# Optimal Natural Encoding Scheme for Discrete Multiplicative Degraded Broadcast Channels

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

*Abstract*— **Certain degraded broadcast channels (DBCs) have the property that the boundary of the capacity region can be achieved by an encoder that combines independent codebooks (one for each receiver) using the same single-letter function that adds distortion to the channel. We call this the natural encoder for the DBC. Natural encoders are known to achieve the capacity region boundary of the broadcast Gaussian channel, and the broadcast binary-symmetric channel. Recently, they have also been shown to achieve the capacity region of the broadcast Z channel. This paper shows that natural encoding achieves the capacity region boundary for discrete multiplicative DBCs. The optimality of the natural encoder also leads to a relatively simple expression for the capacity region for discrete multiplicative DBCs.**

*Index Terms*— **Conditional entropy bound, degraded broadcast channel, discrete multiplicative degraded broadcast channel, natural encoding**

## 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 DBCs is a joint encoding scheme. Certain DBCs have the property that the boundary of the capacity region can be achieved by an encoder that combines independent codebooks (one for each receiver) using the same single-letter function that adds distortion to the channel. We call this the natural encoder for the DBC. Natural encoders are known to achieve the capacity region boundary of the broadcast Gaussian channel [4], the broadcast binary-symmetric channel [2] [5], and discrete additive DBCs [6]. Recently, natural encoding has also been shown to achieve the capacity region of the two-user broadcast Z channel [7].

The discrete multiplicative degraded broadcast channel (DM-DBC) is a discrete DBC whose channel outputs are discrete multiplications (multiplications in a finite field) of the channel input and noise. This paper decomposes the DM-DBC into a group-additive DBC with an extra erasure (zero) symbol. Based on this decomposition, this paper studies a conditional entropy bound for the DM-DBC, and proves that the natural encoding approach achieves the boundary of the capacity region for DM-DBCs.

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 [8] which will be submitted to IEEE transaction on information theory. For more details, please refer to [8].

This paper is organized as follows: Section II provides definitions and states some results from [8] that will be useful. Section III defines the discrete multiplicative DBC and decomposes it into a group-additive DBC with an extra erasure (zero) symbol. Section IV computes the optimal input distribution to achieve the boundary of the capacity region for DM-DBCs. Section V introduces the natural encoding approach and proves that it achieves the capacity region for DM-DBCs. Section VI provides the conclusion.

## II. Definitions and Preliminaries

Let $X \rightarrow Y \rightarrow Z$ be a discrete memoryless DBC 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

Our results depend heavily on the function $F^*$, which we will now define. Let vector $\boldsymbol{q}$ in the simplex $\Delta_k$ of probability $k$-vectors be the distribution of the channel input $X$. For any $H(Y|X) \leq s \leq H(Y)$, 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 $U \rightarrow X \rightarrow Y \rightarrow Z$.

The function $F^*(\cdot)$ is an extension to the function $F(\cdot)$ introduced in [5]. 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 $(\boldsymbol{q}, s)$, and nondecreasing in $s$. The infimum in its definition is attainable. (See [8] for proof.)

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

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

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

for some $\boldsymbol{q} \in \Delta_k$. (See [8] for proof.)

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

For any choice of the integer $l \geq 1$, $\boldsymbol{w} = [w_1, \cdots, w_l]^T \in \Delta_l$ 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 $h_n : \Delta_n \rightarrow \mathrm{R}$ 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 $(\xi,\eta)$-plane. Define $\mathcal{C}^*_{\boldsymbol{q}} = \{(\xi,\eta)|(\boldsymbol{q},\xi,\eta) \in \mathcal{C}\}$ as the projection onto the $(\xi,\eta)$-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 $\eta$, for which $\mathcal{C}^*_{\boldsymbol{q}}$ contains the point $(s,\eta)$. Fig. 1(a) shows how $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ forms a lower boundary of the region $\mathcal{C}^*_{\boldsymbol{q}}$.

