Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 102069, 13 pages
http://dx.doi.org/10.1155/2013/102069

Research Article

Capacity-Equivocation Regions of the DMBCs with Noiseless Feedback

Xinxing Yin,[1] Zhi Xue,[1] and Bin Dai[2]

[1] *Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[2] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*

Correspondence should be addressed to Xinxing Yin; yinxinxing@sjtu.edu.cn

Received 30 January 2013; Accepted 15 July 2013

Academic Editor: Weihai Zhang

The discrete memoryless broadcast channels (DMBCs) with noiseless feedback are studied. The entire capacity-equivocation regions of two models of the DMBCs with noiseless feedback are obtained. One is the degraded DMBCs with rate-limited feedback; the other is the *less* and *reversely less noisy* DMBCs with causal feedback. In both models, two kinds of messages are transmitted. The common message is to be decoded by both the legitimate receiver and the eavesdropper, while the confidential message is only for the legitimate receiver. Our results generalize the secrecy capacity of the degraded wiretap channel with rate-limited feedback (Ardestanizadeh et al., 2009) and the restricted wiretap channel with noiseless feedback (Dai et al., 2012). Furthermore, we use a simpler and more intuitive deduction to get the single-letter characterization of the capacity-equivocation region, instead of relying on the recursive argument which is complex and not intuitive.

1. Introduction

Secure data transmission is an important requirement in wireless communication. Wyner first studied the degraded (the wiretap channel is said to be (physically) degraded if $X \rightarrow Y \rightarrow Z$ form a Markov chain, where X is the channel input and Y and Z are the channel outputs of the legitimate receiver and wiretapper, resp.) wiretap channel in [1], where the output Z^N of the channel to the wiretapper is degraded to the output Y^N of the channel to the legitimate receiver. In Wyner's model, the transmitter aimed to send a confidential message S to the legitimate receiver and keep the wiretapper as ignorant of the message as possible. Wyner obtained the secrecy capacity (the secrecy capacity is the best data transmission rate under perfect secrecy; i.e., the equivocation at the wiretapper $H(S \mid Z^N) = 0$. The formal definition of the secrecy capacity is given in Remark 3) and demonstrated that provable secure communication could be implemented by using information theoretic methods. This model was extended to a more general case by Csiszár and Körner [2], where broadcast channel with confidential messages was studied; see Figure 1. They considered transmitting not only the confidential messages S to the legitimate receiver, but also the common messages W to both the legitimate receiver and the eavesdropper. The capacity-equivocation region for the extended model was determined in [2]. This region contains all the achievable rate triples (R_0, R_1, R_e), where R_0 and R_1 are the rates of the common and confidential messages and R_e is the rate of the confidential message's equivocation. Nevertheless, neither Wyner's model nor Csiszár's model considered feedback.

To explore more ways in achieving secure data transmission, [3–5] studied the effects of the feedback on the capacities of several channel models. They all showed that feedback could help enhance the secrecy in wireless transmission. In [3], Ahlswede and Cai presented both the inner and outer bounds on the secrecy capacity of the wiretap channel with secure causal feedback from the decoder and showed that the outer bound was tight for the degraded case. It was proved that, by using feedback, the secrecy capacity of the (degraded) wiretap channel was increased. After Ahlswede's exploration, Ardestanizadeh et al. studied the wiretap channel with secure rate-limited feedback [4]. The main difference between Ardestanizadeh's model and Ahlswede's model is that the feedback in [4] is independent of the channel outputs, while the feedback in [3] is originated causally from the

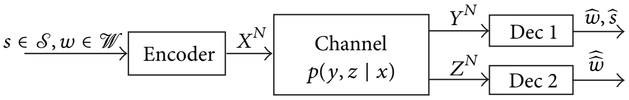


Figure 1: Broadcast channel with confidential messages.

outputs of the channel to the legitimate receiver. In [4], the authors got an outer bound on the wiretap channel with rate-limited feedback through a recursive argument which was effective but not intuitive. They also showed the outer bound was tight for the degraded case. In addition, Dai et al. investigated the secrecy capacity of the restricted wiretap channel with noiseless causal feedback under the assumption that the main channel is independent of the wiretap channel [5].

However, all of these explorations [3–5] focused on sending only the confidential messages. They did not consider sending both the common and confidential messages. In fact, transmitting the two kinds of messages can be seen in many systems with feedback. For example, in the satellite television service, some channels are available to all users for free, but some other channels are only for those who have paid for them. Recently, [6] studied the problem of transmitting both the common and confidential messages in the degraded broadcast channels with feedback. Note that, like [3], the feedback in [6] was originated causally from the legitimate receiver's channel outputs and not rate-limited. Besides, [7–9] studied the broadcast channel with feedback where no secure constraints were imposed.

To further investigate the secure data transmission with both common and confidential messages and noiseless feedback, this paper determines the capacity-equivocation regions of the following two DMBCs with both common and confidential messages. They are unsolved in the previous exploration.

(i) Degraded DMBCs with rate-limited feedback, where the feedback rate is limited by R_f and the feedback is independent of the channel outputs; see Figure 2.

(ii) *Less* and *reversely less noisy* (let X be the input of the DMBC, Y the legitimate receiver's channel output, and Z the eavesdropper's channel output. A DMBC $p(y, z \mid x)$ is said to be *less noisy* if $I(U; Y) \ge I(U; Z)$ for all $p(u, x)$; a DMBC $p(y, z \mid x)$ is said to be *reversely less noisy* if $I(U; Y) \le I(U; Z)$ for all $p(u, x)$, where u is the value of the auxiliary random variable U) DMBCs with noiseless causal feedback, where the feedback is originated causally from the legitimate receiver's channel outputs; see Figure 3.

The two channel models are characterized in Section 2. The main results presented in Section 2 subsume some important previous findings about the secure data transmission with feedback. (1) By setting the auxiliary random variable U to be constant in the secrecy capacity of the first model (see (9) in Remark 3), the secrecy capacity of the degraded wiretap with rate-limited feedback [4] is obtained. (2) By eliminating the common message in the second model, the capacity-equivocation region of restricted wiretap channel with noiseless feedback [5] is obtained. (3) We utilize a simpler and more intuitive deduction to get the single-letter characterization of the capacity-equivocation region, instead of relying on the recursive argument (see [4]) which is complex and not intuitive. (4) We find that even if the eavesdropper is in a better position than the legitimate receiver, provable secure communication could also be implemented in the DMBCs with both common and confidential messages.

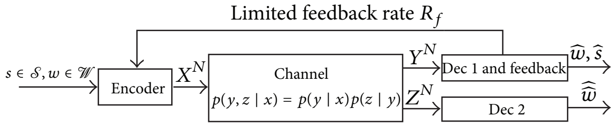

Limited feedback rate R_f
$s \in \mathcal{S}, w \in \mathcal{W}$
Encoder
X^N
Channel
$p(y, z \mid x) = p(y \mid x)p(z \mid y)$
Y^N
Z^N
Dec 1 and feedback
Dec 2
$\widehat{w}, \widehat{s}$
$\widehat{\widehat{w}}$

Figure 2: Degraded DMBCs with rate-limited feedback.

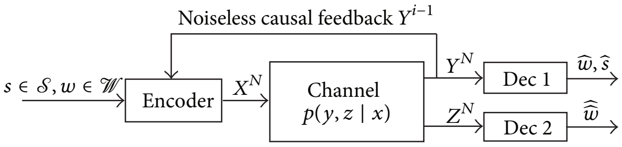

Noiseless causal feedback Y^{i-1}
$s \in \mathcal{S}, w \in \mathcal{W}$
Encoder
X^N
Channel
$p(y, z \mid x)$
Y^N
Z^N
Dec 1
Dec 2
$\widehat{w}, \widehat{s}$
$\widehat{\widehat{w}}$

Figure 3: Less and reversely less noisy DMBCs with noiseless causal feedback.

The remainder of the paper is organized as follows. Section 2 gives the notations and main results, that is, the capacity-equivocation regions of the two channel models. Section 3 proves Theorem 2. Section 4 proves Theorems 4 and 5. Section 5 concludes the whole work.

2. Channel Models and Main Results

2.1. Notations. Throughout this paper, we use calligraphic letters, for example, $\mathcal{X}$, $\mathcal{Y}$, to denote the finite sets and $\|\mathcal{X}\|$ to denote the cardinality of the set $\mathcal{X}$. Uppercase letters, for example, X, Y, are used to denote random variables taking values from finite sets, for example, $\mathcal{X}$, $\mathcal{Y}$. The value of the random variable X is denoted by the lowercase letter x. We use Z_i^j to denote the $(j - i + 1)$-vectors $(Z_i, Z_{i+1}, \ldots, Z_j)$ of random variables for $1 \le i \le j$ and will always drop the subscript when $i = 1$. Moreover, we use $X \sim p(x)$ to denote the probability mass function of the random variable X. For $X \sim p(x)$ and $0 \le \epsilon \le 1$, the set of the typical N-sequences x^N is defined as $\mathcal{T}_X^N(\epsilon) = \{x^N : |\pi(x \mid x^N) - p(x)| \le \epsilon p(x)$ for all $x \in \mathcal{X}\}$, where $\pi(x \mid x^N)$ denotes the frequency of occurrences of letter x in the sequence x^N (for more details about typical sequences, please refer to [10, Chapter 2]). The set of the conditional typical sequences, for example, $\mathcal{T}_{Y|X}^N(\epsilon)$, follows similarly.

2.2. Channel Models and Main Results. This paper studies the secure data transmission for two subclasses of DMBCs with noiseless feedback. One is the case where the feedback is rate-limited and independent of the channel outputs (see

Figure 2); the other is the case where the feedback is originated causally from the channel outputs (see Figure 3). Both models consist of a transmitter and two receivers, named receiver 1 (legitimate receiver) and receiver 2 (eavesdropper). The transmitter aims to convey a common message W to both receivers in addition to a confidential message S intended only for receiver 1. The confidential message S should be kept secret from receiver 2 as much as possible. We use equivocation at receiver 2 to characterize the secrecy of the confidential message. W and S are mutually independent and uniformly distributed over $\mathscr{W}$ and $\mathscr{S}$.

