

The "Most informative boolean function" conjecture holds for high noise

Alex Samorodnitsky

Abstract

We prove the "Most informative boolean function" conjecture of Courtade and Kumar for high noise $\epsilon \geq 1/2 - \delta$, for some absolute constant $\delta > 0$.

Namely, if X is uniformly distributed in $\{0, 1\}^n$ and Y is obtained by flipping each coordinate of X independently with probability ϵ , then, provided $\epsilon \geq 1/2 - \delta$, for any boolean function f holds $I(f(X); Y) \leq 1 - H(\epsilon)$. This conjecture was previously known to hold only for balanced functions [5].

1 Introduction

We start with recalling the conjecture of Courtade and Kumar [1].

Let (X, Y) be jointly distributed in $\{0, 1\}^n$ such that their marginals are uniform and Y is obtained by flipping each coordinate of X independently with probability ϵ . Let H denote the binary entropy function $H(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$. The conjecture of [1] is:

Conjecture 1.1: For all boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$,

$$I(f(X); Y) \leq 1 - H(\epsilon)$$

■

This inequality holds with equality if f is a characteristic function of a subcube of dimension $n-1$. Hence, the conjecture is that such functions are the "most informative" boolean functions.

This note is a follow-up to the paper [5], in which the conjecture was shown to hold for ϵ close to $1/2$ and for balanced boolean functions f . Here we make a few simple modifications to the argument, in order to remove the requirement on the boolean functions to be balanced. This note is not self-contained and we suggest that it should be read as an addendum to [5]. In particular, we use the notation from that paper.

Our main result is

Theorem 1.2: *There exists an absolute constant $\delta > 0$ such that for any noise $\epsilon \geq 0$ with $(1 - 2\epsilon)^2 \leq \delta$ and for any boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ holds*

$$I(f(X); Y) \leq 1 - H(\epsilon)$$

The argument proceeds similarly to [5]. We first argue, following [4], that if a boolean function f is 'informative', meaning that $I(f(X); Y) \geq 1 - H(\epsilon)$, then its Fourier mass is concentrated on the first two levels. By the inequality of [2] (see [2], Theorem 1.1) this implies that f is close to a characteristic function of a subcube. As the last step, we use a modified version of a theorem from [5] to show that for such functions the conjecture holds.

Notation (See [5]): For a function f on $\{0, 1\}^n$ we write $f = \sum_{S \subseteq [n]} \widehat{f}(S) \cdot W_S$ for the Fourier expansion of f . For a nonnegative function f , we let $Ent(f)$ be the entropy of f . For $0 \leq \epsilon \leq 1/2$, we denote by T_ϵ the appropriate noise operator. We note that ([5]) for a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ holds

$$I(f(X); Y) = Ent(T_\epsilon f) + Ent(T_\epsilon(1 - f)) \quad (1)$$

We write $\lambda = (1 - 2\epsilon)^2$ and recall that

$$1 - H(\epsilon) = \frac{1}{\ln 2} \cdot \sum_{k=1}^{\infty} \frac{1}{2k(2k-1)} \cdot \lambda^k \quad (2)$$

Brief overview. The main issue here is dealing with non-balanced functions. We prove two technical claims.

First, we slightly extend the approach of [4] and show that for any nonnegative non-zero function f holds¹

Lemma 1.3:

$$Ent(T_\epsilon f) \leq \frac{1}{\mathbb{E} f} \cdot \left(\frac{1}{2 \ln 2} \cdot \sum_{k=1}^n \widehat{f}^2(\{k\}) \right) \cdot \lambda + O\left(\frac{\mathbb{E} f^2}{\mathbb{E} f} \cdot \lambda^{4/3}\right) + O\left(\frac{\mathbb{E}^2 f^2}{\mathbb{E}^3 f} \cdot \lambda^2\right)$$

Second, we show that the proof of Theorem 1.11 in [5] can be modified to give:

Theorem 1.4: *There exists an absolute constant $\delta > 0$ such that for any noise $\epsilon \geq 0$ with $(1 - 2\epsilon)^2 \leq \delta$ and for any boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ such that*

- $\frac{1}{2} - \delta \leq \mathbb{E} f \leq \frac{1}{2}$;
- *There exists $1 \leq k \leq n$ such that $|\widehat{f}(\{k\})| \geq (1 - \delta) \cdot \mathbb{E} f$*

¹In this paper asymptotic notation hides absolute constants independent of the remaining parameters.

