Nonuniform Indistinguishability and Unpredictability Hardcore Lemmas: New Proofs and Applications to Pseudoentropy*

Maciej Skorski **

maciej.skorski@mimuw.edu.pl Cryptology and Data Security Group, University of Warsaw

Abstract. Hardcore lemmas are results in complexity theory which state that average-case hardness must have a very hard "kernel", that is a subset of instances where the given problem is extremely hard. They find important applications in hardness amplification. In this paper we revisit the following two fundamental results:

- (a) The hardcore lemma for unpredictability, due to Impagliazzo (FOCS '95). It states that if a boolean function f is "moderately" hard to predict on average, then there must be a set of noticeable size on which f is "extremely" hard to predict.
- (b) The hardcore lemma for indistinguishability, proved by Maurer and Tesaro (TCC'10), states that for two random variables X and Y which are ϵ -computationally close, there are events A and B of probability $1-\epsilon$ such that the distributions of X|A and Y|B are "computationally" identical.

Using only the standard min-max theorem and some basic facts about convex approximations in L_p spaces, we provide alternative modular proofs and some generalizations of these results in the nonuniform setting, achieving best possible bounds for (a) and slightly improving the known bounds for (b). As an interesting application, we show a strengthening of the transformation between two most popular pseudoentropy variants: HILL and Metric Entropy, and apply it to show how to extract pseudorandomness from a sequence of metric-entropy sources of poor quality. In this case we significantly improve security parameters, comparing to the best known techniques.

1 Introduction

1.1 Hardcore lemmas and their applications

UNPREDICTABILITY HARDCORE LEMMA. Suppose that we have a function $f: \{0,1\}^n \to \{0,1\}$ that is mildly hard to predict by a class of circuits; for every

^{*} A preliminary version of this work appeared in the Proceedings of Student Research Forum Papers and Posters at SOFSEM 2015 [Sko15]

^{**} This work was partly supported by the WELCOME/2010-4/2 grant founded within the framework of the EU Innovative Economy Operational Programme.

circuit D from our class, D(x) and f(x) agree on at most, say, a 0.99 fraction of inputs x. One of the reasons for that, which could intuitively explain this behavior, is the existence of a "kernel" for this hardness: a set of noticeable size on which f is extremely hard to predict, meaning that there is (almost) no advantage over a random guess. How big this set should be? The intuitive answer is a 0.02 = 2(1-0.99) fraction of input. Indeed, if f cannot be guessed better than with probability $\frac{1}{2}$ on this set, then the probability that D agrees with f is at most $0.02 \cdot \frac{1}{2} + 0.98 \cdot 1 = 0.99$, by the total probability law.

Quite surprisingly, this intuitive characterization is true. The first such result was proved by Impagliazzo [Imp95]. An improved version with the optimal density of the hardcore set was found by Holenstein [Hol05]. Below we present the best possible result due to Klivans and Servedio.

Theorem 1 (Nonuniform Unpredictability Hardcore Lemma [KS03]). Let $f: \{0,1\}^n \to \{0,1\}$ be ϵ -unpredictable by circuits of size s, that is

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathrm{D}(x) = f(x)] \leqslant 1 - \frac{\epsilon}{2}$$

holds for all boolean circuits D over n bits of size at most s. Then for any $\delta \in (0,1)$ there exists a "hardcore" set S of size $\epsilon 2^n$ such that f on S is $1-\delta$ unpredictable by circuits of size $s' = O(s\delta^2/\log(1/\epsilon))$, that is

$$\Pr_{x \leftarrow S}[\mathbf{D}(x) = f(x)] \leqslant \frac{1+\delta}{2}, \quad \textit{for every } \mathbf{D} \textit{ of size at most } s'.$$

Remark 1 (Conventions). Some authors define ϵ -unpredictability in a different manner. We follow the approach of [Hol05]. The definition above is quite intuitive, since 1-unpredictability means that f is totally unpredictable.

Remark 2 (Trade-off between the loss in complexity and quality of the hardcore set). Ideally we want $\delta = 0$ but then we get nothing nontrivial about the indistinguishability. In fact, we cannot guarantee that f on the hardcore is perfectly unpredictable. The loss of $\delta^2/\log(1/\epsilon)$ in complexity is necessary (the matching lower bound is due to Lu, Tsai, and Wu [LTW07]).

Remark 3 (Hardcore for any sampling distribution). Klivans and Servedio proved in fact a more general result, where one samples x from arbitrary distribution V. The hardcore set is replaced then by a distribution "dense" in V. See Theorem 3.

Note that the size of the hardcore set, guaranteed to be at least $2^n \epsilon$, is tight. Indeed, if the second part of the theorem is satisfied, i.e. f is almost unpredictable on a set of size ϵ , it implies that f, on average over the whole domain, cannot be predicted better than $1 - \frac{\epsilon + \delta}{2} \approx 1 - \frac{\epsilon}{2}$ (provided that $\delta \ll \epsilon$). A uniform version, with the tight hardcore density, is given also in [Hol05] and [VZ12]. Constructive versions of the hardcore lemma can be obtained by any boosting algorithm [KS99,BHK09], however such results are not necessarily tight without additional optimization.

INDISTINGUISHABILITY HARDCORE LEMMA. It is well known that if two distributions X_1, X_2 have the statistical distance at most ϵ , then there exist events A_1, A_2 of probability at least $1 - \epsilon$ such that the distributions $X_1 | A_1$ and $X_2 | A_2$ are *identical*. Based on the reduction to the unpredictability hardcore lemma, Maurer and Tessaro proved the following computational generalization of this fact in the nonuniform setting

Theorem 2 (Indistinguishability Hardcore Lemma [MT10]). Let X_1 and X_2 be distributions on $\{0,1\}^n$, with the computational distance ϵ against circuits of size s, that is

$$|\mathbf{E} D(X_1) - \mathbf{E} D(X_2)| < \epsilon$$
 for all D of size s.

Then there exist events A_1 and A_2 of probability $1 - \epsilon$ such that A_1 and A_2 are computationally indistinguishable, that is

$$|\mathbf{E} D(X_1|A_1) - \mathbf{E} D(X_2|A_2)| \leq \delta$$
 for every D of size $s = s\delta^2/128n$.

which states that if two distributions are (computationally) not too far away from each other, then after conditioning on an event of noticeable probability they are almost completely indistinguishable. Since the lower bound $1 - \epsilon$ on the probabilities of hardcore events is tight¹, this theorem can be viewed as a characterization of computational indistinguishability.

APPLICATIONS OF HARDCORE LEMMAS. Hardcore lemmas are fundamental result in complexity theory and find applications in cryptography and learning theory. They are particularly important in the context of hardness amplification, i.e. transforming somewhat hard problems into hard problems. See for instance [LT13, GNW11, MT10, Hol05, Imp95].

1.2 Our results

AN UNPREDICTABILITY HARDCORE LEMMA FROM STANDARD MIN-MAX THEO-REM. We reprove Theorem 1 in its full generality developing a few new ideas. Our approach has the following advantages:

- (a) A new modular proof technique. Our approach is very simple and natural. We observe that it is straightforward to construct a hardcore for any fixed circuit of size s. Then we show that this is possible for any real-valued circuit of the same size. The third step (the only one which loses in complexity) is an approximation argument which shows that there exists a hardcore for any convex combination of circuits of size s. Finally we trivially "switch" the quantifiers by the standard min-max theorem. See Figure 1 for an overview.
- (b) Tight bounds from the standard min-max theorem. In our proof the weight of the hardcore event² for ϵ -unpredictability is guaranteed to be ϵ and

¹ By the similar reasoning as in the unpredictability case

² The hardcore is then understood as the sampling distribution conditioned on an appropriate event of sufficiently big probability.