2.2.1. Degraded DMBCs with Rate-Limited Feedback. The degraded DMBCs with rate-limited feedback (see Figure 2) are under the condition that the channel to receiver 2 is physically degraded from the channel to receiver 1; that is, $p(y,z \mid x) = p(y \mid x)p(z \mid y)$ or $X \rightarrow Y \rightarrow Z$ form a Markov chain, where X is the channel input and Y, Z are observations of receiver 1 and 2. In this model, the encoder encodes the messages (W, S) and feedback into codewords X^N, where N is the length of the codeword. They are transmitted over a discrete memoryless channel (DMC) with transition probability $\prod_{i=1}^{N} p(y_i, z_i \mid x_i)$. Receiver 1 obtains Y^N and decodes the common and confidential messages $(\widehat{W}, \widehat{S})$. Receiver 2 obtains Z^N and decodes the common message $\widehat{W}$. More precisely, we define the encoder-decoder $(N, \Delta, P_{e1}, P_{e2})$ in Definition 1.

Definition 1. The encoder-decoder $(N, \Delta, P_{e1}, P_{e2})$ for the degraded DMBCs with rate-limited feedback (with rate limited by R_f) is defined as follows.

(i) The feedback alphabet $\mathscr{K}$ satisfies $\lim_{N\to\infty}(\log\|\mathscr{K}\|/N) \leq R_f$. The feedback is generated independent of the channel output symbols.

(ii) The stochastic channel encoder φ is specified by a matrix of conditional probability distributions $\varphi(x^N \mid s, w, k)$ which denotes the probability that the message s, w and the feedback k are encoded as the channel input x^N, where $x^N \in \mathscr{X}^N, s \in \mathscr{S}, w \in \mathscr{W}, k \in \mathscr{K}$, and $\sum_{x^N} \varphi(x^N \mid s, w, k) = 1$. Note that $\mathscr{S}$ and $\mathscr{W}$ are the confidential and common message sets.

(iii) Decoder 1 is a mapping $h_1 : \mathscr{Y}^N \rightarrow \mathscr{S} \times \mathscr{W}$. The input of decoder 1 is Y^N, and the output is $\widehat{S}, \widehat{W}$. The decoding error probability of receiver 1 is defined as $P_{e1} = \Pr\{h_1(Y^N) \neq (S, W)\}$. Similarly, Decoder 2 is defined as a mapping $h_2 : \mathscr{Z}^N \rightarrow \mathscr{W}$. The input of decoder 2 is Z^N, and the output is $\widehat{\widehat{W}}$. The decoding error probability of receiver 2 is defined as $P_{e2} = \Pr\{h_2(Z^N) \neq W\}$.

(iv) The equivocation at receiver 2 is defined as

$$\Delta = \frac{1}{N} H\left(S \mid Z^N\right). \tag{1}$$

A rate triple (R_0, R_1, R_e) is said to be *achievable* for the model in Figure 2 if there exists a channel encoder-decoder $(N, \Delta, P_{e1}, P_{e2})$ defined in Definition 1, such that

$$\lim_{N\to\infty} \frac{\log\|\mathscr{W}\|}{N} = R_0, \tag{2}$$

$$\lim_{N\to\infty} \frac{\log\|\mathscr{S}\|}{N} = R_1, \tag{3}$$

$$\lim_{N\to\infty} \frac{\log\|\mathscr{K}\|}{N} = R'_f \leq R_f, \tag{4}$$

$$\lim_{N\to\infty} \Delta \geq R_e, \tag{5}$$

$$P_{e1} \leq \epsilon, \qquad P_{e2} \leq \epsilon, \tag{6}$$

where ϵ is an arbitrary small positive real number, R_0, R_1, R'_f are the rates of the common messages, confidential messages, and feedback, and R_e is the equivocation rate of the confidential messages. Note that the feedback rate is limited by R_f. The capacity-equivocation region is defined as the convex closure of all achievable rate triples (R_0, R_1, R_e). The capacity-equivocation region of the degraded DMBCs with rate-limited feedback is shown in the following theorem.

Theorem 2. *For the degraded DMBCs with limited feedback rate R_f, the capacity-equivocation region is the set*

$$\begin{aligned} \mathscr{R}_d = \Big\{ &(R_0, R_1, R_e) : 0 \leq R_e \leq R_1, \\ &R_0 \leq I(U; Z), \\ &R_1 \leq I(X; Y \mid U), \\ &R_e \leq I(X; Y \mid U) - I(X; Z \mid U) + R_f \Big\}, \end{aligned} \tag{7}$$

where U is an auxiliary random variable and $U \rightarrow X \rightarrow Y \rightarrow Z$ form a Markov chain.

The proof of Theorem 2 is given in Section 3. The remark of Theorem 2 is shown below.

Remark 3. (i) The secrecy capacity of the model in Figure 2 is defined as the maximum rate at which confidential messages can be sent to receiver 1 in perfect secrecy; that is,

$$C_s = \max_{(R_0=0, R_1, R_e=R_1)\in\mathscr{R}} R_1, \tag{8}$$

where $\mathscr{R}$ is the capacity-equivocation region. Therefore, by the definition in (8), the secrecy capacity of the degraded DMBCs with limited feedback rate R_f is

$$\begin{aligned} &C_{sd} \\ &= \max \min \left\{ I(X; Y \mid U), I(X; Y \mid U) - I(X; Z \mid U) + R_f \right\}. \end{aligned} \tag{9}$$

This result subsumes the secrecy capacity of the degraded wiretap channel with rate-limited feedback (see [4]) by setting the auxiliary random variable U to be constant in (9).

(ii) The capacity-equivocation region in (7) is bigger than that in [2] without feedback. This implies that feedback can be used to enhance the secrecy in the DMBCs. Note that this finding had already been verified in [3–6].

2.2.2. Less and Reversely Less Noisy DMBCs with Noiseless Causal Feedback. The model in Figure 3 is based on the assumption that the channel to receiver 1 is independent of the channel to receiver 2; that is, $p(y, z \mid x) = p(y \mid x)p(z \mid x)$. The definition of the encoder-decoder for this model is similar to Definition 1 except for the feedback and the encoder. Different from the model in Figure 2, the feedback in Figure 3 is originated causally from the channel outputs of receiver 1 to the transmitter. The stochastic encoder for this model at time i, $1 \leq i \leq N$, is defined as $f_i(x_i \mid w_i, s_i, y^{i-1})$, where $w_i \in \mathscr{W}$, $s_i \in \mathscr{S}$, $y^{i-1} \in \mathscr{Y}^{i-1}$ (the channel outputs of receiver 1 before time i) and $\sum_{x_i \in \mathscr{X}} f_i(x_i \mid w_i, s_i, y^{i-1}) = 1$.

A rate triple (R_0, R_1, R_e) is said to be *achievable* for the model in Figure 3 if there exists a channel encoder-decoder $(N, \Delta, P_{e1}, P_{e2})$ such that (2), (3), (5), and (6) hold. Note that the definition of "*achievable*" here does not include (4) since the feedback in the model of Figure 3 is not rate limited. The definition of secrecy capacity is the same as that in Remark 3. Then, we present the capacity-equivocation regions of the *less* and *reversely less noisy* DMBCs with noiseless causal feedback in Theorems 4 and 5, respectively.

Theorem 4. *For the less noisy DMBCs with noiseless causal feedback, the capacity-equivocation region is the set*

$$\begin{aligned} \mathscr{R}_l = \{ & (R_0, R_1, R_e) : 0 \leq R_e \leq R_1, \\ & R_0 \leq I(U; Z), \\ & R_1 \leq I(X; Y \mid U), \\ & R_e \leq H(Y \mid Z)\}, \end{aligned} \tag{10}$$

where $U \rightarrow X \rightarrow (Y, Z)$ *form a Markov chain.*

Theorem 5. *For the reversely less noisy DMBCs with noiseless causal feedback, the capacity-equivocation region is the set*

$$\begin{aligned} \mathscr{R}_{rl} = \{ & (R_0, R_1, R_e) : 0 \leq R_e \leq R_1, \\ & R_0 \leq I(U; Y), \\ & R_1 \leq I(X; Y \mid U), \\ & R_e \leq H(Y \mid X)\}, \end{aligned} \tag{11}$$

where $U \rightarrow X \rightarrow (Y, Z)$ *form a Markov chain.*

The proof of Theorems 4 and 5 is given in Section 4. The remark of Theorems 4 and 5 is given below.

Remark 6. (i) By the definition in (8), the secrecy capacity of the *less noisy* DMBCs with noiseless causal feedback is

$$C_{sl} = \max \min \{I(X; Y \mid U), H(Y \mid Z)\}. \tag{12}$$

The secrecy capacity of the *reversely less noisy* DMBCs with noiseless causal feedback is

$$C_{srl} = \max \min \{I(X; Y \mid U), H(Y \mid X)\}. \tag{13}$$

Setting the auxiliary random variable U to be constant in (12) and (13), the capacity-equivocation region of the model in [5] is obtained.

(ii) In the model of Figure 3, it is assumed that the channel to receiver 1 is independent of the channel to receiver 2; that is, $p(y, z \mid x) = p(y \mid x)p(z \mid x)$. This implies $Y \rightarrow X \rightarrow Z$. Therefore, it is easy to see $H(Y \mid X) = H(Y \mid XZ) \leq H(Y \mid Z)$; that is, the upper bound on the equivocation rate R_e in (11) for the reversely less noisy case is smaller than that in (10) for the less noisy case. This tells that when the eavesdropper is in a better position than the legitimate receiver (see the *reversely less noisy* case), the uncertainty about the confidential messages at the eavesdropper is decreased. Besides, from (13), we see that even if the eavesdropper is in a better position, the secrecy capacity is a positive value, which means provable secure communication could also be implemented in such a bad condition.

3. Proof of Theorem 2

In this section, Theorem 2 is proved. The converse part of Theorem 2 gives the outer bound on the capacity-equivocation region of the degraded DMBCs with rate-limited feedback. The proof of the converse part is shown in Section 3.1. The key tools used in the proof include the identification of the random variables and Csiszár's sum equality [2]. In Section 3.2, to prove the direct part of Theorem 2, a coding scheme is provided to achieve the achievable rate triples in $\mathscr{R}_d$. The key ideas in the coding scheme are inspired by [4]. However, [4] only considers the transmission of the confidential messages. Our coding scheme considers both the confidential and common messages.

