Optimal Independent-Encoding Schemes for Input-Symmetric Degraded Broadcast Channels

Bike Xie, *Student Member, IEEE* and Richard D. Wesel, *Senior Member, IEEE*

Abstract— **An input-symmetric (IS) degraded broadcast channel (DBC) is a discrete DBC whose component channels are input-symmetric and the intersection of their input-symmetry groups is transitive. The discrete additive DBC and the group-additive DBC are IS-DBCs. This paper introduces an independent encoding scheme which employs permutation functions of the independent codes. This permutation encoding approach for the group-additive DBC is to employ group additions of the independent codes. This paper shows that the permutation encoding approach achieves the boundary of the capacity region for IS-DBCs, and yields a simple characterization of that capacity region.**

Index Terms— **Degraded broadcast channel, independent encoding, input-symmetric, group-additive degraded broadcast channel, permutation encoding approach.**

I. Introduction

In the 70's, Cover [1], Bergmans [2] and Gallager [3] established the capacity region for degraded broadcast channels (DBCs). The general optimal transmission strategy to achieve the boundary of the capacity region for degraded broadcast channels is a joint encoding scheme. Specifically, the data sent to the user with the most degraded channel is encoded first. Given the encoded bits for that user, an appropriate codebook for the second most degraded channel user is selected, and so forth. Cover [4] also introduced an independent-encoding scheme for general broadcast channels and provided the corresponding achievable rate region. This achievable rate region is not generally the capacity region for broadcast channels. However, combining independently encoded streams, one for each user, can achieve the boundary of the capacity region for some broadcast channels including broadcast Gaussian channels [5], broadcast binary-symmetric channels [2] [6] [7] [8], broadcast Z channels [9] [10] and so on.

Witsenhausen and Wyner made two seminal contributions in [7] and [8]: the notion of minimizing one entropy under the constraint that another related entropy is fixed and the use of input symmetry as a way of solving an entire class of channels with a single unifying approach. Benzel [11] used the first idea to study discrete additive degraded broadcast channels. Recently Liu and Ulukus [12] [13] used both ideas together to extend Benzels results to include the larger class of discrete degraded interference channels (DDIC). Our paper defines what it means for a degraded broadcast channel to be input-symmetric (IS) and applies the constrained entropy minimization approach to a new pair of conditional entropies to show that independent encoding achieves the capacity region of all input-symmetric DBCs.

Benzel [11] studied the discrete additive degraded interference channels (DADIC), whose corresponding DBC is the discrete additive DBC, and proved that the capacity regions for the DADIC is the same as the capacity region for the corresponding discrete additive DBC. Hence, the optimal encoding scheme for the discrete additive DBC is to employ discrete additions of independently encoded streams.

Liu and Ulukus proved that encoder cooperation does not increase the capacity region of DDICs that satisfy five conditions [12] [13]. For these DDICs, independent encoding can achieve the capacity region for the corresponding DBCs as long as the transmitted signal for the DBC can be appropriately defined. Our paper studies the class of input-symmetric DBCs, some of which are not covered in [12] [13]. For any IS-DBC, our paper provides an independent-encoding scheme and proves the independent-encoding scheme achieves the boundary of the capacity region.

The input-symmetric channel was introduced by Witsenhausen and Wyner [8] and studied in [12] [13] and [14]. This paper extends the definition of the input-symmetric channel to the definition of the input-symmetric DBC. This paper introduces an independent-encoding scheme employing permutation functions of independently encoded streams (the permutation encoding approach) for the input-symmetric DBC and proves its optimality. The discrete additive DBC [11] is a special case of the input-symmetric DBC, and the optimal encoding approach for the discrete additive DBC [11] is also a special case of the permutation encoding approach. The group-additive DBC is a class of input-symmetric DBCs whose channel outputs are group additions of the channel input and noise. The permutation encoding approach for the group-additive DBC is the group-addition encoding approach.

This paper is organized as follows: Section II provides definitions and states some results from [10] that will be useful. Section III defines the input-symmetric degraded broadcast channel and provides several examples including the group-additive DBC. Section IV shows that the uniform distribution is the optimal input distribution to achieve the boundary of the capacity region for IS-DBCs. Section V introduces the permutation encoding approach and proves that it achieves the capacity region for IS-DBCs. Section

This work was supported by the Defence Advanced Research Project Agency SPAWAR Systems Center, San Diego, California under Grant N66001-02-1-8938. This work was also supported by Rockwell Collins through contract #4502769987.
The authors are with the Electrical Engineering Department, University of California, Los Angeles, CA 90095 USA (e-mail:xbk@ee.ucla.edu; wesel@ee.ucla.edu).
This conference paper presents part of the ArXiv submission [10] which was submitted to IEEE Transactions on Information Theory. For more details, please refer to [10].

VI provides the conclusion.

