The Annals of Applied Probability
2018, Vol. 28, No. 5, 3094–3101
https://doi.org/10.1214/18-AAP1384

DICTATOR FUNCTIONS MAXIMIZE MUTUAL INFORMATION

BY GEORG PICHLER*,[1], PABLO PIANTANIDA† AND GERALD MATZ*,[1]

Technische Universität Wien and CentraleSupélec-CNRS-Université Paris-Sud*†*

Let $(\mathbf{X}, \mathbf{Y})$ denote n independent, identically distributed copies of two arbitrarily correlated Rademacher random variables (X, Y). We prove that the inequality $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) \le \mathrm{I}(\mathsf{X}; \mathsf{Y})$ holds for any two Boolean functions: $f, g\colon \{-1,1\}^n \to \{-1,1\}$ [$\mathrm{I}(\cdot;\cdot)$ denotes mutual information]. We further show that equality in general is achieved only by the dictator functions $f(\boldsymbol{x}) = \pm g(\boldsymbol{x}) = \pm x_i$, $i \in \{1, 2, \ldots, n\}$.

1. Introduction and main results. Let (X, Y) be two dependent Rademacher random variables on $\{-1, 1\}$, with correlation coefficient $\rho := \mathbb{E}[\mathsf{XY}] \in [-1, 1]$. For given $n \in \mathbb{N}$, let $(\mathbf{X}, \mathbf{Y}) = (\mathsf{X}, \mathsf{Y})^n$ be n independent, identically distributed copies of (X, Y). We will use the notation from [3] for information-theoretic quantities. In particular, $\mathbb{E}[\mathsf{X}]$, $\mathrm{H}(\mathsf{X})$ and $\mathrm{I}(\mathsf{X}; \mathsf{Y})$ denote expectation, entropy and mutual information, respectively. Motivated by problems in computational biology [4], Kumar and Courtade formulated the following conjecture [5], Conjecture 1.

CONJECTURE 1. *For any Boolean function* $f\colon \{-1,1\}^n \to \{-1,1\}$,

$$\mathrm{I}\big(f(\mathbf{X}); \mathbf{Y}\big) \le \mathrm{I}(\mathsf{X}; \mathsf{Y}). \tag{1}$$

This claim—while seemingly innocent at first sight—has received significant interest and resisted several efforts to find a proof (see the discussion in [2], Section IV). Note that $f = \chi_i$ for any dictator function ([6], Definition 2.3), $\chi_i(\boldsymbol{x}) := x_i$, $i \in \{1, 2, \ldots, n\}$ achieves equality in (1).

We next state the main result of this paper, which is a relaxed version of Conjecture 1, involving two Boolean functions.

THEOREM 1. *For any two Boolean functions* $f, g\colon \{-1,1\}^n \to \{-1,1\}$,

$$\mathrm{I}\big(f(\mathbf{X}); g(\mathbf{Y})\big) \le \mathrm{I}(\mathsf{X}; \mathsf{Y}). \tag{2}$$

If (1) were true, this statement would readily follow from the data processing inequality [3], Theorem 2.8.1. Theorem 1 was stated as an open problem in [2] and

Received September 2016; revised January 2018.
[1]Supported by WWTF Grants ICT12-054 and ICT15-119.
MSC2010 subject classifications. Primary 94A15; secondary 94C10.
Key words and phrases. Boolean functions, mutual information, Fourier analysis, binary sequences, binary codes.

[5], Section IV, and separately investigated in [1]. A proof of (2) was previously available only under the additional restrictive assumptions that f and g are equally biased (i.e., $\mathbb{E}[f(\mathbf{X})] = \mathbb{E}[g(\mathbf{X})]$) and satisfy the condition

$$\mathrm{P}\{f(\mathbf{X}) = 1, g(\mathbf{X}) = 1\} \geq \mathrm{P}\{f(\mathbf{X}) = 1\}\mathrm{P}\{g(\mathbf{X}) = 1\}. \tag{3}$$

The reader is invited to see [2], Section IV, for further details. In this paper, we use Fourier-analytic tools to prove Theorem 1 without any additional restrictions on f and g. We suitably bound the Fourier coefficients of f and g, and thereby reduce (2) to an elementary inequality, which is subsequently established. A more detailed discussion of our results and proofs can be found in [7].