### C. U's that achieve $F^*$ and optimal U's for DBCs

In Fig. 1(a), the line with slope $\lambda$ in the $(\xi,\eta)$-plane supporting $\mathcal{C}^*_{\boldsymbol{q}}$ has the equation $\eta = \lambda\xi + \psi(\boldsymbol{q},\lambda)$, where $\psi(\boldsymbol{q},\lambda)$ is the $\eta$-intercept of the tangent line with slope $\lambda$ for $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$. Let $\phi(\boldsymbol{q},\lambda) = h_m(T_{ZX}\boldsymbol{q}) - \lambda h_n(T_{YX}\boldsymbol{q})$. As illustrated in Fig. 1(b), $\psi(\boldsymbol{q},\lambda)$ is the lower convex envelope of $\phi(\boldsymbol{q},\lambda)$ on $\Delta_k$ as shown in [8]. For any $\lambda \geq 0$, the associated point on the boundary of the capacity region may be found (from its unique value of $R_2 + \lambda R_1$) as follows

$$\begin{aligned}
&\max_{\boldsymbol{q}\in\Delta_k} \max\{R_2 + \lambda R_1 | \boldsymbol{p}_X = \boldsymbol{q}\} \\
&= \max_{\boldsymbol{q}\in\Delta_k} \max\{H(Z) - F^*(\boldsymbol{q}, s) + \lambda s - \lambda H(Y|X)\} \\
&= \max_{\boldsymbol{q}\in\Delta_k} (H(Z) - \lambda H(Y|X) - \min\{F^*(\boldsymbol{q}, s) - \lambda s\}) \\
&= \max_{\boldsymbol{q}\in\Delta_k} (H(Z) - \lambda H(Y|X) - \psi(\boldsymbol{q},\lambda)).
\end{aligned} \tag{6}$$

*Theorem 3:* This theorem has two parts:

i) For any fixed $0 \leq \lambda \leq 1$, if a point of the graph of $\psi(\cdot,\lambda)$ is the convex combination of $l$ points of the graph of $\phi(\cdot,\lambda)$ with arguments $\boldsymbol{p}_j$ and weights $w_j$ for $j = 1, \cdots, l$, then

$$F^*\Big(\sum_j w_j \boldsymbol{p}_j, \sum_j w_j h_n(T_{YX}\boldsymbol{p}_j)\Big) = \sum_j w_j h_m(T_{ZX}\boldsymbol{p}_j).$$

Furthermore, for a fixed input distribution $\boldsymbol{q} = \sum_j w_j \boldsymbol{p}_j$, the optimal transmission strategy to achieve the maximum of $R_2 + \lambda R_1$ is determined by $l$,$w_j$ and $\boldsymbol{p}_j$. In particular, the optimal transmission strategy is $|\mathcal{U}| = l$, $\Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$, where $\boldsymbol{p}_{X|U=j}$ denotes the conditional distribution of $X$ given $U = j$.

ii) For a predetermined channel input distribution $\boldsymbol{q}$, if the transmission strategy $|\mathcal{U}| = l$, $\Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$ achieves $\max\{R_2 + \lambda R_1 | \sum_j w_j \boldsymbol{p}_j = \boldsymbol{q}\}$, then the point $(\boldsymbol{q}, \psi(\boldsymbol{q},\lambda))$ is the convex combination of $l$ points of the graph of $\phi(\cdot,\lambda)$ with arguments $\boldsymbol{p}_j$ and weights $w_\lambda$ for $j = 1, \cdots, l$. (See [8] for proof.)

