A Tight Upper Bound on the Mutual Information of Two Boolean Functions

Georg Pichler*, Gerald Matz*, and Pablo Piantanida†

*Institute of Telecommunications, Technische Universität Wien, Vienna, Austria
†Laboratoire des Signaux et Systèmes (L2S), CentraleSupélec-CNRS-Université Paris-Sud, Gif-sur-Yvette, France
Email: {georg.pichler,gerald.matz}@nt.tuwien.ac.at; pablo.piantanida@centralesupelec.fr

***Abstract*—Let (X,Y) be a doubly symmetric binary source. For n i.i.d. copies $(\mathsf{X}^n,\mathsf{Y}^n)$ of (X,Y) we show that $\max\left[\mathrm{I}\big(f(\mathsf{X}^n);g(\mathsf{Y}^n)\big)\right]=\mathrm{I}(\mathsf{X};\mathsf{Y})$, where the maximum is over all Boolean functions $f,g\colon\{0,1\}^n\to\{0,1\}$. This positively resolves a conjecture published by Kumar and Courtade in 2013.**

***Index Terms*—Boolean functions, Mutual Information, Fourier transforms, Binary sequences, Binary codes**

I. Introduction

Let (X,Y) be a a doubly symmetric binary source with parameter $r=\mathrm{P}\{\mathsf{X}=\mathsf{Y}\}$ (DSBS(r), [1, Example 10.1]). The mutual information of X and Y (in bit) [1, Section 2.3] equals $\mathrm{I}(\mathsf{X};\mathsf{Y})=1-\mathrm{h}_0(r)$, where $\mathrm{h}_0(r):=-r\log_2(r)-(1-r)\log_2(1-r)$ is the binary entropy function. Motivated by problems in computational biology [2], Kumar and Courtade formulated the following conjecture [3].

Conjecture 1. *Let $(\mathsf{X}^n,\mathsf{Y}^n)$ be n independent, identically distributed (i.i.d.) copies of a DSBS(r) (X,Y). For any Boolean function $f\colon\{0,1\}^n\to\{0,1\}$,*

$$\mathrm{I}\big(f(\mathsf{X}^n);\mathsf{Y}^n\big)\leq 1-\mathrm{h}_0(r). \tag{1}$$

The dictator functions $f(\boldsymbol{x})=x_i$, $i\in\{1,2,\dots,n\}$, [4, Definition 2.3] achieve equality in (1). To date, no counterexample exists that leads to a mutual information larger than $1-\mathrm{h}_0(r)$. An overview of the work tackling (1) is given in in [5, Section IV]. Ordentlich et al. [6] used Fourier analytic techniques and leveraged hypercontractivity to improve upon previously known bounds on $\mathrm{I}(f(\mathsf{X}^n);\mathsf{Y}^n)$. Kindler et al. [7] studied an analogous problem in Gaussian spaces.

We next state the main result of this paper.

Theorem 2. *Let $(\mathsf{X}^n,\mathsf{Y}^n)$ be n independent, identically distributed copies of $(\mathsf{X},\mathsf{Y})\sim$ DSBS(r). For any two Boolean functions $f,g\colon\{0,1\}^n\to\{0,1\}$,*

$$\mathrm{I}\big(f(\mathsf{X}^n);g(\mathsf{Y}^n)\big)\leq 1-\mathrm{h}_0(r). \tag{2}$$

This statement involving two Boolean functions is weaker than Conjecture 1 (in fact, (2) readily follows from (1) via the data processing inequality [1, Section 2.3]). Theorem 2 was mentioned as an open problem in the original publication [3, Section IV] as well as [5]. A proof was previously only available under the additional restrictive assumptions that f and g are equally biased and satisfy the condition

$$\mathrm{P}\{f(\mathsf{X}^n)=0,\,g(\mathsf{X}^n)=0\}\geq\mathrm{P}\{f(\mathsf{X}^n)=0\}\,\mathrm{P}\{g(\mathsf{X}^n)=0\}. \tag{3}$$

This work was supported by WWTF Grant ICT12-054.

Refer to [5, Section IV] for further details.

In this paper, we prove Theorem 2 without any restrictions using Fourier-analytic tools. By suitably bounding the Fourier coefficients of f and g, we reduce (2) to elementary inequalities, which are subsequently proved. Anantharam et al. [8] had a different approach towards Theorem 2. They conjectured a result concerning the hypercontractivity ribbon of two binary random variables, which would imply Theorem 2. This stronger result still remains open, as our proof does not invoke hypercontractivity but purely relies on Fourier-analytic arguments.

Clearly, the dictator functions $f(\boldsymbol{x})=x_i$, $g(\boldsymbol{y})=y_i$ for any $i\in\{1,2,\dots,n\}$ achieve equality in (2). In an extended version [9] of this paper we show that these maximizers are essentially unique and provide the proofs in greater detail.