A careful inspection of the proof of Theorem 1 reveals that in general, up to sign changes, the dictator functions χ_i, $i \in \{1, 2, \ldots, n\}$ are the unique maximizers of $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y}))$.

PROPOSITION 1. *If* $0 < |\rho| < 1$, *equality in* (2) *is achieved if and only if* $f = \pm g = \pm \chi_i$ *for some* $i \in \{1, 2, \ldots, n\}$.

2. Proof of Theorem 1. Define $[n] := \{1, 2, \ldots, n\}$ and let f, g be two Boolean functions on the Boolean hypercube, that is, $f, g\colon \{-1, 1\}^n \to \{-1, 1\}$. Denote their Fourier expansions (cf. [6], (1.6)) $f(\boldsymbol{x}) = \sum_{\mathcal{S}\subseteq[n]} \hat{f}_{\mathcal{S}} \chi_{\mathcal{S}}(\boldsymbol{x})$ and $g(\boldsymbol{x}) = \sum_{\mathcal{S}\subseteq[n]} \hat{g}_{\mathcal{S}} \chi_{\mathcal{S}}(\boldsymbol{x})$, using the basis $\chi_{\mathcal{S}}(\boldsymbol{x}) := \prod_{i\in\mathcal{S}} x_i$ for $\mathcal{S} \subseteq [n]$. Define

$$a := \frac{1 + \hat{f}_\varnothing}{2} = \mathrm{P}\{f(\mathbf{X}) = 1\},$$
$$b := \frac{1 + \hat{g}_\varnothing}{2} = \mathrm{P}\{g(\mathbf{X}) = 1\}$$

and

$$\theta_\rho := \frac{1}{4} \sum_{\mathcal{S}:|\mathcal{S}|\geq 1} \hat{f}_{\mathcal{S}} \hat{g}_{\mathcal{S}} \rho^{|\mathcal{S}|}.$$

Without loss of generality, we may assume $\frac{1}{2} \leq a \leq b \leq 1$ and $\rho \in [0, 1]$, as mutual information is symmetric and we have, with $\mathbf{Y}^* := \mathrm{sgn}(\rho)\mathbf{Y}$,

$$\mathrm{I}\big(f(\mathbf{X}); g(\mathbf{Y})\big) = \mathrm{I}\big(\mathrm{sgn}(\hat{f}_\varnothing) f(\mathbf{X}); \mathrm{sgn}(\hat{g}_\varnothing) g\big(\mathrm{sgn}(\rho)\mathbf{Y}^*\big)\big). \tag{4}$$

In analogy to [6], Proposition 1.9, the inner product satisfies

$$\langle f, T_\rho g\rangle = \mathbb{E}\big[f(\mathbf{X})g(\mathbf{Y})\big] = \hat{f}_\varnothing \hat{g}_\varnothing + 4\theta_\rho = 1 - 2\mathrm{P}\{f(\mathbf{X}) \neq g(\mathbf{Y})\}, \tag{5}$$

where T_ρ is the noise operator [6], Definition 2.46. Defining $\bar{t} := 1 - t$ for a generic t, we can express the probabilities

$$\begin{aligned} \mathrm{P}\{f(\mathbf{X}) = 1, g(\mathbf{Y}) = -1\} &= a\bar{b} - \theta_\rho, \\ \mathrm{P}\{f(\mathbf{X}) = g(\mathbf{Y}) = 1\} &= ab + \theta_\rho, \end{aligned} \tag{6}$$

$$\begin{aligned} \mathrm{P}\{f(\mathbf{X}) = -1, g(\mathbf{Y}) = 1\} &= \bar{a}b - \theta_\rho, \\ \mathrm{P}\{f(\mathbf{X}) = g(\mathbf{Y}) = -1\} &= \bar{a}\bar{b} + \theta_\rho. \end{aligned} \tag{7}$$

