New Dual Relationships for Error-Correcting Wiretap Codes

Morteza Shoushtari and Willie K. Harrison
Department of Electrical and Computer Engineering
Brigham Young University, Provo, UT, USA
Emails: {morteza.shoushtari,willie.harrison}@byu.edu

2021 IEEE Information Theory Workshop (ITW) | 978-1-6654-0312-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ITW48936.2021.9611443

***Abstract*—In this paper, we consider the equivocation of finite blocklength coset codes when used over binary erasure wiretap channels. We make use of the equivocation matrix in comparing codes that are suitable for scenarios with noisy channels for both the intended receiver and an eavesdropper. Equivocation matrices have been studied in the past only for the binary erasure wiretap channel model with a noiseless channel for the intended recipient. In that case, an exact relationship between the elements of equivocation matrices for a code and its dual code was identified. The majority of work on coset codes for wiretap channels only addresses the noise-free main channel case, and extensions to noisy main channels require multi-edge type codes. In this paper, we supply a more insightful proof for the noiseless main channel case, and identify a new dual relationship that applies when two-edge type coset codes are used for the noisy main channel case. The end result is that the elements of the equivocation matrix for a dual code are known precisely from the equivocation matrix of the original code according to fixed reordering patterns. Such relationships allow one to study the equivocation of codes and their duals in tandem, which simplifies the search for best and/or good finite blocklength codes. This paper is the first work that succinctly links the equivocation/error correction capabilities of dual codes for two-edge type coset coding over erasure-prone main channels.**

I. Introduction

Since the development of the wiretap channel model in the 1970's by Wyner [1], cosets of linear block codes have been known to provide a convenient structure for implementing physical-layer security coding. Many types of secrecy codes have been discovered for an array of wiretap channel variants, and most of them are built from structures similar to the coset coding approach [2]–[4]. Parameters of linear block codes, such as generalized Hamming weights [5], were shown to be capable of predicting a coset code's ability to achieve secure communication, particularly over the wiretap channel of type II [6], and rank properties of generators and parity-check matrices were later shown to quantify the security precisely over the original wiretap channel model with binary erasure channels [7]–[10].

Although many wiretap codes have been designed to achieve information theoretic security in the asymptotic blocklength regime (e.g., [2], [11]), there has been some recent interest in optimal coset coding structures with fixed code size parameters [12], [13]. Consider the wiretap channel model in Fig. 1.

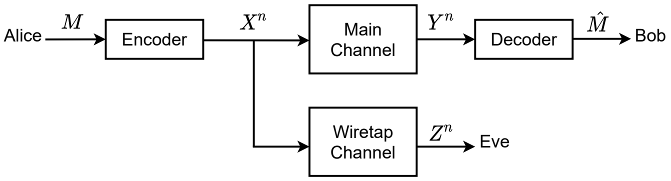

Fig. 1. Wiretap channel model.

Here we see a user named Alice trying to communicate a secret message M to a user named Bob in the presence of an eavesdropper named Eve. The message M is encoded to produce a length-n binary codeword X^n, which is received by Bob through the main channel as Y^n and decoded to form an estimate of the message $\hat{M}$. Eve also receives the transmission through the wiretap channel as Z^n. The goal of the encoder function is to satisfy the following two constraints:

- $\Pr(M \neq \hat{M}) < \delta_r$, (a reliability constraint for Bob),
- $\mathbb{I}(M; Z^n) = \mathbb{H}(M) - \mathbb{H}(M|Z^n) < \delta_s$, (a security constraint for Eve),

where δ_r and δ_s can be set to any desired level. The *equivocation*

$$E = \mathbb{H}(M|Z^n), \tag{1}$$

is considered the most fundamental information theoretic quantification of secrecy [1] (which is often presented in terms of the *leakage* $\mathbb{I}(M; Z^n)$ [14]). In order to identify the best finite blocklength codes for binary erasure wiretap channel models, the equivocation has been recently linked to properties of the code's generator matrix in [7], [9] for the noiseless main channel case, and in [8], [10] for the binary erasure main channel case.