II. Definitions and Preliminaries

Let $X \to Y \to Z$ be a discrete memoryless degraded broadcast channel where $X \in \{1, 2, \cdots, k\}$, $Y \in \{1, 2, \cdots, n\}$ and $Z \in \{1, 2, \cdots, m\}$. Let T_{YX} be an $n \times k$ stochastic matrix with entries $T_{YX}(j, i) = \Pr(Y = j | X = i)$ and T_{ZX} be an $m \times k$ stochastic matrix with entries $T_{ZX}(j, i) = \Pr(Z = j | X = i)$. Thus, T_{YX} and T_{ZX} are the marginal transition probability matrices of the DBC.

A. Conditional entropy bound F^*, DBC capacity regions

Let vector $\boldsymbol{q}$ in the simplex Δ_k of probability k-vectors be the distribution of the channel input X. For any $H(Y|X) \le s \le H(Y)$, define the function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ as the infimum of $H(Z|U)$ with respect to all discrete random variables U such that

- a) $H(Y|U) = s$;
- b) U and Y, Z are conditionally independent given X, i.e., the sequence U, X, Y, Z forms a Markov chain $U \to X \to Y \to Z$.

The function $F^*(\cdot)$ is an extension to the function $F(\cdot)$ introduced in [8]. We will use $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$, $F^*(\boldsymbol{q}, s)$ and $F^*(s)$ interchangeably.

Theorem 1: $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is jointly convex in $(\boldsymbol{q}, s)$ monotonically nondecreasing in s. The infimum in its definition is attainable. (See [10] for proof.)

Theorem 2: The capacity region for the discrete memoryless DBC $X \to Y \to Z$ is the closure of the convex hull of all rate pairs (R_1, R_2) satisfying

$$0 \le R_1 \le I(X; Y), \tag{1}$$

$$R_2 \le H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, R_1 + H(Y|X)), \tag{2}$$

for some $\boldsymbol{q} \in \Delta_k$. (See [10] for proof.)

B. Definitions of $\mathcal{C}$, $\mathcal{C}^*_{\boldsymbol{q}}$, and the (ξ, η)-plane for DBCs

For any choice of the integer $l \ge 1$, $\boldsymbol{w} = [w_1, \cdots, w_l]^T \in \Delta_l$ and $\boldsymbol{p}_j \in \Delta_k, j = 1, \cdots, l$, let U be an l-ary random variable with distribution $\boldsymbol{w}$, and let $T_{XU} = [\boldsymbol{p}_1, \cdots, \boldsymbol{p}_l]$ be the transition probability matrix from U to X. We can compute

$$\boldsymbol{p} = \boldsymbol{p}_X = T_{XU}\boldsymbol{w} = \sum_{j=1}^{l} w_j \boldsymbol{p}_j, \tag{3}$$

$$\xi = H(Y|U) = \sum_{j=1}^{l} w_j h_n(T_{YX}\boldsymbol{p}_j), \tag{4}$$

$$\eta = H(Z|U) = \sum_{j=1}^{l} w_j h_m(T_{ZX}\boldsymbol{p}_j), \tag{5}$$

where $h_n : \Delta_n \to \mathrm{R}$ is the entropy function, i.e., $h_n(p_1, \cdots, p_n) = -\sum p_i \ln p_i$.

Let $\mathcal{C}$ be the set of all $(\boldsymbol{p}, \xi, \eta)$ satisfying (3) (4) and (5) for some choice of l, $\boldsymbol{w}$ and $\boldsymbol{p}_j$. $\mathcal{C}$ is compact, connected, and convex. Let $\mathcal{C}^* = \{ (\xi, \eta) \,|\, (\boldsymbol{q}, \xi, \eta) \in \mathcal{C} \}$ be the projection of the set $\mathcal{C}$ onto the (ξ, η)-plane. Define

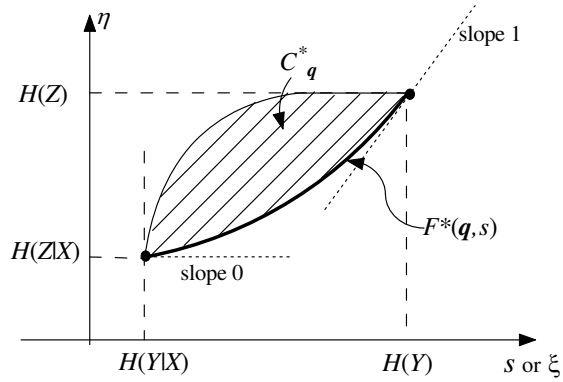

Fig. 1. The illustrations of the curve $F^*(\boldsymbol{q}, s) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ shown in bold and the region $\mathcal{C}^*_{\boldsymbol{q}}$.

$\mathcal{C}^*_{\boldsymbol{q}} = \{(\xi, \eta) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\}$ as the projection onto the (ξ, η)-plane of the subset of $\mathcal{C}$ where $\boldsymbol{p} = \boldsymbol{q}$. $\mathcal{C}^*$ and $\mathcal{C}^*_{\boldsymbol{q}}$ are also compact and convex. By definition, $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is the infimum of all η, for which $\mathcal{C}^*_{\boldsymbol{q}}$ contains the point (s, η). Fig. 1 shows how $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ forms a lower boundary of the region $\mathcal{C}^*_{\boldsymbol{q}}$.