Using (6), (7) and fundamental properties of mutual information [3], Section 2.4, we obtain $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) = \xi(\theta_\rho, a, b)$ with

$$\xi(\theta, a, b) := \mathrm{H}(a) + \mathrm{H}(b) - \mathrm{H}(ab + \theta, a\bar{b} - \theta, \bar{a}b - \theta, \bar{a}\bar{b} + \theta), \tag{8}$$

where, slightly abusing notation, we defined the binary entropy function $\mathrm{H}(p) := \mathrm{H}(p, \bar{p})$ and $\mathrm{H}((p_i)_{i\in\mathcal{I}}) := -\sum_{i\in\mathcal{I}} p_i \log_2 p_i$ for $|\mathcal{I}| > 1$. By the nonnegativity of probabilities (6) and (7), for any $\rho \in [0, 1]$,

$$-\bar{a}\bar{b} \le \theta_\rho \le a\bar{b}. \tag{9}$$

With $\mathcal{P} := \{\mathcal{S} \subseteq [n] : \hat{f}_\mathcal{S}\hat{g}_\mathcal{S} > 0\} \setminus \{\varnothing\}$ and $\mathcal{N} := \{\mathcal{S} \subseteq [n] : \hat{f}_\mathcal{S}\hat{g}_\mathcal{S} < 0\}$, we define

$$\tau^+ := \frac{1}{4}\sum_{\mathcal{S}\in\mathcal{P}} \hat{f}_\mathcal{S}\hat{g}_\mathcal{S}, \qquad \tau^- := \frac{1}{4}\sum_{\mathcal{S}\in\mathcal{N}} \hat{f}_\mathcal{S}\hat{g}_\mathcal{S} \tag{10}$$

and apply the Schwarz inequality to show

$$\tau^+ - \tau^- = \frac{1}{4}\sum_{\mathcal{S}:|\mathcal{S}|\ge 1} |\hat{f}_\mathcal{S}||\hat{g}_\mathcal{S}| \tag{11}$$

$$\le \frac{1}{4}\sqrt{(1 - \hat{f}_\varnothing^2)(1 - \hat{g}_\varnothing^2)} = \sqrt{a\bar{a}b\bar{b}}. \tag{12}$$

As $\theta_1 = \tau^+ + \tau^-$, we combine (9) and (12) to obtain

$$\tau^+ \le \frac{a\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2}, \qquad \tau^- \ge -\frac{\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2}. \tag{13}$$

By definition, $\rho\tau^- \le \theta_\rho \le \rho\tau^+$, and hence, $\theta_\rho \in [\theta_\rho^-, \theta_\rho^+]$, where

$$\begin{aligned} \theta_\rho^- &:= \max\left\{-\bar{a}\bar{b}, -\rho\frac{\bar{a}\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2}\right\}, \\ \theta_\rho^+ &:= \min\left\{a\bar{b}, \rho\frac{a\bar{b} + \sqrt{a\bar{a}b\bar{b}}}{2}\right\}. \end{aligned} \tag{14}$$

The function $\xi(\theta, \alpha, \beta)$ is convex in θ by the concavity of entropy [3], Theorem 2.7.3, and consequently, $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) \le \max_{\theta\in\{\theta_\rho^+, \theta_\rho^-\}} \xi(\theta, a, b)$. Thus, Theorem 1 can be proved by establishing $1 - \mathrm{H}(\frac{\rho+1}{2}) - \xi(\theta, a, b) \ge 0$ for $\theta \in \{\theta_\rho^+, \theta_\rho^-\}$. Furthermore, it suffices to consider $\frac{1}{2} < a < b < 1$ by continuity of ξ.