In [13], the equivocation matrix was first used as a convenient tool with which to study finite blocklength wiretap codes based on coset coding, and additional properties of these matrices were later identified in [15]. The equivocation matrix outlines explicitly the exact equivocation for all possible revealed-bit patterns to a receiver when the code is fixed, and hence allows one to calculate the average equivocation in (1), or the worst-case equivocation given a fixed number of revealed bits to an eavesdropper, as for the wiretap channel of type II. Comparison of small wiretap codes is easily made with equivocation matrices, and this tool allows one to efficiently

This work was funded by the US National Science Foundation (Grant Award #1910812).

978-1-6654-0312-2/21/$31.00 ©2021 IEEE

search for properties of best codes of a fixed size when code properties can be linked to properties of entries in the matrix.

Some of the more interesting properties of these matrices to date are those that link the equivocation matrices of codes with those of their dual codes for the noiseless main channel variant of the binary erasure wiretap channel [13]. This paper augments that result with a simplified and more insightful proof, and then highlights a new dual relationship for two-edge type coset codes, suitable for error correction/secrecy coding over the wiretap channel model with binary erasure channels for both the main and wiretap channels. The results prove that the dual code equivocation matrix, and hence the dual code's equivocation, is fixed and known with reference only to the equivocation matrix of the original code.

The remainder of the paper is organized as follows. Section II provides details regarding the communication model, and sets up the definitions and notation for the paper. The dual relationships for the noiseless main channel and the noisy main channel cases are then stated with proof in Section III. Finally examples are given in Section IV and the paper is concluded in Section V.

II. Problem Setup

In this section, we first establish basic notation for the paper. Capital letters denote random variables (including random vectors) and matrices, calligraphic letters represent alphabets for their associated random variables, lower case letters denote realizations of random variables, and superscripts indicate the length of vectors. All vectors are row vectors, and all codes are binary. By $[\![1,\beta]\!]$, we mean the set of consecutive integers from 1 to β, where $\beta \geq 1$. The set $\mathcal{R}^n$ is comprised of all subsets of $[\![1,n]\!]$, and is used to represent all possible revealed-bit patterns over n transmitted bits. To be clear, $[\![1,n]\!]\backslash r$ will be used to indicate the indices of the erased bits over a binary erasure channel, while the set r contains the indices of those bits that are not erased (i.e., *revealed*). Note that the backslash in $[\![1,n]\!]\backslash r$ indicates the set difference operation, and is often read *delete*. We indicate erasures in received signals y^n and z^n with the symbol '?' when they occur. Finally, sets used as subscripts on matrices indicate submatrices that include only the columns indexed in the set, i.e., H_r is the submatrix of H comprised of only the columns with indices in the set r.

A. Channel Models

The channel models assumed in this paper are variants of the basic wiretap channel model of Fig. 1. The messages to be encoded by Alice are chosen uniformly from the alphabet $\mathcal{M} = \mathbb{F}_2^k$, the set of all possible binary vectors of length k. The encoder function is such that $\mathcal{X}^n \subset \mathbb{F}_2^n$. The wiretapper's channel is always a binary erasure channel (BEC) with erasure probability $\epsilon_w \in [0,1]$, so that $\mathcal{Z}^n = \{0,1,?\}^n$. The main channel is also a BEC with erasure probability $\epsilon_m \in [0,1]$ meaning $\mathcal{Y}^n = \mathcal{Z}^n$. When we deal with the *noiseless main channel case*, then $\epsilon_m = 0$ and $Y^n = X^n$. When we consider the *noisy main channel case*, then $\epsilon_m \in (0,1]$. All erasure channels erase bits independently.

B. General Coset Coding

We adopt a general framework for the encoding operation, where k message bits are always encoded into codewords of blocklength n making the coding rate $R = k/n$. The encoder can use the $n-k$ bits of coding overhead to aid in reliability or secrecy as desired. The number of overhead bits assigned to reliability is α, while the number of overhead bits assigned to secrecy is l, and

$$n = k + \alpha + l. \tag{2}$$

Notice that traditional error-control codes have $l = 0$, while binary coset codes for the noiseless main channel case set $\alpha = 0$. The more interesting set of codes that can both correct errors and keep secrets have both l and α greater than zero.