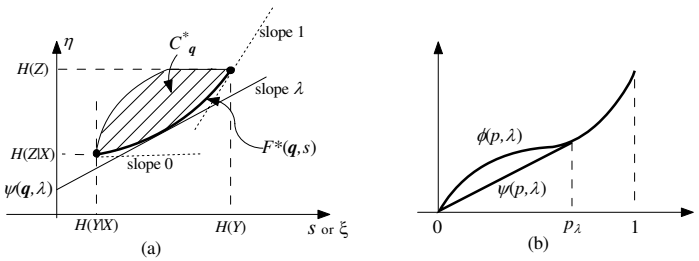


Fig. 1. (a) The illustrations of the curve $F^*(\boldsymbol{q}, s)$ shown in bold, the region $\mathcal{C}^*_{\boldsymbol{q}}$, and the point $(0, \psi(\boldsymbol{q},\lambda))$, (b) The illustrations of $\phi(\cdot,\lambda)$ and $\psi(\cdot,\lambda)$ for the broadcast Z channel.

### D. Example: the two-user broadcast Z channel

An important example, because of the decomposition we will apply to the discrete multiplicative DBC, is the broadcast Z channel with marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1 & \alpha_1 \\ 0 & \beta_1 \end{bmatrix} \text{ and } T_{ZX} = \begin{bmatrix} 1 & \alpha_2 \\ 0 & \beta_2 \end{bmatrix}, \tag{7}$$

where $0 < \alpha_1 \leq \alpha_2 < 1$, $\beta_1 + \alpha_1 = \beta_2 + \alpha_2 = 1$.

Let $\beta_\Delta \triangleq \beta_2/\beta_1$. For $\beta_\Delta \leq \lambda \leq 1$, $\phi''(p,\lambda) \geq 0$ for all $0 \leq p \leq 1$. Therefore, $\phi(p,\lambda)$ is convex in $p$ and thus $\phi(p,\lambda) = \psi(p,\lambda)$ for all $0 \leq p \leq 1$. For $0 \leq \lambda < \beta_\Delta$, $\phi(p,\lambda)$ is concave in $p$ for $p \in [\,0, \frac{\beta_2 - \lambda\beta_1}{\beta_1\beta_2(1-\lambda)}\,]$ and convex in $p$ for $p \in [\frac{\beta_2 - \lambda\beta_1}{\beta_1\beta_2(1-\lambda)}, 1]$. The graph of $\phi(\cdot,\lambda)$ in this case is shown in Fig. 1(b). Since $\phi(0,\lambda) = 0$, $\psi(\cdot,\lambda)$, the lower convex envelope of $\phi(\cdot,\lambda)$, is constructed by drawing the tangent through the origin. Let $(p_\lambda, \phi(p_\lambda,\lambda))$ be the point of contact. The value of $p_\lambda$ is determined by the equation $\phi'_p(p_\lambda,\lambda) = \phi(p_\lambda,\lambda)/p_\lambda$, i.e.,

$$\ln(1 - \beta_2 p_\lambda) = \lambda \ln(1 - \beta_1 p_\lambda). \tag{8}$$

### E. Input-symmetric degraded broadcast channels

Let $\Phi_n$ denote the set of all $n \times n$ permutation matrices. An $n$-input $m$-output channel with transition probability matrix $T_{m\times n}$ is input-symmetric if the set

$$\mathcal{G}_T = \{G \in \Phi_n | \exists \Pi \in \Phi_m, \text{ s.t. } TG = \Pi T\}, \tag{9}$$

where $\Pi$ and $G$ are permutation matrices, 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 $\mathcal{G}_T$ [5] [9]. An important property of input-symmetric channel is that the uniform distribution achieves capacity.

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

$$\mathcal{G}_{T_{YX},T_{ZX}} \triangleq \mathcal{G}_{T_{YX}} \cap \mathcal{G}_{T_{ZX}} \tag{10}$$

$$= \big\{G \in \Phi_k | \exists \Pi_{YX} \in \Phi_n, \Pi_{ZX} \in \Phi_m, \text{ s.t. } T_{YX}G = \Pi_{YX}T_{YX}, T_{ZX}G = \Pi_{ZX}T_{ZX}\big\} \tag{11}$$

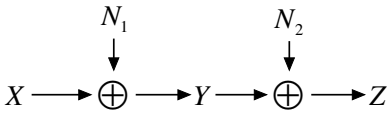


Fig. 2. The group-additive degraded broadcast channel.

