellis-Based Decoding Algorithms for Linear Block Codes. Kluwer, Massachusetts (1998).
11. Liu Z., Chen W., Luo Y.: The relative generalized Hamming weight of linear q-ary codes and their subcodes. Des. Codes Cryptogr. **48**, 111–123 (2008).
12. Luo Y., Mitrpant C., Han Vinck A.J., Chen K.F.: Some new characters on the wire-tap channel of type II. IEEE Trans. Inf. Theory **51**(3), 1222–1229 (2005).
13. Luo Y., Han Vinck A.J., Chen Y.: On the optimum distance profiles about linear block codes. IEEE Trans. Inf. Theory **56**(3), 1007–1014 (2010).
14. Luo Y., Fu F., Mitrpant C., Han Vinck A.J.: Relative MDS pairs. Unpublished manuscript.
15. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1988).
16. Muder D.J.: Minimal trellises for block codes. IEEE Trans. Inf. Theory **34**(5), 1049–1053 (1988).
17. Ozarow L.H., Wyner A.D.: Wire-tap channel II. Bell Labs Tech. J. **63**(10), 2135–2157 (1984).
18. Reuven I., Be'ery Y.: Entropy/length profiles, bounds on the minimal covering of bipartite graphs, and trellis complexity of nonlinear codes. IEEE Trans. Inf. Theory **44**(2), 580–598 (1998).
19. Simonis J.: The effective length of subcodes. Appl. Algebr. Eng. Commun. **5**, 371–377 (1994).
20. Wang P., Luo Y., Han Vinck A.J.: Some upper bounds on the inverse relative dimension/length profile. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E91-A**(12), 3731–3737 (2008).
21. Wei V.K.: Generalized Hamming weights for linear codes. IEEE Trans. Inf. Theory **37**(5), 1412–1418 (1991).
22. Wolf J.K.: Efficient maximum likelihood decoding of linear block codes. IEEE Trans. Inf. Theory **IT-24**(1), 76–80 (1978).
23. Yang Y., Hu Z.: Structure analysis of linear constant weight codes. Acta Electron. Sin. **18**(6), 1–8 (1990).
24. Ytrehus Ø.: On the trellis complexity of certain binary linear block codes. IEEE Trans. Inf. Theory **41**(2), 559–560 (1995).

25. Zhang Z.: Wiretap networks II with partial information leakage. In: 4th International Conference on Communications and Networking in China, Xi'an, China, pp. 1–5 (2009).
26. Zhang Z., Zhuang B.: An application of the relative network generalized Hamming weight to erroneous wiretap networks. In: 2009 IEEE Information Theory Workshop, Taormina, Italy, pp. 70–74 (2009).
27. Zhuang Z., Luo Y., Han Vinck A.J.: Bounds on relative generalized Hamming weight. Unpublished manuscript.