Define $C_{a,b} := \frac{a\bar{b}+\sqrt{a\bar{a}b\bar{b}}}{2}$, $\rho^+ := \min\{\rho, \frac{a\bar{b}}{C_{a,b}}\}$, $\rho^- := \min\{\rho, \frac{\bar{a}\bar{b}}{C_{\bar{a},b}}\}$, and

$$\phi(\rho, a, b) := 1 - \mathrm{H}\left(\frac{\rho + 1}{2}\right) - \xi(\rho C_{a,b}, a, b). \tag{15}$$

Note that

$$\phi(\rho^+, a, b) = 1 - \mathrm{H}\left(\frac{\rho^+ + 1}{2}\right) - \xi(\theta_\rho^+, a, b) \tag{16}$$

$$\leq 1 - \mathrm{H}\left(\frac{\rho + 1}{2}\right) - \xi(\theta_\rho^+, a, b) \tag{17}$$

by the monotonicity of the binary entropy function and accordingly we also have $\phi(\rho^-, \bar{a}, b) \leq 1 - \mathrm{H}(\frac{\rho+1}{2}) - \xi(\theta_\rho^-, a, b)$. Theorem 1 thus follows from the following lemma.

LEMMA 1. *For $0 < \alpha < \beta < 1$ and $\rho \in [0, \frac{\alpha\bar{\beta}}{C_{\alpha,\beta}}]$, we have $\phi(\rho, \alpha, \beta) \geq 0$ with equality if and only if $\rho = 0$.*

Before proving Lemma 1, we note the following facts.

LEMMA 2. *For $x \in (0, 1)$, we have*

$$\frac{1}{x^{-1} - 1} + \log(1 - x) > 0. \tag{18}$$

PROOF. Using Taylor series expansion, we immediately obtain

$$-\log(1 - x) = \sum_{n=1}^{\infty} \frac{x^n}{n} < \sum_{n=1}^{\infty} x^n = \frac{x}{1 - x}. \tag{19}$$

□

The following lemma collects elementary facts about convex/concave functions and follows from elementary properties of convex functions on the real line (see, e.g., [8], Chapter I).

LEMMA 3. *Let $f : U \to \mathbb{R}$ be a continuous function, defined on the compact interval $U := [u_1, u_2] \subset \mathbb{R}$. Assuming that f is twice differentiable on V, where $(u_1, u_2) \subseteq V \subseteq U$, the following properties hold:*

1. *If $f''(u) \geq 0$ for all $u \in (u_1, u_2)$ and $f'(u^*) = 0$ for some $u^* \in V$, then $f(u) \geq f(u^*)$ for all $u \in U$. Furthermore, if additionally $f''(u) > 0$ for all $u \in (u_1, u_2)$, then $f(u) > f(u^*)$ for all $u \in U \backslash \{u^*\}$.*
2. *If $f''(u) \leq 0$ for all $u \in (u_1, u_2)$, then $f(u) \geq \min\{f(u_1), f(u_2)\}$ for all $u \in U$. Furthermore, if $f''(u) < 0$ for all $u \in (u_1, u_2)$, then $f(u) > \min\{f(u_1), f(u_2)\}$ for all $u \in (u_1, u_2)$.*

PROOF OF LEMMA 1. Let $I := \{(\alpha, \beta) \in \mathbb{R}^2 : 0 < \alpha < \beta < 1\}$, fix arbitrary $(\alpha, \beta) \in I$ and define

$$\rho_- := \frac{\max\{\alpha\beta, \bar{\alpha}\bar{\beta}\}}{C_{\alpha,\beta}}, \qquad \rho_\circ := \frac{\min\{\alpha\beta, \bar{\alpha}\bar{\beta}\}}{C_{\alpha,\beta}}, \qquad \rho_+ := \frac{\alpha\bar{\beta}}{C_{\alpha,\beta}}. \tag{20}$$