The basic structure for codes that can both correct errors and keep secrets was first outlined in [2], and later used in [16], [17] for secrecy codes based on two-edge type low-density parity-check (LDPC) codes. Matrix dimensions in these previous works were identified using the rates of codes and subcodes, mainly since the codes were analyzed asymptotically in the blocklength. Since we consider fixed (and even small) codes in this paper, we are free to adopt a more straightforward notation using k, α, and l as defined above. Let $\mathcal{C}$ be an (n,l) linear block code with $l \times n$ generator matrix G and $(n-l)\times n$ parity-check matrix H. Then define the $(n-\alpha)\times n$ matrix

$$G^* = \begin{bmatrix} G' \\ G \end{bmatrix}, \tag{3}$$

where G' is a $k \times n$ matrix comprised of rows from $\mathbb{F}_2^n$ such that G^* has full row rank. The parity-check matrix for $\mathcal{C}$ is comprised of two pieces so that

$$H = \begin{bmatrix} H^* \\ H'' \end{bmatrix}, \tag{4}$$

where H^* is $\alpha \times n$ and forms a basis for the dual space of the rowspace of G^*. The submatrix H'' has dimensions $k \times n$. Note that $GH^T = 0$ and $G^*(H^*)^T = 0$ as indicated by the definitions above. Alice's encoder function then calculates a codeword according to the expression

$$x^n = \begin{bmatrix} m & m' \end{bmatrix} G^* = \begin{bmatrix} m & m' \end{bmatrix} \begin{bmatrix} G' \\ G \end{bmatrix} \tag{5}$$

$$= mG' \oplus m'G, \tag{6}$$

where m' is an l-bit auxiliary message chosen uniformly from $\mathbb{F}_2^l$. Thus, mG' chooses the coset of $\mathcal{C}$, and $m'G$ chooses the specific codeword from that coset uniformly at random.

Such a code is often called a two-edge type code since a basic message-passing decoder using H is comprised of edges corresponding to both H^* and H''. This basic structure is portrayed in Fig. 2, where the edges in the Tanner graph correspond to parity-check equations from either H^* or H'' as labeled. Bob's decoder is then comprised of two steps. First, the decoder attempts to recover as many erased bits as possible, perhaps using message passing over the parity

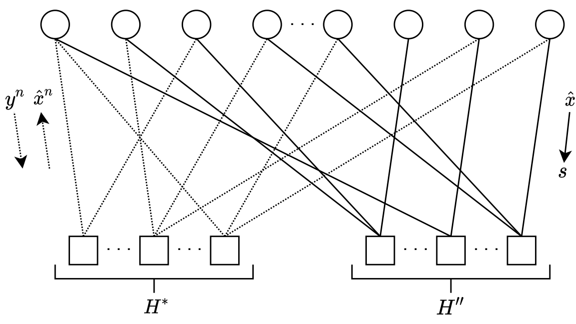

Fig. 2. Tanner graph for decoding two-edge type secrecy codes over a BEC. Circles and squares represent variable nodes and check nodes, respectively. The dotted lines correspond to error correction, and solid lines correspond to parity-check equations that form the mapping from codeword to syndrome.

checks defined by only H^* [18]. The output of this result is $\hat{X}^n$, an estimate of the transmitted codeword X^n. Assuming full recovery of the codeword, the decoder then calculates the syndrome

$$\begin{aligned} s &= x^n(H'')^T = mG'(H'')^T \oplus m'G(H'')^T \qquad (7)\\ &= mG'(H'')^T, \qquad (8)\end{aligned}$$

since H'' is part of H and $GH^T = 0$. Notice that $G'(H'')^T$ forms a bijective mapping between m and s. In [9], [10], it was shown that G' and H'' can be chosen so that $G'(H'')^T$ is the $k \times k$ identity, and therefore, $s = m$ for ease in decoding at Bob.

To better show how the two-edge type decoder works, consider the following, where x^n is any codeword. Let us calculate

$$\begin{aligned} x^n H^T &= \begin{bmatrix} m & m' \end{bmatrix} \begin{bmatrix} G' \\ G \end{bmatrix} \begin{bmatrix} (H^*)^T & (H'')^T \end{bmatrix}, \qquad (9)\\ &= \begin{bmatrix} mG'(H^*)^T & mG'(H'')^T \end{bmatrix} \oplus \\ &\quad \begin{bmatrix} m'G(H^*)^T & m'G(H'')^T \end{bmatrix}, \qquad (10)\\ &= \begin{bmatrix} 0^\alpha & mG'(H'')^T \end{bmatrix} = \begin{bmatrix} 0^\alpha & s \end{bmatrix}, \qquad (11)\end{aligned}$$

where 0^α is a $1 \times \alpha$ row vector of zeros. Notice now that x^n is a codeword if and only if $x^n(H^*)^T = 0^\alpha$ (i.e., H^* is for error correction), and H'' allows the bijective mapping back to the message (i.e., H'' allows one to identify the coset of the codeword).