III. Input-Symmetric Degraded Broadcast Channels

The input-symmetric channel was first introduced in [8] and further studied in [12] [13] [14]. The definition of the input-symmetric channel is as follows: Let Φ_n denote the symmetric group of permutations of n objects by the $n \times n$ permutation matrices. An n-input m-output channel with transition probability matrix $T_{m \times n}$ is input-symmetric if the set

$$\mathcal{G}_T = \{G \in \Phi_n | \exists \Pi \in \Phi_m, \text{ s.t. } TG = \Pi T\} \tag{6}$$

is transitive, which means each element of $\{1, \cdots, n\}$ can be mapped to every other element of $\{1, \cdots, n\}$ by some permutation matrix in $\mathcal{G}_T$ [8]. $\mathcal{G}_T$ is called an input-symmetry group if the channel $T_{m \times n}$ is input-symmetric. An important property of the input-symmetric channel is that the uniform distribution achieves capacity.

Extend the definition of the input-symmetric channel to the input-symmetric DBC as follows:

Definition 1: Input-Symmetric Degraded Broadcast Channel: A discrete memoryless DBC $X \to Y \to Z$ with $|\mathcal{X}| = k$, $|\mathcal{Y}| = n$ and $|\mathcal{Z}| = m$ is input-symmetric if the set

$$\mathcal{G}_{T_{YX},T_{ZX}} \triangleq \mathcal{G}_{T_{YX}} \cap \mathcal{G}_{T_{ZX}} \tag{7}$$

$$= \{G \in \Phi_k | \exists \Pi_{YX} \in \Phi_n, \Pi_{ZX} \in \Phi_m, \text{ s.t. } T_{YX}G = \Pi_{YX}T_{YX}, T_{ZX}G = \Pi_{ZX}T_{ZX}\} \tag{8}$$

is transitive.

Lemma 1: $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group under matrix multiplication.

Proof: Every closed subset of a group is a group. Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a subset of Φ_k, which is a group under matrix multiplication, it suffices to show that $\mathcal{G}_{T_{YX},T_{ZX}}$ is closed under matrix multiplication. Suppose $G_1, G_2 \in \mathcal{G}_{T_{YX},T_{ZX}}$

such that $T_{YX}G_1 = \Pi_{YX,1}T_{YX}$, $T_{ZX}G_1 = \Pi_{ZX,1}T_{ZX}$, $T_{YX}G_2 = \Pi_{YX,2}T_{YX}$ and $T_{ZX}G_2 = \Pi_{ZX,2}T_{ZX}$. Thus,

$$T_{YX}G_1G_2 = \Pi_{YX,1}\Pi_{YX,2}T_{YX}, \tag{9}$$

and

$$T_{ZX}G_1G_2 = \Pi_{ZX,1}\Pi_{ZX,2}T_{ZX}. \tag{10}$$

Therefore, $G_1G_2 \in \mathcal{G}_{T_{YX},T_{ZX}}$. Q.E.D.

Let $l = |\mathcal{G}_{T_{YX},T_{ZX}}|$ and $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$.

Lemma 2: $\sum_{i=1}^{l} G_i = \frac{l}{k}\mathbf{1}\mathbf{1}^T$, where $\frac{l}{k}$ is an integer and $\mathbf{1}$ is an all-ones vector.

Proof: Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group, for all $j = 1, \cdots, l$,

$$G_j\left(\sum_{i=1}^{l} G_i\right) = \sum_{i=1}^{l} G_jG_i = \sum_{i=1}^{l} G_i. \tag{11}$$

Hence, $\sum_{i=1}^{l} G_i$ has k identical columns and k identical rows since $\mathcal{G}_{T_{YX},T_{ZX}}$ is transitive. Thus, $\sum_{i=1}^{l} G_i = \frac{l}{k}\mathbf{1}\mathbf{1}^T$. Q.E.D.

Definition 2: A subset of $\mathcal{G}_{T_{YX},T_{ZX}}$: $\{G_{i_1}, \cdots, G_{i_{l_s}}\}$ is a smallest transitive subset of $\mathcal{G}_{T_{YX},T_{ZX}}$ if

$$\sum_{j=1}^{l_s} G_{i_j} = \frac{l_s}{k}\mathbf{1}\mathbf{1}^T, \tag{12}$$

where $\frac{l_s}{k}$ is the smallest possible integer for which (12) is satisfied.

A. Examples: binary-symmetric DBC and binary-erasure DBC

The class of input-symmetric DBCs includes most of the common discrete memoryless DBCs. For example, the binary-symmetric DBC $X \to Y \to Z$ with marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1-\alpha_1 & \alpha_1 \\ \alpha_1 & 1-\alpha_1 \end{bmatrix} \text{ and } T_{ZX} = \begin{bmatrix} 1-\alpha_2 & \alpha_2 \\ \alpha_2 & 1-\alpha_2 \end{bmatrix},$$

where $0 \le \alpha_1 \le \alpha_2 \le 1/2$, is input-symmetric since

$$\mathcal{G}_{T_{YX},T_{ZX}} = \left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right\} \tag{13}$$

is transitive.