3.1. The Converse Part of Theorem 2. In order to find the identification of the auxiliary random variables that satisfy the capacity-equivocation region characterized by $\mathscr{R}_d$, we prove the converse part for the equivalent region (the fact that the two regions are equivalent follows similarly from [10, Chapter 5, problem 5.8]) containing all the rate triples (R_0, R_1, R_e) such that

$$0 \leq R_e \leq R_1, \tag{14}$$

$$R_0 \leq I(U; Z), \tag{15}$$

$$R_0 + R_1 \leq I(X; Y \mid U) + I(U; Z), \tag{16}$$

$$R_e \leq I(X; Y \mid U) - I(X; Z \mid U) + R_f. \tag{17}$$

Now we show that all *achievable* triples (R_0, R_1, R_e) satisfy (14), (15), (16), and (17).

Condition (14) is proved as follows:

$$\begin{aligned} R_e &\le \lim_{N\to\infty}\Delta \\ &= \lim_{N\to\infty}\frac{H\left(S\mid Z^N\right)}{N} \\ &\le \lim_{N\to\infty}\frac{H(S)}{N} \\ &= R_1. \end{aligned} \tag{18}$$

To prove condition (15), we calculate

$$\begin{aligned} H(W) &= I\left(W;Z^N\right)+H\left(W\mid Z^N\right) \\ &\overset{(a3.1)}{\le} I\left(W;Z^N\right)+\epsilon_1 \\ &= \sum_{i=1}^{N} I\left(W;Z_i\mid Z^{i-1}\right)+\epsilon_1 \\ &= \sum_{i=1}^{N} I\left(W;Z_i\mid Z_{i+1}^N\right)+\epsilon_1 \\ &= \sum_{i=1}^{N}\left[I\left(WY^{i-1};Z_i\mid Z_{i+1}^N\right)-I\left(Y^{i-1};Z_i\mid Z_{i+1}^N W\right)\right]+\epsilon_1 \\ &\le \sum_{i=1}^{N}\left[I\left(WY^{i-1}Z_{i+1}^N;Z_i\right)-I\left(Y^{i-1};Z_i\mid Z_{i+1}^N W\right)\right]+\epsilon_1 \\ &\le \sum_{i=1}^{N} I\left(WK^N Y^{i-1}Z_{i+1}^N;Z_i\right)+\epsilon_1, \end{aligned} \tag{19}$$

where $(a3.1)$ follows from Fano's inequality and ϵ_1 is a small positive number. Note that $K^N = (K_1, K_2, \ldots, K_N)$, where K_i is the feedback symbol at time i, $1 \le i \le N$.

To prove condition (16), we consider

$$\begin{aligned} H(S)+H(W) &= H\left(S\mid WK^N\right)+H(W) \\ &= I\left(S;Y^N\mid WK^N\right)+H\left(S\mid Y^N WK^N\right) \\ &\quad + I\left(W;Z^N\right)+H\left(W\mid Z^N\right) \\ &\overset{(a3.2)}{\le} I\left(S;Y^N\mid WK^N\right)+\epsilon_2 \\ &\quad + I\left(WK^N;Z^N\right)+\epsilon_1 \\ &= \sum_{i=1}^{N} I\left(S;Y_i\mid Y^{i-1}WK^N\right) \\ &\quad + \sum_{i=1}^{N} I\left(WK^N;Z_i\mid Z_{i+1}^N\right)+\epsilon_1+\epsilon_2 \\ &= \sum_{i=1}^{N}\left[I\left(SZ_{i+1}^N;Y_i\mid Y^{i-1}WK^N\right)\right. \\ &\qquad \left.-I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N S\right)\right] \\ &\quad + \sum_{i=1}^{N}\left[I\left(WK^N Y^{i-1};Z_i\mid Z_{i+1}^N\right)\right. \\ &\qquad \left.-I\left(Y^{i-1};Z_i\mid Z_{i+1}^N WK^N\right)\right]+\epsilon_1+\epsilon_2 \\ &= \sum_{i=1}^{N}\left[I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N\right)\right. \\ &\qquad + I\left(S;Y_i\mid Z_{i+1}^N Y^{i-1}WK^N\right) \\ &\qquad \left.-I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N S\right)\right] \\ &\quad + \sum_{i=1}^{N}\left[I\left(WK^N Y^{i-1};Z_i\mid Z_{i+1}^N\right)\right. \\ &\qquad \left.-I\left(Y^{i-1};Z_i\mid Z_{i+1}^N WK^N\right)\right]+\epsilon_1+\epsilon_2 \\ &\le \sum_{i=1}^{N}\left[I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N\right)\right. \\ &\qquad + I\left(S;Y_i\mid Z_{i+1}^N Y^{i-1}WK^N\right) \\ &\qquad \left.-I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N S\right)\right] \\ &\quad + \sum_{i=1}^{N}\left[I\left(WK^N Y^{i-1}Z_{i+1}^N;Z_i\right)\right. \\ &\qquad \left.-I\left(Y^{i-1};Z_i\mid Z_{i+1}^N WK^N\right)\right]+\epsilon_1+\epsilon_2 \\ &\overset{(a3.3)}{=} \sum_{i=1}^{N}\left[I\left(S;Y_i\mid Z_{i+1}^N Y^{i-1}WK^N\right)\right. \\ &\qquad \left.-I\left(Z_{i+1}^N;Y_i\mid Y^{i-1}WK^N S\right)\right] \\ &\quad + \sum_{i=1}^{N} I\left(WK^N Y^{i-1}Z_{i+1}^N;Z_i\right)+\epsilon_1+\epsilon_2 \\ &\le \sum_{i=1}^{N} I\left(S;Y_i\mid Z_{i+1}^N Y^{i-1}WK^N\right) \\ &\quad + \sum_{i=1}^{N} I\left(WK^N Y^{i-1}Z_{i+1}^N;Z_i\right)+\epsilon_1+\epsilon_2, \end{aligned} \tag{20}$$

where ϵ_2 is a small positive number and $(a3.2)$ and $(a3.3)$ follow from Fano's inequality and Csiszár's sum equality [2]; that is, $\sum_{i=1}^{N} I(Z_{i+1}^N;Y_i \mid Y^{i-1}WK^N) = \sum_{i=1}^{N} I(Y^{i-1};Z_i \mid Z_{i+1}^N WK^N)$.

To prove condition (17), we calculate

$$\begin{aligned} H\left(S\mid Z^N\right) &= H\left(S\mid Z^N,W\right)+I\left(S;W\mid Z^N\right) \\ &\le H\left(S\mid Z^N,W\right)+H\left(W\mid Z^N\right) \\ &= I\left(S;K^N,Y^N\mid Z^N,W\right) \\ &\quad + H\left(S\mid Z^N,K^N,Y^N,W\right)+H\left(W\mid Z^N\right) \end{aligned}$$

$$\begin{aligned}
&\le I\left(S;K^N,Y^N \mid Z^N,W\right)\\
&\quad + H\left(S \mid K^N,Y^N\right) + H\left(W \mid Z^N\right)\\
&= I\left(S;K^N \mid Z^N,W\right) + I\left(S;Y^N \mid K^N,Z^N,W\right)\\
&\quad + H\left(S \mid K^N,Y^N\right) + H\left(W \mid Z^N\right)\\
&\le H\left(K^N\right) + I\left(S;Y^N \mid K^N,Z^N,W\right)\\
&\quad + H\left(S \mid K^N,Y^N\right) + H\left(W \mid Z^N\right)\\
&\le NR_f + I\left(S;Y^N \mid K^N,Z^N,W\right) + \epsilon_1 + \epsilon_2.
\end{aligned} \tag{21}$$

The last inequality in (21) follows from the Fano's inequality and the fact that the feedback rate is limited by R_f. Then, $I(S;Y^N \mid K^N,Z^N,W)$ will be calculated as follows:

$$\begin{aligned}
&I\left(S;Y^N \mid K^N,Z^N,W\right)\\
&= \sum_{i=1}^{N} I\left(S;Y_i \mid Y^{i-1}Z^N W K^N\right)\\
&= \sum_{i=1}^{N} I\left(S;Y_i \mid Y^{i-1},Z^{i-1},Z_i,Z_{i+1}^N,W,K^N\right)\\
&=^{(a3.4)} \sum_{i=1}^{N} \Big[I\left(S;Y_i \mid Y^{i-1},Z^{i-1},Z_i,Z_{i+1}^N,W,K^N\right)\\
&\qquad + I\left(Z^{i-1};Y_i \mid Y^{i-1},Z_i^N,W,K^N\right)\\
&\qquad - I\left(Z^{i-1};Y_i \mid Y^{i-1},Z_i^N,W,S,K^N\right)\Big]\\
&= \sum_{i=1}^{N} \Big[I\left(S,Z^{i-1};Y_i \mid Y^{i-1},Z_i,Z_{i+1}^N,W,K^N\right)\\
&\qquad - I\left(Z^{i-1};Y_i \mid Y^{i-1},Z_i^N,W,S,K^N\right)\Big]\\
&= \sum_{i=1}^{N} I\left(S;Y_i \mid Y^{i-1},Z_i,Z_{i+1}^N,W,K^N\right),
\end{aligned} \tag{22}$$

where $(a3.4)$ follows from the Markov chain $Y_i \rightarrow Y^{i-1}Z_i^N W K^N \rightarrow Z^{i-1}$ and $Y_i \rightarrow Y^{i-1}Z_i^N W S K^N \rightarrow Z^{i-1}$. Then, we introduce a random variable Q which is independent of $SWK^N X^N Y^N Z^N$ and uniformly distributed over $\{1,2,\ldots,N\}$. Set $U = Z_{Q+1}^N Y^{Q-1} W K^N Q, V = US, Y = Y_Q, X = X_Q, Z = Z_Q$. It is straightforward to see that $U \rightarrow V \rightarrow X \rightarrow Y \rightarrow Z$ form a Markov chain. After using the standard time sharing argument [10, Section 5.4], (19), (20), and (22) are simplified into

$$\begin{aligned}
H(W) &\le \sum_{i=1}^{N} I\left(WK^N Y^{i-1} Z_{i+1}^N;Z_i\right) + \epsilon_1\\
&= NI(U;Z) + \epsilon_1,
\end{aligned} \tag{23}$$

$$\begin{aligned}
H(S) + H(W) &\le \sum_{i=1}^{N} I\left(S;Y_i \mid Z_{i+1}^N Y^{i-1} W K^N\right)\\
&\quad + \sum_{i=1}^{N} I\left(WK^N Y^{i-1} Z_{i+1}^N;Z_i\right) + \epsilon_1 + \epsilon_2\\
&= NI(S;Y \mid U) + NI(U;Z) + \epsilon_1 + \epsilon_2\\
&= NI(V;Y \mid U) + NI(U;Z) + \epsilon_1 + \epsilon_2,
\end{aligned} \tag{24}$$

$$\begin{aligned}
I\left(S;Y^N \mid K^N,Z^N,W\right) &= \sum_{i=1}^{N} I\left(S;Y_i \mid Y^{i-1},Z_i,Z_{i+1}^N,W,K^N\right)\\
&= NI(S;Y \mid Z,U)\\
&= NI(US;Y \mid Z,U)\\
&= NI(V;Y \mid Z,U).
\end{aligned} \tag{25}$$