We shall adopt the simplified notation $\phi(\rho) := \phi(\rho, \alpha, \beta)$, suppressing the fixed parameters (α, β). For $\rho \in [0, \rho_+)$, we have the derivatives

$$\begin{aligned}\phi'(\rho) &= \frac{1}{2}\log_2\Bigl(\frac{1+\rho}{1-\rho}\Bigr) \\ &\quad + C_{\alpha,\beta}\log_2\Bigl(\frac{(\bar{\alpha}\beta - C_{\alpha,\beta}\rho)(\alpha\bar{\beta} - C_{\alpha,\beta}\rho)}{(\alpha\beta + C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)}\Bigr),\end{aligned} \tag{21}$$

$$\begin{aligned}\phi''(\rho) &= \frac{C_{\alpha,\beta}^2}{\log 2}\Bigl(\frac{1}{C_{\alpha,\beta}^2(1-\rho^2)} - \frac{1}{\bar{\alpha}\beta - C_{\alpha,\beta}\rho} \\ &\quad - \frac{1}{\alpha\bar{\beta} - C_{\alpha,\beta}\rho} - \frac{1}{\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho} - \frac{1}{\alpha\beta + C_{\alpha,\beta}\rho}\Bigr).\end{aligned} \tag{22}$$

We write $\phi''(\rho) = \frac{p(\rho)}{q(\rho)}$, where both p and q are polynomials in ρ, and choose

$$\begin{aligned}q(\rho) &= \log(2)\bigl(1-\rho^2\bigr)(\bar{\alpha}\beta - C_{\alpha,\beta}\rho) \\ &\quad \times (\alpha\bar{\beta} - C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)(\alpha\beta + C_{\alpha,\beta}\rho),\end{aligned} \tag{23}$$

such that $q(\rho) > 0$ for $\rho \in [0, \rho_+)$. By (22), $p(\rho)$ is given by

$$\begin{aligned}p(\rho) &= (\bar{\alpha}\beta - C_{\alpha,\beta}\rho)(\alpha\bar{\beta} - C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)(\alpha\beta + C_{\alpha,\beta}\rho) \\ &\quad - C_{\alpha,\beta}^2\bigl(1-\rho^2\bigr)\bigl((\alpha\bar{\beta} - C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)(\alpha\beta + C_{\alpha,\beta}\rho) \\ &\quad + (\bar{\alpha}\beta - C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)(\alpha\beta + C_{\alpha,\beta}\rho) \\ &\quad + (\bar{\alpha}\beta - C_{\alpha,\beta}\rho)(\alpha\bar{\beta} - C_{\alpha,\beta}\rho)(\alpha\beta + C_{\alpha,\beta}\rho) \\ &\quad + (\bar{\alpha}\beta - C_{\alpha,\beta}\rho)(\alpha\bar{\beta} - C_{\alpha,\beta}\rho)(\bar{\alpha}\bar{\beta} + C_{\alpha,\beta}\rho)\bigr).\end{aligned} \tag{24}$$

This entails $\deg(p) \le 5$ and a careful calculation of the coefficients reveals $\deg(p) \le 3$.

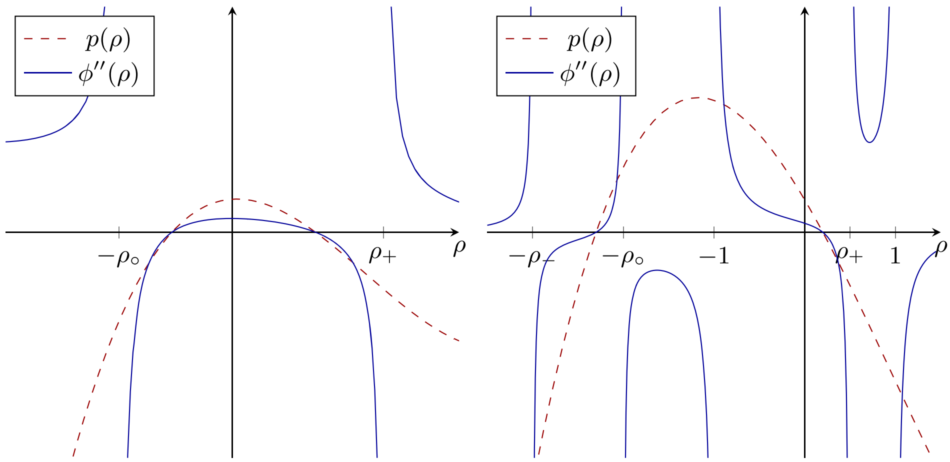
We will now demonstrate that there is a unique point $\rho^* \in (0, \rho_+)$, such that $p(\rho^*) = 0$. To this end, reinterpret $\phi''(\rho)$ as a rational function of ρ on $\mathbb{R}$. We evaluate (24) and use $\alpha < \beta$ to obtain the two inequalities