Another interesting example is the binary-erasure DBC with marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1-a_1 & 0 \\ a_1 & a_1 \\ 0 & 1-a_1 \end{bmatrix} \text{ and } T_{ZX} = \begin{bmatrix} 1-a_2 & 0 \\ a_2 & a_2 \\ 0 & 1-a_2 \end{bmatrix},$$

where $0 \le a_1 \le a_2 \le 1$. It is input-symmetric since its $\mathcal{G}_{T_{YX},T_{ZX}}$ is the same as that of the binary-symmetric DBC as shown in (13).

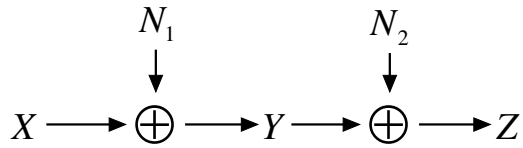

Fig. 2. The group-additive degraded broadcast channel.

B. Example: group-additive DBC

Definition 3: Group-additive Degraded Broadcast Channel: A degraded broadcast channel $X \to Y \to Z$ with $X, Y, Z \in \{1, \cdots, n\}$ is a group-additive degraded broadcast channel if there exist two n-ary random variables N_1 and N_2 such that $Y \sim X \oplus N_1$ and $Z \sim Y \oplus N_2$ as shown in Fig. 2, where $\sim$ denotes identical distribution and $\oplus$ denotes group addition.

The class of group-additive DBCs includes the binary-symmetric DBC and the discrete additive DBC [11] as special cases.

Theorem 3: Group-additive DBCs are input-symmetric.

Proof: For the group-additive DBC $X \to Y \to Z$ with $X, Y, Z \in \{1, \cdots, n\}$, let G_x for $x = 1, \cdots, n$, be 0-1 matrices with entries

$$G_x(i,j) = \begin{cases} 1 & \text{if } j \oplus x = i \\ 0 & \text{otherwise} \end{cases} \text{ for } i, j = 1, \cdots, n. \tag{14}$$

G_x for $x = 1, \cdots, n$, are actually permutation matrices and have the property that $G_{x_1} \cdot G_{x_2} = G_{x_2} \cdot G_{x_1} = G_{x_1 \oplus x_2}$. Let $(\gamma_0, \cdots, \gamma_{n-1})^T$ be the distribution of N_1. Since Y has the same distribution as $X \oplus N_1$, one has

$$T_{YX} = \sum_{x=1}^{n} \gamma_x G_x. \tag{15}$$

Hence, $T_{YX}G_x = G_xT_{YX}$ for all $x = 1, \cdots, n$. Similarly, we have $T_{ZX}G_x = G_xT_{ZX}$ for all $x = 1, \cdots, n$, and so

$$\{G_1, \cdots, G_n\} \subseteq \mathcal{G}_{T_{YX},T_{ZX}}. \tag{16}$$

Since the set $\{G_1, \cdots, G_n\}$ is transitive by definition, $\mathcal{G}_{T_{YX},T_{ZX}}$ is also transitive and hence the group-additive degraded broadcast channel is input-symmetric. Q.E.D.

By definition, $\sum_{j=1}^{n} G_j = \mathbf{1}\mathbf{1}^T$, and hence, $\{G_1, \cdots, G_n\}$ is a smallest transitive subset of $\mathcal{G}_{T_{YX},T_{ZX}}$ for the group-additive DBC.

C. Example: IS-DBC not covered in [12] [13]

The class of DDICs and the corresponding DBCs studied in [12] [13] have to satisfy the condition that the transition probability matrix T_{ZY} is input-symmetric, i.e., $\mathcal{G}_{T_{ZY}}$ is transitive. The input-symmetric DBC, however, does not have to satisfy this condition. The following example provides an IS-DBC which is not covered in [12] [13]. Consider a DBC $X \to Y \to Z$ with transition probability matrices

$$T_{YX} = \begin{bmatrix} a & c \\ b & d \\ c & a \\ d & b \end{bmatrix}, T_{ZY} = \begin{bmatrix} e & f & g & h \\ g & h & e & f \end{bmatrix},$$

and

$$T_{ZX} = T_{ZY}T_{YX} = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}, \tag{17}$$

where $a + c = b + d = 1$, $e + f + g + h = 1$, $\alpha = ae + bf + cg + dh$ and $\beta = ag + bh + ce + df$. This DBC is input-symmetric since its $\mathcal{G}_{T_{YX},T_{ZX}}$ is the same as that of the binary-symmetric DBC as shown in (13). It is not covered in [12] [13] because

$$\mathcal{G}_{T_{ZY}} = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\} \tag{18}$$

is *not* transitive.

IV. Optimal Input Distribution and Capacity Region

Consider the input-symmetric DBC $X \to Y \to Z$ with marginal transition probability matrices T_{YX} and T_{ZX}.

Lemma 3: For any permutation matrix $G \in \mathcal{G}_{T_{YX},T_{ZX}}$ and $(\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$, one has $(G\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$.