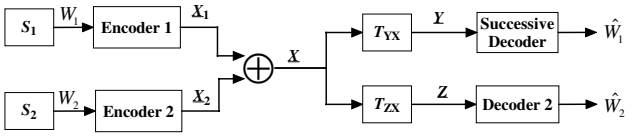


Fig. 3. The group-addition encoding approach.

is transitive.

*Lemma 1:* For any permutation matrix $G \in \mathcal{G}_{T_{YX},T_{ZX}}$ and $(\boldsymbol{p},\xi,\eta) \in \mathcal{C}$, one has $(G\boldsymbol{p},\xi,\eta) \in \mathcal{C}$. (See [8] for proof.)

*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 $H(Y|X) \le s \le H(Y)$. (See [8] for proof.)

*Corollary 2:* A uniform distribution on the alphabet of $X$ achieves the capacity region of any input-symmetric DBC. (See [8] for proof.)

## III. Group-additive and Multiplicative DBCs

### A. Group-additive DBC

*Definition 2:* Group-additive (GA) Degraded Broadcast Channel: A DBC $X \to Y \to Z$ with $X,Y,Z \in \{1,\cdots,n\}$ is a group-additive DBC 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 group-additive DBC is input-symmetric. It includes the broadcast binary-symmetric channel and the discrete additive degraded broadcast channel [6] as special cases.

Fig. 3 shows the group-addition encoding approach, which is to independently encode the message for each of the two users and broadcast the group addition of the two resulting codewords. The group-addition encoding approach achieves the boundary of capacity region for GA-DBCs [8].

### B. Discrete multiplicative DBC

*Definition 3:* Discrete Multiplicative Degraded Broadcast Channel: A discrete memoryless DBC $X \to Y \to Z$ with $X,Y,Z \in \{0,1,\cdots,n\}$ is a discrete multiplicative DBC if there exist two $(n+1)$-ary random variables $N_1$ and $N_2$ such that $Y \sim X \otimes N_1$ and $Z \sim Y \otimes N_2$ as shown in Fig. 4, where $\otimes$ denotes discrete multiplication.

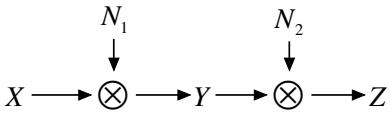


Fig. 4. The discrete multiplicative degraded broadcast channel.

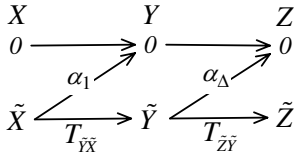


Fig. 5. The channel structure of a discrete multiplicative degraded broadcast channel.

By the definition of field and group, the discrete multiplication of zero and any element in $\{0,1,\cdots,n\}$ is always zero. Also $\{1,\cdots,n\}$ forms a group under discrete multiplication. Hence, the DM-DBC $X \to Y \to Z$ has the channel structure as shown in Fig. 5. The sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$ is a GA-DBC with marginal distributions $T_{\tilde{Y}\tilde{X}}$ and $T_{\tilde{Z}\tilde{X}} = T_{\tilde{Z}\tilde{Y}}T_{\tilde{Y}\tilde{X}}$, where $\tilde{\mathcal{X}}$, $\tilde{\mathcal{Y}}$, $\tilde{\mathcal{Z}} = \{1,\cdots,n\}$. For the DM-DBC $X \to Y \to Z$, if the channel input $X$ is zero, then the channel outputs $Y$ and $Z$ are zeros. If the channel input is a non-zero symbol, the channel output $Y$ is zero with probability $\alpha_1$ and $Z$ is zero with probability $\alpha_2$, where $\alpha_2 = \alpha_1 + (1-\alpha_1)\alpha_\Delta$. Therefore, the marginal transmission probability matrices for $X \to Y \to Z$ are