- we loss a factor of $O\left(\log(1/\epsilon)/\delta^2\right)$ in complexity for the hardcore to be $1-\delta$ unpredictable, which matches the lower bound [LTW07]. The previous proofs which achieve optimal parameters required involved iterative arguments [KS03] or dedicated versions of the min-max theorem [VZ12]. Some authors even suggested that it might be impossible to get the tight parameters using the standard min-max theorem [VZ12].
- (c) New ideas of independent interests. The only technical difficulties in our proof are steps 2 and 3. The tools we have developed to overcome them allows us to give a direct proof (without reduction!) of the indistinguishability hardcore lemma and a variant of the indistinguishability hardcore lemma dedicated for computational entropy.

Below, in Figure 1, we sketch our proof strategy. We have managed to separate a lossless use of the min-max theorem from a standard approximation argument which is responsible for the only loss in complexity.

Fig. 1: An overview of our proof technique.

A quantitative comparison with versions of Theorem 1 is given in Table 1.

				Sampling
Result	Author	Proof technique	Complexity loss	distribution
Unpredictability Hardcore	[Hol05]	standard min-max theorem hardcore density optimization	$O(n/\delta^2)$	Uniform
	[KS03]	boosting	$O\left(\frac{\log(1/\epsilon)}{\delta^2}\right)$	Arbitrary
	, ,	dedicated min-max theorem hardcore density optimization	$O\left(\frac{\log(1/\epsilon)}{\delta^2}\right)$	Arbitrary
	This paper Theorem 3	standard min-max theorem convex approximation	$O\left(\min\left(\frac{n}{\delta^2}, \frac{\log(1/\epsilon)}{\delta^2}\right)\right)$	Arbitrary

Table 1: Our unpredictability hardcore lemma compared to previous works

A SIMPLIFIED AND IMPROVED REDUCTION FROM TO UNPREDICTABILITY HARD-CORES. We show an alternative proof for the indistinguishability hardcore lemma of Maurer and Tessaro. In [MT10] the non-trivial reduction goes from the indistinguishability hardcore lemma to the "standard" unpredictability hardcore lemma, that is where inputs are sampled from the uniform distribution. On the contrary, we find it much easier and natural to reduce it to unpredictability of some predicate which explicitly depends on the distributions X_1, X_2 (it is simply equal to the sign of the difference between probability mass functions). In our reduction we achieve better numerical constants and improve the factor depending on the dimension, replacing n by $\Delta^2 \log(1/\delta)$ where Δ is the statistical distance of X_1 and X_2 . The comparison with Theorem 2 is given in Table 2.

Result	Author	Proof technique	Complexity loss
Indistinguishability	[MT10]	Reduction (to unpredictability hardcore)	$O(n/\delta^2)$
Hardcore	This paper Theorem 4	Simpler Reduction (general unpredictability hardcore)	$O\left(\min\left(\frac{\Delta^2 n}{s^2}, \frac{\Delta^2 \log(\Delta/\epsilon)}{s^2}\right)\right)$

Table 2: Our indistinguishability hardcore lemma compared to previous works

A DIRECT PROOF OF THE INDISTINGUISHABILITY HARDCORE LEMMA. Adapting the proof given for the unpredictability case, we derive the (nonuniform) Indistinguishability Hardcore Lemma of Maurer and Tessaro directly, that is without reducing it to unpredictability hardcore lemmas. This might be important for lower bounds. Indeed, lower bounds on unpredictability hardcore lemmas do not imply lower bounds for the indistinguishability. For more details, see Corollary 3 in Section 4.

AN INDISTINGUISHABILITY HARDCORE LEMMA FOR PSEUDOENTROPY. In some situations, for instance in extracting entropy, we do not really need our distribution X to be indistinguishable from a particular Y but rather from a class of distributions Y (which is a weaker requirement). In particular, consider the following alternatives to formalize the statement "X almost has min-entropy k":

- (i) X is (s, δ) -close to having property P, if there exists a distribution Y with min-entropy k such that for every circuit D of size s, we have $\Delta^{D}(X; Y) \leq \delta$
- (ii) X is (s, δ) -close to having property P, if for every D of size s there exists a distribution Y with min-entropy k such that we have $\Delta^{D}(X;Y) \leq \delta$.

where $\Delta^{\mathcal{D}}(X;Y) = \mathbf{E} \, \mathcal{D}(X) - \mathbf{E} \, \mathcal{D}(Y)$ is the advantage of the attacker D. For case (i), we obtain the notion of the HILL entropy [HILL99]. In case (ii) we obtain a relaxed notion called metric pseudoentropy [BSW03]. Metric pseudoentropy is widely used as a convenient substitute of HILL entropy and find many application in studying pseudorandomness [VZ12, FOR12, DP08, BSW03]. It is known [BSW03] that metric entropy with parameters (s, ϵ) can be converted into HILL entropy with no loss in the amount and the parameters $(s', \epsilon') = (O(s \cdot \delta^2/n), \epsilon + \delta)$ for any δ . We obtain a nice and much stronger version of this transformation: if X has metric entropy of quality (s, ϵ) (even against weakest deterministic circuits) then after conditioning on an event of probability $1 - \epsilon$, it has the same amount of HILL entropy of quality $(O(s \cdot \delta^2/n), \delta)$.

APPLICATION: EXTRACTING PSEUDORANDOMNESS FROM PSEUDOENTROPY OF POOR QUALITY. Using our generalized indistinguishability hardcore lemma, we prove that for a sequence of independent distributions X_1, \ldots, X_ℓ , each having metric-entropy k with parameters (s, ϵ) for some $large \ \epsilon$ and against deterministic circuits of size s, the concatenated string $X = X_1, X_2, \ldots, X_\ell$ has HILL entropy roughly $(1 - \epsilon)\ell k$ with parameters $(s', \delta') = (\delta, s\delta^2\ell^{-2}/n)$. In other words, for a metric pseudoentropy source of quality (s, ϵ) we achieve, sampling many times,

the entropy extraction rate $\alpha = 1 - \epsilon^3$ with good security. Comparing to the state of art we save a quite large factor δ^2 in security⁴.

1.3 Outline of the paper

Section 2 provides necessary definitions for hardness of unpredictability, computational indistinguishability and computational entropy. In Section 3 we present a generalization of the unpredictability hardcore lemma and a slightly simplified proof of the indistinguishability hardcore lemma. A hardcore lemma dedicated for pseudoentropy is given in Section 4. An application to the problem of extracting from a pseudoentropy source of very bad quality is discussed in Section 5.

2 Preliminaries

COMPUTATIONAL AND STATISTICAL INDISTINGUISHABILITY. Let X and Y be two random variables taking values in the same space. The advantage of D in distinguishing between X and Y is defined to be $\Delta^{\mathrm{D}}(X;Y) = \mathbf{E}\,\mathrm{D}(X) - \mathbf{E}\,\mathrm{D}(Y)$. The statistical distance between two random variables X and Y, is defined as $\Delta(X;Y) = \frac{1}{2}\sum_{x}|\Pr[X=x] - \Pr[Y=x]|$ and is equal to the maximum of $\Delta^{\mathrm{D}}(X;Y)$ over all [0,1]-valued functions D. The computational distance between X and Y is defined as $\max_{\mathrm{D}\in\mathcal{D}}|\Delta^{\mathrm{D}}(X;Y)|$ where \mathcal{D} is a fixed class of boolean functions. We say that X and Y are (s,ϵ) -close or (s,ϵ) -indistinguishable if $\Delta^{\mathrm{D}}(X;Y) \leqslant \epsilon$ for all D of size at most s.