II. Notation and Definitions

It will be convenient to use the binary set $\Omega:=\{-1,1\}$ instead of $\{0,1\}$. Then, (X,Y) are two dependent Rademacher random variables on Ω, i.e., with expectation $\mathbb{E}[\mathsf{X}]=\mathbb{E}[\mathsf{Y}]=0$. We define $\rho:=\mathbb{E}[\mathsf{XY}]$ and say that X and Y are ρ-correlated. Note that $r:=\mathrm{P}\{\mathsf{X}=\mathsf{Y}\}=\frac{1}{2}(1+\rho)$. Furthermore, let $(\mathbf{X},\mathbf{Y}):=(\mathsf{X},\mathsf{Y})^n$ be n i.i.d. copies of (X,Y). We will need several Fourier-analytic properties of Boolean functions. For details, the reader is referred to [4, Sections 1 and 2]. In particular, we need the inner product of two functions $f,g\colon\Omega^n\to\mathbb{R}$, defined as $\langle f,g\rangle:=\mathbb{E}[f(\mathbf{X})g(\mathbf{X})]$. The canonical base functions are defined by $\chi_S(\boldsymbol{x}):=\prod_{i\in S}x_i$ for every $S\subseteq[n]:=\{1,2,\dots,n\}$. Then we write the Fourier coefficients of f as $\hat{f}(S):=\langle f,\chi_S\rangle$, for all $S\subseteq[n]$, satisfying Plancherel's theorem $\langle f,g\rangle=\sum_{S\subseteq[n]}\hat{f}(S)\hat{g}(S)$. We define the noise operator as the conditional expectation $T_\rho f(\boldsymbol{x}):=\mathbb{E}[f(\mathbf{Y})|\mathbf{X}=\boldsymbol{x}]$, which satisfies $\widehat{T_\rho f}(S)=\rho^{|S|}\hat{f}(S)$, where $|S|$ denotes the number of elements in S. Furthermore, for $f,g\colon\Omega^n\to\Omega$ we define $\alpha:=\mathbb{E}[f(\mathbf{X})]=\hat{f}(\varnothing)$, $\beta:=\mathbb{E}[g(\mathbf{X})]=\hat{g}(\varnothing)$ and $a:=\mathrm{P}\{f(\mathbf{X})=1\}=\frac{1}{2}(1+\alpha)$, $b:=\mathrm{P}\{g(\mathbf{X})=1\}=\frac{1}{2}(1+\beta)$. For convenience we define $\bar{t}:=1-t$ for $t\in\mathbb{R}$ and use $\log_2(\,\cdot\,)$ and $\log(\,\cdot\,)$ to denote the binary and the natural logarithm, respectively. We use the convention that the sign of zero equals one and denote (higher-order) derivatives by (multiple) superscript primes.

III. Proof of the Main Result

We first show that Theorem 2 is equivalent to the next theorem, which is the restriction of Theorem 2 (formulated in terms of Ω instead of $\{0,1\}$) to the special case of nonnegative ρ, α, and β. In order to prove Theorem 2, it thus suffices to prove Theorem 3.

Theorem 3. *Let $(\mathbf{X},\mathbf{Y})$ be n i.i.d. copies of the ρ-correlated random variables (X,Y) with $\rho = 2r-1 \geq 0$. For any two Boolean functions $f,g\colon \Omega^n \to \Omega$ with $\hat{g}(\varnothing) \geq \hat{f}(\varnothing) \geq 0$,*

$$\mathrm{I}\big(f(\mathbf{X});g(\mathbf{Y})\big) \leq 1-\mathrm{h}_0(r). \tag{4}$$

A. Proof of Equivalence of Theorems 2 and 3

Theorem 3 follows from Theorem 2 since Theorem 2 holds for any correlation and any two Boolean functions and thus necessarily for $\rho \geq 0$ and $\beta \geq \alpha \geq 0$ (recall that $\alpha = \hat{f}(\varnothing)$, $\beta = \hat{g}(\varnothing)$). To show that Theorem 3 implies Theorem 2, we need to prove that Theorem 3 remains true for arbitrary α, β, ρ.

For n i.i.d. random variables (X,Y) with arbitrary $\rho = 2r-1$, define $\widetilde{\mathbf{Y}} := \mathrm{sgn}(\rho)\mathbf{Y}$ such that the components of $\mathbf{X}$ and $\widetilde{\mathbf{Y}}$ are i.i.d. and $|\rho|$-correlated ($\widetilde{r} := (1+|\rho|)/2$). Furthermore, for arbitrary Boolean functions $f(\boldsymbol{x})$ and $g(\boldsymbol{y})$ define $f^{(0)}(\boldsymbol{x}) := \mathrm{sgn}(\alpha)f(\boldsymbol{x})$, $g^{(0)}(\boldsymbol{y}) := \mathrm{sgn}(\beta)g(\boldsymbol{y})$, and $g^{(1)}(\widetilde{\boldsymbol{y}}) := g^{(0)}(\mathrm{sgn}(\rho)\widetilde{\boldsymbol{y}}) = g^{(0)}(\boldsymbol{y})$; we have $\hat{f}^{(0)}(\varnothing) = |\alpha| \geq 0$ and $\hat{g}^{(0)}(\varnothing) = \hat{g}^{(1)}(\varnothing) = |\beta| \geq 0$. Since mutual information is not affected by applying one-to-one functions, it follows that $\mathrm{I}(f(\mathbf{X});g(\mathbf{Y})) = \mathrm{I}(f^{(0)}(\mathbf{X});g^{(0)}(\mathbf{Y}))$. We may assume without loss of generality that $|\alpha| \leq |\beta|$; otherwise, we swap $f^{(0)}$ and $g^{(0)}$ without affecting $\mathrm{I}(f^{(0)}(\mathbf{X});g^{(0)}(\mathbf{Y}))$, which is symmetric in $f^{(0)}$ and $g^{(0)}$. In total, we have

$$\begin{aligned}\mathrm{I}\big(f(\mathbf{X});g(\mathbf{Y})\big) &= \mathrm{I}\Big(f^{(0)}(\mathbf{X});g^{(0)}(\mathbf{Y})\Big)\\ &= \mathrm{I}\Big(f^{(0)}(\mathbf{X});g^{(1)}(\widetilde{\mathbf{Y}})\Big)\\ &\overset{(a)}{\leq} 1-\mathrm{h}_0(\widetilde{r}) = 1-\mathrm{h}_0(r),\end{aligned}$$

where inequality (a) follows from Theorem 3 and we used that the binary entropy is symmetric around $\frac{1}{2}$.