$$T_{YX} = \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1)T_{\tilde{Y}\tilde{X}} \end{bmatrix}, \tag{12}$$

$$T_{ZY} = \begin{bmatrix} 1 & \alpha_\Delta \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_\Delta)T_{\tilde{Z}\tilde{Y}} \end{bmatrix}, \tag{13}$$

and

$$\begin{aligned} T_{ZX} = T_{ZY}T_{YX} &= \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1)T_{\tilde{Y}\tilde{X}} \end{bmatrix} \begin{bmatrix} 1 & \alpha_\Delta \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_\Delta)T_{\tilde{Z}\tilde{Y}} \end{bmatrix} \\ &= \begin{bmatrix} 1 & \alpha_2 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_2)T_{\tilde{Z}\tilde{Y}} \end{bmatrix}, \end{aligned} \tag{14}$$

where $\mathbf{1}$ is an all-one vector and $\mathbf{0}$ is an all-zero vector.

## IV. Optimal Input Distribution for DM-DBCs

The sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$ is a group-additive DBC, which is input-symmetric, and hence, $\mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$ is transitive. For any $n \times n$ permutation matrix $\tilde{G} \in \mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$ with $T_{\tilde{Y}\tilde{X}}\tilde{G} = \Pi_{\tilde{Y}\tilde{X}}T_{\tilde{Y}\tilde{X}}$ and $T_{\tilde{Z}\tilde{X}}\tilde{G} = \Pi_{\tilde{Z}\tilde{X}}T_{\tilde{Z}\tilde{X}}$, the $(n+1)\times(n+1)$ permutation matrix

$$G = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G} \end{bmatrix} \tag{15}$$

has

$$T_{YX}G = \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1)T_{\tilde{Y}\tilde{X}} \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G} \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \Pi_{\tilde{Y}\tilde{X}} \end{bmatrix} T_{YX} \tag{16}$$

and so $G \in \mathcal{G}_{T_{YX}}$. Similarly, $G \in \mathcal{G}_{T_{ZX}}$, and hence $G \in \mathcal{G}_{T_{YX},T_{ZX}}$. Therefore, any non-zero element in $\{0,1,\cdots,n\}$ can be mapped to any other non-zero element in $\{0,1,\cdots,n\}$ by some permutation matrix in $\mathcal{G}_{T_{YX},T_{ZX}}$, however, no matrix in $\mathcal{G}_{T_{YX},T_{ZX}}$ maps zero to non-zero element or non-zero element to zero. Hence, any permutation matrix $G \in \mathcal{G}_{T_{YX},T_{ZX}}$ has the structure (15) for

some $\tilde{G} \in \mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$. These results are summarized in the following Lemma:

*Lemma 2:* Let $\mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}} = \{\tilde{G}_1, \cdots, \tilde{G}_l\}$. Hence, $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$, where

$$G_j = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G}_j \end{bmatrix}, \text{ for } j = 1, \ldots, l. \tag{17}$$

Now we state and prove that the uniform distributed $\tilde{X}$ is optimal for the DM-DBC.

*Lemma 3:* Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}}) \in \Delta_{n+1}$ be the distribution of channel input $X$, where $\boldsymbol{p}_{\tilde{X}}$ is the distribution of $\tilde{X}$. For any DM-DBC, $\mathcal{C}^*_{\boldsymbol{p}_X} \subseteq \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$ and $\mathcal{C}^* = \bigcup_{q\in[0,1]} \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$, where $\boldsymbol{u} \in \Delta_n$ denotes the uniform distribution. (See [8] for proof.)