HARDNESS OF UNPREDICTABILITY. A boolean function $f:\{0,1\}^n \to \{0,1\}$ is said to be (s,δ) -unpredictable if $\Pr_{x\leftarrow\{0,1\}^n}[\mathrm{D}(x)=f(x)]\leqslant 1-\delta/2$ for all D of size at most s. We also say that f is δ -hard against circuits of size s. We say that that f is (s,δ) -unpredictable under the distribution V if $\Pr_{x\leftarrow V}[\mathrm{D}(x)=f(x)]\leqslant 1-\delta/2$ for all D of size at most s.

MEASURES AND DENSE DISTRIBUTIONS. X is δ-dense in Y if $\Pr[X = x] \leq \Pr[Y = x]/\delta$ for all x.

CIRCUITS. By $\mathcal{D}^{\{0,1\},s}$ and $\mathcal{D}^{[0,1],s}$ we denote the set of boolean and, respectively, real-valued circuits of size at most s.

COMPUTATIONAL ENTROPY. There are many ways to define computational analogues of entropy. We follow the most popular approach, which is based on the concept of computational indistinguishability.

Definition 1 (HILL Pseudoentropy [HILL99]). Let X be a distribution with the following property: there exists Y of min-entropy at least k such that for all circuits D of size at most s we have $|\Delta^{D}(X;Y)| \leq \epsilon$. Then we say that X has k bits of HILL entropy of quality (s, ϵ) and denote by $\mathbf{H}^{HILL}_{s,\epsilon}(X) \geq k$.

³ Understood as the ratio of the number of extracted bit to the length of the input.

⁴ We note that the following issues makes this problem challenging: (a) since ϵ is large, no hybrid technique can be applied and (b) pseudoentropy is *only* against deterministic adversaries so no extractor can be directly applied

It is known that for HILL Entropy all kind of circuits: deterministic boolean, deterministic real valued and randomized boolean, are equivalent (with the same size s). The following definition differs in the order of quantifiers

Definition 2 (Metric Pseudoentropy [BSW03]). Let X be a distribution with the following property: for every deterministic boolean (respectively: deterministic real valued or boolean randomized) circuit D of size at most s there exists Y of min-entropy at least k such that $|\Delta^D(X;Y)| \leq \epsilon$. Then we say that X has k bits of deterministic (respectively: deterministic real valued or boolean randomized) metric entropy of quality (s,ϵ) and denote by $\mathbf{H}^{\text{Metric,det}\{0,1\}}_{s,\epsilon}(X) \geqslant k$ (respectively: $\mathbf{H}^{\text{Metric,det}[0,1]}_{s,\epsilon}(X)$ and $\mathbf{H}^{\text{Metric,rand}}_{s,\epsilon}(X)$).

APPROXIMATING CONVEX HULLS. The following facts are useful when we want to approximate possibly long convex combinations of functions by a combination of few functions; in particular, when we use the min-max theorem and need to approximate any mixed strategy by an efficient strategy.

Lemma 1 ([BSW03]). Let \mathcal{X} be a finite domain, ν be a distribution on \mathcal{X} and let \mathcal{G} be any set of functions $g: \mathcal{X} \to [-1,1]$ and let \overline{g} be a convex combinations of functions from \mathcal{G} . Then for any $\epsilon \in (0,1)$ and for some $k \leq \frac{\log |\mathcal{X}|}{2\epsilon^2}$, there exist functions g_1, \ldots, g_k such that

$$\max_{x \in \mathcal{X}} \left| \overline{g}(x) - \left(\frac{1}{k} \sum_{i=1}^{k} g_i(x) \right) \right| \leqslant \epsilon$$

Lemma 2 (Convex approximation in L^p **spaces** [DDGS97]). Let \mathcal{X} be a finite domain, ν be a distribution on \mathcal{X} . Fix a number $1 \leq p < +\infty$ and for any function f on \mathcal{X} define $||f||_p = (\mathbf{E}_{x\leftarrow\nu}|f(x)|^p)^{\frac{1}{p}}$. Let \mathcal{G} be any set of real functions on \mathcal{X} , let \overline{g} be a convex combinations of functions from \mathcal{G} and K > 0 be such that for all $g \in \mathcal{G}$ we have $||\overline{g} - g||_p \leq K$. Then for any $\ell > 0$ there exists a convex combination $g' = \sum_{i=1}^{\ell} \alpha_i g_i$ of functions $g_1, \ldots, g_k \in \mathcal{G}$ such that

$$\|\overline{g} - g'\|_p \leqslant \frac{KC_p}{\ell^{1 - \frac{1}{t}}}$$

where $t = \min(2, p)$ and $C_p = 1$ if $1 \le p \le 2$, $C_p = \sqrt{2} [\Gamma((p+1)/2)/\sqrt{\pi}]^{1/p}$ for 2 .

3 Hardcore Lemmas

3.1 Hardcore lemma for unpredictability

Below we prove a general hardcore lemma for unpredictability.

Theorem 3 (Unpredictability Hardcore Lemma for arbitrary distributions). Let V be an arbitrary distribution on $\{0,1\}^n$ and suppose that an n-bit boolean function f is (s,ϵ) -unpredictable under V. Then for any δ there exists an event A of probability at least 2ϵ such that f is $(s', 1-\delta)$ -unpredictable under V|A, where $s' = O\left(s\delta^2 \cdot \max\left(1/n, 1/\log(1/\epsilon)\right)\right)$.

Note that f is essentially almost unbiased under V|A: by applying trivial distinuguishers $D \equiv 1$ and $D \equiv 0$ we get $\frac{1}{2} - \delta \leqslant \Pr[f(V|A) = 1] \leqslant \frac{1}{2} + \delta$. For some technical reasons we need the following observation, which states that the hardcore event "preserves" unbiased predicates.

Corollary 1 (Unpredictability Hardcore Lemma for unbiased predicates). Suppose that Theorem 3 holds for f and V such that $\mathbf{P}(f(V) = -1) = \frac{1}{2} = \mathbf{P}(f(V) = 1)$. Then the hardcore event A can be chosen in such a way that $\mathbf{P}(f(V|A) = -1) = \mathbf{P}(f(V|A) = 1) = \frac{1}{2}$, with the additional loss of a factor O(1) in circuit size.

The proof of Corollary 1 appears in Appendix A. It is relatively simple and uses the idea of "mass-shifting". The proof of Theorem 3 appears in Appendix B.

3.2 Hardcore lemma for indistinguishability - reduction to unpredictability case

The following lemma shows that indistinguishability of two distributions is equivalent to the hardness of predicting some boolean function, which explicitly depends on these distributions. This function is quite natural: it equals the sign of the difference between the probability mass functions.

Lemma 3. Let \mathcal{D} be a class of boolean functions, $X,Y \in \{0,1\}^n$ be random variables, and let $\Delta = \Delta(X,Y)$ be different than 0. Then the following are equivalent:

- (a) X and Y are (\mathcal{D}, ϵ) -indistinguishable
- (b) f(x) is $(\mathcal{D}, 1 \epsilon/\Delta)$ -unpredictable under V, where f(x) is the indicator of the set $\{x : \mathbf{P}_X(x) > \mathbf{P}_Y(x)\}$ and the distribution of V is given by $\mathbf{P}_V(x) = |\mathbf{P}_X(x) \mathbf{P}_Y(x)|/2\Delta$.

