Computational Indistinguishability: Algorithms vs. Circuits

Oded Goldreich
Department of Computer Science
and Applied Mathematics
Weizmann Institute of Science
Rehovot, ISRAEL.
E-mail: oded@wisdom.weizmann.ac.il

Bernd Meyer
Pegasusstraße 14
85716 Unterschleißheim
GERMANY.
E-mail: Bernd.Meyer@munich.netsurf.de

December 19, 1996

Abstract

We present a simple proof to the existence of a probability ensemble with tiny support which cannot be distinguished from the uniform ensemble by any recursive computation. Since the support is tiny (i.e, sub-polynomial), this ensemble can be distinguished from the uniform ensemble by a (non-uniform) family of small circuits. It also provides an example of an ensemble which cannot be (recursively) distinguished from the uniform by one sample, but can be so distinguished by two samples. In case we only wish to fool probabilistic polynomial-time algorithms the ensemble can be constructed in slightly super-exponential time.

1 Introduction

Computational indistinguishability, introduced by Goldwasser and Micali [4] and defined in full generality by Yao [7], is a central concept of complexity theory. Two probability ensembles, $\{X_n\}_{n\in\mathbf{N}}$ and $\{Y_n\}_{n\in\mathbf{N}}$, where both X_n and Y_n range over $\{0,1\}^n$, are said to be indistinguishable by a complexity class if for every machine M in the class the difference $\mathrm{Prob}(M(X_n)=1)-\mathrm{Prob}(M(Y_n)=1)$ is a negligible function in n (i.e., decreases faster than $1/p(n)$ for any positive polynomial p).

It has been known for a while (cf., [7, 5, 3]) that there exists probability ensembles which are statistically far from the uniform ensemble and yet computationally indistinguishable from it: In [7, 5] indistinguishability is with respect to (probabilistic) polynomial-time algorithms, whereas in [3] indistinguishability is with respect to polynomial-size circuits. A simple proof is via the Probabilistic Method: If you fix any function $d:\{0,1\}^n\mapsto\{0,1\}$, and select at random $O(\frac{t}{\epsilon^2})$ strings of length n, then with probability greater than $1-2^{-t}$ the average value of d over this sample will be within $\pm\epsilon$ of the average over the entire domain $\{0,1\}^n$. Using a standard enumeration of Turing machines this means that for any super-polynomial function $s:\mathbf{N}\mapsto\mathbf{N}$ there exists a probability ensemble, with support size bounded by $s(\cdot)$, which is indistinguishable from the uniform ensemble by any (halting) Turing machine. Clearly, time bounds on the distinguishing machines yield obvious bounds on the time required to construct the ensemble. Furthermore, the same argument can be applied to non-uniform families of circuits (e.g., all polynomial-size circuits).

In [6], two probability ensembles, having sparse but disjoint supports, are shown to be indistinguishable by probabilistic polynomial-time algorithms. Specifically, the support size is n^2 and the distinguishing probability is exponentially vanishing in n. It seems that the argument in [6] cannot yield either a support of size $o(n\log n)$ nor zero distinguishing probability. Here we present a simpler proof of the following stronger result:

Proposition 1 (main result): *Let $\mathcal{M}$ be an enumeration of halting* (probabilistic) *Turing machines, and $t : \mathbf{N} \mapsto \mathbf{N}$ be any non-decreasing and unbounded function. Then, there exists a probability ensemble, $\{R_n\}$, so that, for every $n \in \mathbf{N}$:*

1. *The support of R_n has size at most $t(n) + 1$.*
2. *For each one of the first $t(n)$ machines in $\mathcal{M}$, denoted M,*

$$\mathrm{Prob}(M(R_n)=1) = \mathrm{Prob}(M(U_n)=1)$$

   where U_n denotes the uniform distribution over $\{0,1\}^n$.

Furthermore, in case $\mathcal{M}$ is the set of probabilistic polynomial-time machines, the distribution R_n can be constructed in time $e(n)$, where $e : \mathbf{N} \mapsto \mathbf{N}$ is any function which grows faster than $2^{\mathrm{poly}(n)}$.

As immediate corollaries we get

Corollary 1 *There exists a probability ensemble, $\{R_n\}$, which is indistinguishable from the uniform ensemble by probabilistic polynomial-time machines but is distinguishable from it by a family of polynomial-size circuits.*

(Hint: the ensemble is as in Proposition 1. The n^{th} circuit incorporates the support of R_n and outputs 1 if and only if the input is in the support.)