Substituting (25) into (21) and utilizing (5), we get

$$\begin{aligned}
R_e &\le \lim_{N\to\infty} \Delta\\
&= \lim_{N\to\infty} \frac{H\left(S \mid Z^N\right)}{N}\\
&\le \lim_{N\to\infty} \frac{NR_f + I\left(S;Y^N \mid K^N,Z^N,W\right) + \epsilon_1 + \epsilon_2}{N}\\
&= I(V;Y \mid Z,U) + R_f\\
&= I(V;Y \mid U) - I(V;Z \mid U) + R_f.
\end{aligned} \tag{26}$$

The last equality in (26) follows from the Markov chain $U \rightarrow V \rightarrow Y \rightarrow Z$.

To finish the proof of (16) and (17), we need to show that $I(V;Y \mid U) \le I(X;Y \mid U)$ and $I(V;Y \mid U) - I(V;Z \mid U) \le I(X;Y \mid U) - I(X;Z \mid U)$. We first prove $I(V;Y \mid U,X) = 0$ and $I(V;Z \mid U,X) = 0$:

$$\begin{aligned}
I(V;Y \mid U,X) &= H(Y \mid U,X) - H(Y \mid U,V,X)\\
&=^{(a3.5)} H(Y \mid X) - H(Y \mid X)\\
&= 0,\\
I(V;Z \mid U,X) &= H(Z \mid U,X) - H(Z \mid U,V,X)\\
&=^{(a3.6)} H(Z \mid X) - H(Z \mid X)\\
&= 0,
\end{aligned} \tag{27}$$

where $(a3.5)$ follows from the Markov chains $U \rightarrow X \rightarrow Y$ and $(UV) \rightarrow X \rightarrow Y$ and $(a3.6)$ follows from the Markov chains $U \rightarrow X \rightarrow Z$ and $(UV) \rightarrow X \rightarrow Z$. Utilizing (27), we obtain

$$\begin{aligned} I(V;Y \mid U) &= I(V,X;Y \mid U) - I(X;Y \mid U,V) \\ &= I(X;Y \mid U) + I(V;Y \mid U,X) - I(X;Y \mid U,V) \\ &= I(X;Y \mid U) - I(X;Y \mid U,V), \end{aligned} \tag{28}$$

$$\begin{aligned} I(V;Z \mid U) &= I(V,X;Z \mid U) - I(X;Z \mid U,V) \\ &= I(X;Z \mid U) + I(V;Z \mid U,X) - I(X;Z \mid U,V) \\ &= I(X;Z \mid U) - I(X;Z \mid U,V). \end{aligned} \tag{29}$$

From (28), it is straightforward to see that $I(V;Y \mid U) \leq I(X;Y \mid U)$. This proves condition (16).

Then, we prove $I(V;Y \mid U) - I(V;Z \mid U) \leq I(X;Y \mid U) - I(X;Z \mid U)$. Since the channel model in Figure 1 is (physically) degraded, $I(X;Y \mid U = u, V = v) - I(X;Z \mid U = u, V = v) \geq 0$ holds for every (u,v), which implies

$$I(X;Y \mid U,V) - I(X;Z \mid U,V) \geq 0. \tag{30}$$

Therefore, utilizing (28), (29), and (30), we get

$$\begin{aligned} I(V;Y \mid U) - I(V;Z \mid U) &= I(X;Y \mid U) - I(X;Z \mid U) \\ &\quad - [I(X;Y \mid U,V) - I(X;Z \mid U,V)] \\ &\leq I(X;Y \mid U) - I(X;Z \mid U). \end{aligned} \tag{31}$$

This proves condition (17).

The converse part of Theorem 2 is proved.

3.2. A Coding Scheme Achieving $\mathcal{R}_d$. A coding scheme is provided to achieve the achievable triples $(R_0, R_1, R_e) \in \mathcal{R}_d$. The key methods used in the scheme include the superposition coding, rate splitting, and random binning. The confidential message is split into two parts. One part is reliably transmitted using superposition coding and random binning; the other part is securely transmitted with the help of the feedback. Note that Section 3.1 has already given the outer bound on the capacity-equivocation region. When $R_f \geq I(X;Z \mid U)$, it can be seen from (9) that the secrecy capacity for the degraded DMBCs with rate-limited feedback always equals to $I(X;Y \mid U)$. Therefore, in order to investigate the effects of the feedback, the feedback rate $R_f < I(X;Z \mid U)$ will only be considered in this subsection.

We need to prove that all the triples $(R_0, R_1, R_e) \in \mathcal{R}_d$ for the model of Figure 2 with any feedback rate R'_f limited by R_f are *achievable* (see Definition 1). This subsection is organized as follows. The codebook generation and encoding scheme is given in Section 3.2.1. The decoding scheme is given in Section 3.2.2. The analysis of error probability and equivocation are shown in Sections 3.2.3 and 3.2.4, respectively.

3.2.1. Codebook Generation and Encoding. Split the confidential message into two parts; that is, $\mathcal{S} = (\mathcal{M}_1, \mathcal{M}_2)$. The corresponding variables M_1, M_2 are uniformly distributed over $\{1, 2, 3, \ldots, 2^{NR'}\}$ and $\{1, 2, 3, \ldots, 2^{NR'_f}\}$, where (when $R_f \geq R_1$, the confidential message S can be totally protected by using part of the feedback (as the shared key between the transmitter and receiver 1). The remaining part of the feedback is redundant. Therefore, in order to study the effects of the feedback on the capacity region, only $R_f < R_1$ comes into our consideration)

$$\begin{gathered} 0 \leq R'_f \leq R_f, \\ R' = R_1 - R'_f > 0. \end{gathered} \tag{32}$$

It is important to notice that R_1 is the rate of the private message $\mathcal{S}$, which consists of $\mathcal{M}_1$ and $\mathcal{M}_2$. This means that

$$\begin{aligned} R_1 &= \lim_{N \to \infty} \frac{\log(\|\mathcal{M}_1\| \|\mathcal{M}_2\|)}{N} \\ &= \lim_{N \to \infty} \left(\frac{\log \|\mathcal{M}_1\|}{N} + \frac{\log \|\mathcal{M}_2\|}{N} \right). \end{aligned} \tag{33}$$

Define the index sets $\mathcal{J}_N$, $\mathcal{L}_N$, $\mathcal{F}_N$, and $\mathcal{M}_N$ satisfying

$$\begin{gathered} \lim_{N \to \infty} \frac{1}{N} \log \|\mathcal{J}_N\| = I(X;Z \mid U) - R'_f, \\ \lim_{N \to \infty} \frac{1}{N} \log \|\mathcal{L}_N\| = I(X;Y \mid U) - I(X;Z \mid U), \\ \lim_{N \to \infty} \frac{1}{N} \log \|\mathcal{F}_N\| = R'_f, \\ \lim_{N \to \infty} \frac{1}{N} \log \|\mathcal{M}_N\| = I(U;Z). \end{gathered} \tag{34}$$

We use $j \in \mathcal{J}_N$, $l \in \mathcal{L}_N$, $f \in \mathcal{F}_N$, $m \in \mathcal{M}_N$ to index the codeword x^N. Take $\mathcal{W} \subset \mathcal{M}_N$ such that (2) holds. Since $R_1 \leq I(X;Y \mid U)$, it is easy to see $\|\mathcal{J}_N \times \mathcal{L}_N \times \mathcal{F}_N\| \geq 2^{NR_1}$. Therefore, let $\mathcal{M}_1 = \mathcal{D}_N \times \mathcal{L}_N$, $\mathcal{M}_2 = \mathcal{F}_N$, where $\mathcal{D}_N$ is an arbitrary set such that (3) holds. Let g_j be a mapping of $\mathcal{J}_N$ into $\mathcal{D}_N$ partitioning $\mathcal{J}_N$ into subsets of size $\|\mathcal{J}_N\|/\|\mathcal{D}_N\|$; that is,

$$g_j : \mathcal{J}_N \longrightarrow \mathcal{D}_N, \tag{35}$$

where $g_j(j) = d$, $j \in \mathcal{J}_N$, $d \in \mathcal{D}_N$.

For each $w \in \mathcal{W}$, we generate a codeword $u^N(w)$ according to $\prod_{i=1}^{N} p(u_i)$. Then, for each $u^N(w)$, a codebook $\mathcal{CB}_w$ (see Figure 4) containing $\|\mathcal{J}_N\| \cdot \|\mathcal{L}_N\| \cdot \|\mathcal{F}_N\|$ codewords x^N_{jlfm} is constructed according to $\prod_{i=1}^{N} p(x_i \mid u_i)$, where $j \in \mathcal{J}_N$, $l \in \mathcal{L}_N$, $f \in \mathcal{F}_N$, $m = w \in \mathcal{M}$. Those x^N are put into $\|\mathcal{L}_N\| \cdot \|\mathcal{F}_N\|$ bins so that each bin contains $\|\mathcal{J}_N\|$ codewords. Each bin is indexed by (l, f), where $l \in \mathcal{L}_N$, $f \in \mathcal{F}_N$. Then, we divide each bin into $\|\mathcal{D}_N\|$ subbins such that each subbin contains $\|\mathcal{J}_N\|/\|\mathcal{D}_N\|$ codewords. The codebook structure is presented in Figure 4.