Proof. For any boolean D we obtain

$$\begin{split} \mathbf{E} \operatorname{D}(X) - \mathbf{E} \operatorname{D}(Y) &= \sum_{x} (\mathbf{P}_{X}(x) - \mathbf{P}_{Y}(x)) \operatorname{D}(x) \\ &= 2 \Delta \left(\operatorname{Pr}[f(V) = 1] \operatorname{\mathbf{E}}[\operatorname{D}(V) | f(V) = 1] \right. \\ &\left. - \operatorname{Pr}[f(V) = 0] \operatorname{\mathbf{E}}[\operatorname{D}(V) | f(V) = 0] \right) \end{split}$$

Observe that $\Pr[f(V) = 1] = \Pr[f(V) = 0] = \frac{1}{2}$. Therefore

$$\mathbf{E}\,\mathrm{D}(X) - \mathbf{E}\,\mathrm{D}(Y) = 2\Delta \left(-\frac{1}{2} + \frac{1}{2}\,\mathbf{E}[\mathrm{D}(V)|f(V) = 1] + \frac{1}{2}\,\mathbf{E}[(1-\mathrm{D}(V))|f(V) = 0] \right).$$

Since D is boolean, the last equation is equivalent to

$$\mathbf{E}\,\mathrm{D}(X) - \mathbf{E}\,\mathrm{D}(Y) = 2\Delta\left(\Pr[\mathrm{D}(V) = f(V)] - \frac{1}{2}\right),$$

which finishes the proof.

Based on Lemma 3 we prove the following result

Theorem 4 (Indistinguishability Hardcore Lemma). Suppose that X and Y are distributions (s, ϵ) -indistinguishable by boolean circuits Then for any $\delta > 0$ there exist events A(X), A(Y), both of equal probability at least $1 - \epsilon$, such that X|A(X) and Y|A(Y) are $(O\left(s \cdot \delta^2/\log(\Delta(X;Y)/\epsilon)\right), \Delta(X;Y) \cdot \delta)$ indistinguishable.

Proof. From the construction of V, we obtain that f is $(s, 1 - \epsilon/\Delta(X, Y))$ -unpredictable under V. From Theorem 3 we obtain that there exists a hard-core A with probability at least $1 - \epsilon/\Delta(X, Y)$ such that f is extremely unpredictable under V|A. This hardcore event can be described as follows: there exists a measure $M = M_A$ that satisfies $M(x) \leq \mathbf{P}_V(x)$ and $\mathbf{P}(A) = \mu(M) \geq 1 - \epsilon/\Delta(X, Y)$ and such that f(x) is unpredictable for sampling according to M, i.e. $\mathbf{P}_{x \leftarrow M}(D(x) = f(x)) < 1/2 + \delta$. The distribution V|A is then defined by $\mathbf{P}_{V|A} = \mathbf{P}_M$. Consider the events $S^- = \{x : f(x) = 0\}$ and $S^+ = \{x : f(x) = 1\}$. From the definition of V and f it follows that $\mathbf{P}_V(S^-) = \mathbf{P}_V(S^+) = \frac{1}{2}$. As shown in Corollary 1, the sets S^+, S^- can be assumed to be perfectly unbiased also under V|A. Define now two measures $M_0 = M_X$ and $M_1 = M_Y$ as follows:

$$M_0(x) = \begin{cases} \mathbf{P}_X(x) - 2\Delta(X, Y) \left(\mathbf{P}_V(x) - M'(x) \right) & \text{if } \mathbf{P}_X(x) > \mathbf{P}_Y(x) \\ \mathbf{P}_X(x) & \text{otherwise} \end{cases}$$
(1)

and similarly,

$$M_1(x) = \begin{cases} \mathbf{P}_Y(x) - 2\Delta(X, Y) \left(\mathbf{P}_V(x) - M'(x) \right) & \text{if } \mathbf{P}_X(x) < \mathbf{P}_Y(x) \\ \mathbf{P}_Y(x) & \text{otherwise} \end{cases}$$
(2)

Note that both measures are well defined since $\mathbf{P}_V(x) = |\mathbf{P}_X(x) - \mathbf{P}_Y(x)| / 2\Delta(X, Y)$ and $M'(x) \leq \mathbf{P}_V(x)$. Then from the definition of (V, A) and the definition of f it follows that

$$\mu(M_0) = 1 - 2\Delta(X, Y) \sum_{x: f(x)=1} \mathbf{P}_V(x) + 2\Delta(X, Y) \sum_{x: f(x)=1} M'(x)$$

$$= 1 - \Delta(X, Y) + 2\Delta(X, Y) \mathbf{P}(A) \cdot \mathbf{P}_{V|A} \left(S^+\right)$$

$$= 1 - \Delta(X, Y) \mathbf{P}(A^c)$$

$$\geqslant 1 - \epsilon$$
(3)

and similarly that the same estimate holds for $\mu(M_1)$. Observe also that since S^+ and S^- are perfectly unbiased with respect to M', and since the same holds for V, we have $\mu(M_0) = \mu(M_1)$. These measures give rise to the joint distributions X, A(X) and Y, A(Y) for some events A(X), A(Y) with probabilities at least $\mu(M_0) = \mu(M_1)$. It remains to calculate the advantage in distinguishing. Let V' and f' be a distribution and a predicate corresponding to X|A(X) and Y|A(Y) according to the statement of Lemma 3. Observe that $M_0(x) > M_1(x)$ if and only if f(x) = 1, hence f'(x) = f(x). Since $|M_0(x) - M_1(x)| = 2\Delta(X, Y)M'(x)$ for

every x, we get $\mathbf{P}_V(x) = M'(x)/\mu(M') = \mathbf{P}_{V|A}(x)$ and $\Delta(X|A(X),Y|A(Y)) = \Delta(X,Y)$. Therefore

$$\Delta^{D}(X|A(X), Y|A(Y)) = \Delta(X, Y) \cdot (2\mathbf{P}_{x \leftarrow V'}(D(x) = f'(x)) - 1)$$

$$= \Delta(X, Y) \cdot (2\mathbf{P}_{x \leftarrow V|A'}(D(x) = f(x)) - 1)$$

$$< \Delta(X, Y) \cdot \delta, \tag{4}$$

and we have finished the proof.

Remark 4. We note that without Corollary 1 we would obtain a slightly weaker version of the indistinguishability hardcore lemma where the probability of the hardcore events is guaranteed to be at least $1 - \epsilon - \delta$, which is very close to the optimal $1 - \epsilon$ and equally good in applications.

4 Indistinguishability Hardcore Lemma for Pseudoentropy

In this section we prove the following theorem, which gives the existence of a "HILL-entropy-hardcore" for metric pseudoentropy.

Theorem 5 (Indistinguishability Hardcore Lemma for pseudoentropy). Suppose that $\mathbf{H}_{s,\epsilon}^{\mathrm{Metric,det}\{0,1\}}(X) \geqslant k$. Then for any δ and $s' = O\left(s \cdot \delta^2/n\right)$ there exists an event A of probability $1 - \epsilon$ such that $\mathbf{H}_{s',\delta}^{\mathrm{HILL}}(X|A) \geqslant k - \log(1/(1 - \epsilon))$.

This theorem shows that metric entropy not only can be converted to HILL entropy with the loss of factor δ in advantage and δ^2 in circuit size; It has a hardcore of HILL entropy with the same quality parameters. Before we give the proof, let us observe that this result implies the transformation between metric and HILL entropy (up to the lose of at most one bit)

Corollary 2 (Metric entropy - HILL entropy transformation [BSW03]). Suppose that $\mathbf{H}_{s,\epsilon}^{\text{Metric,det}\{0,1\}}(X) \geqslant k$. Then $\mathbf{H}_{s',\epsilon'}^{\text{HILL}}(X) \geqslant k$ where $s' = O\left(s \cdot \delta^2/n\right)$ and $\epsilon' = \epsilon + \delta$.