Corollary 2 *There exists a probability ensemble, $\{R_n\}$, which is indistinguishable from the uniform ensemble by probabilistic polynomial-time machines but is distinguishable from it by a polynomial-time algorithm which gets two* (independently drawn) *samples from the distribution.*

(Hint: again, the ensemble is as in Proposition 1. An algorithm, which gets two samples, outputs 1 if and only if both samples are identical.) We comment that both [1, 6] present a result related to the last corollary. Specifically, they present two ensembles, each with at most two n-bit strings in their support, for which all single-sample algorithms have vanishing distinguishing probability whereas a simple two-sample algorithm has constant distinguishing probability. Note that in the corollary above the size of the support of R_n is small (e.g., $\log\log n$) but not a constant. Yet, the distinguishing probability based on a single sample is zero.

We stress that all results in the paper are absolute (i.e., do not require any unproven assumptions). On the other hand, the fact that the ensembles are not constructible in polynomial-time is unavoidable, since analogous results for polynomial-time constructible (sampleable) ensembles imply the existence of one-way functions (cf., [2]).

2 Proof of Main Result

Suppose that you want to construct a distribution with small support which fools (i.e., looks random to) a single machine, denoted M. Then all you need is two strings, $x, y \in \{0,1\}^n$, so that

$$\mathrm{Prob}(M(x) = 1) \leq \mathrm{Prob}(M(U_n) = 1) \quad (1)$$
$$\mathrm{Prob}(M(y) = 1) \geq \mathrm{Prob}(M(U_n) = 1) \quad (2)$$

Fixing these x and y, there exists an $\alpha \in [0,1]$ so that defining the distribution R_n so that $R_n = x$ with probability α and $R_n = y$ otherwise, you get

$$\text{Prob}(M(R_n) = 1) = \text{Prob}(M(U_n) = 1)$$

Thus, machine M cannot distinguish R_n from U_n.

All that is needed for proving the main result is to generalize the argument so that we can fool t machines *simultaneously*. To this end consider the 2^n (t-dimensional) vectors corresponding to the probabilities that each of the t machines outputs 1 on each of the strings in $\{0,1\}^n$. Specifically, the vector associated with $x \in \{0,1\}^n$ has $\text{Prob}(M_i(x) = 1)$ in its i^{th} component, where M_i is the i^{th} machine (that we are trying to fool). Assume, without loss of generality, that these 2^n vectors span a t-dimensional vector space.[1] Observe that the average of these vectors, denoted $\bar{v}$, is a vector of probabilities with $\text{Prob}(M_i(U_n) = 1)$ as its i^{th} component. The average vector $\bar{v}$ is in the convex hull of all 2^n former vectors, and thus there must exist $t+1$ vectors which (also) have $\bar{v}$ in their convex hull. Let $v_1, ..., v_{t+1}$ denote a set of such $t+1$ vectors. Then, by definition, there exists $\alpha_1, ..., \alpha_{t+1}$ non-negative and summing up to 1, so that the vector $\sum_{j=1}^{t+1} \alpha_j v_j$ equals the vector $\bar{v}$. Using the x_j's corresponding to these vectors with the coefficients α_j's, we get the desired distribution. Specifically, we define R_n so that $\text{Prob}(R_n = x_j) = \alpha_j$, for $j = 1, ..., t+1$. Clearly, for $i = 1, ..., t$,

$$\text{Prob}(M_i(R_n)=1) \;=\; \sum_{j=1}^{t+1} \alpha_i \cdot \text{Prob}(M_i(x_j)=1) \;=\; \text{Prob}(M_i(U_n)=1)$$

References

[1] M.J. Fischer, and S.A. Paleologou. On the Indistinguishability of Probabilistic Ensembles. Unpublished manuscript, 1994.

[2] O. Goldreich. A Note on Computational Indistinguishability. *IPL*, Vol. 34, pp. 277–281, May 1990.

[3] O. Goldreich, and H. Krawczyk. On Sparse Pseudorandom Ensembles. *Random Structures and Algorithms*, Vol. 3, No. 2, (1992), pages 163–174.

[4] S. Goldwasser, and S. Micali. Probabilistic Encryption. *JCSS*, Vol. 28, No. 2, pages 270–299, 1984. Preliminary version in *14th STOC*, 1982.

[5] L.A. Levin, private communication, mid 1980's.

[6] B. Meyer. Constructive Separation of Classes of Indistinguishable Ensembles. *Structure in Complexity Theory*, 1994, pages 198–204.

[7] A.C. Yao. Theory and Application of Trapdoor Functions. In *23rd FOCS*, pages 80–91, 1982.

[1] Otherwise consider the coordinates which span a full dimensional space.