Holds

$$\text{Ent}(T_\epsilon f) + \text{Ent}(T_\epsilon(1-f)) \leq 1 - H(\epsilon)$$

Theorem 1.2 is an easy corollary of these two claims and the result of [2].

Organization. This paper is organized as follows. We deduce Theorem 1.2 from Lemma 1.3 and Theorem 1.4 in Section 2. We prove Lemma 1.3 in Section 3, and Theorem 1.4 in Section 4.

2 Proof of Theorem 1.2

It is known (see [1]) that for any boolean function f holds $I(f(X); Y) \leq \lambda \cdot H(\mathbb{E} f)$, where H is the binary entropy function. This immediately implies the validity of Conjecture 1.1 for boolean functions with expectation lying in $[0, c] \cup [1 - c, 1]$, for some absolute constant $0 < c < 1/2$.

In addition, we may assume, by symmetry, that $\mathbb{E} f \leq 1/2$. Combining these two observations, it remains to consider the case

$$c \leq \mathbb{E} f \leq 1/2 \tag{3}$$

Let f be a boolean function with $I(f(X); Y) \geq 1 - H(\epsilon)$. By (1) this is the same as

$$\text{Ent}(T_\epsilon f) + \text{Ent}(T_\epsilon(1-f)) \geq 1 - H(\epsilon)$$

On the other hand, applying Lemma 1.3 to the functions f and $1 - f$ and taking into account (3) gives

$$\text{Ent}(T_\epsilon f) + \text{Ent}(T_\epsilon(1-f)) \leq \frac{1}{\mathbb{E} f(1 - \mathbb{E} f)} \cdot \left(\frac{1}{2 \ln 2} \cdot \sum_{k=1}^n \widehat{f}^2(\{k\}) \right) \cdot \lambda + O(\lambda^{4/3})$$

Combining these two inequalities and observing that (2) implies $1 - H(\epsilon) \geq \frac{\lambda}{2 \ln 2}$ shows

$$\sum_{k=1}^n \widehat{f}^2(\{k\}) \geq \mathbb{E} f \cdot (1 - \mathbb{E} f) - O(\lambda^{1/3})$$

Recall that for a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ holds $\mathbb{E} f^2 = \mathbb{E} f$, and hence $\sum_{S \neq \emptyset} \widehat{f}^2(S) = \mathbb{E} f(1 - \mathbb{E} f)$. This means that the preceding inequality implies $\sum_{|S| \geq 2} \widehat{f}^2(S) \leq O(\lambda^{1/3})$.

We now proceed similarly to the proof of Theorem 1.11 in [5]. If λ is sufficiently small, the application of the inequality of [2], or of its a precise version due to [3] (see Theorem 5.5 in [5]), and taking into account (3), imply that f meets the conditions of Theorem 1.4, and hence Conjecture 1.1 holds for f .

3 Proof of Lemma 1.3

We may and will assume, by homogeneity, that $\mathbb{E} f = 1$.

Let us introduce some notation. For $x \in \{0, 1\}^n$, let x^c be the complement of x , that is the element of $\{0, 1\}^n$ with $x_i^c = 1 - x_i$ for all $1 \leq i \leq n$.

For a nonnegative function g on $\{0, 1\}^n$, let g_0 be the 'even' part of g defined by $g_0(x) = (g(x) + g(x^c))/2$, and let $g_1 = g - g_0$ be the 'odd' part of g . By definition, $g_0(x) = g_0(x^c)$ and $g_1(x) = -g_1(x^c)$. Note also that $|g_1| \leq g_0$.