Proof: Since $(\boldsymbol{p}, \xi, \eta)$ satisfies (3) (4) and (5) for some choice of l, $\boldsymbol{w}$ and $\boldsymbol{p}_j$,

$$\sum_{j=1}^{l} w_j G\boldsymbol{p}_j = G\boldsymbol{p} \tag{19}$$

$$\sum_{j=1}^{l} w_j h_n(T_{YX}G\boldsymbol{p}_j) = \sum_{j=1}^{l} w_j h_n(\Pi_{YX}T_{YX}\boldsymbol{p}_j) = \xi \tag{20}$$

$$\sum_{j=1}^{l} w_j h_m(T_{ZX}G\boldsymbol{p}_j) = \sum_{j=1}^{l} w_j h_m(\Pi_{YX}T_{ZX}\boldsymbol{p}_j) = \eta. \tag{21}$$

Hence, $(G\boldsymbol{p}, \xi, \eta)$ satisfies (3) (4) and (5) for the choice of l, $\boldsymbol{w}$ and $G\boldsymbol{p}_j$,$j = 1, \cdots, l$. Q.E.D.

Corollary 1: $\forall \boldsymbol{p} \in \Delta_k$ and $G \in \mathcal{G}_{T_{YX},T_{ZX}}$, one has $\mathcal{C}^*_{G\boldsymbol{p}} = \mathcal{C}^*_{\boldsymbol{p}}$, and so $F^*(G\boldsymbol{p}, s) = F^*(\boldsymbol{p}, s)$ for any $H(Y|X) \leq s \leq H(Y)$.

Lemma 4: For any input-symmetric DBC, $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$, where $\boldsymbol{u}$ denotes the uniform distribution.

Proof: For any $(\xi, \eta) \in \mathcal{C}^*$, there exists a distribution $\boldsymbol{p}$ such that $(\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$. Let $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$. By Corollary 1, $(G_j\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$ for all $j = 1, \cdots, l$. By the convexity of the set $\mathcal{C}$,

$$(\boldsymbol{q}, \xi, \eta) = (\sum_{j=1}^{l} G_j\boldsymbol{p}\ , \xi, \eta) \in \mathcal{C}, \tag{22}$$

where $\boldsymbol{q} = \sum_{j=1}^{l} G_j\boldsymbol{p}$. Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group , for any permutation matrix $G' \in \mathcal{G}_{T_{YX},T_{ZX}}$,

$$G'\boldsymbol{q} = \sum_{j=1}^{l} G'G_j\boldsymbol{p} = \sum_{j=1}^{l} G_j\boldsymbol{p} = \boldsymbol{q}. \tag{23}$$

Since $G'\boldsymbol{q} = \boldsymbol{q}$, the ith entry and the jth entry of $\boldsymbol{q}$ are the same if G' permutes i^{th} row to j^{th} row. Since the set $\mathcal{G}_{T_{YX},T_{ZX}}$ for an input-symmetric DBC is transitive, all the entries of $\boldsymbol{q}$ are the same, and so $\boldsymbol{q} = \boldsymbol{u}$. This implies that $(\xi, \eta) \in \mathcal{C}^*_{\boldsymbol{u}}$. Since (ξ, η) is arbitrarily taken from $\mathcal{C}^*$, one has $\mathcal{C}^* \subseteq \mathcal{C}^*_{\boldsymbol{u}}$. On the other hand, by definition, $\mathcal{C}^* \supseteq \mathcal{C}^*_{\boldsymbol{u}}$. Therefore, $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$. Q.E.D.

Now we state and prove that the uniformly distributed X is optimal for input-symmetric DBCs.

Theorem 4: The capacity region of any input-symmetric DBC can be achieved by using a uniformly distributed X. As a consequence, the capacity region is

$$\begin{aligned} \bar{\text{co}}\Big\{(R_1, R_2) :& R_1 \leq s - h_n(T_{YX}\boldsymbol{e_1}), \\ & R_2 \leq h_m(T_{ZX}\boldsymbol{u}) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{u}, s), \\ & h_n(T_{YX}\boldsymbol{e_1}) \leq s \leq h_n(T_{YX}\boldsymbol{u})\Big\}, \end{aligned} \tag{24}$$

where $\boldsymbol{e_1} = (1, 0, \cdots, 0)^T$, $n = |\mathcal{Y}|$, and $m = |\mathcal{Z}|$.

Proof: Let $\boldsymbol{q} = (q_1, \cdots, q_k)^T$ be the distribution of the channel input X for the input-symmetric DBC $X \to Y \to Z$. Since $\mathcal{G}_{T_{YX}}$ is transitive, the columns of T_{YX} are permutations of each other. Thus,

$$H(Y|X) = \sum_{i=1}^{k} H(Y|X = i) \tag{25}$$

$$= \sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e_i}) \tag{26}$$

$$= \sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e_1}) \tag{27}$$

$$= h_n(T_{YX}\boldsymbol{e_1}), \tag{28}$$

which is independent of $\boldsymbol{q}$. Let $l = |\mathcal{G}_{T_{YX},T_{ZX}}|$ and $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$.