Proof (Proof of Corollary 2). We apply Theorem 5 obtaining a distribution Y|A which is (s', δ) -indistinguishable from X|A, and then we define $\Pr[Y' = x] = \Pr[A] \cdot \Pr[Y = x|A] + 2^{-n} \Pr[A^c]$. Note that $\mathbf{H}_{\infty}(Y') \geqslant k-1$ and Y' is $(s', \epsilon + \delta)$ -indistinguishable from X. We remark that one can actually show without the loss of 1 bit, because Theorem 5 actually is slightly stronger that stated, namely $\mathbf{H}^{\mathrm{HLL}}_{s',\delta}(X|A) \geqslant k - \log(1/(1-\epsilon))$ can be replaced by the following: X|A is (s', δ) -indistinguishable from Y|A where Y has k bits of min-entropy.

The proof strategy for Theorem 5 is exactly the same as in the case of Theorem 3. The full proof is given in Appendix C. Note that the result in Theorem 5 with much worse parameters follows by converting metric-entropy into HILL entropy using Corollary 2 and then applying Theorem 2. This way we lose δ^4 in circuit size.

Corollary 3 (Direct proof of the Indistinguishability Hardcore Lemma). The proof of Theorem 5 can be easily adapted to give a direct proof of Theorem 4 without reducing it to Theorem 3. Namely, in the proof we replace the condition $M_2 \leq 2^{-k}$ by $M_2 \leq \mathbf{P}_Y$.

5 Applications: extracting from metric pseudoentropy of poor quality

Suppose that we have a source of metric pseudoentropy that produces samples secure against deterministic adversaries of high complexity but only with a very big advantage ϵ (for instance, $\epsilon=0.25$). Since the metric entropy is only against deterministic adversaries, for which it is not known [FOR12] if we can extract pseudorandomness directly⁵, one needs to convert in into the HILL entropy. However, it still does not solve the problem of large ϵ . In the next step one can use Theorem 2 to prove that a concatenated sequence of many samples has large HILL entropy⁶., with the rate of roughly $1-\epsilon$. This approach loses $O\left(\delta^4\right)$ in security. Below we show that these two steps can be done at the same time which allows us to save a factor of $O\left(\delta^2\right)$ in security.

Theorem 6. Suppose that X_i , for $i=1,\ldots,\ell$, are independent n-bit random variables such that $\mathbf{H}_{s,\epsilon}^{\mathrm{Metric,det}\{0,1\}}(X) \geqslant k$. Then for any $\gamma > 0$ we have

$$\mathbf{H}^{\mathrm{HILL}}_{s',\delta'}(X) \geqslant (1-\epsilon-\gamma)\ell\left(k-\log(1/(1-\epsilon))\right),$$

where
$$s' = O\left(s \cdot \delta^2/n\ell^2\right)$$
 and $\delta' = \delta + 2\exp(-2\ell\gamma^2)$

Proof. Fix δ and let $s' = O\left(s \cdot \delta^2/n\right)$. We apply Theorem 5 to X_i , for $i = 1, \ldots, \ell$, obtaining hardcore events A_i of probability at least $1 - \epsilon$ such that $\mathbf{H}^{\mathrm{HILL}}_{s',\delta}(X_i|A_i) \geq k - \log(1/(1-\epsilon))$. By the Chernoff Bound we know that the probability that $m = \ell(1-\epsilon-\gamma)$ of them happen simultaneously, is at least $1 - 2\exp(-2\ell\gamma^2)$. The result follows now by the observation that concatenating ℓ random variables Y_1, \ldots, Y_ℓ of HILL entropy k_1, \ldots, k_ℓ with parameters (s', δ) yields a distribution of HILL entropy $k_1 + k_2 + \ldots + k_\ell$ with parameters $(s', \ell\delta)$ (the proof follows by a standard hybrid argument).

6 Acknowledgments

The author would like to thank Krzysztof Pietrzak for helpful discussions, and the anonymous referee for valuable criticism.

⁵ The problem of randomized vs deterministic adversaries is the matter of metric entropy only; for the HILL entropy all kind of circuits are equivalent

 $^{^{6}}$ Maurer and Tessaro construct in the same way a PRG from a weak PRG

7 Conclusion

An interesting open problem is to check if the indistinguishability hardcore lemma can be derived from the unpredictability hardcore lemma, that is show the reduction in other direction than in [MT10] and this paper. Another problem worth of mentioning is the question about lower bounds on the necessary loss in security for indistinguishability hardcore lemma.

References

- BHK09. Boaz Barak, Moritz Hardt, and Satyen Kale, *The uniform hardcore lemma via approximate bregman projections*, SODA '09, Society for Industrial and Applied Mathematics, 2009, pp. 1193–1200.
- BSW03. Boaz Barak, Ronen Shaltiel, and Avi Wigderson, Computational analogues of entropy., RANDOM-APPROX, vol. 2764, Springer, 2003, pp. 200–215.
- DDGS97. M.J. Donahue, C. Darken, L. Gurvits, and E. Sontag, Rates of convex approximation in non-hilbert spaces, Constructive Approximation 13 (1997), no. 2, 187–220.
- DP08. Stefan Dziembowski and Krzysztof Pietrzak, *Leakage-resilient cryptography*, FOCS '08, IEEE Computer Society, 2008, pp. 293–302.
- FOR12. Benjamin Fuller, Adam O'Neill, and Leonid Reyzin, A unified approach to deterministic encryption: New constructions and a connection to computational entropy, TCC'12, Springer-Verlag, 2012, pp. 582–599.
- GNW11. Oded Goldreich, Noam Nisan, and Avi Wigderson, Studies in complexity and cryptography, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 273–301.
- HILL99. Johan Hastad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby, A pseudorandom generator from any one-way function, SIAM J. Comput. 28 (1999), no. 4, 1364–1396.
- Hol05. Thomas Holenstein, Key agreement from weak bit agreement, STOC '05, ACM, 2005, pp. 664–673.
- Imp95. R. Impagliazzo, *Hard-core distributions for somewhat hard problems*, FOCS '95, IEEE Computer Society, 1995, pp. 538–.
- KS99. Adam R. Klivans and Rocco A. Servedio, *Boosting and hard-core sets*, FOCS '99, IEEE Computer Society, 1999, pp. 624–.
- KS03. _____, Boosting and hard-core set construction, Mach. Learn. **51** (2003), no. 3, 217–238.
- LT13. Huijia Lin and Stefano Tessaro, Amplification of chosen-ciphertext security, Advances in Cryptology EUROCRYPT 2013, Springer Berlin Heidelberg, 2013, pp. 503–519.
- LTW07. Chi-Jen Lu, Shi-Chun Tsai, and Hsin-Lung Wu, On the complexity of hard-core set constructions, ICALP'07, Springer-Verlag, 2007, pp. 183–194.
- MT10. Ueli Maurer and Stefano Tessaro, A hardcore lemma for computational indistinguishability, TCC'10, Springer-Verlag, 2010, pp. 237–254.
- Sko15. Maciej Skorski, Indistinguishability and unpredictability hardcore lemmas:

 New proofs with applications to pseudoentropy, Student Research Forum at
 SOFSEM 2015, 2015, pp. 78–89.
- VZ12. S. Vadhan and C. J. Zheng, Characterizing pseudoentropy and simplifying pseudorandom generator constructions, STOC '12, ACM, 2012, pp. 817–836.