We will need the following well-known (and easy to verify) fact:

$$g_0 = \sum_{|S| \text{ even}} \widehat{g}(S) \cdot W_S \quad \text{and} \quad g_1 = \sum_{|S| \text{ odd}} \widehat{g}(S) \cdot W_S$$

We start with an auxiliary claim.

Lemma 3.1: *For any nonnegative function g with expectation 1 holds*

$$Ent(g) = Ent(g_0) + \mathbb{E}_x g_0(x) \cdot \left(1 - H\left(\frac{1 - |g_1(x)|/g_0(x)}{2}\right)\right)$$

Here for x such that $g_0(x) = g_1(x) = 0$, the expression $g_0(x) \cdot \left(1 - H\left(\frac{1 - |g_1(x)|/g_0(x)}{2}\right)\right)$ is interpreted as 0.

Proof: We have

$$\begin{aligned} Ent(g) &= \mathbb{E}_x g(x) \log g(x) = \frac{1}{2} \cdot \mathbb{E}_x \left(g(x) \log g(x) + g(x^c) \log g(x^c) \right) = \\ &= \frac{1}{2} \cdot \mathbb{E}_x \left((g_0(x) + g_1(x)) \cdot \log (g_0(x) + g_1(x)) + (g_0(x) - g_1(x)) \cdot \log (g_0(x) - g_1(x)) \right) \end{aligned}$$

It is easy to verify that for any $0 \leq b \leq a$ holds

$1/2 \cdot \left((a+b) \log(a+b) + (a-b) \log(a-b) \right) = a \log a + a \cdot \left(1 - H\left(\frac{1-b/a}{2}\right)\right)$, where the last expression should be interpreted as 0 for $a = b = 0$.

Using this identity with $a = g_0(x)$ and $b = g_1(x)$ gives the claim of the lemma. ■

Next, as in [4], we upper bound $1 - H\left(\frac{1-x}{2}\right)$ by $\frac{1}{2 \ln 2} \cdot x^2 + \left(1 - \frac{1}{2 \ln 2}\right) \cdot x^4$.

This gives

$$Ent(g) \leq Ent(g_0) + \frac{1}{2 \ln 2} \cdot \mathbb{E}_x \frac{g_1^2(x)}{g_0(x)} + \left(1 - \frac{1}{2 \ln 2}\right) \cdot \mathbb{E}_x \frac{g_1^4(x)}{g_0^3(x)}$$

Substitute $g = T_\epsilon f$. It is easy to verify $(T_\epsilon f)_i = T_\epsilon(f_i)$ for any function f and for $i = 0, 1$. Consequently:

$$Ent(T_\epsilon f) \leq Ent(T_\epsilon f_0) + \frac{1}{2 \ln 2} \cdot \mathbb{E}_x \frac{(T_\epsilon f_1(x))^2}{T_\epsilon f_0(x)} + \left(1 - \frac{1}{2 \ln 2}\right) \cdot \mathbb{E}_x \frac{(T_\epsilon f_1(x))^4}{(T_\epsilon f_0(x))^3}$$

We upper bound each of the summands on the RHS separately.

1. The first summand. Note that $\mathbb{E} T_\epsilon f_0 = \mathbb{E} f_0 = \mathbb{E} f = 1$. Hence, by Lemma 5.4 in [5],

$$\begin{aligned} Ent(T_\epsilon f_0) &\leq O\left(\sum_S |S| \cdot \widehat{T_\epsilon f_0}^2(S)\right) = O\left(\sum_S |S| \lambda^{|S|} \widehat{f_0}^2(S)\right) = \\ &O\left(\sum_{|S| \text{ even}} |S| \lambda^{|S|} \widehat{f}^2(S)\right) = O(\mathbb{E} f^2 \cdot \lambda^2) \end{aligned}$$

2. The second summand. First we argue that $T_\epsilon f_0$ is bounded away from 0 with high probability. Recall that $\mathbb{E} T_\epsilon f_0 = 1$, and note that $Var(T_\epsilon f_0) = \sum_{S \neq \emptyset} \widehat{T_\epsilon f_0}^2(S) = O(\lambda^2 \cdot \mathbb{E} f^2)$. Hence, by Chebyshev's inequality, for any $0 \leq \alpha < 1$ holds $Pr\{T_\epsilon f_0 \leq \alpha\} \leq O((\lambda^2 \cdot \mathbb{E} f^2) / (1 - \alpha)^2)$.