B. Auxiliary Results

Before proving Theorem 3, we need to establish several auxiliary results.

Lemma 4. *For any $\rho \in [-1,1]$ the bounds*

$$\alpha+\beta-1 \leq \langle f, T_\rho g\rangle \leq 1+\alpha-\beta$$

hold.

Proof. As $f-1 \leq 0$, $f+1 \geq 0$, and $g-1 \leq 0$, we obtain the desired bounds

$$\begin{aligned}0 &\leq \langle f-1, T_\rho(g-1)\rangle = \langle f, T_\rho g\rangle - \alpha - \beta + 1,\\ 0 &\geq \langle f+1, T_\rho(g-1)\rangle = \langle f, T_\rho g\rangle - \alpha + \beta - 1.\end{aligned}$$

■

The following lemma, stated without proof, is a simple consequence of Taylor's Theorem [10, Theorem 5.15].

Lemma 5. *Consider a function $\phi\colon I \to \mathbb{R}$ defined on the interval $I := [t_1,t_2]$ with $t_1 < t_2$. If the first-order derivative ϕ' is continuous on I and the second-order derivative $\phi''(t)$ exists for every $t \in I^o := (t_1,t_2)$, then the following two properties hold:*

1) *If $\phi''(t) \geq 0$, $t \in I^o$, and $\phi'(t^*) = 0$ for some $t^* \in I$, then $\phi(t) \geq \phi(t^*)$ for all $t \in I$.*
2) *If $\phi''(t) \leq 0$, $t \in I^o$, then $\phi(t) \geq \min\{\phi(t_1),\phi(t_2)\}$ for all $t \in I$.*

We will furthermore need the following powerful lemma, which allows us to obtain the necessary bounds on the parameters of the joint distribution of $f(\mathbf{X})$ and $g(\mathbf{Y})$.

Lemma 6. *Let $f,g\colon \Omega^n \to \Omega$ with $0 \leq \alpha \leq \beta \leq 1$ and define $\mathcal{P} := \{S \subseteq [n] : \hat{f}(S)\hat{g}(S) > 0\}\backslash\{\varnothing\}$, $\mathcal{N} := \{S \subseteq [n] : \hat{f}(S)\hat{g}(S) < 0\}$. Then the following inequalities hold:*

$$\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) \leq 2\Big(a\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big), \tag{5}$$

$$\sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) \geq -2\Big(\bar{a}\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big). \tag{6}$$

Proof. We will show the inequalities

$$\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) - \sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) \leq 4\sqrt{a\bar{a}b\bar{b}} \tag{7}$$

$$\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) + \sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) \geq -4\bar{a}\bar{b} \tag{8}$$

$$\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) + \sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) \leq 4a\bar{b}. \tag{9}$$

Then, (5) follows by adding (7) to (9) and (6) is obtained by subtracting (7) from (8).

Subtracting the means of f and g yields the unbiased functions $f_0 := f-\alpha$, $g_0 := g-\beta$. We then define f_1 and g_1 in terms of their Fourier transforms $\hat{f}_1(S) := |\hat{f}_0(S)|$ and $\hat{g}_1(S) := |\hat{g}_0(S)|$. With the norm $\|f\| := \sqrt{\langle f,f\rangle}$, we obtain (7) as

$$\begin{aligned}\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) - \sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) &= \langle f_1, g_1\rangle\\ &\overset{(a)}{\leq} \|f_1\|\|g_1\|\\ &= 4\sqrt{\bar{a}a\bar{b}b},\end{aligned}$$

where we used the Cauchy-Schwarz inequality [11, 4.2] in (a). To show (8) and (9), we use

$$\begin{aligned}\sum_{S\in\mathcal{P}} \hat{f}(S)\hat{g}(S) + \sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) &= \sum_{S\subseteq[n]} \hat{f}_0(S)\hat{g}_0(S)\\ &= \langle f_0, g_0\rangle = \langle f-\alpha, g-\beta\rangle\\ &= \langle f,g\rangle - \alpha\beta.\end{aligned} \tag{10}$$

The bounds $\alpha+\beta-1 \leq \langle f,g\rangle \leq 1+\alpha-\beta$ follow from Lemma 4 with $\rho = 1$. Inserting these bounds into (10) yields (8) and (9). ■

Definition 7. *For $\frac{1}{2} \leq a \leq b < 1$ define the function*

$$\begin{aligned}\phi_{a,b}(t) := b\,\mathrm{h}_0\left(\frac{1}{2}\left(1+\frac{a}{b}-\frac{1-t}{2b}\right)\right)\\ + \bar{b}\,\mathrm{h}_0\left(\frac{1}{2}\left(1+\frac{\bar{a}}{\bar{b}}-\frac{1-t}{2\bar{b}}\right)\right)\end{aligned} \tag{11}$$

for $t \in [1-2(\bar{b}+\bar{a}), 1-2(b-a)]$.