A Proof of Corollary 1

Proof (Proof of Corollary 1). Let $M(x) = \Pr[V = x, A]$. Since $M(x) \leq \mathbf{P}_V(x)$ and we have $M(S^-)$, $M(S^+) \leq \frac{1}{2}$. Suppose that $M(S^+) - M(S^-) = 2\delta_0$. Then $M\left(S^{-}\right) = \frac{\mu(M)}{2} - \delta_{0}$ and $M\left(S^{+}\right) = \frac{\mu(M)}{2} + \delta_{0}$. Suppose $\delta_{0} > 0$. Since $M\left(S^{-}\right) \leqslant \mathbf{P}\left(S^{-}\right) - \delta_{0}$ and $M\left(S^{+}\right) \geqslant \delta_{0}$, we can define the measure M' by decreasing the mass of S^+ by δ_0 and moving it to S^- in such a way that $M'(x) \leq \mathbf{P}_V(x)$ still holds on S^- . For the case $\delta_0 < 0$ observe that $M(S^+) \leq \mathbf{P}(S^+) - (-\delta_0)$ and $M(S^{-}) \ge -\delta_0$ thus we proceed similarly by decreasing the mass of S^{-} by $(-\delta_0)$ and moving it to S^+ in such a way that $M'(x) \leq \mathbf{P}_V(x)$ holds on S^+ . Therefore, in both cases we have $M'(x) \leq \mathbf{P}_V(x)$. Clearly $M'(S^+) = M'(S^-)$. Thus the measure M' gives rise to a distribution V, A'. While constructing M'from M we only shift a mass between disjoint sets, hence $\mu(M) = \mu(M')$ and $\mathbf{P}(A) = \mathbf{P}(A')$. It remains to show, that under distribution V|A' the function f is still unpredictable. Applying trivial distinguishers D=1 and D=-1 to unpredictability under V|A, we get $M(S^+), M(S^-) \leq (1/2 + \delta)\mathbf{P}(A)$. Since $M(S^{+}) + M(S^{-}) = \mathbf{P}(A)$ it follows then that $2 |\delta_{0}| = |M(S^{+}) - M(S^{-})| \le$ $2\delta \mathbf{P}(A)$. Since the total mass that of M that is shifted to M' is equal to δ_0 , we have $||M'-M||_1 = \sum |M'(x)-M(x)| \le 2|\delta_0| \le 2\delta \mathbf{P}(A)$. Since $\mathbf{P}(A') = \mathbf{P}(A)$, this implies $\Delta(V|A,V|A') \leq 2\delta$. Therefore, for every D of size s' we obtain $\mathbf{P}_{x \leftarrow V|A'}(D(x) = f(x)) < \frac{1}{2} + \delta + 2\delta$. Replacing δ with $\delta/3$ changes the circuit size only by a (small) constant factor.

B Proof of Theorem 3

Proof. In this proof, for convenience, we assume that boolean functions take values in $\{-1,1\}$.

Step 1. We extended the concept of unpredictability to all real-valued functions. The following straightforward but very useful property is easy to check:

Lemma 4. Let f and D be boolean. Then f is ϵ -unpredictable by D under V if and only if $\mathbf{E}_{x\leftarrow V}D(x)f(x) \leq 1 - \epsilon$.

Step 2. We show how to construct a hardcore for a *single boolean* attacker D. For some technical reasons, we need actually a slightly stronger statement, namely a construction for a function D which takes values -1, 0, 1.

Lemma 5. Suppose that for a distribution V, a function D with values in $\{-1,0,1\}$ and a boolean function f we have $\mathbf{E}_{x\leftarrow V}D(x)f(x)=\pm\delta$. Then there is a measure M such that $M(x) \leq \mathbf{P}_V(x)$, $\mu(M) \geq 1-\delta$ and $\mathbf{E}_{x\leftarrow M}D(x)f(x)=0$.

Proof. By replacing D by -D we can assume that $\mathbf{E}_{x \leftarrow V} D(x) f(x) = \delta > 0$. Let $S_1 = \{x : D(x) f(x) > 0\}$. If follows that $\Pr[V \in S_1] = \sum_{x \in S_1} \mathbf{P}_V(x) D(x) \ge \delta$. Now we define $M(x) = \mathbf{P}_V(x) \cdot (\Pr[V \in S^1] - \delta) / \Pr[V \in S_1]$ for $x \in S_1$ and $M(x) = \mathbf{P}_V(x)$ otherwise. M satisfies the required properties.

Step 3. We argue that the same is true for real-valued functions D.

Lemma 6. Suppose that f is ϵ -unpredictable by boolean circuits of size s under a distribution V. Then for every real-valued D of size $s' \approx s$ there exists a measure M such that $M(x) \leq \mathbf{P}_V(x)$ for every x, $\mu(M) \geq \epsilon$ and $\mathbf{E}_{x \leftarrow M} D(x) f(x) = 0$.

Proof. Suppose not. Since the set of feasible measures M is convex, this is we must have either $\mathbf{E}_{x \leftarrow M} \mathrm{D}(x) f(x) > 0$ for all M or $\mathbf{E}_{x \leftarrow M} \mathrm{D}(x) f(x) < 0$ for all M. By eventually replacing D with $-\mathrm{D}$ we obtain that there exists a real-valued circuit D of size s such that for all measures M satisfying the constraints

$$\sum_{x} D(x)f(x)M(x) > 0.$$

Now we give a characterization of the measure that minimizes the left-hand side in the inequality above.

Claim 1. Let M_0 be an optimal solution of the following problem

minimize
$$\sum_{x} D(x) f(x) M(x)$$
s.t.
$$\begin{cases} M(x) \leq \mathbf{P}_{V}(x) \\ \mu(M) \geq \epsilon \end{cases}$$

Define $S = \{x : \operatorname{sgnD}(x) = f(x)\}$ and let $p = \mathbf{P}(V \in S)$. Let x_i for $i = 1, \dots, M$ be the elements of S, enumerated in such a way that $|\mathbf{D}(x_i)| \geqslant |\mathbf{D}(x_{i+1})|$. Let N be the maximal number such that $N \leqslant M$ and $\sum_{i=1}^{N} \mathbf{P}_V(x_i) \leqslant \min(1 - \epsilon, p)$. Then the measure M_0 defined by $M_0(x) = 0$ if $x = x_i$ for some $i \in [1, N]$ and $M_0(x) = \mathbf{P}_V(x)$ otherwise, is the minimizer.

Proof. It is clear that for the optimal measure M_0 , the mass of $\mathbf{P}_V(x)$ is decreased only if $f(x)\mathbf{D}(x) > 0$ and keeps unchanged if $f(x)\mathbf{D}(x) < 0$. Thus, the total mass we cut is equal to at most

$$\sum_{x: \ \mathrm{D}(x)f(x)>0} \mathbf{P}_V(x) = p$$

In the other hand, it is bounded from above by $1 - \epsilon$ due to the constraint $\mu(M) \ge \epsilon$. The last observation is that if D(x)f(x) > 0, the greater the absolute value of D(x) is, the more mass we cut.