*Theorem 4:* The capacity region of the DM-DBC can be achieved by using the transmission strategies such that $\tilde{X}$ is uniformly distributed, i.e., the distribution of $X$ has $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$. As a consequence, the capacity region is the convex hull of the closure of all $(R_1, R_2)$ satisfying

$$\begin{aligned} R_1 \leq & s - qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}), & (18)\\ R_2 \leq & h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) \\ & - F^*_{T_{YX},T_{ZX}}((1-q, q\boldsymbol{u}^T)^T, s), & (19) \end{aligned}$$

for some $0 \leq q \leq 1$ and

$$qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}) \leq s \leq h((1-\alpha_1)q) + (1-\alpha_1)q\ln(n).$$

*Proof*: Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}})^T$ be the distribution of the channel input $X$, where $\boldsymbol{p}_{\tilde{X}} = (p_1, \cdots, p_n)^T$. Since $\mathcal{G}_{T_{\tilde{Y}\tilde{X}}}$ is transitive and the columns of $T_{\tilde{Y}\tilde{X}}$ are permutations of each other,

$$\begin{aligned} H(Y|X) &= \sum_{i=0}^{n} H(Y|X=i) & (20)\\ &= (1-q)H(Y|X=0) + \sum_{i=1}^{n} qp_i h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_i}) & (21)\\ &= \sum_{i=1}^{n} qp_i h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}) & (22)\\ &= qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}), & (23) \end{aligned}$$

which is independent with $\boldsymbol{p}_X$. Let $\mathcal{G}_{T_{YX},T_{ZX}}=\{G_1,\cdots,G_l\}$.

$$\begin{aligned} H(Z) &= h_{n+1}(T_{ZX}\boldsymbol{p}_X) & (24)\\ &= \frac{1}{l}\sum_{i=1}^{l} h_{n+1}(T_{ZX}G_i\boldsymbol{p}_X) & (25)\\ &\leq h_{n+1}(T_{ZX}\frac{1}{l}\sum_{i=1}^{l} G_i\boldsymbol{p}_X) & (26)\\ &= h_{n+1}\left(T_{ZX}(1-q, q\boldsymbol{u}^T)^T\right) & (27)\\ &= h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) & (28) \end{aligned}$$

where (26) follows from Jensen's inequality. Since $\mathcal{C}^*_{\boldsymbol{p}_X} \subseteq \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$ from Lemma 3,

$$F^*(\boldsymbol{p}_X, s) \geq F^*((1-q, q\boldsymbol{u}^T)^T, s). \tag{29}$$

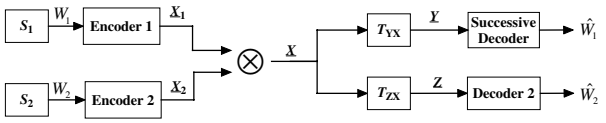


Fig. 6. The natural encoding approach for DM-DBCs.

Plugging (23), (28) and (29) into Theorem 2, the capacity region for DM-DBCs is

$$\begin{aligned} & \bar{\text{co}}\Big[ \bigcup_{\boldsymbol{p}_X\in\Delta_k} \big\{(R_1,R_2): R_1 \leq s - H(Y|X), \\ & \qquad R_2 \leq H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)\big\}\Big] & (30)\\ \subseteq\ & \bar{\text{co}}\Big[ \bigcup_{\boldsymbol{p}_X\in\Delta_k} \big\{(R_1,R_2): R_1 \leq s - h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}), \\ & \qquad R_2 \leq h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) \\ & \qquad\quad - F^*_{T_{YX},T_{ZX}}((1-q, q\boldsymbol{u}^T)^T, s)\big\}\Big] & (31)\\ =\ & \bar{\text{co}}\Big[ \bigcup_{q\in[0,1]} \big\{(R_1,R_2): R_1 \leq s - qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}), \\ & \qquad R_2 \leq h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) \\ & \qquad\quad - F^*_{T_{YX},T_{ZX}}((1-q, q\boldsymbol{u}^T)^T, s)\big\}\Big] & (32)\\ =\ & \bar{\text{co}}\Big[ \bigcup_{\boldsymbol{p}_X=(1-q,q\boldsymbol{u}^T)^T} \big\{(R_1,R_2): R_1 \leq s - H(Y|X), \\ & \qquad R_2 \leq H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)\big\}\Big] & (33)\\ \subseteq\ & \bar{\text{co}}\Big[ \bigcup_{\boldsymbol{p}_X\in\Delta_k} \big\{(R_1,R_2): R_1 \leq s - H(Y|X), \\ & \qquad R_2 \leq H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)\big\}\Big], & (34) \end{aligned}$$

