

# A Note on Some Inequalities Used in Channel Polarization and Polar Coding

T. S. Jayram and Erdal Arkan, *Fellow, IEEE*

**Abstract**—We give a unified treatment of some inequalities that are used in the proofs of channel polarization theorems involving a binary-input discrete memoryless channel.

**Index Terms**—Channel polarization, polar coding, Bhattacharyya parameter, Jensen-Shannon divergence, Hellinger distance.

## I. INTRODUCTION

THIS note provides a direct proof of an inequality [7, Proposition 11] in channel polarization theory. This inequality (the BEC inequality for short) is of basic importance in channel polarization as it characterizes an extremal property of the binary erasure channel (BEC) in that context. The proof of the BEC inequality in [7] used an indirect argument based on certain properties of channel polarization process. The approach here starts from first principles and provides a concise proof of the BEC inequality. As a side benefit, the present approach leads to a number of new inequalities that may be useful in channel polarization theory. This note also draws attention to an inequality by Lin [2] on distances between probability distributions that is equivalent to the above inequality on the extremal property of the BEC.

## II. RESULTS

Let  $W$  be a binary-input discrete memoryless channel with  $W(y|x)$  denoting the transition probability that output letter  $y \in \mathcal{Y}$  is received given that input  $x \in \{0, 1\}$  is sent. Assume without loss of generality that the channel is non-degenerate, i.e.,  $W(y|0) + W(y|1) > 0$  for every  $y \in \mathcal{Y}$ . Let the symmetric capacity be defined as<sup>1</sup>:

$$I(W) := \sum_y \sum_{x \in \{0,1\}} \frac{1}{2} W(y|x) \log \frac{W(y|x)}{\frac{1}{2} W(y|0) + \frac{1}{2} W(y|1)}$$

and the Bhattacharyya parameter as:

$$Z(W) := \sum_y \sqrt{W(y|0)W(y|1)}$$

Below, we prove various inequalities relating the Bhattacharyya parameter to the symmetric capacity.

Manuscript received July 5, 2016; accepted January 28, 2017. Date of publication June 20, 2017; date of current version July 12, 2018.

T. S. Jayram is with the IBM Almaden Research Center, San Jose, CA 95120 USA (e-mail: jayram@us.ibm.com).

Communicated by A. W. Eckford, Associate Editor for Communications.

E. Arkan is with the Department of Electrical-Electronics Engineering, Bilkent University, 06800 Ankara, Turkey (e-mail: arkan@ee.bilkent.edu.tr). Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TIT.2017.2717598

<sup>1</sup>log denotes the binary logarithm and ln denotes the natural logarithm.

Let  $\mathcal{H}(q) := -q \log(q) - (1-q) \log(1-q)$  denote the binary entropy function. Also define the Bhattacharyya function  $\mathcal{B}(q) := 2\sqrt{q(1-q)}$ . Both  $\mathcal{H}(q)$  and  $\mathcal{B}(q)$  are concave functions whose common domain and range are both equal to the interval  $[0, 1]$ . Define:

$$\phi : u \in [0, 1] \mapsto \mathcal{H}\left(\frac{1-\mathcal{B}(\frac{1-u}{2})}{2}\right) = \mathcal{H}\left(\frac{1-\sqrt{1-u^2}}{2}\right)$$

It can be verified that  $\phi$  is a bijection and that  $\phi(\mathcal{B}(q)) = \mathcal{H}(q)$  for all  $q \in [0, 1]$ . Anantharam *et al.* [1] studied  $\phi$  in a different setting and showed that it is convex. We reprove this below and demonstrate other properties of  $\phi$  that yield useful relationships between  $I(W)$  and  $Z(W)$  in a unified manner.

**Lemma 1:**  $0 < \phi''(u) < \phi'(u)/u$ , for all  $u \in (0, 1)$ .

**Proof:** Let  $v = \sqrt{1-u^2} \in (0, 1)$  to simplify the calculations. Taking derivatives of  $\phi$  we obtain:

$$\frac{1}{u} \cdot \frac{d\phi}{du} = \frac{1}{\ln 2} \cdot \frac{\alpha(v)}{v} \quad (1)$$

$$\frac{d^2\phi}{du^2} = \frac{1}{\ln 2} \cdot \frac{\alpha(v) - v}{v^3}, \quad (2)$$

where  $\alpha(v)$  above denotes the inverse hyperbolic tangent function, i.e.,  $\alpha : v \in (0, 1) \mapsto \frac{1}{2} \log\left(\frac{1+v}{1-v}\right)$ .