As a conclusion from Claim 1 we get that $\mu(M_0) = \max(\epsilon, 1-p)$. From the definition of M_0 we have that

$$\min_{\substack{M \leq M \leq \mathbf{P}_V \\ \mu(M) \geqslant \epsilon}} \sum_{x} \mathrm{D}(x) f(x) M(x) = \sum_{x} \mathrm{D}(x) f(x) M_0(x)$$

Let $D_1(x) := D(x) \cdot \mathbf{1}_{\{f>0\}}$ and $D_2(x) := D(x) \cdot \mathbf{1}_{\{f<0\}}$. Then we have

$$\mathbf{E}_{x \leftarrow M_0} D(x) f(x) = \mathbf{E}_{x \leftarrow M_0} D_1^+(x) - \mathbf{E}_{x \leftarrow M_0} D_1^-(x) - \mathbf{E}_{x \leftarrow M_0} D_2^+(x) + \mathbf{E}_{x \leftarrow M_0} D_2^-(x)$$

By applying the formula $\mathbf{E}Y = \int\limits_{t \in [0,1]} \mathbf{P}(Y>t) \; \mathrm{d}t$ (valid for any random variable

 $Y \in [0,1]$) to $Y = \mathbf{P}_{M_0}$ we obtain that for some $t = t_0 \in (0,1)$ and D' defined by $D'(x) = \operatorname{sgnD}(x) \cdot \mathbf{1}_{|D(x)| > t_0}$ we get

$$\Pr[D_1^+(Y) > t_0] - \Pr[D_1^-(Y) > t_0] - \Pr[D_2^+(Y) > t_0] + \Pr[D_2^-(Y) > t_0] > 0,$$

which is equivalent to

$$\mathbf{E}_{x \leftarrow M_0} \mathbf{D}'(x) f(x) > 0.$$

Observe that, by the construction, $\operatorname{sgn} D' = \operatorname{sgn} D$ and $|D(x_1)| \ge |D(x_2)|$ is equivalent to $|D'(x_1)| \ge |D'(x_2)|$. Therefore, applying the characterization given by Claim 1 to the two cases: D, M_0 and D', M_0 , we obtain that M_0 is a minimizer for both circuits. Therefore

$$\min_{\substack{M: M \leq \mathbf{P}_V \\ u(M) \geq \epsilon}} \sum_{x} \mathbf{D}'(x) f(x) M(x) = \sum_{x} \mathbf{D}'(x) f(x) M_0(x) > 0$$

which gives us a contraddiction to Lemma 5.

Step 4. We argue that Lemma 6 holds approximately for all convex combinations of circuits of size comparable to s. Let D" be a convex combination of real-valued circuits of size $s'' = O\left(s\delta^2/\log(1/\epsilon)\right)$. From Lemma 2 applied to D", we obtain that for some real-valued circuit D' of size $s' \approx s$ we have

$$\left(\underbrace{\mathbf{E}}_{x \leftarrow V} \left| \mathbf{D}''(x) - \mathbf{D}'(x) \right|^p \right)^{\frac{1}{p}} = O\left(\delta \cdot \sqrt{p/\log(1/\epsilon)}\right)$$
 (5)

Let M be the "hardcore" measure corresponding to D' according to Lemma 6. Since |f| = 1 and $\mathbf{E}_{x \leftarrow M} D'(x) f(x) = 0$, we obtain

$$\underset{x \leftarrow M}{\mathbf{E}} \mathbf{D}''(x) f(x) \leqslant \underset{x \leftarrow M}{\mathbf{E}} \left| \mathbf{D}''(x) - \mathbf{D}'(x) \right| \tag{6}$$

By the Hölder Inequality we obtain

$$\underset{x \leftarrow M}{\mathbf{E}} \left| \mathbf{D}''(x) - \mathbf{D}'(x) \right| \leqslant \left(\underset{x \leftarrow V}{\mathbf{E}} \left(\frac{\mathbf{P}_M(x)}{\mathbf{P}_V(x)} \right)^q \right)^{\frac{1}{q}} \cdot \left(\underset{x \leftarrow V}{\mathbf{E}} \left| \mathbf{D}''(x) - \mathbf{D}'(x) \right|^p \right)^{\frac{1}{p}}$$
(7)

We will show that

$$\left(\underset{x \leftarrow V}{\mathbf{E}} (\mathbf{P}_M(x)/\mathbf{P}_V(x))^q\right)^{\frac{1}{q}} \leqslant (1/\epsilon)^{\frac{1}{p}} \tag{8}$$

Indeed, consider the set \mathcal{M} of all distributions ϵ -dense in V. By definition, we have $\mathbf{P}_M \in \mathcal{M}$. Since the expression on the left-hand side of Equation (8) is convex with respect to \mathbf{P}_M , its maximum over \mathcal{M} is achieved on one of *extreme*

points of the set \mathcal{M} . It is easy to check that the extreme points **P** of \mathcal{M} satisfy $\mathbf{P}(x) = \mathbf{P}_V(x)/\epsilon$ for all but at most one $x \in \text{supp}(\mathbf{P})^7$. For any such \mathbf{P} we have

$$\underset{x \leftarrow V}{\mathbf{E}} \left(\frac{\mathbf{P}(x)}{\mathbf{P}_{V}(x)} \right)^{q} \leqslant \frac{1}{\epsilon^{q}} \cdot \epsilon \cdot (1 - \mathbf{P}(x')) + \left(\frac{\mathbf{P}(x')}{\mathbf{P}_{V}(x')} \right)^{q} \cdot \mathbf{P}_{V}(x')$$

where x' is the point such that $0 < \mathbf{P}(x') \leq \mathbf{P}_V(x)/\epsilon$. Since the right-hand is convex with respect to P(x'), it is maximized either for P(x') = 0 or P(x') = 0 $\mathbf{P}_V(x)/\epsilon$. In any case, it is at most ϵ^{1-q} . Let $p=2\log(1/\epsilon)$. Combining Equation (6), Equation (7), Equation (8) and Equation (5) we get

$$\underset{x \leftarrow M}{\mathbf{E}} D''(x) f(x) \le \delta. \tag{9}$$

Alternatively, we can use of Lemma 1, with $s'' = O(s\delta^2/n)$.

Step 5. By applying the min-max theorem we reverse the order of quantifiers: we obtain that there exists a measure M satisfying $\mu(M) \ge \epsilon$ and $M(x) \le \epsilon$ $\mathbf{P}_{V}(x)$ such that Equation (9) hold for all circuits D" of size s. By replacing D'' with -D'' we see that these inequalities hold in absolute values. It remains to observe that the measure M gives rise to a joint distribution (V, A) where $M(x) = \Pr[V = x, A = 1]$. In particular, $\Pr[A = 1] = \mu(M) \ge \epsilon$.

\mathbf{C} Proof of Theorem 5

Proof (Proof of Theorem 5). By considering the functions $P(X = x, A_1)$ and $P(Y = x, A_2)$ for some events A_1, A_2 , it is easy to see that, equivalently, we need to find measures M_1, M_2 which satisfy the following conditions:

- $\begin{array}{ll} \text{(a)} \ \ M_1 \leqslant \mathbf{P}_X(x) \ \text{and} \ M_2 \leqslant 2^{-k} \\ \text{(b)} \ \ \mu(M_1) = \mu(M_2) \geqslant 1 \epsilon \\ \text{(c)} \ \ \Delta^D\left(\mathbf{P}_{M_1},\mathbf{P}_{M_2}\right) \leqslant \delta \ \text{for every} \ D \ \text{of size} \ s'. \end{array}$

First, we show how to construct measures satisfying these conditions only for one fixed boolean circuit D

Claim 2. Let \mathcal{X} be a finite domain. Suppose that we are given a boolean function D and two probability distributions μ_1, μ_2 on \mathcal{X} , such that $\Delta^D(\mu_1, \mu_2) = \epsilon$. Then there exist measures M_1, M_2 such that:

- (a) $M_i(x) \leq \mu_i(x)$ for every x and i,
- (b) $\mu(M_1) = \mu(M_2) = 1 \epsilon$, (c) $\sum_{x} D(x)M_1(x) = \sum_{x} D(x)M_2(x)$.