where $\bar{\text{co}}$ denotes the convex hull of the closure. Note that (30) and (34) are identical, hence (30 - 34) are all equal. Therefore, (32) expresses the capacity region for the DM-DBC, which also means that the capacity region can be achieved by using the transmission strategies such that the broadcast signal $X$ has distribution $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$. Q.E.D.

## V. Natural Encoding and Capacity Region for DM-DBCs

The natural encoding approach for the discrete multiplicative DBC is shown in Fig. 6. $W_1$ is the message for User 1 who sees the better channel $T_{YX}$ and $W_2$ is the message for User 2 who sees the worse channel $T_{ZX}$. The natural encoding approach is first to independently encode these two messages into two codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$ respectively, and then to broadcast $\boldsymbol{X}$ which is obtained by applying the single-letter multiplication function $X = X_2 \otimes X_1$ on the symbols of the codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$.

The distribution of $X_2$ is constrained to be $\boldsymbol{p}_{X_2} = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$ and hence the distribution of the broadcast signal $X$ also has $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$, which the previous section proved to be the optimal input distribution for the DM-DBC.

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.

Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}})^T$ be the distribution of the channel input $X$, where $\boldsymbol{p}_{\tilde{X}}$ is the distribution of sub-channel input $\tilde{X}$. For the DM-DBC $X \to Y \to Z$,

$$\phi(\boldsymbol{p}_X, \lambda) = h_{n+1}(T_{ZX}\boldsymbol{p}_X) - \lambda h_{n+1}(T_{YX}\boldsymbol{p}_X) \quad (35)$$

$$= h_{n+1}\left(\begin{bmatrix} 1-q+q\alpha_2 \\ q(1-\alpha_2)T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}} \end{bmatrix}\right) - \lambda h_{n+1}\left(\begin{bmatrix} 1-q+q\alpha_1 \\ q(1-\alpha_1)T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}} \end{bmatrix}\right) \quad (36)$$

$$= h(q(1-\alpha_2)) - q(1-\alpha_2)h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}}) - \lambda\left(h(q(1-\alpha_1)) - q(1-\alpha_1)h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})\right) \quad (37)$$

$$= h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2\big(h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}}) - \frac{\lambda}{1-\alpha_\Delta}h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})\big), \quad (38)$$

where $\beta_1 = 1-\alpha_1$ and $\beta_2 = 1-\alpha_2$.

For the sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$, define $\tilde{\phi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta}) = h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}}) - \frac{\lambda}{1-\alpha_\Delta}h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})$. Define $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$ as follows:

$$\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda) = h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2\tilde{\psi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta}), \quad (39)$$

where $\tilde{\psi}$ is the lower envelope of $\tilde{\phi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta})$ in $\boldsymbol{p}_{\tilde{X}}$ . With this definition, note that $\psi(\boldsymbol{p}_X, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$, is also the lower envelope of $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$.

*Lemma 4:* $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_X$ at $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ is on the lower envelope of $\varphi(q, \boldsymbol{u}, \lambda)$ in $q$. (See [8] for proof.)

Lemma 4 indicates that the lower envelope of $\phi(\cdot, \lambda)$ at $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ can be decomposed into two steps. First, for any fixed $q$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_{\tilde{X}}$ is $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$. Second, for $\boldsymbol{p}_{\tilde{X}} = \boldsymbol{u}$, the lower envelope of $\varphi(q, \boldsymbol{u}, \lambda)$ in $q$ coincides with $\psi(\boldsymbol{p}_X, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_X$.