The Taylor series of  $\alpha(v)$  equals  $\sum_{n \geq 1} \frac{v^{2n-1}}{2n-1}$  which converges absolutely for  $v \in (0, 1)$ . Therefore:

$$\frac{\phi'(u)}{u} = \frac{1}{\ln 2} \cdot \left(1 + \sum_{n \geq 1} \frac{v^{2n}}{2n+1}\right)$$

$$\phi''(u) = \frac{1}{\ln 2} \cdot \left(\frac{1}{3} + \sum_{n \geq 1} \frac{v^{2n}}{2n+3}\right)$$

Comparing the right hand side of both expressions term by term, the desired inequality follows for all  $u \in (0, 1)$ .  $\square$

**Lemma 2:** The function  $\phi(u)$  is strictly convex whereas the function  $\phi(\sqrt{w})$  is strictly concave over their domain  $[0, 1]$ .

**Proof:** Since  $\phi(u)$  is continuous over its domain  $[0, 1]$ , and  $\phi''(u) > 0$  for all  $u \in (0, 1)$  by Lemma 1, it follows that  $\phi(u)$  is strictly convex.

Define  $\psi(w) := \phi(\sqrt{w})$  and let  $u = \sqrt{w}$ . Now  $\psi''(w) = \frac{1}{4u^2} \cdot (\phi''(u) - \phi'(u)/u) < 0$  by Lemma 1, for all  $u \in (0, 1)$ . Since  $\psi(w)$  is also continuous over  $[0, 1]$ , it is strictly concave.  $\square$

As a consequence, we obtain the following inequalities.

**Lemma 3:** For all  $u \in [0, 1]$ :

- (a)  $\phi(u) \leq u$  with equality only at  $u \in \{0, 1\}$ ;
- (b)  $\phi(u) \geq u^2$  with equality only at  $u \in \{0, 1\}$ ; and

(c)  $\phi(u) \geq 1 + (u - 1)/\ln 2$  with equality only at  $u = 1$ .

Lemma 3(a) can be restated as  $\mathcal{H}(q) \leq \mathcal{B}(q)$ , as shown by Lin [2, Th. 8]. Lemma 3(b) can be restated as  $\mathcal{H}(q) \geq \mathcal{B}(q)^2$ , as shown by Arıkan [3]. The lower bounds given in Lemma 3(b) and Lemma 3(c) are incomparable: when  $u = 0$ , Lemma 3(b) is tight but not Lemma 3(c); when  $u = 1 - \varepsilon$  for some small  $\varepsilon > 0$ , then  $\phi(u) = 1 - \varepsilon \log e + \Theta(\varepsilon^2)$ . Up to the linear term this matches the bound given by Lemma 3(c) but we get a worse bound with Lemma 3(b).

*Proof (of Lemma 3):* The proof uses the convexity statements in Lemma 2. The inequality in part (a) follows by convexity:  $\phi(u) \leq (1 - u) \cdot \phi(0) + u \cdot \phi(1) = u$ . Note that  $\phi(u) - u = 0$  for  $u \in \{0, 1\}$  and by strict convexity of the function  $\phi(u) - u$ , this value is achieved only at the end points.

The inequality in part (b) follows by concavity:  $\phi(\sqrt{w}) \geq (1 - w) \cdot \phi(\sqrt{0}) + w \cdot \phi(\sqrt{1}) = w$ ; now set  $w = u^2$ . By strict concavity, the minimum of  $\phi(\sqrt{w}) - w$  is achieved only at the end points so equality holds only at  $w = u \in \{0, 1\}$ .

For part (c), let  $\ell(u)$  denote the right side of the inequality. We show that  $\ell(u)$  is the tangent line at  $u = 1$  which by convexity would establish the inequality. By definition the tangent at  $u = 1$  equals  $\phi(1) + (u - 1)\phi'(1)$  so we need to show that  $\phi'(1) = \frac{1}{\ln 2}$ . By eq. (1), we have:

$$\begin{aligned} \phi'(1) &= \lim_{u \rightarrow 1} \frac{\phi'(u)}{u} = \lim_{x \rightarrow 0} \frac{\alpha(x)}{x \ln 2} \\ &= \frac{1}{\ln 2} \cdot \lim_{x \rightarrow 0} \alpha'(x) = \frac{1}{\ln 2} \cdot \lim_{x \rightarrow 0} \frac{1}{1 - x^2} = \frac{1}{\ln 2} \end{aligned}$$

Now  $\phi(u) = \ell(u)$  at  $u = 1$  and by strict convexity of  $\phi(u) - \ell(u)$ , its minimum is achieved only at this point.  $\square$

The above properties of  $\phi$  have the following implications for relating  $I(W)$  to  $Z(W)$ . Under the uniform distribution on the input  $\{0, 1\}$ , let  $Y$  denote the output induced by the channel, i.e., for each output letter  $y \in \mathcal{Y}$ ,  $p_Y(y) = \frac{1}{2}(W(y|0) + W(y|1))$ . Define the random variable:

$$U(y) := \mathcal{B}(Q(y)), \quad \text{where } Q(y) := \frac{W(y|0)}{W(y|0) + W(y|1)}$$

The law of  $Q$  is referred to as the Blackwell measure of  $W$  in [4]. Related measures, giving alternative characterizations of a binary-input memoryless channel, have been used extensively in the context of information combining in [5, Ch. 4], and more specifically in polar coding in [6, p. 30].