Proof. Assume $\sum_{x} D(x)\mu_1(x) - \sum_{x} D(x)\mu_2(x) = \epsilon$ (the other case is symmetric). By decreasing the measure μ_1 on the set $\{x: D(x)=1\}$ we define a measure M_1 such that $M_1(x) \leqslant \mu_1(x)$ and $\mu(M_1) = 1 - \epsilon$ and $\sum_{x} D(x)M_1(x) = \sum_{x} D(x)\mu_2(x)$.

Now consider $\{x: D(x) = 0\}$ and proceed similarly to obtain M_2 from μ_2 .

 $^{^{7}}$ This observation can be viewed as a generalization of the well-known fact that the extreme points for the set of all high min-entropy distributions are flat distributions.

Next we argue that the same is also possible for a real-valued circuit. This is the main technical difficulty in the proof.

Claim 3. Suppose that for any boolean D of size s there exist measures M_1, M_2 such that $M_1(x) \leq \mathbf{P}_X(x)$ and $M_2(x) \leq 2^{-k}$ for every x and $\mu(M_1) = \mu(M_2) \geq 1 - \epsilon$ and $\left| \sum_x D(x) M_1(x) - \sum_x D(x) M_2(x) \right| \leq \delta$. Then the same is true for real-valued circuits of size D.

Proof. Suppose not. Since feasible measure M_1, M_2 form convex sets, we have either $\sum_{x} D(x) M_1(x) - \sum_{x} D(x) M_2(x) < -\delta$ for all feasible M_1, M_2 or $\sum_{x} D(x) M_1(x) - \sum_{x} D(x) M_2(x) > \delta$ for all feasible M_1, M_2 . Replacing D with D^c if necessary we can assume that for all measures M_1, M_2 satisfying the corresponding constraints, the following inequality holds

$$\sum_{x} D(x)M_1(x) - \sum_{x} D(x)M_2(x) > \delta.$$
(10)

We will characterize the measures $M_1 = M_1^+, M_2 = M_2^+$ which maximize the left-hand side of Equation (10), similarly as in Claim 1 in the proof of Theorem 3.

Claim 4. Suppose that the measures $M_1 = M_1^+, M_2 = M_2^+$ minimize

$$\sum_{x} D(x)M_1(x) - \sum_{x} D(x)M_2(x) > \delta,$$

subject to constraints $M_1(x) \ge 0$ and $M_2(x) \ge 0$ for all $x, \sum_x M_1(x) = 1 - \epsilon = \sum_x M_2(x), M_1(x) \le \mathbf{P}_X(x)$ and $M_2(x) \le a$ for all x. Let x_1, \ldots, x_N , where $N = 2^n$, be all the elements of $\{0,1\}^n$ sorted such that $\mathbf{D}(x_i) \ge \mathbf{D}(x_{i+1})$ and let T be the maximal number such that $\sum_{i=1}^T \mathbf{P}_X(x) \le \epsilon$. The optimal measures M_1^+, M_2^+ can be characterized as follows: $M_1^+(x_i) = 0$ for $i = 1, 2 \ldots, T, M_1^+(x_{T+1}) = \epsilon - \sum_{i=1}^T \mathbf{P}_X(x)$, and $M_1^+(x_i) = \mathbf{P}_X(x_i)$ for i > T+1; $M_2^+(x_i) = a$ for $i = 1, \ldots, \lfloor (1-\epsilon)/a \rfloor, M_2^+(x_{2^k+1}) = (1-\epsilon)/a - a \lfloor (1-\epsilon)/a \rfloor$.

Proof (Proof of Claim). The characterization of M_1^+ follows from the simple observation that if we have $D(x') \ge D(x)$, 0 < M(x') and $M(x) < \mathbf{P}_X(x)$, then we can decrease M(x') by δ and increase M(x) by $\delta = \min(M(x'), \mathbf{P}_X(x) - M(x))$ decreasing (or at least not increasing) the value of $\sum_x M(x)D(x)$. Consider now M_2^+ . Suppose that $D(x') \ge D(x)$, M(x') < a and 0 < M(x). Then we increase M on x' by δ and decrease M on x by δ , where $\delta = \min(a - M(x'), M(x))$, and increasing (or at least not decreasing) the value of $\sum_x D(x)M(x)$.

Since for every x we have $D(x) = \int_0^1 [D(x) \ge t] dt$, for some positive number t_0 and $D'(x) = [D(x) > t_0]$ we obtain

$$\sum_{x} D'(x) M_1^+(x) - \sum_{x} D'(x) M_2^+(x) \ge \delta.$$

The circuit D' is comparable in size to D and is boolean. Observe now that M_1^+ and M_2^- are also minimizers for D'. This follows by Claim 4 since the extreme measures depends only on the *ordering* of the values $\{D(x)\}_x$ and D', as a threshold, is a monotone transform of D.

Finally, by an approximation argument, we show that suitable measures exist for every D being a convex combination of circuit of size s'.

Claim 5. For any $D \in \operatorname{conv}\left(\mathcal{D}^{\det,\{0,1\},s'}\right)$ there exist measures M_1, M_2 such that $M_1(x) \leqslant \mathbf{P}_X(x)$ and $M_2(x) \leqslant 2^{-k}$ for every x and $\mu(M_1) = \mu\left(M_2\right) \geqslant 1 - \epsilon$ and $\left|\sum_x D(x) M_1(x) - \sum_x D(x) M_2(x)\right| \leqslant \delta$.

Proof (Proof of Claim). We know by Lemma 1 that any convex combination of circuits of size at most s' can be approximated up to the error δ by a convex combination of $\ell = O(n/\delta^2)$ of them. Let $D' = \sum_{i=1}^m a_i D_i$ be such a convex combination approximating D. Define M_1, M_2 as a measures corresponding to the real-valued circuit D'.

Claim 6. There exist measures M_1 and M_2 such that $M_1(x) \leq \mathbf{P}_X(x)$ and $M_2(x) \leq 2^{-k}$ for every x and $\mu(M_1) = \mu(M_2) \geq 1 - \epsilon$ and such that for every D of size at most s' we have $\left|\sum_x D(x)M_1(x) - \sum_x D(x)M_2(x)\right| \leq \delta$.

Proof. Consider a game where one player choses a cricuit D of size at most s' and the second choses a pair of measures (M_1, M_2) where M_1, M_2 satisfy $M_i(x) \leq \mathbf{P}_{X_i}(x)$ for every x and $\mu(M_1) = \mu\left(M_2\right) \geqslant 1 - \epsilon$. Let the payoff matrix be given by $\sum_x D(x) M_1(x) - \sum_x D(x) M_2(x)$. By combining the claim with the min-max theorem we get measures M_1, M_2 satisfying the same conditions and such that for every D of size at most s' we have

$$\sum_{x} D(x)M_1(x) - \sum_{x} D(x)M_2(x) \leqslant \delta. \tag{11}$$

Applying this to D^c and using $\mu(M_1) = \mu(M_2)$ we get also

$$\sum_{x} D(x)M_1(x) - \sum_{x} D(x)M_2(x) \geqslant -\delta.$$
(12)

for all circuits of size at most s'-1. Thus the proof is finished.

Define $\mathbf{P}(X_i = x, A_i) = M_i(x)$. Since $M_i(x) \leq \mathbf{P}(X_i = x)$ the events A_i are well defined. We have $\mathbf{P}(A_i) = \mu(M_i) \geq 1 - \epsilon$. Finally note that since $\mu(M_1) = \mu(M_2)$ we have $\mathbf{E}D(X_1|A_1) - \mathbf{E}D(X_2|A_2) = \left(\sum_x D(x)M_1(x) - \sum_x D(x)M_2(x)\right)/\mu(M_1)$. Therefore, the result follows.