We next show that the function $\phi_{a,b}(t)$ is concave.

Lemma 8. *For $\frac{1}{2} \leq a \leq b < 1$ and $1-2(\bar{b}+\bar{a}) < t < 1-2(b-a)$, we have $\phi''_{a,b}(t) \leq 0$.*

Proof. We calculate the derivatives

$$\phi'_{a,b}(t) = \frac{1}{4}\log_2\left(\frac{(2(b-a)+\bar{t})(2(\bar{b}-\bar{a})+\bar{t})}{(2(b+a)-\bar{t})(2(\bar{b}+\bar{a})-\bar{t})}\right)$$

$$\phi''_{a,b}(t) = -\frac{1}{4\log(2)}\bigg(\frac{1}{2(b-a)+\bar{t}} + \frac{1}{2(\bar{b}-\bar{a})+\bar{t}} + \frac{1}{2(b+a)-\bar{t}} + \frac{1}{2(\bar{b}+\bar{a})-\bar{t}}\bigg). \tag{12}$$

The proof is concluded by observing that each term in (12) is nonnegative if $\frac{1}{2} \le a \le b < 1$ and $2(b-a) < \bar{t} < 2(\bar{b}+\bar{a})$. ∎

The following result on $\phi_{a,b}(t)$ follows from elementary results in real analysis. Although conceptually simple, the proof is rather lengthy and therefore deferred to Section IV.

Lemma 9. *For $\frac{1}{2} \le a \le b < 1$ and $0 \le \rho \le 1$, let*

$$t_0 := 1 - 2\min\Big\{\bar{a}+\bar{b}, a\bar{b}+b\bar{a}+\rho\Big(\bar{a}\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big)\Big\}, \tag{13}$$

$$t_1 := 1 - 2\max\Big\{b-a, a\bar{b}+b\bar{a}-\rho\Big(a\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big)\Big\}. \tag{14}$$

Then,

$$\mathrm{h}_0(a) - \phi_{a,b}(t_0) \le 1 - \mathrm{h}_0(r), \tag{15}$$

$$\mathrm{h}_0(a) - \phi_{a,b}(t_1) \le 1 - \mathrm{h}_0(r). \tag{16}$$

C. Proof of Theorem 3

It is easy to see that $b = 1$ entails $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) = 0 \le 1 - \mathrm{h}_0(r)$. Thus, we assume in the following $\frac{1}{2} \le a \le b < 1$. We can then write $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y}))$ as

$$\begin{aligned}\mathrm{I}\big(f(\mathbf{X}); g(\mathbf{Y})\big) &= \mathrm{h}_0(a) - b\,\mathrm{h}_0(\mathrm{P}\{f(\mathbf{X})=1|g(\mathbf{Y})=1\}) \\ &\quad - \bar{b}\,\mathrm{h}_0(\mathrm{P}\{f(\mathbf{X})=-1|g(\mathbf{Y})=-1\}).\end{aligned} \tag{17}$$

In order to prove (4), we need suitable bounds for $\mathrm{P}\{f = \pm 1 | g = \pm 1\}$. In analogy to [4, Proposition 1.9] we have

$$\langle f, T_\rho g\rangle = 2\mathrm{P}\{f(\mathbf{X}) = g(\mathbf{Y})\} - 1, \tag{18}$$

where T_ρ is the noise operator. For any two binary random variables (A, B) on Ω^2 it is easily checked, that

$$\begin{aligned}&\mathrm{P}\{\mathsf{A}=1, \mathsf{B}=1\} \\ &\quad = \frac{1}{2}\big(\mathrm{P}\{\mathsf{A}=1\} + \mathrm{P}\{\mathsf{B}=1\} + \mathrm{P}\{\mathsf{A}=\mathsf{B}\} - 1\big).\end{aligned} \tag{19}$$

Combining (18) and (19) yields

$$\begin{aligned}&\mathrm{P}\{f(\mathbf{X})=1|g(\mathbf{Y})=1\} \\ &\quad = \frac{\mathrm{P}\{f(\mathbf{X})=1, g(\mathbf{Y})=1\}}{\mathrm{P}\{g(\mathbf{Y})=1\}} \\ &\quad = \frac{1}{2b}\big(a+b+\mathrm{P}\{f(\mathbf{X})=g(\mathbf{Y})\}-1\big) \\ &\quad = \frac{1}{2}\bigg(1+\frac{a}{b}-\frac{1-\langle f, T_\rho g\rangle}{2b}\bigg)\end{aligned} \tag{20}$$

and similarly we also obtain

$$\mathrm{P}\{f(\mathbf{X})=-1|g(\mathbf{Y})=-1\} = \frac{1}{2}\bigg(1+\frac{\bar{a}}{\bar{b}}-\frac{1-\langle f, T_\rho g\rangle}{2\bar{b}}\bigg). \tag{21}$$

Substituting (20) and (21) in (17) yields with (11),

$$\mathrm{I}\big(f(\mathbf{X}); g(\mathbf{Y})\big) = \mathrm{h}_0(a) - \phi_{a,b}\big(\langle f, T_\rho g\rangle\big).$$

From [4, Proposition 2.47] we have

$$\langle f, T_\rho g\rangle = \sum_{S\subseteq[n]} \rho^{|S|}\hat{f}(S)\hat{g}(S).$$