Let $\mathcal{K} = \{1, 2, 3, \ldots, 2^{NR'_f}\}$, where $k \in \mathcal{K}$ is the key sent to the transmitter from receiver 1 through the secure feedback

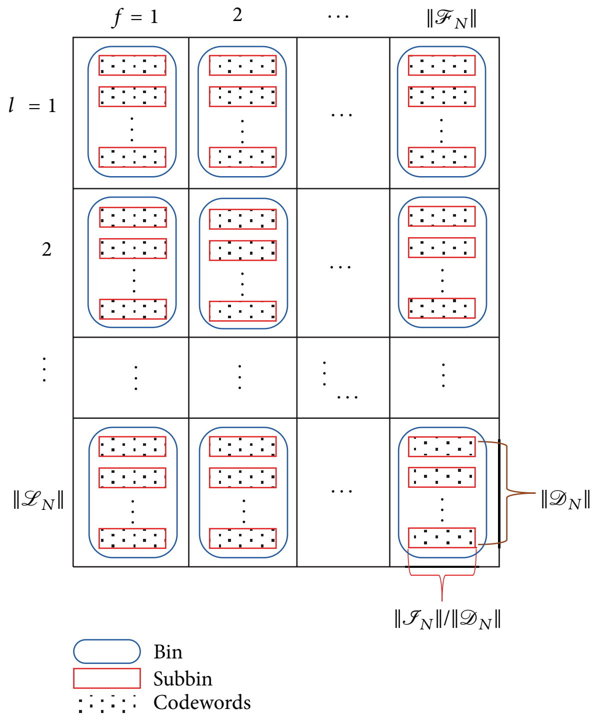


FIGURE 4: The codebook $\mathscr{CB}_w$ for each $u^N(w)$.

link. It is kept secret from receiver 2. The corresponding variable K is uniformly distributed over $\mathscr{K}$ and independent of S and W.

In order to send $s = (d, l, m_2) \in \mathscr{D}_N \times \mathscr{L}_N \times \mathscr{F}_N$ and $w \in \mathscr{W}$, a codeword x^N_{jlfm} is chosen as follows. According to the common message w, we first find the sequence $u^N(w)$. For the determined $u^N(w)$, there is a corresponding codebook $\mathscr{CB}_w$; see Figure 4. Then, the corresponding codeword x^N_{jlfm} is sent into the channel, where j is chosen randomly from the set $g_j^{-1}(d)$, $f = k \oplus m_2$, and $m = w$ (here $\oplus$ is modulo addition over $\mathscr{F}_N$). Figure 4 shows how to select x^N_{jlfm} in detail. According to $u^N(w)$, we can find the corresponding codebook $\mathscr{CB}_w$. In the codebook $\mathscr{CB}_w$, we choose the corresponding bin according to f and l. Then, in that bin, the subbin is found according to d. Finally, a codeword x^N (which is denoted by x^N_{jlfm}) is randomly chosen from that subbin.

3.2.2. Decoding. Receiver 2 tries to find a unique sequence $u^N(\widehat{w})$ such that $(u^N(\widehat{w}), z^N) \in T^N_{UZ}(\epsilon_1)$. If there exists such a unique sequence, decoder 2 outputs $\widehat{w}$; otherwise, an error is declared. Since the size of $\mathscr{W}$ is smaller than $2^{NI(U;Z)}$, the decoding error probability for receiver 2 approaches zero.

For receiver 1, he can also decode the common message $\widehat{w}$ since the output of channel 2 is a degraded version of the output of channel 1. Then, receiver 1 tries to find a unique codeword $x^N_{\hat{j}\hat{l}\hat{f}\widehat{m}}$ indexed by $\hat{j}$, $\hat{l}$, $\hat{f}$, $\widehat{m}$, such that $(x^N_{\hat{j}\hat{l}\hat{f}\widehat{m}}, y^N) \in T^N_{XY|U}(\epsilon_2)$. If there exists such a unique codeword $x^N_{\hat{j}\hat{l}\hat{f}\widehat{m}}$, receiver 1 calculates $\hat{f} \ominus k$ as $\widehat{m}_2$ (here $\ominus$ is modulo subtraction over $\mathscr{F}_N$, and $\widehat{m} = \widehat{w}$) and finds $\hat{d}$ according to $g_j(\hat{j})$. Note that receiver 1 knows the secret key k. Decoder 1 outputs $\hat{s} = (\hat{d}, \hat{l}, \widehat{m}_2)$ and $\widehat{w}$. If no such $x^N_{\hat{j}\hat{l}\hat{f}\widehat{m}}$ or more than one such $x^N_{\hat{j}\hat{l}\hat{f}\widehat{m}}$ exist, an error is declared.

3.2.3. Analysis of Error Probability. Since the number of $u^N(w)$ is upper bound by $2^{NI(U;Z)}$ and the DMBCs under discussion are degraded, both receivers can decode the common message w with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1]. Moreover, it can be calculated that given the codeword $u^N(w)$, the number of x^N is

$$\|\mathscr{F}_N\| \cdot \|\mathscr{J}_N\| \cdot \|\mathscr{L}_N\| = 2^{NI(X;Y|U)}. \tag{36}$$

So, after determining the codeword $u^N(w)$, receiver 1 can decode the codeword x^N with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1]. This proves (6).

3.2.4. Analysis of Equivocation. The proof of (5) is given below:

$$\begin{aligned} H(S \mid Z^N) &= H(M_1, M_2 \mid Z^N) \\ &= H(M_1 \mid Z^N) + H(M_2 \mid Z^N, M_1) \\ &\geq H(M_1 \mid Z^N) + H(M_2 \mid Z^N, M_1, K \oplus M_2) \\ &\overset{(b3.1)}{=} H(M_1 \mid Z^N) + H(M_2 \mid K \oplus M_2) \\ &\overset{(b3.2)}{=} H(M_1 \mid Z^N) + H(M_2) \\ &\overset{(b3.3)}{=} H(M_1 \mid Z^N) + NR'_f, \end{aligned} \tag{37}$$

where $(b3.1)$ follows from the Markov chain $M_2 \rightarrow M_2 \oplus K \rightarrow (Z^N, M_1)$, $(b3.2)$ follows from the fact that M_2 is independent of $M_2 \oplus K$, and $(b3.3)$ follows from that M_2 is uniformly distributed over $\{1, 2, 3, \ldots, 2^{NR'_f}\}$. The proof of the fact that M_2 is independent of $M_2 \oplus K$ is shown as follows (the proof can also be seen in [6]):

$$\begin{aligned} &p(M_2 \oplus K = a) \\ &\quad = \sum_k p(M_2 \oplus K = a \mid K = k)\, p(K = k) \\ &\quad \overset{(b3.4)}{=} \sum_k p(M_2 \oplus K = a \mid K = k) \frac{1}{\|\mathscr{F}_N\|} \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\|\mathscr{F}_N\|}\sum_k p\left(M_2 \oplus K = a \mid K = k\right) \\
&= \frac{1}{\|\mathscr{F}_N\|}\sum_k p\left(M_2 = a \ominus k \mid K = k\right) \\
&=^{(b3.5)} \frac{1}{\|\mathscr{F}_N\|}\sum_k p\left(M_2 = a \ominus k\right) \\
&= \frac{1}{\|\mathscr{F}_N\|} \\
p&\left(M_2 \oplus K = a, M_2 = m_2\right) \\
&= p\left(K = a \ominus m_2, M_2 = m_2\right) \\
&=^{(b3.6)} p\left(K = a \ominus m_2\right) p\left(M_2 = m_2\right) \\
&=^{(b3.7)} \frac{1}{\|\mathscr{F}_N\|} \cdot \frac{1}{\|\mathscr{F}_N\|},
\end{aligned} \tag{38}$$

where $(b3.5)$ and $(b3.6)$ follow from that M_2 is independent of K, and $(b3.4)$ and $(b3.7)$ follow from that M_2 and K are both uniformly distributed over $\mathscr{F}_N$. According to (38),

$$\begin{aligned}
p&\left(M_2 \oplus K = a, M_2 = m_2\right) \\
&\quad = p\left(M_2 \oplus K = a\right) p\left(M_2 = m_2\right).
\end{aligned} \tag{39}$$

Therefore, M_2 is independent of $M_2 \oplus K$.

Next, we focus on the first term in (37). The method of the equivocation analysis in [2] will be used:

$$\begin{aligned}
H&\left(M_1 \mid Z^N\right) \\
&\geq H\left(M_1 \mid Z^N, W\right) \\
&= H\left(M_1, Z^N \mid W\right) - H\left(Z^N \mid W\right) \\
&= H\left(M_1, Z^N, X^N \mid W\right) - H\left(X^N \mid M_1, Z^N, W\right) \\
&\quad - H\left(Z^N \mid W\right) \\
&= H\left(M_1, X^N \mid W\right) + H\left(Z^N \mid M_1, X^N, W\right) \\
&\quad - H\left(X^N \mid M_1, Z^N, W\right) - H\left(Z^N \mid W\right) \\
&\geq H\left(X^N \mid W\right) + H\left(Z^N \mid M_1, X^N, W\right) \\
&\quad - H\left(X^N \mid M_1, Z^N, W\right) - H\left(Z^N \mid W\right).
\end{aligned} \tag{40}$$

Note that W in inequality (40) is the random variable of the common message $\mathscr{W}$. The four terms $H(X^N \mid W)$, $H(Z^N \mid M_1, X^N, W)$, $H(X^N \mid M_1, Z^N, W)$, and $H(Z^N \mid W)$ will be bounded as follows.