$$H(Z) = h_m(T_{ZX}\boldsymbol{q}) \tag{29}$$

$$= \frac{1}{l}\sum_{i=1}^{l} h_m(T_{ZX}\boldsymbol{q}) \tag{30}$$

$$= \frac{1}{l}\sum_{i=1}^{l} h_m(T_{ZX}G_i\boldsymbol{q}) \tag{31}$$

$$\leq h_m(T_{ZX}\frac{1}{l}\sum_{i=1}^{l} G_i\boldsymbol{q}) \tag{32}$$

$$= h_m(T_{ZX}\boldsymbol{u}), \tag{33}$$

where (32) follows from Jensen's inequality. Since $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$ for the input-symmetric DBC,

$$F^*(\boldsymbol{q}, s) \geq F^*(\boldsymbol{u}, s). \tag{34}$$

Plugging (28), (33) and (34) into Theorem 2, the capacity region for input-symmetric DBCs is

$$\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\big\{(R_1,R_2): R_1\le s-H(Y|X),$$
$$R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\big\}\Big] \quad (35)$$
$$\subseteq \bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\big\{(R_1,R_2): R_1\le s-h_n(T_{YX}\boldsymbol{e_1}),$$
$$R_2\le h_m(T_{ZX}\boldsymbol{u})-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\big\}\Big] \quad (36)$$
$$=\bar{\text{co}}\Big\{(R_1,R_2): R_1\le s-h_n(T_{YX}\boldsymbol{e_1}),$$
$$R_2\le h_m(T_{ZX}\boldsymbol{u})-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\Big\} \quad (37)$$
$$=\bar{\text{co}}\Big\{(R_1,R_2): \boldsymbol{p}_X=\boldsymbol{u}, R_1\le s-H(Y|X),$$
$$R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\Big\} \quad (38)$$
$$\subseteq \bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\big\{(R_1,R_2): R_1\le s-H(Y|X),$$
$$R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\big\}\Big], \quad (39)$$

Note that (35) and (39) are identical expressions, hence (35 - 39) are all equal. Therefore, (24) and (37) express the capacity region for the input-symmetric DBC, which also means that the capacity region can be achieved by using the transmission strategies such that the broadcast signal X is uniformly distributed. Q.E.D.

V. Optimality of Permutation Encoding

The permutation encoding approach is an independent-encoding scheme which achieves the capacity region for input-symmetric DBCs. The block diagram of this approach is shown in Fig. 3. In Fig. 3, W_1 is the message for User 1, which sees the better channel T_{YX}, and W_2 is the message for User 2, which sees the worse channel T_{ZX}. The permutation encoding approach is first to independently encode these two messages into two codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$, and then to combine these two independent codewords using a single-letter operation.

Let $\mathcal{G}_s$ be a smallest transitive subset of $\mathcal{G}_{T_{YX},T_{ZX}}$. Denote $k=|\mathcal{X}|$ and $l_s=|\mathcal{G}_s|$. Use a random coding technique to design the codebook for User 1 according to the k-ary random variable X_1 with distribution $\boldsymbol{p_1}$ and the codebook for User 2 according to the l-ary random variable X_2 with uniform distribution. Let $\mathcal{G}_s=\{G_1,\cdots,G_{l_s}\}$. Define the permutation function $g_{x_2}(x_1)=x$ if the permutation matrix G_{x_2} maps the x_1^{th} column to the xth column, where $x_2\in\{1,\cdots,l_s\}$ and $x,x_1\in\{1,\cdots,k\}$. Hence, $g_{x_2}(x_1)=x$ if and only if the x_1^{th} row, x^{th} column entry of G_{x_2} is 1. The permutation encoding approach is then to broadcast $\boldsymbol{X}$ which is obtained by applying the single-letter permutation function $X=g_{X_2}(X_1)$ on symbols of codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$. Since X_2 is uniformly distributed and $\sum_{j=1}^{l_s}G_j=\frac{l_s}{k}\boldsymbol{1}\boldsymbol{1}^T$, the broadcast signal X is also uniformly distributed.

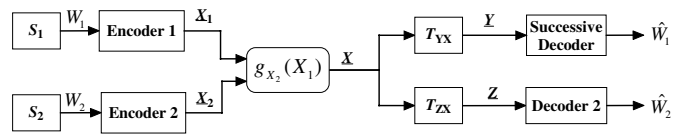

Fig. 3. The block diagram of the permutation encoding approach

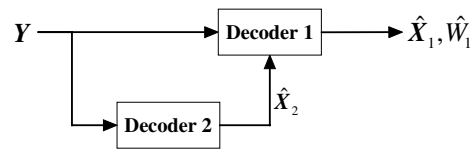

Fig. 4. The structure of the successive decoder for input-symmetric DBCs

User 2 receives $\boldsymbol{Z}$ and decodes the desired message directly. User 1 receives $\boldsymbol{Y}$ and successively decodes the message for User 2 and then for User 1. The structure of the successive decoder is shown in Fig. 4. Note that Decoder 1 in Fig. 4 is *not* a joint decoder even though it has two inputs $\boldsymbol{Y}$ and $\boldsymbol{\hat{X}_2}$.