We obtain the lower bound

$$\begin{aligned}\langle f, T_\rho g\rangle &= \alpha\beta + \sum_{S\in\mathcal{P}} \rho^{|S|}\hat{f}(S)\hat{g}(S) + \sum_{S\in\mathcal{N}} \rho^{|S|}\hat{f}(S)\hat{g}(S) \\ &\overset{(a)}{\ge} \alpha\beta + \sum_{S\in\mathcal{N}} \rho^{|S|}\hat{f}(S)\hat{g}(S) \\ &\overset{(b)}{\ge} \alpha\beta + \rho\sum_{S\in\mathcal{N}} \hat{f}(S)\hat{g}(S) \\ &\overset{(c)}{\ge} \alpha\beta - 2\rho\Big(\bar{a}\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big) \\ &= 1 - 2\Big(a\bar{b}+b\bar{a}+\rho\Big(\bar{a}\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big)\Big),\end{aligned} \tag{22}$$

where (a) follows from $\rho \ge 0$ and $\hat{f}(S)\hat{g}(S) \ge 0$ for $S \in \mathcal{P}$, (b) follows as $\varnothing \notin \mathcal{N}$, $\rho \in [0,1]$ and $\hat{f}(S)\hat{g}(S) \le 0$ for $S \in \mathcal{N}$, and in (c) we applied Lemma 6. Using Lemma 6 we also obtain the upper bound

$$\langle f, T_\rho g\rangle \le 1 - 2\Big(a\bar{b}+b\bar{a}-\rho\Big(a\bar{b}+\sqrt{a\bar{a}b\bar{b}}\Big)\Big). \tag{23}$$

From Lemma 4 we obtain $1 - 2(\bar{a}+\bar{b}) \le \langle f, T_\rho g\rangle \le 1 - 2(b-a)$. Combining these bounds with (22) and (23) yields $t_0 \le \langle f, T_\rho g\rangle \le t_1$ with t_0 and t_1 as defined in Lemma 9. This implies

$$\begin{aligned}\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) &= \mathrm{h}_0(a) - \phi_{a,b}\big(\langle f, T_\rho g\rangle\big) \\ &\overset{(d)}{\le} \mathrm{h}_0(a) - \min_{t\in\{t_0,t_1\}} \phi_{a,b}(t) \\ &\overset{(e)}{\le} 1 - \mathrm{h}_0(r),\end{aligned}$$

where (d) follows from Lemma 8 and part 2 of Lemma 5, and (e) follows from Lemma 9.

IV. Proof of Lemma 9

The proof of Lemma 9 consists of a series of lemmas, all of which follow from elementary results in real analysis.

A. Auxiliary Results

Lemma 10. *For $x \in (0,1)$, $y \in [0,1]$ and $z > 0$,*

$$\psi_1(x,z) := \frac{1}{x^{-z}-1} + \log(1-x^z) \ge 0, \tag{24}$$

$$\psi_2(x,y) := 1 - \mathrm{h}_0\bigg(\frac{1+y}{2}\bigg) - \mathrm{h}_0(x) + x\mathrm{h}_0(\bar{x}\bar{y}) + \bar{x}\mathrm{h}_0(x\bar{y}) \ge 0, \tag{25}$$

$$\psi_3(y) := 1 - \mathrm{h}_0\bigg(\frac{1}{2}+\frac{y}{1+y}\bigg) - \mathrm{h}_0\bigg(\frac{y}{1+y}\bigg) + \frac{1}{1+y}\mathrm{h}_0(y) \ge 0. \tag{26}$$

Proof. To show (24), observe that $\psi_1(x,z)$ increases in x (verify $\frac{\partial}{\partial x}\psi_1(x,z) \ge 0$) and $\lim_{x\downarrow 0}\psi_1(x,z) = 0$.

To prove the bound (25), apply part 1 of Lemma 5 to $\psi_2(x,y)$ as a function of y for any fixed $x \in (0,1)$ to obtain $\psi_2(x,y) \ge \psi_2(x,0) = 0$ for all $y \in [0,1]$.

For (26), note that $\psi_3(0) = \psi_3(1) = 0$. We obtain $y^* = \frac{2}{3}$ as the unique solution to $\psi_3'(y^*) = 0$ on $(0,1)$. The bound then follows from the observation $\psi_3(\frac{2}{3}) > 0$. ∎

Based on Lemma 10 we show the following two lemmas, which capture the main portion of the proof of Lemma 9.

Lemma 11. *For $0 < a \leq b < 1$,*

$$\psi(a,b) := 1 - \mathrm{h}_0\left(\frac{1}{2} + \frac{\sqrt{a\bar{b}}}{\sqrt{a\bar{b}} + \sqrt{\bar{a}b}}\right) - \mathrm{h}_0(a) + b\mathrm{h}_0\left(\frac{a}{b}\right) \geq 0.$$