$$p(0) = \alpha\bar{\alpha}\beta\bar{\beta}\bigl(\alpha\bar{\alpha}\beta\bar{\beta} - C_{\alpha,\beta}^2\bigr) > 0 \tag{25}$$

and

$$p(\rho_+) = -\bigl(C_{\alpha,\beta}^2 - (\alpha\bar{\beta})^2\bigr)(\beta - \alpha)\bar{\beta}\alpha < 0. \tag{26}$$

The number of roots of p in $(0, \rho_+)$ is thus odd and at most equal to its degree, that is, either one or three. If we have $\rho_\circ \le 1$, then evaluation of (24) readily yields $p(-\rho_\circ) \le 0$. If, on the other hand, $\rho_\circ > 1$, we obtain $p(-\rho_-) \le 0$ from (24). Thus, p has at least one negative root and a unique root $\rho^* \in (0, \rho_+)$. Figure 1 qualitatively illustrate the behavior of $p(\rho)$ and $\phi''(\rho)$.



(a) $\rho_\circ < 1$ (b) $\rho_\circ > 1$

FIG. 1. *Sketch of $p(\rho)$ and $\phi''(\rho)$.*

Consequently, $\phi''(\rho) > 0$ for $\rho \in (0, \rho^*)$. By part 1 of Lemma 3, $\phi(\rho) > \phi(0) = 0$ for $\rho \in (0, \rho^*]$ as $\phi'(0) = 0$. Since $\phi''(\rho) < 0$ for $\rho \in (\rho^*, \rho_+)$, we have $\phi(\rho) > \min\{\phi(\rho^*), \phi(\rho_+)\}$ for all $\rho \in (\rho^*, \rho_+)$, by part 2 of Lemma 3. In total, $\phi(\rho) > \min\{0, \phi(\rho_+)\}$ for $\rho \in (0, \rho_+)$.

As $\phi(0) = 0$, it remains to show that $\phi(\rho_+, \alpha, \beta) > 0$ for $(\alpha, \beta) \in I$. To this end, we introduce the transformation

$$(\alpha, \beta) \longmapsto (c, x) := \left(\frac{\log \frac{\alpha}{\beta}}{\log \frac{\alpha\bar{\beta}}{\bar{\alpha}\beta}}, \sqrt{\frac{\alpha\bar{\beta}}{\bar{\alpha}\beta}} \right), \tag{27}$$

a bijective mapping from I to $(0,1)^2$ with the inverse

$$(c, x) \longmapsto (\alpha, \beta) = \left(\frac{x^{2c} - x^2}{1 - x^2}, \frac{1 - x^{2-2c}}{1 - x^2} \right). \tag{28}$$

In terms of c and x, we have $\phi(\rho_+, \alpha, \beta) = \psi(c, x)$, where

$$\psi(c, x) := 1 - \mathrm{H}\left(\frac{1}{2} + \frac{x}{1+x} \right) - \mathrm{H}\left(\frac{x^{2c} - x^2}{1 - x^2} \right) + \frac{1 - x^{2-2c}}{1 - x^2} \mathrm{H}(x^{2c}) \tag{29}$$

$$= 1 - \mathrm{H}\left(\frac{1 + 3x}{2 + 2x} \right) + \frac{\mathrm{H}(x^2)}{1 - x^2} + \frac{x^{2c}\mathrm{H}(x^{2-2c}) + x^{2-2c}\mathrm{H}(x^{2c})}{x^2 - 1}. \tag{30}$$