C. Equivocation Matrices

In [10], it was shown that

$$\begin{aligned} \mathbb{H}(M|Z^n = z^n) &= \mathbb{H}(M) - \operatorname{rank} G^*_{r(z^n)} + \operatorname{rank} G_{r(z^n)} \\ &= k - \operatorname{rank} G^*_{r(z^n)} + \operatorname{rank} G_{r(z^n)}, \qquad (12)\end{aligned}$$

where $r(z^n) = \{i | z_i \neq ?\}$. Notice that the value of the revealed bits (either ones or zeros) in z^n is not important when calculating the exact equivocation at the eavesdropper since the expression is only a function of the *pattern* of revealed bits. This allows us to simplify the equivocation expression in (1) to

$$\begin{aligned} E = \mathbb{H}(M|Z^n) &= \sum_{r \in \mathcal{R}^n} p(r)\{\mathbb{H}(M|r)\} \\ &= \sum_{\mu=0}^{n} \underbrace{(1-\epsilon_w)^\mu \epsilon_w^{n-\mu}}_{p(r)} \sum_{r \in \mathcal{R}^n : |r| = \mu} \underbrace{k - \operatorname{rank} G^*_r + \operatorname{rank} G_r}_{\mathbb{H}(M|r)}. \qquad (13)\end{aligned}$$

This means that we only need to know the number of patterns of size μ that maintain e bits of equivocation for $\mu \in [\![0, n]\!]$ and $e \in [\![0, k]\!]$ to calculate (1).

An equivocation matrix [13], [15] is a $(k+1) \times (n+1)$ matrix A, where the (e, μ)th entry of the matrix $a_{e,\mu}$ is equal to the number of revealed-bit patterns of size μ that maintain e bits of equivocation for $\mu \in [\![0, n]\!]$ and $e \in [\![0, k]\!]$. We start indexing at $(0, 0)$ in the bottom left corner to maintain the structural similarities between the matrix and $\mathbb{H}(M|Z^n)$ as a function of μ.

III. Dual Relationships for Equivocation Matrices

The purpose of this paper is to identify links between equivocation matrices for codes and their dual codes, and thereby establish relationships between the equivocation (1) for the two codes. The definition of a dual code, however, is different for the $\alpha = 0$ case (for designing codes when the main channel is noiseless) and the $\alpha > 0$ case (for designing codes that allow Bob to correct erasures). For all cases considered in the paper, we assume $l > 0$, meaning we always dedicate at least one bit of overhead for causing confusion at the eavesdropper.

A. Noiseless Main Channel Case

For the noiseless main channel case, let us examine the code construction in Section II-B and point out some simplifications. For this case, $\alpha = 0$ since $Y^n = X^n$, and the entire overhead in the code can be assigned to secrecy, i.e., $l = n - k$. Thus, G^* is $n \times n$, H^* is empty, and the first step in the decoder (i.e., correcting errors) is not needed at Bob's receiver. Notice that (12) reduces to

$$\mathbb{H}(M|r) = k - |r| + \operatorname{rank} G_r, \qquad (14)$$

since G^* must have full column rank [10].

For this case, let $\mathcal{C}$ be an $(n, n-k)$ linear block code with parity check matrix H and generator matrix G. Also consider the (n, k) dual code of $\mathcal{C}$ and call it $\mathcal{C}^\perp$ with generator matrix H and parity-check matrix G. Let $a_{e,\mu}$ denote the number of revealed-bit patterns with μ revealed bits leading to an equivocation of e bits when coset coding with $\mathcal{C}$. Also let $a^\perp_{e,\mu}$ denote the number of revealed-bit patterns with μ revealed bits leading to an equivocation of e bits when coset coding with $\mathcal{C}^\perp$ (i.e., when G takes the role of H, H takes the role of G, and the $n \times n$ generator for the dual code is constructed by adding rows to H to form a full-rank $n \times n$ matrix). Notice that when the dual code is used, the coding rate is $(n-k)/n$. The entire coding overhead is used for secrecy in both cases, meaning k bits for the dual code and $(n-k)$ bits for the original code.