Proof. We first consider the case $b = a$ where we have $\psi(a,a) = 1 - \mathrm{h}_0(a) \geq 0$. Thus, assume in the following $0 < a < b < 1$. We introduce the variable transformation

$$x := \sqrt{\frac{a\bar{b}}{\bar{a}b}}, \qquad c := \frac{\log\left(\frac{a}{b}\right)}{\log\left(\frac{a\bar{b}}{\bar{a}b}\right)},$$

with range $(x,c) \in (0,1)^2$. The inverse for $0 < a < b < 1$ is given by

$$a = \frac{x^{2c} - x^2}{1 - x^2}, \qquad b = \frac{1 - x^{2-2c}}{1 - x^2}.$$

Now we redefine $\psi(a,b)$ in terms of x and c as

$$\begin{aligned}\widetilde{\psi}(x,c) := 1 - \mathrm{h}_0\left(\frac{1}{2} + \frac{x}{1+x}\right) - \mathrm{h}_0\left(\frac{x^{2c} - x^2}{1 - x^2}\right) \\ + \frac{1 - x^{2-2c}}{1 - x^2}\mathrm{h}_0\left(x^{2c}\right)\end{aligned}$$

for $(x,c) \in (0,1)^2$. Fix a particular $x \in (0,1)$ and define $\gamma_x(c) := \widetilde{\psi}(x,c)$ for $c \in (0,1)$. We obtain

$$\begin{aligned}\gamma_x'(c) = \frac{2\log(x)}{(x^2-1)\log(2)}\big(2x^{2c}c\log(x) \\ + x^{2-2c}\log(1 - x^{2c}) - x^{2c}\log(x^{2c} - x^2)\big),\end{aligned}$$

where clearly $\gamma_x'(\frac{1}{2}) = 0$. The second-order derivative is

$$\gamma_x''(c) = \frac{4\log(x)^2 x^{2c}}{(1-x^2)\log(2)}\widetilde{\gamma}_x(c)$$

with

$$\begin{aligned}\widetilde{\gamma}_x(c) &:= \left(\frac{1}{x^{-2+2c} - 1} + \log(1 - x^{2-2c})\right) \\ &\quad + \frac{x^2}{x^{4c}}\left(\log(1 - x^{2c}) + \frac{1}{x^{-2c} - 1}\right) \qquad (27) \\ &\overset{(a)}{\geq} 0\end{aligned}$$

where (a) follows by applying (24) in Lemma 10 to each term in (27). Since $\widetilde{\gamma}_x$ determines the sign of γ_x'', we have $\gamma_x''(c) \geq 0$ for $c \in (0,1)$. Applying part 1 of Lemma 5 to γ_x entails $\gamma_x(c) \geq \gamma_x(\frac{1}{2})$ for $c \in (0,1)$ as we already established $\gamma_x'(\frac{1}{2}) = 0$. We conclude the proof by remarking that $\gamma_x(\frac{1}{2}) = \widetilde{\psi}(x, \frac{1}{2}) \geq 0$ (26) in Lemma 10. ∎

Lemma 12. *For $0 < a \leq b < 1$ and $0 \leq \rho \leq \frac{2\sqrt{a\bar{b}}}{\sqrt{a\bar{b}} + \sqrt{\bar{a}b}}$,*

$$\begin{aligned}\phi(\rho) := 1 - \mathrm{h}_0\left(\frac{1+\rho}{2}\right) - \mathrm{h}_0(a) + b\,\mathrm{h}_0\left(a + \rho\frac{a\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2b}\right) \\ + \bar{b}\,\mathrm{h}_0\left(a - \rho\frac{a\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2\bar{b}}\right) \geq 0.\end{aligned}$$

Proof. We use the short-hand notations

$$A := \frac{a\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2},$$

$$\rho_1 := \frac{2\sqrt{a\bar{b}}}{\sqrt{a\bar{b}} + \sqrt{\bar{a}b}} = \frac{a\bar{b}}{A},$$
$$\rho_0 := \frac{\min\{ab, \bar{a}\bar{b}\}}{A},$$
$$\rho_{-1} := \frac{\max\{ab, \bar{a}\bar{b}\}}{A}.$$

In case $b = a$, we have $A = a\bar{a}$ and

$$\begin{aligned}\phi(\rho) &= 1 - \mathrm{h}_0\left(\frac{1+\rho}{2}\right) - \mathrm{h}_0(a) + a\mathrm{h}_0(\bar{a}\bar{\rho}) + \bar{a}\mathrm{h}_0(a\bar{\rho}) \\ &\geq 0\end{aligned}$$

by (25) in Lemma 10. Assuming $0 < a < b < 1$, we will now show $\phi(\rho) \geq 0$ for $\rho \in [0, \rho_1]$. We obtain for $\rho \in [0, \rho_1)$

$$\begin{aligned}\phi'(\rho) = \frac{1}{2}\log_2\left(\frac{1+\rho}{1-\rho}\right) \\ + A\log_2\left(\frac{(\bar{a}b - A\rho)(a\bar{b} - A\rho)}{(ab + A\rho)(\bar{a}\bar{b} + A\rho)}\right) \qquad (28)\end{aligned}$$

and

$$\begin{aligned}\phi''(\rho) = \frac{A^2}{\log(2)}\bigg(\frac{1}{A^2(1-\rho^2)} - \frac{1}{\bar{a}b - A\rho} - \frac{1}{a\bar{b} - A\rho} \\ - \frac{1}{\bar{a}\bar{b} + A\rho} - \frac{1}{ab + A\rho}\bigg).\end{aligned}$$

Note, that $\phi'(\rho_1)$ and $\phi''(\rho_1)$ are undefined, but

$$\lim_{\rho \uparrow \rho_1} \phi'(\rho) = \lim_{\rho \uparrow \rho_1} \phi''(\rho) = -\infty. \qquad (29)$$