We fix a particular $x \in (0,1)$ and use the simplified notation $\psi(c) := \psi(c, x)$, obtaining the derivatives

$$\begin{aligned}\psi'(c) = {} & \frac{2\log(x)}{(x^2-1)\log(2)}\big[2x^{2c}c\log(x) \\ & + x^{2(1-c)}\log(1-x^{2c}) - x^{2c}\log(x^{2c}-x^2)\big],\end{aligned} \tag{31}$$

$$\begin{aligned}\psi''(c) = {} & \frac{4\log(x)^2x^{2c}}{(1-x^2)\log(2)}\bigg[\bigg(\frac{1}{x^{-2(1-c)}-1} + \log(1-x^{2(1-c)})\bigg) \\ & + \frac{x^2}{x^{4c}}\bigg(\log(1-x^{2c}) + \frac{1}{x^{-2c}-1}\bigg)\bigg].\end{aligned} \tag{32}$$

By applying Lemma 2 twice, we obtain $\psi''(c) > 0$. Thus, $\psi(c) > \psi(\frac{1}{2})$ by part 1 of Lemma 3 as $\psi'(\frac{1}{2}) = 0$. It remains to show that $\gamma(x) := \psi(\frac{1}{2}, x) > 0$. Note that $\gamma(0) = \gamma(1) = 0$ and

$$\gamma'(x) = \frac{1}{(1+x)^2}\log_2\big[(1+3x)(1-x)\big], \tag{33}$$

for $x \in [0,1)$. If $\gamma(x) \le 0$ for any $x \in (0,1)$ then f necessarily attains its minimum in $(0,1)$ and there exists $x^* \in (0,1)$ with $\gamma(x^*) \le 0$ and $\gamma'(x^*) = 0$. As $x^* = \frac{2}{3}$ is the only point in $(0,1)$ with $\gamma'(x^*) = 0$ and $\gamma(\frac{2}{3}) = \log_2(\frac{27}{25}) > 0$, this concludes the proof. $\square$

3. Proof of Proposition 1. We may assume $0 < \rho < 1$ and $\frac{1}{2} \le a \le b \le 1$ by virtue of (4). Clearly, $g = \pm f = \pm\chi_i$ for some $i \in [n]$ is a sufficient condition to maximize $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y}))$. A careful inspection of the proof of Theorem 1 shows that this condition is also necessary.

In the following, we will use the notation of Section 2. As $b = 1$ implies $\mathrm{I}(f(\mathbf{X}); g(\mathbf{Y})) = 0$, we assume $\frac{1}{2} \le a \le b < 1$. For equality in Theorem 1, we need either $\phi(\rho^+, a, b) = 0$ or $\phi(\rho^-, \bar{a}, b) = 0$. By Lemma 1, $\phi(\rho^-, \bar{a}, b) > 0$ unless $\bar{a} = a = \frac{1}{2}$, which in turn implies $\phi(\rho^-, \bar{a}, b) = \phi(\rho^+, a, b)$. The equality $\phi(\rho^+, a, b) = 0$ can only occur for $b = a$, implying $\rho^+ = \rho$. We want to show that $\phi(\rho, a, a) = 0$ implies $a = \frac{1}{2}$. For $a \ne \frac{1}{2}$, we have

$$\frac{\partial\phi}{\partial\rho}(\rho, a, a) = \frac{1}{2}\log_2\bigg(\frac{1+\rho}{1-\rho}\bigg) - a\bar{a}\log_2\bigg(\frac{\rho}{a\bar{a}\bar{\rho}^2} + 1\bigg), \tag{34}$$

$$\frac{\partial^2\phi}{\partial\rho^2}(\rho, a, a) = \frac{\rho(1-2a)^2}{\log(2)(a+\rho\bar{a})(1-a\bar{\rho})(1-\rho^2)} > 0. \tag{35}$$