Therefore, taking $\alpha = 1 - \lambda^{1/3}$,

$$\begin{aligned} \mathbb{E}_x \frac{(T_\epsilon f_1(x))^2}{T_\epsilon f_0(x)} &\leq Pr\{f_0 \leq 1 - \lambda^{1/3}\} + (1 + O(\lambda^{1/3})) \cdot \mathbb{E}_x (T_\epsilon f_1(x))^2 = \\ &O(\mathbb{E} f^2) \cdot \lambda^{4/3} + (1 + O(\lambda^{1/3})) \cdot \left(\left(\sum_{k=1}^n \widehat{f}^2(\{k\})\right) \cdot \lambda + O(\mathbb{E} f^2) \cdot \lambda^3\right) = \\ &\left(\sum_{k=1}^n \widehat{f}^2(\{k\})\right) \cdot \lambda + O(\mathbb{E} f^2 \cdot \lambda^{4/3}) \end{aligned}$$

3. The third summand. Note that $\mathbb{E} f_1 = 0$. Hence, by Lemma 1 in [4] (where the requirement on f to be boolean does not seem to be necessary) we have, for a sufficiently small λ and for some absolute constant $c > 0$ that

$$\mathbb{E}_x (T_\epsilon f_1(x))^4 \leq O\left(\left(\mathbb{E}_x (T_{c \cdot \epsilon} f_1(x))^2\right)^2\right) = O((\mathbb{E} f^2)^2 \cdot \lambda^2)$$

We can now upper bound the third summand using the Chebyshev inequality. Taking

$$\alpha = 1/2 \text{ gives } \mathbb{E}_x \frac{\left(T_\epsilon f_1(x)\right)^4}{\left(T_\epsilon f_0(x)\right)^3} \leq O\left(\left(\mathbb{E} f^2\right)^2 \cdot \lambda^2\right).$$

Combining these estimates leads to the claim of Lemma 1.3. ■

4 Proof of Theorem 1.4

The proof of this theorem follows very closely that of Theorem 1.11 in [5]. Here we briefly describe the few required modifications. This proof is not self-contained and, in particular, borrows notation and refers to claims from the proof of Theorem 1.11 in their original numbering.

As in (17) in that proof, we have that

$$\begin{aligned} Ent(T_\epsilon f) &\leq \lambda_2 \cdot \mathbb{E}_{|B|=\lambda_2 n, 1 \in B} \left(Ent(h | B) - Ent(h | \{1\}) \right) + \\ (1 - \lambda_2) \cdot \mathbb{E}_{|B|=\lambda_2 n, 1 \notin B} Ent(h | B) &+ \mathbb{E} h \cdot \phi \left(Ent \left(\frac{h}{\mathbb{E} h} \mid \{1\} \right), \epsilon_2 \right) + e(n) \end{aligned} \quad (4)$$

Applying this bound to the function $1 - f$ gives

$$\begin{aligned} Ent(T_\epsilon(1 - f)) &\leq \lambda_2 \cdot \mathbb{E}_{|B|=\lambda_2 n, 1 \in B} \left(Ent((1 - h) | B) - Ent((1 - h) | \{1\}) \right) + \\ (1 - \lambda_2) \cdot \mathbb{E}_{|B|=\lambda_2 n, 1 \notin B} Ent((1 - h) | B) &+ \mathbb{E}(1 - h) \cdot \phi \left(Ent \left(\frac{1 - h}{\mathbb{E}(1 - h)} \mid \{1\} \right), \epsilon_2 \right) + e(n) \end{aligned} \quad (5)$$

The following three claims, which upperbound the summands on the RHS of (4), are given, correspondingly, by Lemmas 5.1 and 5.2, and as an intermediary step in the proof of Lemma 5.3 in [5].