In particular, for the group-additive DBC with $Y\sim X\oplus N_1$ and $Z\sim Y\oplus N_2$, the permutation function $g_{x_2}(x_1)$ is the group addition $x_2\oplus x_1$. Hence the permutation encoding approach for the group-additive DBC is the group-addition encoding approach, which independently encodes the message for each of the two users and broadcasts the group addition of the two resulting codewords. The successive decoder for the group-additive DBC is shown in Fig. 5, where

$$\tilde{y}=y\oplus(-\hat{x}_2). \quad (40)$$

From the coding theorem for DBCs [2] [3], the achievable region of the permutation encoding approach for the input-

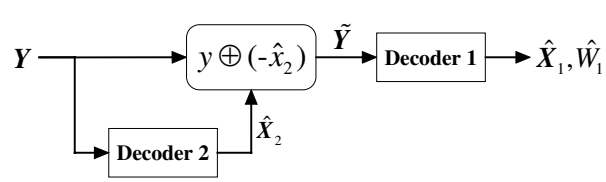

Fig. 5. The structure of the successive decoder for group-additive DBCs

symmetric DBC is determined by

$$
\begin{aligned}
R_1 &\le I(X;Y|X_2) && (41)\\
&= H(Y|X_2) - H(Y|X) && (42)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) H(Y|X_2 = x_2) \\
&\qquad - \sum_{x=1}^{k} \Pr(X = x) H(Y|X = x) && (43)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_n(T_{YX} G_{x_2} \boldsymbol{p_1}) \\
&\qquad - \sum_{x=1}^{k} \Pr(X = x) h_n(T_{YX} \boldsymbol{e}_x) && (44)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_n(\Pi_{YX,x_2} T_{YX} \boldsymbol{p_1}) \\
&\qquad - \sum_{x=1}^{k} \Pr(X = x) h_n(T_{YX} \boldsymbol{e}_1) && (45)\\
&= h_n(T_{YX} \boldsymbol{p_1}) - h_n(T_{YX} \boldsymbol{e}_1), && (46)
\end{aligned}
$$

and

$$
\begin{aligned}
R_2 &\le I(X_2;Z) && (47)\\
&= H(Z) - H(Z|X_2) && (48)\\
&= h_m(T_{ZX}\boldsymbol{u}) - \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_m(T_{ZX} G_{x_2} \boldsymbol{p_1}) && (49)\\
&= h_m(T_{ZX}\boldsymbol{u}) - \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_m(\Pi_{ZX,x_2} T_{ZX} \boldsymbol{p_1}) && (50)\\
&= h_m(T_{ZX}\boldsymbol{u}) - h_m(T_{ZX}\boldsymbol{p_1}), && (51)\\
& && (52)
\end{aligned}
$$

where $\boldsymbol{u}$ is the k-ary uniform distribution, $\boldsymbol{p}_1$ is the distribution of X_1, and $\boldsymbol{e}_x$ is a 0-1 vector such that the xth entry is 1 and all other entries are 0. Hence, the achievable region is

$$
\begin{aligned}
\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p_1} \in \Delta_k} \big\{ (R_1, R_2) : R_1 &\le h_n(T_{YX}\boldsymbol{p_1}) - h_n(T_{YX}\boldsymbol{e_1}), \\
R_2 &\le h_m(T_{ZX}\boldsymbol{u}) - h_m(T_{ZX}\boldsymbol{p_1}) \big\} \Big] && (53)
\end{aligned}
$$

Define $\tilde{F}(s)$ as the infimum of $h_m(T_{ZX}\boldsymbol{p_1})$ with respect to all distributions $\boldsymbol{p_1}$ such that $h_n(T_{YX}\boldsymbol{p_1}) = s$. Hence the achievable region (53) can be expressed as

$$
\begin{aligned}
\big\{ (R_1, R_2) : & R_1 \le s - h_n(T_{YX}\boldsymbol{e_1}), \\
& R_2 \le h_m(T_{ZX}\boldsymbol{u}) - \underline{\text{env}}\tilde{F}(s), \\
& h_n(T_{YX}\boldsymbol{e_1}) \le s \le h_n(T_{YX}\boldsymbol{u}) \big\}, && (54)
\end{aligned}
$$

where $\underline{\text{env}}\tilde{F}(s)$ denotes the lower convex envelope of $\tilde{F}(s)$. In order to show that the achievable region (54) is the same as the capacity region (24) for the input-symmetric DBC, it suffices to show that

$$
\underline{\text{env}}\tilde{F}(s) \le F^*(\boldsymbol{u}, s) \qquad (55)
$$

For any $U \to X$ with uniformly distributed X,

$$
\begin{aligned}
H(Z|U) &= \sum_u \Pr(U = u) H(Z|U = u) && (56)\\
&= \sum_u \Pr(U = u) h_m(T_{ZX} \boldsymbol{p}_{X|U=u}) && (57)\\
&\ge \sum_u \Pr(U = u) \tilde{F}(h_n(T_{YX} \boldsymbol{p}_{X|U=u})) && (58)\\
&\ge \sum_u \Pr(U = u) \underline{\text{env}}\tilde{F}(h_n(T_{YX} \boldsymbol{p}_{X|U=u})) && (59)\\
&\ge \underline{\text{env}}\tilde{F}(\sum_u \Pr(U = u) h_n(T_{YX} \boldsymbol{p}_{X|U=u})) && (60)\\
&= \underline{\text{env}}\tilde{F}(H(Y|U)), && (61)
\end{aligned}
$$

where $\boldsymbol{p}_{X|U=u}$ is the conditional distribution of X given $U = u$. Some of these steps are justified as follows:

- (58) follows from the definition of $\tilde{F}(s)$;
- (60) follows from Jensen's inequality.