Rewrite the channel parameters  $I(W)$  and  $Z(W)$  as expectations of appropriate functions of  $U$ :

$$\begin{aligned} Z(W) &= \sum_y p_Y(y) \mathcal{B}(Q(y)) = \mathbb{E} \mathcal{B}(Q) = \mathbb{E} U \\ 1 - I(W) &= \sum_y p_Y(y) \mathcal{H}(Q(y)) = \mathbb{E} \mathcal{H}(Q) = \mathbb{E} \phi(U) \end{aligned} \quad (3)$$

**Theorem 4:**  $Z(W) \geq 1 - I(W) \geq \phi(Z(W))$

*Proof:* Applying Lemma 3(a) and then using the fact that  $\phi$  is convex (Lemma 2) yields:  $\mathbb{E} U \geq \mathbb{E} \phi(U) \geq \phi(\mathbb{E} U)$ . Now substitute the identities in eq. (3).  $\square$

By Lemma 3, the first inequality is tight iff  $U \in \{0, 1\}$  with probability 1. In other words, the inequality is tight iff

the channel  $W$  is such that  $W(y|0)W(y|1) = 0$  or  $W(y|0) = W(y|1)$  for each output  $y$ . A channel with this property is called a binary erasure channel (BEC). Indeed, this inequality was proved by Arıkan [7, Proposition 11] by an indirect argument, using an extremal property of the BEC in channel polarization.

The second inequality is tight iff  $U$  is constant with probability 1. Divide the outputs into two classes based on the predicate  $W(y|0) > W(y|1)$ ; this is operationally equivalent to a binary symmetric channel (BSC), i.e., a binary-input channel for which there exists a constant  $0 \leq \epsilon \leq \frac{1}{2}$  such that each  $y$  satisfies  $\epsilon \cdot W(y|x) = (1 - \epsilon) \cdot W(y|1 - x)$  for some  $x \in \{0, 1\}$ .

Now Lemma 3(b) implies that  $\phi(Z(W)) \geq Z(W)^2$  so we obtain:  $1 - I(W) \geq Z(W)^2$  (cf. [3]). Equality holds only when  $Z(W) \in \{0, 1\}$ . Equivalently, the distributions  $W(\cdot|0)$  and  $W(\cdot|1)$  are either identical or have disjoint support. Next Lemma 3(c) implies that  $I(W) + Z(W) \cdot \log e \leq \log e$ . Equality holds only when  $Z(W) = 1$ , i.e., the distributions  $W(\cdot|0)$  and  $W(\cdot|1)$  are identical. To summarize:

**Corollary 5:** For a binary input symmetric channel  $W$ :

- 1)  $I(W) + Z(W) \geq 1$ . Equality holds only for the BEC.
- 2)  $I(W) + \phi(Z(W)) \leq 1$ . Equality holds only for the BSC.
- 3)  $I(W) + Z(W)^2 \leq 1$ . Equality holds iff  $Z(W) \in \{0, 1\}$ .
- 4)  $I(W) \cdot \ln 2 + Z(W) \leq 1$ . Equality holds iff  $Z(W) = 1$ .

Finally, we note that these inequalities can be restated in terms of distances between probability distributions, which was the original motivation of Lin [2]. Let  $P$  and  $Q$  be two distributions on  $\mathcal{Y}$ . Identify  $W(\cdot|0)$  with  $P$  and  $W(\cdot|1)$  with  $Q$ . Then the Hellinger distance  $H(P, Q)$  equals  $\sqrt{1 - Z(W)}$  and the Jensen–Shannon divergence  $\text{JS}(P, Q)$  equals  $I(W)$ . Thus Corollary 5 can be restated as follows:

**Proposition 6:** For two distributions  $P$  and  $Q$ :

$$H^2(P, Q) \leq \text{JS}(P, Q) \leq H^2(P, Q) \cdot \min(\log e, 2 - H^2(P, Q))$$

## ACKNOWLEDGMENT

This work was jointly done at the Simons Institute for the Theory of Computing at UC Berkeley. The authors would like to thank the institute for their invitation to participate in the Information Theory Program during Jan. 2015 – June 2016.

## REFERENCES

- [1] V. Anantharam, A. A. Gohari, S. Kamath, and C. Nair, “On hypercontractivity and the mutual information between Boolean functions,” in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Oct. 2013, pp. 13–19.
- [2] J. Lin, “Divergence measures based on the Shannon entropy,” *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 145–151, Jan. 1991.
- [3] E. Arıkan, “Source polarization,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2010, pp. 899–903.
- [4] M. Raginsky, “Channel polarization and Blackwell measures,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 56–60.
- [5] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
- [6] E. Şaşıoğlu, “Polarization and polar codes,” *Found. Trends Commun. Inf. Theory*, vol. 8, no. 4, pp. 259–381, 2012.
- [7] E. Arıkan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.