1. $\mathbb{E}_{|B|=\lambda_2 n, 1 \in B} \left(Ent(h | B) - Ent(h | \{1\}) \right) \leq O \left(\lambda_2 \cdot \gamma + \gamma^2 \ln \left(\frac{1}{\gamma} \right) \right) + e(n)$
2. $\mathbb{E}_{|B|=\lambda_2 n, 1 \notin B} Ent(h | B) \leq O \left(\lambda_2^2 \cdot \gamma + \lambda_2 \cdot \gamma^2 \ln \left(\frac{1}{\gamma} \right) \right)$
3. $\phi \left(Ent \left(\frac{h}{\mathbb{E} h} \mid \{1\} \right), \epsilon_2 \right) \leq \left(1 - H(\epsilon) \right) - \Omega(\lambda \cdot \alpha) + e(n)$

We now deal with (5). Repeating the argument, with the necessary (minor) differences, leads to the same first two bounds:

$$\mathbb{E}_{|B|=\lambda_2 n, 1 \in B} \left(Ent((1-h) | B) - Ent((1-h) | \{1\}) \right) \leq O\left(\lambda_2 \cdot \gamma + \gamma^2 \ln\left(\frac{1}{\gamma}\right) \right) + e(n)$$

and

$$\mathbb{E}_{|B|=\lambda_2 n, 1 \notin B} Ent((1-h) | B) \leq O\left(\lambda_2^2 \cdot \gamma + \lambda_2 \cdot \gamma^2 \ln\left(\frac{1}{\gamma}\right) \right)$$

Indeed, this should not be surprising since, roughly speaking, these two bounds for h are obtained by analysing the behavior of the squares of non-trivial Fourier coefficients of this function; and this behavior is the same for h and for $1-h$.

As to the third bound above, it is replaced, following the argument in the proof of Lemma 5.3, by

$$\phi\left(Ent\left(\frac{1-h}{\mathbb{E}(1-h)} \mid \{1\}\right), \epsilon_2 \right) \leq (1 - H(\epsilon)) - \Omega(\lambda \cdot \gamma) + e(n)$$

Combining all the bounds above gives

$$Ent(T_{\epsilon} f) + Ent(T_{\epsilon}(1-f)) \leq (1 - H(\epsilon)) - \Omega(\lambda \cdot \gamma) + o_{\lambda, \gamma \rightarrow 0}(\lambda \cdot \gamma) + e(n)$$

Since $\lambda, \gamma \leq O(\delta)$, this implies that for a sufficiently small $\delta > 0$ holds

$$Ent(T_{\epsilon} f) + Ent(T_{\epsilon}(1-f)) \leq (1 - H(\epsilon)) + e(n)$$

The error term can be removed by a direct product argument (see [5]), completing the proof of the theorem.

■

References

- [1] T. Courtade and G. Kumar, *Which boolean functions maximize mutual information on noisy inputs?* IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4515-4525, 2014.
- [2] E. Friedgut, G. Kalai, and A. Naor, *Boolean functions whose Fourier transform is concentrated on the first two levels*, Advances in Applied Mathematics, 2002.
- [3] J. Jendrej, K. Oleszkiewicz, and J. O. Wojtaszczyk, *On some extensions of the FKN theorem*, preprint, 2013.

- [4] O. Ordentlich, O. Shayevitz, and O. Weinstein, *An Improved Upper Bound for the Most Informative Boolean Function Conjecture*, arXiv preprint. [Online]. Available: <http://arxiv.org/abs/1505.05794>.
- [5] A. Samorodnitsky, *On the entropy of a noisy function*, arXiv preprint. [Online]. Available: <http://arxiv.org/abs/1508.01464>.