The following lemma is partially from [13] and establishes the dual relationship for this case. We improve the lemma here with an additional statement, and provide a cleaner, more insightful proof.

Lemma 1. *When coset coding with $\mathcal{C}$,*

$$\operatorname{rank} G_r = \operatorname{rank} H_{[\![1,n]\!]\setminus r} - k + |r| \tag{15}$$

for all $r \in \mathcal{R}^n$, and therefore, $a_{e,\mu} = a^{\perp}_{e+\mu-k,n-\mu}$.

Proof. Let us consider the equivocation with respect to H, and point out that

$$\hat{s} = z^n H^T = x^n_r (H_r)^T \oplus z^n_{[\![1,n]\!]\setminus r} (H_{[\![1,n]\!]\setminus r})^T, \tag{16}$$

since the revealed bits across a binary erasure channel are guaranteed to be without error. The vector $z^n_{[\![1,n]\!]\setminus r}$ is comprised of $n-|r|$ '?' symbols, and the number of unique solutions possible for $\hat{s}$ is $2^{\operatorname{rank} H_{[\![1,n]\!]\setminus r}}$. Thus,

$$\mathbb{H}(M|r) = \operatorname{rank} H_{[\![1,n]\!]\setminus r}. \tag{17}$$

Combining (17) with (14) establishes (15). It is now straightforward to apply (15) to the case when $\mathcal{C}^{\perp}$ is used for coset coding to show that for every $r \in \mathcal{R}^n$ that gives equivocation e with $|r| = \mu$ when coding with $\mathcal{C}$, there exists a unique pattern of size $n-\mu$, namely $[\![1,n]\!]\setminus r$, that gives equivocation $e+\mu-k$ when coding with $\mathcal{C}^{\perp}$. □

B. Binary Erasure Main Channel Case

When the main channel is assumed to be an erasure channel, we require the full construction outlined in Section II-B with no simplifications. Let $\mathcal{C}$ denote the (n,l) binary linear block code with generator G and parity-check matrix H as outlined above. We also require a specific choice of G' to fully define G^*, and a decomposition of H into H^* and H''.

In this case, it becomes trickier to define a dual code since the performance of the code relies on the choice of G' as well as G. We require H^* to be orthogonal to both G and G', but H'' only to be orthogonal to G. In this case, we can find a valid construction if we define the *dual* code to be the code formed by letting G and H^* interchange roles, and G' and H'' interchange roles. The original code has a coding rate of k/n, with α bits of overhead assigned to error control and l bits of overhead assigned to securing the message. The dual code with this construction also has a coding rate of k/n, but with l bits of overhead assigned to error control and α bits of overhead assigned to security.

Once again, let $a_{e,\mu}$ denote the number of revealed-bit patterns with μ revealed bits leading to an equivocation of e bits when coset coding with the original code, and let $a^{\perp}_{e,\mu}$ denote the number of revealed-bit patterns with μ revealed bits leading to an equivocation of e bits when coset coding with the dual code. In this case, a new dual relationship exists as outlined in the following lemma.

Lemma 2. *When coset coding with the original code construction, then*

$$k - \operatorname{rank} G^*_r + \operatorname{rank} G_r = \operatorname{rank} H_{[\![1,n]\!]\setminus r} - \operatorname{rank} H^*_{[\![1,n]\!]\setminus r} \tag{18}$$

for all $r \in \mathcal{R}^n$, and therefore, $a_{e,\mu} = a^{\perp}_{k-e,n-\mu}$.