Moreover, we have

$$\begin{aligned}\phi''(0) &= \frac{A^2}{\log(2)}\left(\frac{1}{A^2} - \frac{1}{\bar{a}b} - \frac{1}{a\bar{b}} - \frac{1}{\bar{a}\bar{b}} - \frac{1}{ab}\right) \\ &= \frac{1}{\log(2)}\left(1 - \frac{A^2}{a\bar{a}b\bar{b}}\right) \\ &= \frac{1}{\log(2)}\left(1 - \left(\frac{\sqrt{a\bar{b}} + \sqrt{\bar{a}b}}{\sqrt{\bar{a}b} + \sqrt{\bar{a}b}}\right)^2\right) \\ &> 0, \qquad (30)\end{aligned}$$

as $a\bar{b} < \bar{a}b$. We can write $\phi''(\rho) = \frac{p(\rho)}{q(\rho)}$, where both p and q are polynomials in ρ. We choose

$$\begin{aligned}q(\rho) = \log(2)(1-\rho^2)(\bar{a}b - A\rho)(a\bar{b} - A\rho) \\ \cdot (\bar{a}\bar{b} + A\rho)(ab + A\rho).\end{aligned}$$

and notice that for $\rho \in [0, \rho_1)$

$$q(\rho) > 0. \qquad (31)$$

Calculating the coefficients of $p(\rho)$ reveals that its degree is at most 3. We will now demonstrate that there is one unique point $\rho^* \in (0, \rho_1)$ with $p(\rho^*) = 0$. To this end, reinterpret $\phi''(\rho)$ as a rational function in ρ on $\mathbb{R}$. By (29) to (31), we know that the number of zeros of $p(\rho)$ in $(0, \rho_1)$ is odd and less than its degree, i.e., either one or three. We next show that $p(\rho)$ has at least one zero in $(-\infty, 0)$, ensuring that there is only one zero in $(0, \rho_1)$. Distinguish the following cases.

- $\rho_0 < 1$: We have $q(\rho) > 0$ for $\rho \in (-\rho_0, 0)$, $\phi''(0) > 0$ and $\lim_{\rho \downarrow -\rho_0} \phi''(\rho) = -\infty$. Thus, there is an odd number of zeros in $(-\rho_0, 0)$.

- $\rho_0 = 1$: Note that $p(-1) = 0$.
- $\rho_0 = \rho_{-1}$: Observe that $p(-\rho_0) = 0$.
- $\rho_{-1} > \rho_0 > 1$: Let $I := (-\rho_{-1}, -\rho_0)$ and observe that $q(\rho) > 0$ for $\rho \in I$. Thus, there needs to be an odd number of zeros in I as $\lim_{\rho\downarrow -\rho_{-1}} \phi''(\rho) = -\infty$ and $\lim_{\rho\uparrow -\rho_0} \phi''(\rho) = \infty$.

Consequently, $\phi''(\rho) \geq 0$ for $\rho \in (0, \rho^*)$ and by inspection of (28) we have $\phi'(0) = 0$. Thus, by part 1 of Lemma 5, $\phi(\rho) \geq \phi(0) = 0$ for $\rho \in [0, \rho^*]$. Furthermore, $\phi''(\rho) \leq 0$ for $\rho \in (\rho^*, \rho_1)$ and therefore, for any $\varepsilon \in (0, \rho_1 - \rho^*)$, we have $\phi(\rho) \geq \min\{\phi(\rho^*), \phi(\rho_1 - \varepsilon)\}$ for all $\rho \in (\rho^*, \rho_1 - \varepsilon)$ by part 2 of Lemma 5 . From (29) and the mean value theorem [10, Theorem 5.10], $\phi(\rho_1 - \varepsilon) \geq \phi(\rho_1)$ for all $\varepsilon \in (0, \varepsilon_0)$ for some suitably small $\varepsilon_0 > 0$. This implies that $\phi(\rho) \geq \min\{\phi(\rho^*), \phi(\rho_1)\}$ for $\rho \in (\rho^*, \rho_1)$ as ε was arbitrary. In summary, we have $\phi(\rho) \geq \min\{0, \phi(\rho_1)\}$ for $\rho \in [0, \rho_1]$ and finish the proof by remarking that $\phi(\rho_1) \geq 0$ was shown in Lemma 11. ∎

B. Proof of Lemma 9

We will show inequalities (15) and (16) by distinguishing four cases. Starting with (15), first assume

$$1 - 2(\bar{a} + \bar{b}) \geq 1 - 2\Big(a\bar{b} + b\bar{a} + \rho\Big(\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}}\Big)\Big),$$

which is equivalent to $\rho \geq \frac{2\sqrt{\bar{a}\bar{b}}}{\sqrt{\bar{a}\bar{b}}+\sqrt{ab}}$. Now, $t_0 = 1 - 2(\bar{a} + \bar{b})$ by (13) and

$$\begin{aligned}
&1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + \phi_{a,b}(t_0) \\
&\quad = 1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + b\mathrm{h}_0\Big(\frac{\bar{a}}{\bar{b}}\Big) \\
&\quad \overset{(a)}{\geq} 1 - \mathrm{h}_0\left(\frac{1}{2} + \frac{\sqrt{\bar{a}\bar{b}}}{\sqrt{\bar{a}\bar{b}} + \sqrt{ab}}\right) - \mathrm{h}_0(a) + b\mathrm{h}_0\Big(\frac{\bar{a}}{\bar{b}}\Big) \\
&\quad \overset{(b)}{\geq} 0,
\end{aligned}$$

where (a) follows from the monotonicity of $\mathrm{h}_0(\,\cdot\,)$ on $[\frac{1}{2}, 1]$ and (b) follows from Lemma 11 using the substitution $a \mapsto \bar{a}$.