*Theorem 5:* The natural encoding approach with time sharing achieves the boundary of the capacity region for the discrete multiplicative DBC.

*Proof :* Theorem 4 shows that the boundary of the capacity region for the DM-DBC can be achieved by using transmission strategies with uniformly distributed $\tilde{X}$, i.e., the input distribution $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$. For $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$, $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$ can be attained by the convex combination of points on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$. Since $\varphi(q, \boldsymbol{u}, \lambda) = h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2\tilde{\psi}(\boldsymbol{u}, \frac{\lambda}{1-\alpha_\Delta})$, which is the sum of $\phi(q, \lambda)$ for the broadcast Z channel and $q$ times the constant $\beta_2\tilde{\psi}(\boldsymbol{u}, \frac{\lambda}{1-\alpha_\Delta})$. Hence, by a discussion analogous to Section II-D, $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$ can be attained by the convex combination of 2 points on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$. One point is at $q = 0$ and $\varphi(0, \boldsymbol{u}, \lambda) = 0$. The other point is at $q = p_\lambda$, where $p_\lambda$ is determined by (8).

Note that the point (0,0) on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$ is also on the graph of $\phi(\boldsymbol{p}_X, \lambda)$. By Theorem 3, the point $(p_\lambda, \varphi(p_\lambda, \boldsymbol{u}, \lambda))$ is the convex combination of $n$ points on the graph of $\phi(\boldsymbol{p}_X, \lambda)$, which corresponds to the group-addition encoding approach for the sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$ because the group-addition encoding approach is optimal for the group-additive DBC $\tilde{X} \to \tilde{Y} \to \tilde{Z}$. Therefore, by Theorem 3, an optimal transmission strategy for the DM-DBC $X \to Y \to Z$ has the structure as shown in Fig. 7.

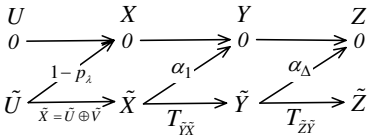


Fig. 7. The optimal transmission strategy for the discrete multiplicative degraded broadcast channel.

If the auxiliary random variable $U = 0$, then the channel input $X = 0$. If $U$ is a non-zero symbol, then $X = 0$ with probability $1 - p_\lambda$. In the case where $U$ and $X$ are both non-zero, $\tilde{X}$ can be obtained as $\tilde{X} = \tilde{U} \oplus \tilde{V}$, where $\oplus$ is the group addition in the group-additive degraded broadcast sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$, $\tilde{U}$ is uniformly distributed and $\tilde{V}$ is an $n$-ary random variable. By the definition of group addition and discrete multiplication, the transmission strategy with the structure in Fig. 7 is the natural encoding approach. Q.E.D.

## VI. Conclusion

This paper shows that the natural encoding of Fig. 6 is optimal for two-user DM-DBCs. Its achievable rate region is also a single-letter characterization of the capacity region for DM-DBCs. Hence, the capacity region for the DM-DBC in Fig. 4 is

$$\bar{\text{co}}\Big[\bigcup_{p_U, p_V}\big\{(R_1, R_2) : R_2 \le H(U\otimes V\otimes N_2) - H(U\otimes V\otimes N_2|U)$$
$$R_1 \le H(U\otimes V\otimes N_1|U) - H(U\otimes V\otimes N_1|U\otimes V)\big\}\Big]. \quad (40)$$

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

[5] 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.

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

[7] B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel. Optimal transmission strategy and capacity region for broadcast Z channels. In *IEEE Information Theory Workshop 2007*, Lake Tahoe, USA, Sep 2007.

[8] B. Xie and R. D. Wesel. Optimal Independent-Encoding Schemes for Several Classes of Discrete Degraded Broadcast Channels. In *ArXiv:0811.4162v2*, Jan. 14 2009.

[9] 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.