Proof. Once again, let us consider the equivocation with respect to H, and point out that

$$\begin{aligned} z^n H^T &= x^n_r (H_r)^T \oplus z^n_{[\![1,n]\!]\setminus r} (H_{[\![1,n]\!]\setminus r})^T, && (19)\\ &= x^n_r \left[(H^*_r)^T \quad (H''_r)^T \right] \\ &\quad \oplus z^n_{[\![1,n]\!]\setminus r} \left[(H^*_{[\![1,n]\!]\setminus r})^T \quad (H''_{[\![1,n]\!]\setminus r})^T \right] && (20)\\ &= \left[0^{\alpha} \quad \hat{s} \right], && (21) \end{aligned}$$

where $\hat{s}$ is an estimate of the syndrome. Let

$$a = x^n_r (H^*_r)^T \tag{22}$$

$$b = x^n_r (H''_r)^T. \tag{23}$$

Then,

$$z^n_{[\![1,n]\!]\setminus r} \left[(H^*_{[\![1,n]\!]\setminus r})^T \quad (H''_{[\![1,n]\!]\setminus r})^T \right] = \left[-a \quad \hat{s} - b \right], \tag{24}$$

for fixed a and b. The vector $z^n_{[\![1,n]\!]\setminus r}$ is comprised of $n-|r|$ '?' symbols, and the number of unique solutions possible for $\hat{s}$ is $2^{\operatorname{rank} H_{[\![1,n]\!]\setminus r} - \operatorname{rank} H^*_{[\![1,n]\!]\setminus r}}$, since the total number of solutions without the error-control constraints would be $2^{\operatorname{rank} H_{[\![1,n]\!]\setminus r}}$, but the error-control constraints reduce the exponent by $\operatorname{rank} H^*_{[\![1,n]\!]\setminus r}$. Thus,

$$\mathbb{H}(M|r) = \operatorname{rank} H_{[\![1,n]\!]\setminus r} - \operatorname{rank} H^*_{[\![1,n]\!]\setminus r}. \tag{25}$$

Combining (25) and (12) establishes (18). It is now straightforward to apply (18) to the case when the dual code is used for coset coding to show that for every $r \in \mathcal{R}^n$ that gives equivocation e with $|r| = \mu$ when coding with the original code, there exists a unique pattern of size $n-\mu$, namely $[\![1,n]\!]\setminus r$, that gives equivocation $k-e$ when coding with the dual code. □

IV. Examples and Discussion

The lemmas can be better understood with reference to a set of examples. In particular, examples make the structural relationships of the equivocation matrices between codes and their duals more clear.

A. Example for Noiseless Main Channel Case

Let us consider coset coding for the noiseless main channel case with $n=7$, $k=3$, and $l=4$. We set

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \tag{26}$$

with

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{27}$$

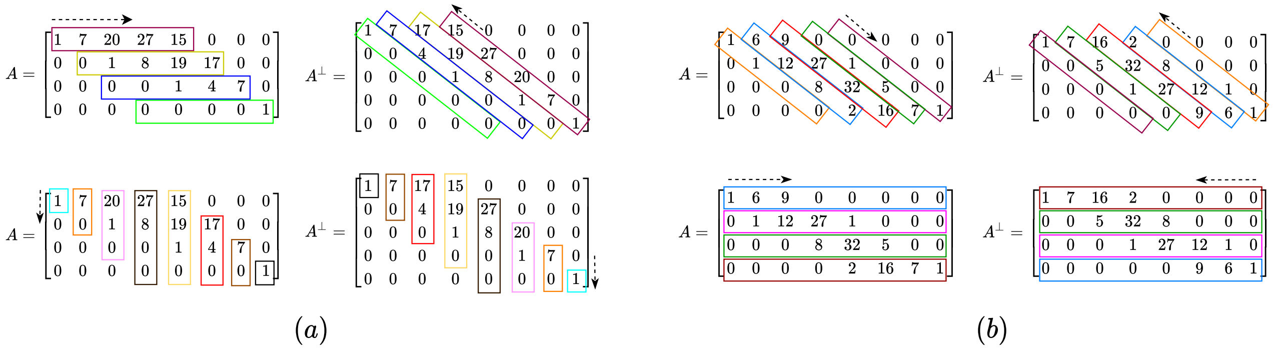

Fig. 3. (a) Equivocation matrices for a code and its dual for the noiseless main channel case with dual relation specified in Lemma 1 outlined. (b) Equivocation matrices for a code and its dual for the binary erasure main channel case with dual relation specified in Lemma 2 outlined.