Conversely, assume $\rho < \frac{2\sqrt{\bar{a}\bar{b}}}{\sqrt{\bar{a}\bar{b}}+\sqrt{ab}}$, which entails $t_0 = 1 - 2\Big(a\bar{b} + b\bar{a} + \rho\Big(\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}}\Big)\Big)$ by (13) and

$$\begin{aligned}
&1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + \phi_{a,b}(t_0) \\
&\quad = 1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + b\mathrm{h}_0\left(a - \rho\frac{\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}})}{2b}\right) \\
&\qquad + \bar{b}\mathrm{h}_0\left(a + \rho\frac{\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}})}{2\bar{b}}\right) \overset{(c)}{\geq} 0,
\end{aligned}$$

where (c) follows from Lemma 12 with the substitution $a \mapsto \bar{a}$. This finishes the proof of (15).

The proof of (16) follows from Lemmas 11 and 12 in a similar fashion. For $\rho \geq \frac{2\sqrt{ab}}{\sqrt{a\bar{b}}+\sqrt{\bar{a}b}}$ we have $t_1 = 1 - 2(b - a)$ by (14) and obtain

$$\begin{aligned}
&1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + \phi_{a,b}(t_1) \\
&\quad = 1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + b\mathrm{h}_0\Big(\frac{a}{b}\Big) \\
&\quad \overset{(d)}{\geq} 1 - \mathrm{h}_0\left(\frac{1}{2} + \frac{\sqrt{ab}}{\sqrt{a\bar{b}} + \sqrt{\bar{a}b}}\right) - \mathrm{h}_0(a) + b\mathrm{h}_0\Big(\frac{a}{b}\Big) \\
&\quad \overset{(e)}{\geq} 0,
\end{aligned}$$

where (d) follows from the monotonicity of $\mathrm{h}_0(\,\cdot\,)$ and (e) is a consequence of Lemma 11.

Conversely, for $t_1 = 1 - 2\Big(a\bar{b} + b\bar{a} - \rho\Big(a\bar{b} + \sqrt{a\bar{a}b\bar{b}}\Big)\Big)$ we obtain

$$\begin{aligned}
&1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + \phi_{a,b}(t_1) \\
&\quad = 1 - \mathrm{h}_0(r) - \mathrm{h}_0(a) + b\mathrm{h}_0\Big(a + \frac{\rho}{2b}\Big(a\bar{b} + \sqrt{a\bar{a}b\bar{b}}\Big)\Big) \\
&\qquad + \bar{b}\mathrm{h}_0\Big(a - \frac{\rho}{2\bar{b}}\Big(a\bar{b} + \sqrt{a\bar{a}b\bar{b}}\Big)\Big) \\
&\quad \overset{(f)}{\geq} 0,
\end{aligned}$$

where (f) follows from Lemma 12.

V. Discussion

By splitting the Fourier coefficients into their positive and negative parts, we were able to improve upon previous proof strategies and dispense with the assumptions of equal bias and positive correlatedness (3). This key idea is expressed in Lemma 6 and allowed us to reduce the statement of Theorem 2 to elementary inequalities, which were subsequently proved. These inequalities—in particular Lemma 12, which contains Lemmas 10 and 11 as special cases—required considerable effort. They might turn out to be useful in the context of other converse proofs concerning the optimization of rate regions with binary random variables.

Although we provided a conclusive and complete proof for the tight upper bound on the mutual information of two Boolean functions, Conjecture 1 remains open. Our proof might provide some insight into the general problem. However, it seems unlikely that the idea behind Lemma 6 can be applied to resolve Conjecture 1 affirmatively.

Acknowledgment

The first author would like to thank Günther Koliander for valuable discussion regarding the proofs of Lemmas 11 and 12.

References

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

[2] J. G. Klotz, D. Kracht, M. Bossert, and S. Schober, "Canalizing Boolean functions maximize mutual information," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2139–2147, Apr. 2014.

[3] G. R. Kumar and T. A. Courtade, "Which Boolean functions are most informative?" in *Proc. IEEE Int. Symp. on Inform. Theory*, Istanbul, Turkey, Jul. 2013, pp. 226–230.

[4] R. O'Donnell, *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[5] T. A. Courtade and G. R. Kumar, "Which Boolean functions maximize mutual information on noisy inputs?" *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4515–4525, Aug. 2014.

[6] O. Ordentlich, O. Shayevitz, and O. Weinstein, "An improved upper bound for the most informative Boolean function conjecture," *preprint*, 2015. [Online]. Available: http://arxiv.org/abs/1505.05794

[7] G. Kindler, R. O'Donnell, and D. Witmer, "Remarks on the most informative function conjecture at fixed mean," *preprint*, 2016. [Online]. Available: http://arxiv.org/abs/1506.03167

[8] V. Anantharam, A. A. Gohari, S. Kamath, and C. Nair, "On hypercontractivity and the mutual information between Boolean functions," in *Proc. 51st Allerton Conf. Commun., Control, Comput.*, 2013, pp. 13–19.

[9] G. Pichler, P. Piantanida, and G. Matz, "Dictator functions maximize mutual information," *Ann. of Probability (submitted)*, 2016. [Online]. Available: http://arxiv.org/abs/1604.02109

[10] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed. McGraw-Hill, 1976.

[11] ——, *Real and Complex Analysis*, 3rd ed. McGraw-Hill, 1987.