Therefore, by definition, $\underline{\text{env}}\tilde{F}(s) \le F^*(\boldsymbol{u}, s)$.

The results of this subsection may be summarized in the following theorem.

Theorem 5: The permutation encoding approach achieves the boundary of the capacity region for input-symmetric DBCs. The capacity region is expressed in (24), (53), and (54).

Corollary 2: The group-addition encoding approach achieves the boundary of the capacity region for group-additive degraded broadcast channels.

VI. Conclusion

A discrete degraded broadcast channel $X \to Y \to Z$ is input-symmetric if the input-symmetry group $\mathcal{G}_{T_{YX}, T_{ZX}}$ is transitive. The IS-DBC includes the binary-symmetric DBC, the discrete additive DBC and the group-additive DBC. The permutation encoding approach for IS-DBCs is an independent encoding scheme which employs permutation functions of the independently encoded streams. This permutation encoding approach for the group-additive DBC is the group-addition encoding approach, which employs group additions of the independently encoded streams. The permutation encoding approach achieves the boundary of the capacity region for IS-DBCs. The capacity

region is

$$\begin{aligned}
&\bar{\text{co}}\Big\{(R_1,R_2):R_1 \le s - h_n(T_{YX}\boldsymbol{e_1}),\\
&\qquad\qquad R_2 \le h_m(T_{ZX}\boldsymbol{u}) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s),\\
&\qquad\qquad h_n(T_{YX}\boldsymbol{e_1}) \le s \le h_n(T_{YX}\boldsymbol{u})\Big\}\\
&= \bar{\text{co}}\Big[\bigcup_{\boldsymbol{p_1}\in\Delta_k}\big\{(R_1,R_2): R_1 \le h_n(T_{YX}\boldsymbol{p_1}) - h_n(T_{YX}\boldsymbol{e_1}),\\
&\qquad\qquad R_2 \le h_m(T_{ZX}\boldsymbol{u}) - h_m(T_{ZX}\boldsymbol{p_1})\big\}\Big].
\end{aligned}$$

References

[1] T. M. Cover. Broadcast channels. *IEEE Trans. Inform. Theory*, IT-18:2–14, January 1972.

[2] P. P. Bergmans. Random coding theorem for broadcast channels with degraded components. *IEEE Trans. Inform. Theory*, IT-19:197–207, March 1973.

[3] R. G. Gallager. Capacity and coding for degraded broadcast channels. *Probl. Pered. Inform.*, 10:3–14, July–Sept. 1974.

[4] T. M. Cover. An chievable rate region for the broadcast channel. *IEEE Trans. Inform. Theory*, IT-21:399–404, 1975.

[5] P. P. Bergmans. A simple converse for broadcast channels with additive white Gaussian noise. *IEEE Trans. Inform. Theory*, IT-20:279–280, March 1974.

[6] A. D. Wyner. A theorem on the entropy of certain binary sequences and applications: Part II. *IEEE Trans. Inform. Theory*, IT-19:772–777, Nov 1973.

[7] H. Witsenhausen. Entropy inequalities for discrete channels. *IEEE Trans. Inform. Theory*, IT-20(5):610–616, Sep 1974.

[8] H. Witsenhausen and A. Wyner. A conditional entropy bound for a pair of discrete random variables. *IEEE Trans. Inform. Theory*, IT-21(5):493–501, Sep 1975.

[9] B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel. Optimal transmission strategy and explicit capacity region for broadcast Z channels. *IEEE Trans. Inform. Theory*, 53:4296–4304, 2008.

[10] B. Xie and R. D. Wesel. Optimal Independent-Encoding Schemes for Several Classes of Discrete Degraded Broadcast Channels. *submitted to IEEE Trans. Inform. Theory and ArXiv:0811.4162v3*, Feb. 5 2009.

[11] R. Benzel. The capacity region of a class of discrete additive degraded interference channels. *IEEE Trans. Inform. Theory*, IT-25:228–231, 1979.

[12] N. Liu and S. Ulukus. The capacity region of a class of discrete degraded interference channels. In *Information Theory and Applications 2007*, UCSD, San Diego, USA, Jan 29-Feb 2 2007.

[13] N. Liu and S. Ulukus. The capacity region of a class of discrete degraded interference channels. *IEEE Trans. Inform. Theory*, 54(9):4372–4378, Sep 2008.

[14] B. Xie and R. D. Wesel. A mutual information invariance approach to symmetry in discrete memoryless channels. In *Information Theory and Application 2008*, UCSD, San Diego, USA, Jan. 27-Feb. 1 2008.