Here G' can be any 3×7 binary matrix such that G^* is full rank. The equivocation matrix for this code is given as A in Fig. 3(a). When considering the dual code, G and H interchange roles, and the full rank generator is formed by adding any 4×7 binary matrix to H such that the collection of rows makes a full-rank generator. The dual case has $n = 7$, $k = 4$, and $l = 3$, and the equivocation matrix for the dual case is given as $A^\perp$ in Fig. 3(a). The dual relation specified in Lemma 1 is clearly highlighted in the figure in two ways.

B. Example for Erasure Main Channel Case

For the binary erasure main channel case, consider

$$G^* = \left[\begin{array}{c} G' \\ \hdashline G \end{array}\right] = \left[\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hdashline 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{array}\right], \tag{28}$$

and

$$H = \left[\begin{array}{c} H^* \\ \hdashline H'' \end{array}\right] = \left[\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hdashline 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right], \tag{29}$$

to define the original code. This code has $n = 7$, $k = 3$, $l = 2$, and $\alpha = 2$. Recall that we form the dual code by letting G and H^* interchange roles, and G' and H'' interchange roles. In this case, all interchanging matrices have the same size, so the dual case also has $n = 7$, $k = 3$, $l = 2$, and $\alpha = 2$. The equivocation matrices for both the original code and the dual code are given in Fig. 3(b), and the dual relation from Lemma 2 is highlighted in the figure in two different ways.

C. Discussion

Note that the lemmas in this paper allow one to simplify the search for good or even best codes. For example, if one finds a code that optimizes the structure of each column of the equivocation matrix A, then the optimal structure of $A^\perp$ is guaranteed by Lemma 1. The result of Lemma 2 is a bit more subtle. Here, the dual code is a code that exchanges the number of error correcting bits and number of secrecy bits. Thus, if $\mathcal{C}$ is good for secrecy, then $\mathcal{C}^\perp$ is good for reliability. The relationships between A and $A^\perp$ allow one to infer these tradeoffs precisely after analyzing only one of the two codes.

V. Conclusion

In this paper, we presented relationships between equivocation matrices of finite block length wiretap codes and their duals for two cases: the binary erasure wiretap channel with a noiseless main channel, and the binary erasure wiretap channel with a binary erasure main channel. The result indicates that knowledge of the equivocation matrix for one code gives exact knowledge of the equivocation matrix for the other code. The dual relations allow one to study codes and their duals simultaneously using the equivocation matrix approach. This is particularly useful in the search for best and/or good finite blocklength codes, since the discovery of a best code for fixed size parameters implies that the dual code is also best for its size parameters for the noiseless main channel case, and a specific link between secrecy and error correction is made between the two-edge type codes used when the main channel is prone to erasures. This marks the first work on dual relations for multi-edge type wiretap codes.

References

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

[2] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[3] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sept. 2013.

[4] M. R. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[5] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.

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

[7] V. Rajaraman and A. Thangaraj, "Eg-ldpc codes for the erasure wiretap channel," in *Proc. IEEE National Conference On Communications (NCC)*, Chennai, IN, 2010, pp. 1–5.

[8] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, 2011.

[9] J. Pfister, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *Proc. IEEE Int. Conf. Communications (ICC)*, May 2017, pp. 1–6.

[10] W. K. Harrison, "Exact equivocation expressions for wiretap coding over erasure channel models," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2687–2691, 2020.

[11] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[12] S. Al-Hassan, M. Z. Ahmed, and M. Tomlinson, "Secrecy coding for the wiretap channel using best known linear codes," in *Proc. Global Information Infrastructure Symp. (GIIS)*, 2013, pp. 1–6.

[13] W. K. Harrison and M. R. Bloch, "On dual relationships of secrecy codes," in *Proc. Allerton Conf. Communication, Control, Computing*, Oct. 2018, pp. 366–372.

[14] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[15] W. K. Harrison and M. R. Bloch, "Attributes of generators for best finite blocklength coset wiretap codes over erasure channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, July 2019, pp. 827–831.

[16] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *Proc. Asilomar Conference Signals, Systems, Computers (SS&C)*, 2009, pp. 834–838.

[17] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, St. Petersburg, RU, 2011, pp. 2393–2397.

[18] T. Richardson and R. Urbanke, *Modern Coding Theory*. New York, NY: Cambridge University Press, 2008.