Given $w \in \mathscr{W}$, the number of x^N is $\|\mathscr{J}_N\| \cdot \|\mathscr{L}_N\| \cdot \|\mathscr{F}_N\|$. By applying [12, Lemma 2.5], we obtain

$$\begin{aligned}
H\left(X^N \mid W\right) &\geq \log\left(\|\mathscr{J}_N\| \cdot \|\mathscr{L}_N\| \cdot \|\mathscr{F}_N\|\right) - 1 \\
&= NI\left(X; Y \mid U\right) - 1.
\end{aligned} \tag{41}$$

Since $(M_1, W) \rightarrow X^N \rightarrow Z^N$ and the channel to receiver 2 is discrete memoryless, it is easy to get

$$\begin{aligned}
H\left(Z^N \mid M_1, X^N, W\right) &= H\left(Z^N \mid X^N\right) \\
&= NH\left(Z \mid X\right).
\end{aligned} \tag{42}$$

With the knowledge of $(d, l) \in \mathscr{M}_1$ and $w \in \mathscr{W}$, the number of x^N is

$$\begin{aligned}
2^{NR'_f} \cdot \frac{\|\mathscr{J}_N\|}{\|\mathscr{D}_N\|} &< 2^{NR'_f} \cdot \|\mathscr{J}_N\| \\
&= 2^{NR'_f} \cdot 2^{N(I(X;Z|U) - R'_f)} \\
&= 2^{NI(X;Z|U)}.
\end{aligned} \tag{43}$$

So, receiver 2 can decode the codeword x^N with error probability approaching zero by using the standard channel coding theorem [11, Theorem 7.7.1]. Therefore, using Fano's inequality, we get

$$H\left(X^N \mid M_1, Z^N, W\right) \longrightarrow 0. \tag{44}$$

Moreover, using the similar deduction in [2, Section 4], we get

$$\begin{aligned}
H\left(Z^N \mid W\right) &\leq \log\left\|T^N_{Z|U}\left(\epsilon_1\right)\right\| \\
&\leq NH\left(Z \mid U\right).
\end{aligned} \tag{45}$$

Substituting (41), (42), (44), and (45) into (40), we get

$$\begin{aligned}
H&\left(M_1 \mid Z^N\right) \\
&\geq NI\left(X; Y \mid U\right) + NH\left(Z \mid X\right) - NH\left(Z \mid U\right) \\
&= NI\left(X; Y \mid U\right) - NI\left(X; Z \mid U\right),
\end{aligned} \tag{46}$$

where the equality in (46) follows from the Markov chain $U \rightarrow X \rightarrow Z$.

Finally, (5) is verified by substituting (46) into (37):

$$\begin{aligned}
\lim_{N\to\infty} \Delta &= \lim_{N\to\infty} \frac{H\left(S \mid Z^N\right)}{N} \\
&\geq \lim_{N\to\infty}\left(\frac{H\left(M_1 \mid Z^N\right)}{N} + R'_f\right) \\
&\geq \lim_{N\to\infty}\left(\frac{NI\left(X; Y \mid U\right) - NI\left(X; Z \mid U\right)}{N} + R'_f\right) \\
&= I\left(X; Y \mid U\right) - I\left(X; Z \mid U\right) + R'_f \\
&\geq R_e.
\end{aligned} \tag{47}$$

This completes the proof of Theorem 2.

4. Proof of Theorems 4 and 5

In this section, Theorems 4 and 5 are proved. In the model of Figure 3, it is assumed that the channel to receiver 1 is independent of the channel to receiver 2; that is, $p(y,z \mid x) = p(y \mid x)p(z \mid x)$. To prove Theorem 4, we first give the outer bound on the capacity-equivocation region of the *less noisy* DMBCs with noiseless causal feedback in Section 4.1. Then, a coding scheme is provided to achieve the outer bound. Similarly, to prove Theorem 5, the outer bound on the capacity-equivocation region of the *reversely less noisy* DMBCs with noiseless causal feedback is given in Section 4.2. Moreover, we also provide a coding scheme to achieve the outer bound. The methods used to prove the converse parts of the two theorems are from [5]. The coding schemes are inspired by [3, 5].

4.1. Less Noisy DMBCs with Noiseless Causal Feedback. We first show the converse part of Theorem 4, and then we prove the direct part of Theorem 4 by providing a coding scheme.

In order to find the identification of the auxiliary random variables that satisfy the capacity-equivocation region characterized by $\mathscr{R}_l$, we prove the converse part for the equivalent region containing all the rate triples (R_0, R_1, R_e) such that

$$0 \le R_e \le R_1, \tag{48}$$

$$R_0 \le I(U;Z), \tag{49}$$

$$R_0 + R_1 \le I(X;Y \mid U) + I(U;Z), \tag{50}$$

$$R_e \le H(Y \mid Z). \tag{51}$$

The proof of (48), (49), and (50) follows exactly the same line of proving (14), (15), and (16) in Section 3 except for the identification of the auxiliary random variable U, V (which will be given subsequently) and therefore is omitted. We focus on proving (51):

$$\begin{aligned}
H\left(S \mid Z^N\right) &\le H\left(S \mid Z^N\right) + I\left(S; Z^N \mid Y^N\right) \\
&= H\left(S \mid Z^N\right) + H\left(S \mid Y^N\right) - H\left(S \mid Y^N, Z^N\right) \\
&= I\left(S; Y^N \mid Z^N\right) + H\left(S \mid Y^N\right) \\
&\le H\left(Y^N \mid Z^N\right) + H\left(S \mid Y^N\right) \\
&= \sum_{i=1}^{N} H\left(Y_i \mid Y^{i-1}, Z^N\right) + H\left(S \mid Y^N\right) \\
&\le \sum_{i=1}^{N} H\left(Y_i \mid Z_i\right) + \epsilon_3,
\end{aligned} \tag{52}$$

where ϵ_3 is a small positive number. The last inequality in (52) follows from the fact that conditioning does not increase *entropy* and Fano's inequality. To complete the proof of (51), define a time-sharing random variable Q which is uniformly distributed over $1, 2, \ldots, N$ and independent of $SWX^NY^NZ^N$. Set $U = Z_{Q+1}^N Y^{Q-1} WQ$, $V = US$, $X = X_Q$, $Y = Y_Q$, $Z = Z_Q$. It is easy to see $U \rightarrow V \rightarrow X \rightarrow (Y, Z)$ form a Markov chain. After using the standard time-sharing argument [10, Section 5.4], (52) simplifies to

$$H\left(S \mid Z^N\right) \le NH(Y \mid Z) + \epsilon_3. \tag{53}$$

Finally, utilizing $\lim_{N\to\infty}\Delta \ge R_e$ in the definition of "*achievable*" and (53), we obtain (51). This completes the proof of the converse part of Theorem 4.

Next, a coding scheme is presented to achieve the rate triple $(R_0, R_1, R_e) \in \mathscr{R}_l$. We should prove that all triples $(R_0, R_1, R_e) \in \mathscr{R}_l$ are *achievable*. Note that the noiseless feedback for the less noisy DMBCs is causally transmitted from receiver 1 to the transmitter. The scheme includes codebook generation and encoding scheme in Section 4.1.1, decoding scheme in Section 4.1.2, analysis of error probability in Section 4.1.3, and equivocation analysis in Section 4.1.4. Techniques like block Markov coding, superposition coding, and random binning are used.

To serve the block Markov coding, let random vectors U^N, X^N, Y^N, and Z^N consist of n blocks of length N. Let $W^n \triangleq (W_1, \ldots, W_n)$ stand for the common messages of n blocks, where $W_1, \ldots, W_n$ are independent and identically distributed random variables over $\mathscr{W}$. Let $S^n \triangleq (S_2, \ldots, S_n)$ stand for the confidential messages of n blocks, where $S_2, \ldots, S_n$ are independent and identically distributed random variables over $\mathscr{S}$. Note that in the first block, there is no S_1. Let $\widetilde{Z}^n = (\widetilde{Z}_1, \widetilde{Z}_2, \ldots, \widetilde{Z}_n)$, $\widetilde{Z}^{\overline{b}} = (\widetilde{Z}_1, \widetilde{Z}_2, \ldots, \widetilde{Z}_{b-1}, \widetilde{Z}_{b+1}, \ldots, \widetilde{Z}_n)$, where $\widetilde{Z}_b$ is the output vector at receiver 2 at the end of the bth block, where $1 \le b \le n$. Similarly, $\widetilde{Y}_b$ denotes the output vector at receiver 1 at the end of the bth block, and $\widetilde{X}_b$ denotes the input vector of the channel in the bth block. These notations coincide with [6].

4.1.1. Codebook Generation and Encoding. Let the common message set $\mathscr{W}$ and the confidential message set $\mathscr{S}$ satisfy

$$\begin{aligned}
\lim_{N\to\infty} \frac{\log \|\mathscr{W}\|}{N} &= R_0, \\
\lim_{N\to\infty} \frac{\log \|\mathscr{S}\|}{N} &= R_1,
\end{aligned} \tag{54}$$

where R_0 and R_1 satisfy (10).

Fix $p(u)$ and $p(x \mid u)$. In the bth block, $1 \le b \le n$, we generate 2^{NR_0} independent and identically distributed (i.i.d) sequences $u^N(w_b)$ according to $\prod_{i=1}^{N} p(u_i)$, where $w_b \in$

$\mathcal{W}$ is the common message to be sent in the bth block. For each $u^N(w_b)$, generate $2^{NI(X;Y|U)}$ codewords $x^N(u^N(w_b))$ according to $\prod_{i=1}^{N} p(x_i \mid u_i)$. Put the $2^{NI(X;Y|U)}$ codewords into 2^{NR_1} bins, so each bin contains $2^{N(I(X;Y|U)-R_1)}$ codewords. The 2^{NR_1} bins are denoted by $Q_1, Q_2, \ldots, Q_{\|\mathcal{S}\|}$, where $\|\mathcal{S}\| = 2^{NR_1}$. The codebook structure is shown in Figure 5. Reveal all the codebooks to the transmitter, receiver 1, and receiver 2.

Let g be a mapping from $\mathcal{Y}^N$ into $\mathcal{S}$. Reveal the mapping g to the transmitter, receiver 1, and receiver 2. Define a random variable $S' = g(Y^N)$ uniformly distributed over $\mathcal{S}$ and independent of the confidential message S. It can be similarly proved from (39) that $S \oplus S'$ is independent of S. In the first block, that is, $b = 1$, to send the common message w_1 (note that there is no confidential message to be sent in the first block), the transmitter tries to find $u^N(w_1)$ and randomly choose a codeword $x^N(u^N(w_1))$ from the corresponding $2^{NI(X;Y|U)}$ codewords. In the bth block ($b = 2, 3, \ldots, n$), to send the common message w_b and confidential message s_b, the transmitter calculates $s'_b = g(\widetilde{y}_{b-1})$ and randomly chooses a codeword $x^N(u^N(w_b), s_b)$ from the bin $Q_{s_b \oplus s'_b}$. Here, $\widetilde{y}_{b-1}$ is the output vector of the $(b-1)$th block at receiver 1, and $\oplus$ is the modulo addition over $\mathcal{S}$.