Part (1) of Lemma 3 now yields $0 = \phi(0, a, a) < \phi(\rho, a, a)$ as $\frac{\partial\phi}{\partial\rho}(0, a, a) = 0$. By the strict convexity of $\xi(\theta, \frac{1}{2}, \frac{1}{2})$ in θ, necessarily $\theta_\rho = \frac{\langle f, T_\rho g\rangle}{4} \in \{\theta_\rho^+, \theta_\rho^-\} = \pm\frac{\rho}{4}$. The Cauchy–Schwarz inequality, together with [6], Proposition 2.50, yields $\rho^2 = \langle f, T_\rho g\rangle^2 = \langle T_{\sqrt{\rho}} f, T_{\sqrt{\rho}} g\rangle^2 \le \langle f, T_\rho f\rangle\langle g, T_\rho g\rangle \le \rho^2$. Thus, necessarily $g = \pm f = \pm\chi_i$ for some $i \in [n]$ by [6], Proposition 2.50.

4. Discussion. The key idea underlying the proof of Theorem 1 is to split $\theta_1 = \tau^+ + \tau^-$ into its positive and negative part (see Section 2). After reducing the problem to the inequality in Lemma 1, the remaining proof is routine analysis. Lemma 1 might turn out to be useful in the context of other converse proofs, in particular for the optimization of rate regions with binary random variables.

Acknowledgments. The authors would like to thank the anonymous referee for very helpful comments that greatly improved the readability of the paper. The first author also wants to thank Günther Koliander for valuable discussions.

REFERENCES

[1] ANANTHARAM, V., GOHARI, A. A., KAMATH, S. and NAIR, C. (2013). On hypercontractivity and the mutual information between Boolean functions. In *Proc*. 51*st Annual Allerton Conference on Communication*, *Control*, *and Computing* 13–19.

[2] COURTADE, T. A. and KUMAR, G. R. (2014). Which Boolean functions maximize mutual information on noisy inputs? *IEEE Trans*. *Inform*. *Theory* **60** 4515–4525. MR3245339

[3] COVER, T. M. and THOMAS, J. A. (2006). *Elements of Information Theory*, 2nd ed. Wiley, Hoboken, NJ. MR2239987

[4] KLOTZ, J. G., KRACHT, D., BOSSERT, M. and SCHOBER, S. (2014). Canalizing Boolean functions maximize mutual information. *IEEE Trans*. *Inform*. *Theory* **60** 2139–2147. MR3181516

[5] KUMAR, G. R. and COURTADE, T. A. (2013). Which Boolean functions are most informative? In *Proc*. *IEEE Int*. *Symp*. *on Inform*. *Theory* 226–230. DOI:10.1109/ISIT.2013.6620221.

[6] O'DONNELL, R. (2014). *Analysis of Boolean Functions*. Cambridge Univ. Press, New York. MR3443800

[7] PICHLER, G. (2017). Clustering by mutual information. Ph.D. thesis, Vienna Univ. Technology.

[8] ROBERTS, A. W. and VARBERG, D. E. (1973). *Convex Functions*. *Pure and Applied Mathematics* **57**. Academic Press, New York. MR0442824

G. PICHLER
G. MATZ
INSTITUTE OF TELECOMMUNICATIONS
TECHNISCHE UNIVERSITÄT WIEN
GUSSHAUSSTRASSE 25/E389
1040 VIENNA
AUSTRIA
E-MAIL: georg.pichler@gmail.com
gerald.matz@nt.tuwien.ac.at

P. PIANTANIDA
CENTRALESUPÉLEC-CNRS-UNIVERSITÉ PARIS-SUD
3 RUE JOLIOT-CURIE
F-91192 GIF-SUR-YVETTE CEDEX
FRANCE
E-MAIL: pablo.piantanida@centralesupelec.fr