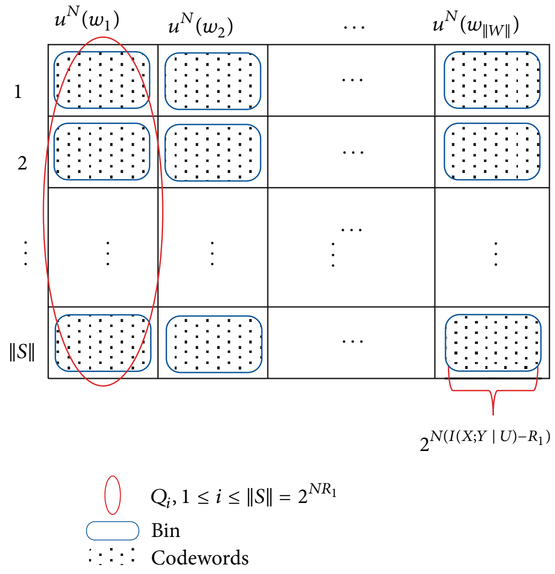


Figure 5: The codebook structure.

4.1.2. Decoding

4.1.2. Decoding. In the first block, as there is no confidential message, only the common message needs to be decoded for both receivers. For receiver 2, he tries to find a unique sequence $u^N(\widehat{\widehat{w}}_1)$ such that $(u^N(\widehat{\widehat{w}}_1), \widetilde{z}_1) \in T^N_{UZ}(\epsilon'_1)$, where ϵ'_1 is a small positive number. If there exists such a unique sequence, decoder 2 outputs $\widehat{\widehat{w}}_1$; otherwise, an error is declared. For receiver 1, he tries to find a unique sequence $u^N(\widehat{w}_1)$ such that $(u^N(\widehat{w}_1), \widetilde{y}_1) \in T^N_{UY}(\epsilon''_1)$, where ϵ''_1 is a small positive number. If there exists such a unique sequence, output is $\widehat{w}_1$; otherwise, declare an error.

In the bth block, $2 \le b \le n$, receiver 2 aims to decode the common message, and receiver 1 aims to decode both confidential and common messages. The method of decoding the common message w_b for both receivers follows the same as that in the first block. Then, receiver 1 tries to find a unique sequence $x^N(u^N(\widehat{w}_b), \widehat{s}_b)$ such that $(x^N(u^N(\widehat{w}_b), \widehat{s}_b), \widetilde{y}_b) \in T^N_{XY|U}(\epsilon'_2)$, where ϵ'_2 is a small positive number. If there exists such a unique sequence in one bin, denoting the corresponding index of that bin by s''_b, receiver 1 calculates $s''_b \ominus s'_b$ as $\widehat{s}_b$ (here $\ominus$ is modulo subtraction over $\mathcal{S}$, and receiver 1 knows $s'_b = g(\widetilde{y}_{b-1})$); otherwise, declare an error.

4.1.3. Analysis of Error Probability

4.1.3. Analysis of Error Probability. Since the number of $u^N(w_b)$ is upper bounded by $2^{NI(U;Z)}$, receiver 2 can decode the common message w_b with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1]. Moreover, since the DMBCs under discussion in Section 4.1 are *less noisy*, receiver 1 can also decode the common message with error probability approaching zero. It can be calculated that given the codeword $u^N(w_b)$, the number of x^N is $2^{NI(X;Y|U)}$. So, after determining the codeword $u^N(w_b)$, receiver 1 can decode the codeword x^N with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1] and obtain the confidential message with the help of the feedback.

4.1.4. Analysis of Equivocation

4.1.4. Analysis of Equivocation. In this part, $\lim_{N\to\infty}\Delta \ge R_e$ is proved by utilizing the methods in [5, 6]:

$$
\begin{aligned}
\lim_{N\to\infty} \Delta &= \lim_{N,n\to\infty} \frac{H\left(S^n \mid \widetilde{Z}^n\right)}{nN} \\
&= \lim_{N,n\to\infty} \sum_{i=2}^{n} \frac{H\left(S_i \mid S^{i-1}, \widetilde{Z}^n\right)}{nN} \\
&=^{(a4.1)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_i\right)}{nN} \\
&\ge \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_i, \widetilde{Z}_{i-1}, S_i \oplus S'_i\right)}{nN} \\
&=^{(a4.2)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_{i-1}, S_i \oplus S'_i\right)}{nN} \\
&=^{(a4.3)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} \min\left\{NH\left(Y \mid Z\right), \log \|\mathcal{S}\|\right\}}{nN} \\
&= \lim_{n\to\infty} \frac{\sum_{i=2}^{n} \min\left\{H\left(Y \mid Z\right), R_1\right\}}{n} \\
&= \min\left\{H\left(Y \mid Z\right), R_1\right\} \\
&\ge^{(a4.4)} R_e.
\end{aligned}
\tag{55}
$$

In the above deduction, $(a4.1)$ follows from $S_i \to \widetilde{Z}_i \to (S^{i-1}, \widetilde{Z}^{\bar{i}})$. $(a4.2)$ follows from $S_i \to (S_i \oplus S'_i, \widetilde{Z}_{i-1}) \to \widetilde{Z}_i$. $(a4.3)$ follows from the fact that receiver 2 can choose a better way to intercept the secret key at will and $S_i \oplus S'_i$ is independent of S_i and uniformly distributed over $\mathcal{S}$. (a4.4) follows from (10).

This completes the proof of Theorem 4.

4.2. Reversely Less Noisy DMBCs with Noiseless Causal Feedback. In this subsection, Theorem 5 will be proved. The converse part will be shown first, and then a coding scheme is given for proving the direct part.

In order to find the identification of the auxiliary random variables that satisfy the capacity-equivocation region characterized by $\mathcal{R}_{rl}$, we prove the converse part for the equivalent region containing all the rate triples (R_0, R_1, R_e) such that

$$0 \le R_e \le R_1, \tag{56}$$

$$R_0 \le I(U;Y), \tag{57}$$

$$R_0 + R_1 \le I(X;Y \mid U) + I(U;Y), \tag{58}$$

$$R_e \le H(Y \mid X). \tag{59}$$

The inequalities (56), (57), and (58) can be proved using similar deduction of the converse part of Theorem 2 in Section 3 except for the identification of the auxiliary random variables. We focus on (59):

$$\begin{aligned}
H&\left(S \mid Z^N\right) \\
&= H\left(S \mid X^N, Z^N\right) + I\left(S; X^N \mid Z^N\right) \\
&\overset{(b4.1)}{=} H\left(S \mid X^N\right) + I\left(X^N; S \mid Z^N\right) \\
&= H\left(S, Y^N \mid X^N\right) - H\left(Y^N \mid X^N, S\right) \\
&\quad + I\left(X^N; S \mid Z^N\right) \\
&= H\left(Y^N \mid X^N\right) + H\left(S \mid Y^N, X^N\right) \\
&\quad - H\left(Y^N \mid X^N, S\right) + I\left(X^N; S \mid Z^N\right) \\
&\le H\left(Y^N \mid X^N\right) + H\left(S \mid Y^N, X^N\right) + I\left(X^N; S \mid Z^N\right) \\
&\le H\left(Y^N \mid X^N\right) + H\left(S \mid Y^N, X^N\right) + H\left(X^N \mid Z^N\right) \\
&\overset{(b4.2)}{=} H\left(Y^N \mid X^N\right) + H\left(S \mid Y^N, X^N\right) \\
&\quad + H\left(X^N \mid Y^N\right) \\
&= H\left(Y^N \mid X^N\right) + H\left(S, X^N \mid Y^N\right) \\
&\overset{(b4.3)}{=} H\left(Y^N \mid X^N\right) + H\left(S \mid Y^N\right) \\
&= \sum_{i=1}^{N} H\left(Y_i \mid Y^{i-1}, X^N\right) + H\left(S \mid Y^N\right) \\
&\overset{(b4.4)}{\le} \sum_{i=1}^{N} H\left(Y_i \mid X_i\right) + \epsilon_3,
\end{aligned} \tag{60}$$

where (b4.1) from the Markov chain $S \to X^N \to Z^N$, (b4.2) from the assumption that the channel is *reversely less noisy* (by setting $U = X$), (b4.3) from that X^N is a function of S, Y^N, and (b4.4) from the fact that conditioning does not increase *entropy* and Fano's inequality. To complete the proof of (59), define a time-sharing random variable Q which is uniformly distributed over $\{1, 2, \ldots, N\}$ and independent of $SWX^NY^NZ^N$. Set $U = Z_{Q+1}^N Y^{Q-1} WQ$, $V = US$, $X = X_Q$, $Y = Y_Q$, $Z = Z_Q$. It is easy to see $U \to V \to X \to (Y, Z)$ form a Markov chain. After using the standard time-sharing argument [10, Section 5.4], (60) simplifies to

$$H\left(S \mid Z^N\right) \le NH(Y \mid X) + \epsilon_3. \tag{61}$$

Finally, utilizing $\lim_{N\to\infty} \Delta \ge R_e$ in the definition of "*achievable*" and (61), we obtain (59). This completes the proof of the converse part of Theorem 5.

Next, a coding scheme will be provided for achieving the triple $(R_0, R_1, R_e) \in \mathcal{R}_{rl}$. We should prove that all triples $(R_0, R_1, R_e) \in \mathcal{R}_{rl}$ are *achievable*. The *codebook generation*, *encoding*, and *decoding* follow exactly the lines of the coding scheme for the *less noisy* case in Section 4.1. We present the *analysis of error probability* and *equivocation* as follows.

4.2.1. Analysis of Error Probability. Since the number of $u^N(w_b)$ is upper bounded by $2^{NI(U;Y)}$, receiver 1 can decode the common message w_b with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1]. Moreover, since the DMBCs under discussion in Section 4.2 are *reversely less noisy*, receiver 2 can also decode the common message with error probability approaching zero. It can be calculated that given the codeword $u^N(w_b)$, the number of x^N is $2^{NI(X;Y|U)}$. So, after determining the codeword $u^N(w_b)$, receiver 1 can decode the codeword x^N with error probability approaching zero by applying the standard channel coding theorem [11, Theorem 7.7.1] and obtain the confidential message with the help of the feedback.

4.2.2. Analysis of Equivocation. In this part, $\lim_{N\to\infty} \Delta \ge R_e$ will be proved. Special attention should be paid to receiver 2 since the DMBCs are *reversely less noisy*; that is, $I(U;Z) \ge I(U;Y)$ for all $p(u,x)$, which implies $2^{NI(X;Z|U)} \ge 2^{NI(X;Y|U)}$. Therefore, receiver 2 can also decode the codeword x^N. With the knowledge of x^N and z^N, receiver 2 can guess receiver 1's channel output y^N from the conditional typical set $\mathcal{T}^N_{Y|XZ}(\epsilon_3)$. Note that receiver 2 can intercept the confidential messages in two ways. One is guessing the secret key s_b' from $\mathcal{S}$ directly; the other is guessing the channel output $\widetilde{y}_{b-1}$ and finding s_b' through $g(\widetilde{y}_{b-1})$ indirectly. Intuitively, receiver 2 will always choose a better way to implement eavesdropping. More formally,

$$\begin{aligned}
\lim_{N\to\infty} \Delta &= \lim_{N,n\to\infty} \frac{H\left(S^n \mid \widetilde{Z}^n\right)}{nN} \\
&= \lim_{N,n\to\infty} \sum_{i=2}^{n} \frac{H\left(S_i \mid S^{i-1}, \widetilde{Z}^n\right)}{nN}
\end{aligned}$$

$$
\begin{aligned}
&=^{(b4.5)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_i, \widetilde{Z}_{i-1}\right)}{nN} \\
&\geq \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_i, \widetilde{Z}_{i-1}, \widetilde{X}_{i-1}, S_i \oplus S_i'\right)}{nN} \\
&=^{(b4.6)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} H\left(S_i \mid \widetilde{Z}_{i-1}, \widetilde{X}_{i-1}, S_i \oplus S_i'\right)}{nN} \\
&=^{(b4.7)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} \min\left\{NH\left(Y \mid XZ\right), \log \|\mathcal{S}\|\right\}}{nN} \\
&=^{(b4.8)} \lim_{N,n\to\infty} \frac{\sum_{i=2}^{n} \min\left\{NH\left(Y \mid X\right), \log \|\mathcal{S}\|\right\}}{nN} \\
&= \lim_{n\to\infty} \frac{\sum_{i=2}^{n} \min\left\{H\left(Y \mid X\right), R_1\right\}}{n} \\
&= \min\left\{H\left(Y \mid X\right), R_1\right\} \\
&\geq^{(b4.9)} R_e.
\end{aligned}
\tag{62}
$$

In the above deduction, $(b4.5)$ follows from $S_i \rightarrow (\widetilde{Z}_i, \widetilde{Z}_{i-1}) \rightarrow (S^{i-1}, \widetilde{Z}^{i-2}, \widetilde{Z}_{i+1}^{n})$. $(b4.6)$ follows from $S_i \rightarrow (S_i \oplus S_i', \widetilde{Z}_{i-1}, \widetilde{X}_{i-1}) \rightarrow \widetilde{Z}_i$. $(b4.7)$ follows from the fact that receiver 2 can choose a better way to intercept the secret key at will, and $S_i \oplus S_i'$ is independent of S_i and uniformly distributed over $\mathcal{S}$. Note that the number of $y^N \in T_{Y|XZ}^{N}(\epsilon_3)$ is about $2^{NH(Y|XZ)}$ based on the property of strong *typical* sequence [10]. $(b4.8)$ follows from the fact that Y is independent of Z conditioning on X, which is obtained from the assumption $p(y, z \mid x) = p(y \mid x)p(z \mid x)$. $(b4.9)$ follows from (11).

This completes the proof of Theorem 5.

5. Conclusion

This paper studies two models of the DMBCs with noiseless feedback. One is the degraded DMBCs with rate-limited feedback; the other is the *less* and *reversely less noisy* DMBCs with feedback. The difference between them is that the feedback in the first model is independent of the channel outputs and rate limited, while the feedback in the second model is originated causally from the channel outputs. The capacity-equivocation regions of the two models are obtained in this paper. We should point out that the second model studied in this paper is under the assumption that the channel to receiver 1 (the legitimate receiver) is independent of the channel to receiver 2 (the eavesdropper); that is, the channel output Y^N is independent of Z^N given the channel input X^N. However, without this assumption, the capacity-equivocation region remains unknown for the general DMBCs with noiseless feedback.

Acknowledgments

This work was supported in part by the National Science Foundation of China under Grant no. 60932003 and Grant no. 61271220. The authors also would like to thank the anonymous reviewers for helpful comments.

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*, vol. 4123, pp. 258–275, Springer, Berlin, Germany, 2006.

[4] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, 2009.

[5] B. Dai, A. J. Han Vinck, Y. Luo, and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 244–248, Cambridge, Mass, USA, July 2012.

[6] B. Dai, A. J. Han Vinck, and Z. Zhuang, "Degraded broadcast channel with side information,confidential messages and noiseless feedback," in press, http://arxiv.org/abs/1201.2859.

[7] A. El Gamal, "The feedback capacity of degraded broadcast channels," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 379–381, 1978.

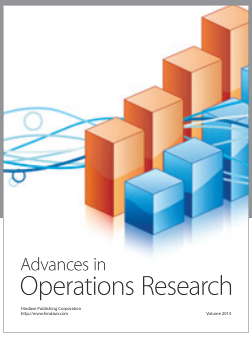
[8] O. Shayevitz and M. Wigger, "On the capacity of the discrete memoryless broadcast channel with feedback," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1329–1345, 2013.

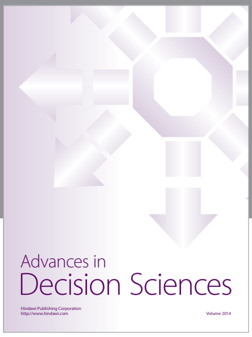
[9] R. Venkataramanan and S. Pradhan, "An achievable rate region for the broadcast channel with feedback," *IEEE Transactions on Information Theory*. In press, http://arxiv.org/abs/1105.2311.

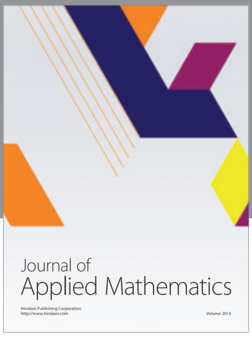
[10] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge University Press, Cambridge, Mass, USA, 2011.

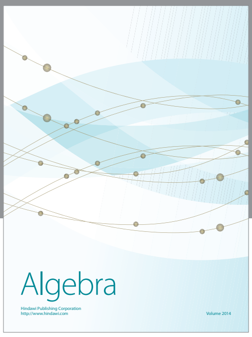
[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, New York, NY, USA, 1991.

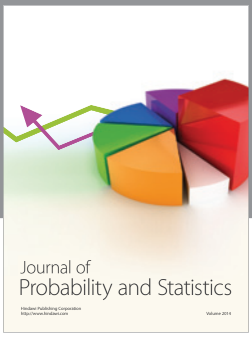
[12] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," in *Foundations and Trends in Communications and Information Theory*, vol. 5, pp. 355–580, Now Publishers, Hanover, Mass, USA, 2008.


Advances in
Operations Research

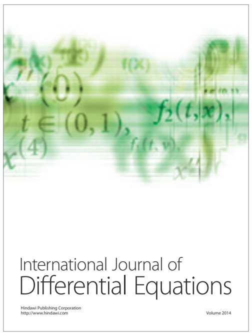

Advances in
Decision Sciences


Journal of
Applied Mathematics

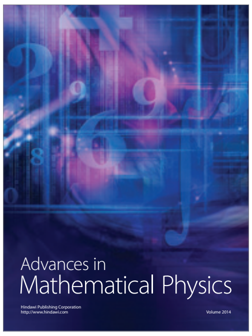

Algebra

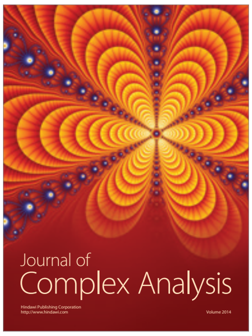

Journal of
Probability and Statistics

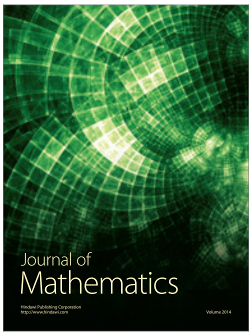
The Scientific
World Journal

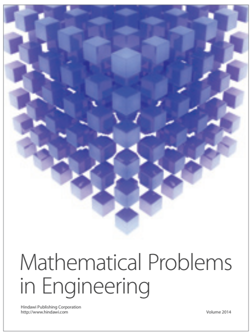

International Journal of
Differential Equations

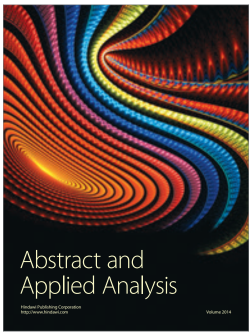
International Journal of
Combinatorics

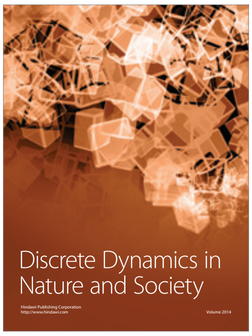

Advances in
Mathematical Physics

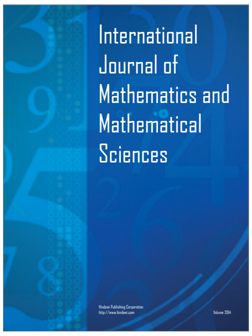

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

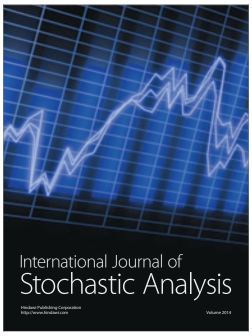

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization