Electronic Colloquium on Computational Complexity, Report No. 90 (2017)

The coin problem for product tests *

Chin Ho Lee Emanuele Viola

May 15, 2017

Abstract

Let $X_{m,\varepsilon}$ be the distribution over m bits $(X_1, \ldots, X_m)$ where the X_i are independent and each X_i equals 1 with probability $(1+\varepsilon)/2$ and 0 with probability $(1-\varepsilon)/2$. We consider the smallest value ε^* of ε such that the distributions $X_{m,\varepsilon}$ and $X_{m,0}$ can be distinguished with constant advantage by a function $f : \{0,1\}^m \to S$ which is the product of k functions $f_1, f_2, \ldots, f_k$ on disjoint inputs of n bits, where each $f_i : \{0,1\}^n \to S$ and $m = nk$.

We prove that $\varepsilon^* = \Theta(1/\sqrt{n \log k})$ if $S = \{0,1\}$ and if $S = \{-1,1\}$, while $\varepsilon^* = \Theta(1/\sqrt{nk})$ if S is the set of unit-norm complex numbers.

1 Introduction

Let $X_{m,\varepsilon}$ be the distribution over m bits $(X_1, \ldots, X_m)$, where the X_i are independent and each X_i equals 1 with probability $(1+\varepsilon)/2$ and 0 with probability $(1-\varepsilon)/2$. The *ε-coin problem* is the problem of distinguishing the distributions $X_{m,\varepsilon}$ and $X_{m,0}$ (note that the latter is the uniform distribution). A threshold function gives the best possible distinguishing advantage; the coin problem is therefore most interesting in computational models that cannot compute thresholds. The study of the coin problem goes back at least to the seminal papers by Ajtai [Ajt83] and Valiant [Val84] about computing majority and approximate majority by low-depth circuits. Since then, the coin problem has been extensively studied and has found applications in a striking variety of contests, including barriers to circuit lower bounds [SV10], pseudorandom generators [BV10], quantum computing [Aar10], and multiparty computation [CDI+13].

Shaltiel and Viola [SV10] give an AC^0 reduction from Majority to the coin problem, thereby obtaining negative results for the coin problem for bounded-depth circuits with various types of gates. Aaronson [Aar10] and Cohen, Ganor, and Raz [CGR14] improve the parameters of the negative result for AC^0.

Brody and Verbin [BV10], and Steinberger [Ste13] study the ε-coin problem for small-width branching programs. A generalization of the problem is studied in [CGR14]. For

*College of Computer and Information Science, Northeastern University. Supported by NSF grant CCF-1319206.

ISSN 1433-8092

constant width [BV10, Ste13] obtain tight bounds on ε. However, the case of larger widths remains open and looks very difficult.

In this work we consider a special case of large-width branching programs which we call *product tests*. A product test is a function f on nk bits which equals the product of k functions $f_1, f_2, \ldots, f_k$ on k disjoint inputs of n bits. We will consider f_i with three different ranges: $\{0,1\}$, $\{-1,1\}$, and unit-norm complex numbers. We will settle the coin problem for each of these ranges.

The model of product tests has been extensively studied in pseudorandomness [AKS87, Nis92, NZ96, INW94, EGL+98, ASWZ96, Lu02, Vio14, Wat13, GMR+12, GY14, GKM15, HLV17], at least in part with the hope that it will be useful to understand general branching programs. Thus it seems natural to study the coin problem for product tests.

First, we prove that if the f_i have range $\{-1,1\}$ then a product test cannot solve the ε-coin problem for $\varepsilon = o(1/\sqrt{n \log k})$.

Theorem 1. *Let $f\colon \{0,1\}^{nk} \to \{-1,1\}$ be a product of k functions $f_1, \ldots, f_k\colon \{0,1\}^n \to \{-1,1\}$, each on disjoint input of n bits. Let $\alpha \in (0, 1/4]$ and $\varepsilon = \alpha/(32\sqrt{n \log(k/\alpha)})$.*

We have $|\mathrm{E}[f(X_{nk,0})] - \mathrm{E}[f(X_{nk,\varepsilon})]| \le O(\alpha \log(1/\alpha))$.

This result applies as stated even if the f_i have range $\{0,1\}$ instead of $\{-1,1\}$ thanks to the following folklore fact.

Fact 2. *Let $X = (X_1, X_2, \ldots, X_k)$ and $Y = (Y_1, Y_2, \ldots, Y_k)$ be two distributions on $(\{0,1\}^n)^k$. Then*

$$\max_{f_1,f_2,\ldots,f_k:\{0,1\}^n\to\{0,1\}} |\operatorname*{E}_X[\prod_{i\le k} f_i(X_i)] - \operatorname*{E}_Y[\prod_{i\le k} f_i(Y_i)]| \le \max_{f_1,f_2,\ldots,f_k:\{0,1\}^n\to\{-1,1\}} |\operatorname*{E}_X[\prod_{i\le k} f_i(X_i)] - \operatorname*{E}_Y[\prod_{i\le k} f_i(Y_i)]|.$$

Note all that's changing is the range of the f_i.

We then show that Theorem 1 is tight, even for range $\{0,1\}$.

Theorem 3. *For every $k \in [n^2, 2^n]$, there exists an $\varepsilon = O(1/\sqrt{n \log k})$, and a function $f\colon \{0,1\}^{nk} \to \{0,1\}$ that is a product of k functions $f_1, \ldots, f_k\colon \{0,1\}^n \to \{0,1\}$, each on disjoint input of n bits, such that $\Pr[f(X_{nk,0}) = 1] - \Pr[f(X_{nk,\varepsilon}) = 1] \ge 1/100$.*

To summarize, we have established that, for both $S = \{0,1\}$ and $S = \{-1,1\}$, $\varepsilon^* = \Theta(1/\sqrt{n \log k})$ is the smallest value of ε such that the distributions $X_{m,\varepsilon}$ and $X_{m,0}$ can be distinguished with constant advantage by a function $f : \{0,1\}^m \to S$ which is the product of k functions $f_1, f_2, \ldots, f_k$ on disjoint inputs of n bits, where each $f_i : \{0,1\}^n \to S$ and $m = nk$. For comparison, recall that for arbitrary boolean functions on nk bits the corresponding value is $\varepsilon^* = \Theta(1/\sqrt{nk})$ (that $\varepsilon^* = \Omega(1/\sqrt{nk})$ also follows from Claim 8 in this paper; and Claim 10 extends this to complex-valued functions).

Finally, we note that if the range is enlarged to the set $\mathbb{C}_{=1} := \{z \in \mathbb{C} : |z| = 1\}$ of complex numbers with unit norm, the picture changes completely and product tests are as powerful as arbitrary functions.

Claim 4. *For every integer k and $\varepsilon > 0$, there exists $f\colon \{-1,1\}^{nk} \to \mathbb{C}_{=1}$ which is a product of k functions $f_1, \ldots, f_k\colon \{0,1\}^n \to \mathbb{C}_{=1}$, each on disjoint input of n bits, such that $|\mathrm{E}[f(X_{nk,0})] - \mathrm{E}[f(X_{nk,\varepsilon})]| \geq 1.5 - e^{-\Omega(\varepsilon^2 nk)}$.*

After some preliminaries, we prove our statements in the same order in which they appear in the introduction.

2 Preliminaries

We use the notation $\pm\alpha$ in the RHS of an equality to indicate that the equality holds if we replace $\pm\alpha$ with z for some z such that $|z| \leq \alpha$. We use this notation multiple times, with the meaning that each occurrence is replaced by a possibly different z.

Throughout the paper all logarithms are in base 2, and we will use the following bounds.

Claim 5 (Hoeffding's inequality)**.** *Let $X_1, \ldots, X_n \in [-1,1]$ be n independent and identically distributed variables with $\mathrm{E}[X_i] = \mu$ for each i. We have*

$$\Pr[|\sum_{i=1}^{n} X_i - \mu n| \geq t] \leq 2e^{-t^2/2n}.$$

Claim 6 (Maclaurin's inequality (cf. [Ste04]))**.** *Let $z_1, \ldots, z_k$ be k non-negative numbers. For any $i \in \{0, \ldots, k\}$, we have*

$$S_i(z_1, \ldots, z_k) := \sum_{S:|S|=i} \prod_{j \in S} z_j \leq (e/i)^i (\sum_{j=1}^{k} z_j)^i.$$

To get a sense of the inequality, note that if the z_i's equal to 1 then it becomes the standard upper bound on the binomial coefficient $\binom{k}{i} \leq (ek/i)^i$.

Next we formally define our main distributions.

Definition 7. *Let $X_{n,\varepsilon} = (X_1, \ldots, X_n)$ be the distribution over n bits, where the X_i's are independent and each X_i equals 1 with probability $(1+\varepsilon)/2$ and 0 with probability $(1-\varepsilon)/2$. Let $N_{n,\varepsilon}$ denote the sum of the X_i's.*

Note that we have $\mathrm{E}[N_{n,\varepsilon}] = (1+\varepsilon)n/2$.

3 Proof of Theorem 1

We start with the following claim about a single function on n bits. Note that in particular this claim implies the well-known fact that one function cannot solve the ε-coin problem for $\varepsilon = o(1/\sqrt{n})$.

Claim 8. *For every $\alpha \in [0,1]$ and $\beta \in (0, 1/2]$, let $\varepsilon = \alpha/(32\sqrt{n \log(1/\beta)})$. For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have $\Pr[f(X_{n,\varepsilon}) = 1] = \Pr[f(X_{n,0}) = 1](1 \pm \alpha) \pm \beta$.*

Proof. For a string $x \in \{0,1\}^n$, we use $wt(x)$ to denote its Hamming weight. The high-level idea is that if $wt(x)$ is far from $n/2$, then by Hoeffding's inequality we can bound above the probability of both $X_{n,\varepsilon}$ and $X_{n,0}$ hitting x by β. Otherwise, since the two probabilities differ by a multiplicative factor of $(1+\varepsilon)^{wt(x)}(1-\varepsilon)^{n-wt(x)}$, we can use the fact that $wt(x)$ is close to $n/2$ to show that this factor is within $1 \pm \alpha$.

To proceed, let $S := \{x \in \{0,1\}^n : f(x) = 1\}$. Let $T = 4\sqrt{n \log(1/\beta)}$, $S_1 := \{x \in S : |wt(x) - n/2| \le T\}$ and $S_2 := \{x \in S : |wt(x) - n/2| > T\}$.

Since $\beta \le 1/2$, we have $\log(1/\beta) \ge 1$ and so

$$\varepsilon n/2 = \alpha\sqrt{n}/(64\sqrt{\log(1/\beta)}) \le \sqrt{n}/64 \le T/2.$$

By Hoeffding's inequality,

$$\begin{aligned}
\Pr[X_{n,\varepsilon} \in S_2] &\le \Pr[|N_{n,\varepsilon} - n/2| > T] \\
&\le \Pr[|N_{n,\varepsilon} - (1+\varepsilon)n/2| > T - \varepsilon n/2] \\
&= \Pr[|N_{n,\varepsilon} - \mathrm{E}[N_{n,\varepsilon}]| > T - \varepsilon n/2] \\
&\le \Pr[|N_{n,\varepsilon} - \mathrm{E}[N_{n,\varepsilon}]| > T/2] \\
&\le 2e^{-2\log(1/\beta)} \le 2\beta^2 \le \beta,
\end{aligned}$$

and the same bound holds for $\Pr[X_{n,0} \in S_2]$. So the two probabilities differ by at most β in absolute value.

Now we show that $\Pr[X_{n,\varepsilon} \in S_1] = \Pr[X_{n,0} \in S_1](1 \pm \alpha)$. We have

$$\begin{aligned}
\Pr[X_{n,\varepsilon} \in S_1] &= \sum_{x \in S_1} \Pr[X_{n,\varepsilon} = x] \\
&= 2^{-n} \sum_{x \in S_1} (1+\varepsilon)^{wt(x)}(1-\varepsilon)^{n-wt(x)} \\
&= 2^{-n} \sum_{x \in S_1} (1+\varepsilon)^{n/2-(n/2-wt(x))}(1-\varepsilon)^{n/2+(n/2-wt(x))} \\
&= 2^{-n} \sum_{x \in S_1} (1-\varepsilon^2)^{n/2} \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{wt(x)-n/2}.
\end{aligned}$$

Recall that $T = 4\sqrt{n\log(1/\beta)}$ and $\varepsilon = \alpha/(32\sqrt{n\log(1/\beta)})$. Thus $T\varepsilon = \alpha/8$. We first give a lower bound on the sum. As $\varepsilon^2 n \le \alpha$, we have $(1-\varepsilon^2)^{n/2} \ge 1 - n\varepsilon^2/2 \ge 1 - \alpha/2$. Also,

$$\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{wt(x)-n/2} \ge \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{|wt(x)-n/2|} \ge \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{T} = \left(1 - \frac{2\varepsilon}{1+\varepsilon}\right)^{T} \ge 1 - 2T\varepsilon = 1 - \alpha/4.$$

Therefore,

$$\begin{aligned}2^{-n}\sum_{x\in S_1}(1-\varepsilon^2)^{n/2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{wt(x)-n/2} &\geq 2^{-n}\sum_{x\in S_1}(1-\alpha/2)(1-\alpha/4)\\ &\geq 2^{-n}\sum_{x\in S_1}(1-\alpha)\\ &= \Pr[X_{n,0}\in S_1](1-\alpha).\end{aligned}$$

Now we bound above the sum. We have

$$(1-\varepsilon^2)^{n/2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{wt(x)-n/2} \leq \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{T} = \left(1+\frac{2\varepsilon}{1-\varepsilon}\right)^{T} \leq e^{\frac{2T\varepsilon}{1-\varepsilon}} \leq e^{4T\varepsilon} = e^{\alpha/2} \leq 1+\alpha,$$

where the last inequality follows from the inequality $e^x \leq 1+2x$ for all $x\in[0,1]$. Hence,

$$2^{-n}\sum_{x\in S_1}(1-\varepsilon^2)^{n/2}\left(\frac{1+\varepsilon}{1-\varepsilon}\right)^{wt(x)-n/2} \leq 2^{-n}\sum_{x\in S_1}(1+\alpha) = \Pr[X_{n,0}\in S_1](1+\alpha).$$

Putting the lower and upper bounds together, we have

$$\begin{aligned}\Pr[f(X_{n,\varepsilon})=1] &= \Pr[X_{n,\varepsilon}\in S_1]+\Pr[X_{n,\varepsilon}\in S_2]\\ &= (1\pm\alpha)\Pr[X_{n,0}\in S_1]+\Pr[X_{n,0}\in S_2]\pm\beta\\ &= (1\pm\alpha)(\Pr[X_{n,0}\in S_1]+\Pr[X_{n,0}\in S_2])\pm\beta\\ &= (1\pm\alpha)\Pr[f(X_{n,0})=1]\pm\beta\end{aligned}$$

as claimed. □

We will apply the following lemma to Claim 8.

Lemma 9. *Let $k\geq 2$ be an integer and $\alpha\in(0,1/2]$ be a real number. For $i\in\{1,\ldots,k\}$, let $a_i, a_i'\in[0,1]$ be any two real numbers such that $a_i' = a_i(1\pm\alpha)\pm\alpha/k$. We have*

$$\left|\prod_{i\leq k}(1-a_i)-\prod_{i\leq k}(1-a_i')\right| \leq O(\alpha\log(1/\alpha)).$$

Proof. We consider two cases depending on whether $\sum_{i\leq k}a_i > 2\log(1/\alpha)$.

If $\sum_{i\leq k}a_i > 2\log(1/\alpha)$, then as $\alpha\leq 1/2$, we have

$$\prod_{i\leq k}(1-a_i') \leq e^{-\sum_{i\leq k}a_i'} \leq e^{-\sum_{i\leq k}(a_i(1-\alpha)-\alpha/k)} \leq e^{-2\log(1/\alpha)(1-\alpha)+\alpha} \leq e^{-\log(1/\alpha)+\alpha} \leq \alpha\cdot e^{\alpha} \leq 2\alpha,$$

and the same bound holds for $\prod_{i\leq k}(1-a_i)$. So $|\prod_{i\leq k}(1-a_i)-\prod_{i\leq k}(1-a_i')| \leq O(\alpha\log(1/\alpha))$.

If $\sum_{i\le k} a_i \le 2\log(1/\alpha)$, then as $a_i = a_i(1\pm\alpha)\pm\alpha/k$, we have

$$\begin{aligned}\prod_{i\le k}(1-a_i') &= \prod_{i\le k}(1-a_i(1\pm\alpha)\pm\alpha/k)\\ &= \prod_{i\le k}(1-a_i\pm\alpha a_i\pm\alpha/k)\\ &= \prod_{i\le k}(1-a_i)\pm\left(\sum_{i=1}^{k}\sum_{S\subseteq\{1,2,\ldots,k\}:|S|=i}\prod_{j\in S}(\alpha a_j+\alpha/k)\prod_{j\notin S}(1-a_j)\right)\\ &= \prod_{i\le k}(1-a_i)\pm\left(\sum_{i=1}^{k}\alpha^i\sum_{S:|S|=i}\prod_{j\in S}(a_j+1/k)\right).\end{aligned}$$

So $|\prod_{i\le k}(1-a_i')-\prod_{i\le k}(1-a_i)|\le\sum_{i=1}^{k}\alpha^i S_i(z_1,\ldots,z_k)$, where

$$S_i(z_1,\ldots,z_k)=\sum_{S:|S|=i}\prod_{j\in S}z_j,\quad\text{and}\quad z_j:=a_j+1/k.$$

Since each $z_j\ge 0$, by Claim 6 we have

$$S_i(z_1,\ldots,z_k)\le(e/i)^i(\sum_{j\le k}z_j)^i\le(e/i)^i(2\log(1/\alpha)+1)^i=(2e\log(\sqrt{2}/\alpha)/i)^i,$$

because $\sum_{j\le k}a_j\le 2\log(1/\alpha)$. Applying the bound to each $S_i(a_1,\ldots,a_k)$ we have

$$\left|\prod_{i\le k}(1-a_i')-\prod_{i\le k}(1-a_i)\right|\le\sum_{i=1}^{k}\left(\frac{2e\alpha\log(\sqrt{2}/\alpha)}{i}\right)^i=O(\alpha\log(1/\alpha)),$$

because $2e\alpha\log(\sqrt{2}/\alpha)\le 1$ for sufficiently small α. □

As a warm-up for the proof of Theorem 1, let us first consider the case where the functions f_i have range $\{0,1\}$.

Proof of the variant of Theorem 1 where the f_i have range $\{0,1\}$. Let q_i and q_i' denote $\Pr[f_i(X_{n,0})=0]$ and $\Pr[f_i(X_{n,\varepsilon})=0]$ respectively. Applying Claim 8 to $1-f_i$ with $\beta=\alpha/k\le 1/2$, we have $q_i'=q_i(1\pm\alpha)\pm\alpha/k$. Since

$$\Pr[f(X_{nk,0})=1]=1-\prod_{i\le k}(1-q_i)\quad\text{and}\quad\Pr[f(X_{nk,\varepsilon})=1]=1-\prod_{i\le k}(1-q_i'),$$

it suffices to bound above $|\prod_{i\le k}(1-q_i)-\prod_{i\le k}(1-q_i')|$ by $O(\alpha\log(1/\alpha))$. This follows from applying Lemma 9 to q_i and q_i'. □

The proof for range $\{-1,1\}$ instead of $\{0,1\}$ needs to deal with more cases.

Proof of Theorem 1. We look at the bias $|\mathrm{E}[f_i(X_{n,0})]|$ of each f_i. There are two cases: if one of them is small, then we argue that both $|\mathrm{E}[f(X_{nk,0})]|$ and $|\mathrm{E}[f(X_{nk,\varepsilon})]|$ are small and so is $|\mathrm{E}[f(X_{nk,0})] - \mathrm{E}[f(X_{nk,\varepsilon})]|$. Otherwise, every f_i has large bias, and so using Claim 8 we show that both $\mathrm{E}[f_i(X_{n,0})]$ and $\mathrm{E}[f_i(X_{n,\varepsilon})]$ have the same sign. In this case we apply Claim 9 to their absolute values.

To proceed, for each $i \in \{1, \ldots, k\}$, define $g_i(x) := (1 - f_i(x))/2 \in \{0, 1\}$. Let p_i and p'_i denote $\Pr[g_i(X_{n,0}) = 1]$ and $\Pr[g_i(X_{n,\varepsilon}) = 1]$ respectively. Note that $\mathrm{E}[f_i(X_{n,\varepsilon})] = 1 - 2p_i$ and $\mathrm{E}[f_i(X_{n,0})] = 1 - 2p'_i$. Applying Claim 8 to g_i with $\beta = \alpha/k \leq 1/2$, we have $p'_i = p_i(1 \pm \alpha) \pm \alpha/k$.

Suppose for some $i \in \{1, \ldots, k\}$, $|\mathrm{E}[f_i(X_{n,0})]| \leq 4\alpha \leq 1$. Then by our definition of g_i we have $p_i = 1/2 \pm 2\alpha$. Since $p'_i = p_i(1 \pm \alpha) \pm \alpha/k$, we have

$$\begin{aligned} p'_i &\leq (1/2 + 2\alpha)(1 + \alpha) + \alpha/k \\ &= 1/2 + 2\alpha(1 + \alpha) + \alpha/2 + \alpha/k \\ &\leq 1/2 + 3\alpha + \alpha/2 + \alpha/2, \\ &= 1/2 + 4\alpha, \end{aligned}$$

and

$$\begin{aligned} p'_i &\geq (1/2 - 2\alpha)(1 - \alpha) - \alpha/k \\ &= 1/2 - 2\alpha(1 - \alpha) - \alpha/2 - \alpha/k \\ &\geq 1/2 - 2\alpha - \alpha/2 - \alpha/2 \\ &= 1/2 - 3\alpha. \end{aligned}$$

Hence we have $-3\alpha \leq \mathrm{E}[f_i(X_{n,\varepsilon})] \leq 4\alpha$. Therefore

$$\begin{aligned} |\mathrm{E}[f(X_{nk,0})] - \mathrm{E}[f(X_{nk,\varepsilon})]| &\leq |\mathrm{E}[f(X_{nk,0})]| + |\mathrm{E}[f(X_{nk,\varepsilon})]| \\ &\leq |\mathrm{E}[f_i(X_{n,0})]| + |\mathrm{E}[f_i(X_{n,\varepsilon})]| \\ &\leq 8\alpha \\ &= O(\alpha \log(1/\alpha)). \end{aligned}$$

Now we can assume that for all $i \in \{1, \ldots, k\}$, $|\mathrm{E}[f_i(X_{n,0})]| > 4\alpha$. If $\mathrm{E}[f_i(X_{n,0})] > 4\alpha$ then $p_i < 1/2 - 2\alpha$, and

$$\begin{aligned} p'_i &< (1/2 - 2\alpha)(1 + \alpha) + \alpha/k \\ &= 1/2 - 2\alpha(1 + \alpha) + \alpha/2 + \alpha/k \\ &\leq 1/2 - 2\alpha + \alpha/2 + \alpha/2 \\ &\leq 1/2, \end{aligned}$$

and hence $\mathrm{E}[f_i(X_{n,\varepsilon})] \geq 0$. Otherwise, $\mathrm{E}[f_i(X_{n,0})] < -4\alpha$ and so $p_i > 1/2 + 2\alpha$, then we

have

$$\begin{aligned} p_i' &> (1/2 + 2\alpha)(1-\alpha) - \alpha/k \\ &= 1/2 + 2\alpha(1-\alpha) - \alpha/2 - \alpha/k \\ &\geq 1/2 + \alpha - \alpha/2 - \alpha/2 \\ &= 1/2, \end{aligned}$$

and so $\mathrm{E}[f_i(X_{n,\varepsilon})] \leq 0$. Hence, we can assume that for every $i \in \{1, \ldots, k\}$, $\mathrm{E}[f_i(X_{n,0})]$ and $\mathrm{E}[f_i(X_{n,\varepsilon})]$ have the same sign, which implies that $\mathrm{E}[f(X_{nk,0})]$ and $\mathrm{E}[f(X_{nk,\varepsilon})]$ also have the same sign.

Therefore, it suffices to bound above $||\mathrm{E}[f(X_{nk,0})]| - |\mathrm{E}[f(X_{nk,\varepsilon})]||$. Let $q_i := 1 - p_i$ and $q_i' := 1 - p_i'$. Applying Claim 8 to $1 - g_i$ with $\beta = \alpha/k \leq 1/2$, we also have $q_i' = q_i(1 \pm \alpha) \pm \alpha/k$.

Observe that

$$|\mathrm{E}[f_i(X_{n,0})]| = 1 - 2\min\{p_i, q_i\} \quad \text{and} \quad |\mathrm{E}[f_i(X_{n,\varepsilon})]| = 1 - 2\min\{p_i', q_i'\}.$$

Thus, if we define $m_i := 2\min\{p_i, q_i\}$ and $m_i' := 2\min\{p_i', q_i'\}$, then $|\mathrm{E}[f_i(X_{n,0})]| = 1 - m_i$ and so $|\mathrm{E}[f(X_{nk,0})]| = \prod_{i \leq k} |\mathrm{E}[f_i(X_{n,0})]| = \prod_{i \leq k}(1 - m_i)$. Similarly, we have $|\mathrm{E}[f(X_{nk,\varepsilon})]| = \prod_{i \leq k}(1 - m_i')$. Note that $m_i, m_i' \in [0, 1]$, and recall that $p_i' = p_i(1 \pm \alpha) \pm \alpha/k$ and $q_i' = q_i(1 \pm \alpha) \pm \alpha/k$, which together imply $m_i' = m_i(1 \pm \alpha) \pm 2\alpha/k$. Applying Lemma 9 to m_i and m_i', we have

$$\begin{aligned} |\mathrm{E}[f(X_{nk,0})] - \mathrm{E}[f(X_{nk,\varepsilon})]| &= ||\mathrm{E}[f(X_{nk,0})]| - |\mathrm{E}[f(X_{nk,\varepsilon})]|| \\ &= \left| \prod_{i \leq k}(1 - m_i) - \prod_{i \leq k}(1 - m_i') \right| \\ &= O(\alpha \log(1/\alpha)), \end{aligned}$$

proving the claim. □

3.1 Other proofs

Proof of Fact 2. Replace $f_i(x)$ with the equal quantity $\mathrm{E}_{z_i \in \{0,1\}}[(-1)^{(1+f_i(x))z_i}]$. Then use linearity of expectation and the triangle inequality to write

$$\begin{aligned} &|\mathop{\mathrm{E}}_{X}[\prod_{i \leq k} f_i(X_i)] - \mathop{\mathrm{E}}_{Y}[\prod_{i \leq k} f_i(Y_i)]| \\ &= \left| \mathop{\mathrm{E}}_{z_1, z_2, \ldots, z_k \in \{0,1\}} \left[\mathop{\mathrm{E}}_{X}[\prod_{i \leq k} (-1)^{(1+f_i(X_i))z_i}] - \mathop{\mathrm{E}}_{Y}[\prod_{i \leq k} (-1)^{(1+f_i(Y_i))z_i}] \right] \right| \\ &\leq \mathop{\mathrm{E}}_{z_1, z_2, \ldots, z_k \in \{0,1\}} |\mathop{\mathrm{E}}_{X}[\prod_{i \leq k} (-1)^{(1+f_i(X_i))z_i}] - \mathop{\mathrm{E}}_{Y}[\prod_{i \leq k} (-1)^{(1+f_i(Y_i))z_i}]|. \end{aligned}$$

Hence, there is a fixed value of the z_i for which the inequality still holds. For fixed z_i, the functions $x \mapsto (-1)^{(1+f_i(x))z_i}$ have range $\{-1, 1\}$. □

Proof of Theorem 3. First, note that we can assume $k \in [n^2, 2^{\alpha n}]$ for any desired constant $\alpha > 0$, because if k is larger one can make the other functions identically 1 and the expression for ε does not change.

Let u' be the largest integer such that $2^{-n}\binom{n}{n/2-u'} \geq 1/k$. For each $i \in \{1, \ldots, k\}$, define $f_i \colon \{0,1\}^n \to \{0,1\}$ to be 1 if and only if $\sum_{j \leq n} x_j \neq n/2 - u'$. We have

$$\Pr[f(X_{nk,0}) = 1] = \left(1 - 2^{-n}\binom{n}{n/2-u'}\right)^k \leq (1 - 1/k)^k \leq 1/e.$$

We will show that $u' = \Theta(1/\sqrt{n \log k})$, and for $\varepsilon := 1/u'$, we have

$$\Pr[f(X_{n,\varepsilon}) = 1] \geq 1 - c/k \tag{1}$$

for a constant $c \in [0, 0.45]$. Assuming both, we have

$$\begin{aligned}\Pr[f(X_{nk,0}) = 1] - \Pr[f(X_{nk,\varepsilon}) = 1] &\geq (1 - c/k)^k - 1/e \\ &\geq e^{-2c} - 1/e \\ &\geq e^{-0.9} - 1/e \\ &\geq 1/100,\end{aligned}$$

where the second inequality follows from the inequality $1 - x \geq e^{-2x}$ for $x \in [0, 1/2]$, proving the claim.

It remains to show that $u = \Theta(1/\sqrt{n \log k})$ and that Inequality (1) holds. Let $H(x) := -x \log x - (1-x)\log(1-x)$ be the binary entropy function. Using the approximations

$$\frac{2^{nH(t/n)}}{n+1} \leq \binom{n}{t} \leq 2^{nH(t/n)} \quad \text{and} \quad H(\frac{1}{2} - \gamma) = 1 - \Theta(\gamma^2),$$

we have that for every integer $u \geq 0$

$$2^{-\Theta(u^2/n) - \log(n+1)} \leq 2^{-n}\binom{n}{n/2-u} \leq 2^{-\Theta(u^2/n)}.$$

Since $k \geq n^2$, from the bounds above we have $u' = \sqrt{(n \log k)/c'}$ for some $c' > 0$.

Now we show Inequality (1). First we establish that $\Pr[N_{n,0} = n/2 - u'] \in [1/k, 2/k]$. The lower bound holds by definition of u', and the upper bound is proved next. We have

$$\begin{aligned}\Pr[N_{n,0} = n/2 - u'] &= 2^{-n}\binom{n}{n/2-u'} \\ &= 2^{-n}\binom{n}{n/2-u'-1}\left(\frac{n - (n/2 - u') + 1}{n/2 - u'}\right) \\ &= \Pr[N_{n,0} = n/2 - u' - 1]\left(1 + \frac{2u'+1}{n/2-u'}\right).\end{aligned}$$

Since $k \le 2^{\alpha n}$, we have $u' = \sqrt{(n \log k)/c'} \le \sqrt{\alpha/c'} \cdot n \le n/8$ for a sufficiently small constant $\alpha > 0$. Hence,

$$1 + \frac{2u'+1}{n/2-u'} \le 2.$$

Also, by the definition of u', we have $\Pr[N_{n,0} = n/2 - u' - 1] < 1/k$. Therefore,

$$\Pr[N_{n,0} = n/2 - u'] = \Pr[N_{n,0} = n/2 - u' - 1]\left(1 + \frac{2u'+1}{n/2-u'}\right) \le 2/k,$$

as desired.

Now, by the definition of f_i,

$$\begin{aligned}\Pr[f_i(X_{n,\varepsilon}) = 0] &= 2^{-n}\binom{n}{n/2-u'}(1+\varepsilon)^{n/2-u'}(1-\varepsilon)^{n/2+u'} \\ &= \Pr[N_{n,0} = n/2-u'](1-\varepsilon^2)^{n/2}\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{u'}.\end{aligned}$$

It follows from

$$(1-\varepsilon^2)^{n/2}\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{u'} \le \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{u'} = \left(1 - \frac{2\varepsilon}{1+\varepsilon}\right)^{u'} \le e^{-\frac{2\varepsilon u'}{1+\varepsilon}} = e^{-\frac{2}{1+\varepsilon}} \le e^{-1.5}$$

that $\Pr[f_i(X_{n,\varepsilon}) = 0] \le (2/k) \cdot e^{-1.5} \le 0.446/k$, showing Inequality (1). □

We made no effort to optimize the constants in the above proof, but we point out that by picking $\varepsilon = c/u'$ for a constant $c > 1$ we can improve the distinguishing advantage from $1/100$ to a larger constant.

Proof of Claim 4. For ease of presentation, we will work with inputs over $\{-1, 1\}$ instead of $\{0, 1\}$, by translating each input bit x by $1 - 2x$. Hence, each X_i equals -1 with probability $(1+\varepsilon)/2$ and 1 with probability $(1-\varepsilon)/2$. We also use the random variable $N_{n,\varepsilon}$ to denote the sum of n independent X_i's. Note that in this case we have $\mathrm{E}[N_{n,\varepsilon}] = -\varepsilon n$.

Let $m := nk$. The idea is to rotate along the complex unit circle with respect to the number of -1's in the input x, so that if the number of -1's in x is close to $m/2$ we are close to the point 1, whereas if it is close to $(1+\varepsilon)m/2$, we are close to the point -1. Then the claim follows from Hoeffding's inequality.

Specifically, for each $\ell \in \{1, \ldots, k\}$, define $f_\ell \colon \{0,1\}^n \to \mathbb{C}_{=1}$ to be $f_\ell(x) := e^{i\frac{\pi}{\varepsilon m}\sum_{j \le n} x_j}$. Note that

$$f(x_1, \ldots, x_k) = \prod_{\ell \le k} f_\ell(x_\ell) = e^{i\frac{\pi}{\varepsilon m}\sum_{j \le m} x_j}.$$

Observe that when $\sum_{j \le m} x_j$ is close to $0 = \mathrm{E}[N_{m,0}]$, $f(x)$ is close to 1, whereas when $\sum_{j \le m} x_j$ is close to $-\varepsilon m = \mathrm{E}[N_{m,\varepsilon}]$, $f(x)$ is close to -1. By Hoeffding's inequality, we have for $\tau = 0$ and $\tau = \varepsilon$,

$$\Pr[|N_{m,\tau} - \tau m| > \varepsilon m/2] \le 2e^{-\Omega(\varepsilon^2 m)}.$$

Conditioned on the events $|N_{m,\tau} - \tau m| \leq \varepsilon m/2$ for both $\tau = 0$ and $\tau = \varepsilon$, we have $f(X_{m,\tau}) = e^{i\pi\tau/\varepsilon} \cdot e^{i\pi\theta}$ for some $\theta \in [-0.5, 0.5]$. Hence,

$$|f(X_{m,0}) - f(X_{m,\varepsilon})| = |1 \cdot e^{i\pi\theta} - (-1) \cdot e^{i\pi\theta'}| = |e^{i\pi\theta} + e^{i\pi\theta'}|$$

for some $\theta, \theta' \in [-0.5, 0.5]$, which is at least

$$\min_{\theta,\theta' \in [-0.5,0.5]} |e^{i\pi\theta} + e^{i\pi\theta'}| \geq \min_{\theta,\theta' \in [-0.5,0.5]} \Re(e^{i\pi\theta} + e^{i\pi\theta'}) = 2 \min_{\theta \in [-0.5,0.5]} \cos\theta \geq 2\cos(0.5) \geq 1.5,$$

where $\Re$ denotes the real part and the last inequality follows from the inequality $\cos(\alpha) \geq 1 - \alpha^2$. Therefore,

$$\begin{aligned} |\mathrm{E}[f(X_{m,0})] - \mathrm{E}[f(X_{m,\varepsilon})]| &\geq (1 - 2e^{-\Omega(\varepsilon^2 m)}) \cdot 1.5 \\ &= 1.5 - e^{-\Omega(\varepsilon^2 m)} \end{aligned}$$

as desired. □

To provide a slightly more complete picture of the effect of changing range on the distinguishing advantage, we include the following claim which shows that, for a single function, range $\mathbb{C}_{=1}$ and range $\{0, 1\}$ are equivalent.

Claim 10. *Let X and Y be two discrete random variables over the same support Z. We have*

$$\max_{f\colon Z \to \mathbb{C}_{=1}} |\mathrm{E}[f(X)] - \mathrm{E}[f(Y)]| = 2 \max_{g\colon Z \to \{0,1\}} |\mathrm{E}[g(X) - \mathrm{E}[g(Y)]|.$$

Proof. Let p and q be the probability mass functions of X and Y respectively. We will use the well-known fact that

$$2 \max_{g\colon Z \to \{0,1\}} |\mathrm{E}[g(X)] - \mathrm{E}[g(Y)]| = \sum_{z \in Z} |p(z) - q(z)|$$

and work with the quantity on the R.H.S.

For any $f\colon Z \to \mathbb{C}_{=1}$ we have

$$\begin{aligned} |\mathrm{E}[f(X)] - \mathrm{E}[f(Y)]| &= |\sum_{z \in Z} p(z)f(z) - q(z)f(z)| \\ &= |\sum_{z \in Z} (p(z) - q(z))f(z)| \\ &\leq \sum_{z \in Z} |p(z) - q(z)||f(z)| \\ &\leq \sum_{z \in Z} |p(z) - q(z)|. \end{aligned}$$

On the other hand, define $f\colon Z \to \mathbb{C}_{=1}$ to be $f(z) = 1$ if $p(z) \geq q(z)$ and -1 otherwise. We have

$$\begin{aligned}\sum_{z\in Z}|p(z)-q(z)| &= \sum_{z:p(z)\geq q(z)}(p(z)-q(z)) + \sum_{z:p(z)<q(z)}(q(z)-p(z)) \\ &= \sum_{z\in Z}(p(z)-q(z))f(z) \\ &= \mathrm{E}[f(X)] - \mathrm{E}[f(Y)].\end{aligned}$$

The claim follows. □

References

[Aar10] Scott Aaronson. BQP and the polynomial hierarchy. In *42nd ACM Symp. on the Theory of Computing (STOC)*, pages 141–150. ACM, 2010.

[Ajt83] Miklós Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1–48, 1983.

[AKS87] Miklós Ajtai, János Komlós, and Endre Szemerédi. Deterministic simulation in logspace. In *19th ACM Symp. on the Theory of Computing (STOC)*, pages 132–140, 1987.

[ASWZ96] Roy Armoni, Michael E. Saks, Avi Wigderson, and Shiyu Zhou. Discrepancy sets and pseudorandom generators for combinatorial rectangles. In *37th IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 412–421, 1996.

[BV10] Joshua Brody and Elad Verbin. The coin problem, and pseudorandomness for branching programs. In *51th IEEE Symp. on Foundations of Computer Science (FOCS)*, 2010.

[CDI+13] Gil Cohen, Ivan Bjerre Damgård, Yuval Ishai, Jonas Kölker, Peter Bro Miltersen, Ran Raz, and Ron D. Rothblum. Efficient multiparty protocols via log-depth threshold formulae - (extended abstract). In *Int. Cryptology Conf. (CRYPTO)*, pages 185–202, 2013.

[CGR14] Gil Cohen, Anat Ganor, and Ran Raz. Two sides of the coin problem. In *Workshop on Randomization and Computation (RANDOM)*, pages 618–629, 2014.

[EGL+98] Guy Even, Oded Goldreich, Michael Luby, Noam Nisan, and Boban Velickovic. Efficient approximation of product distributions. *Random Struct. Algorithms*, 13(1):1–16, 1998.

[GKM15] Parikshit Gopalan, Daniek Kane, and Raghu Meka. Pseudorandomness via the discrete fourier transform. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 903–922, 2015.

[GMR+12] Parikshit Gopalan, Raghu Meka, Omer Reingold, Luca Trevisan, and Salil Vadhan. Better pseudorandom generators from milder pseudorandom restrictions. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2012.

[GY14] Parikshit Gopalan and Amir Yehudayoff. Inequalities and tail bounds for elementary symmetric polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:19, 2014.

[HLV17] Elad Haramaty, Chin Ho Lee, and Emanuele Viola. Bounded independence plus noise fools products. In *Conf. on Computational Complexity (CCC)*, 2017.

[INW94] Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In *26th ACM Symp. on the Theory of Computing (STOC)*, pages 356–364, 1994.

[Lu02] Chi-Jen Lu. Improved pseudorandom generators for combinatorial rectangles. *Combinatorica*, 22(3):417–433, 2002.

[Nis92] Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. of Computer and System Sciences*, 52(1):43–52, February 1996.

[Ste04] J. Michael Steele. *The Cauchy-Schwarz master class.* MAA Problem Books Series. Mathematical Association of America, Washington, DC; Cambridge University Press, Cambridge, 2004.

[Ste13] John P. Steinberger. The distinguishability of product distributions by read-once branching programs. In *IEEE Conf. on Computational Complexity (CCC)*, pages 248–254, 2013.

[SV10] Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. *SIAM J. on Computing*, 39(7):3122–3154, 2010.

[Val84] Leslie G. Valiant. Short monotone formulae for the majority function. *J. Algorithms*, 5(3):363–366, 1984.

[Vio14] Emanuele Viola. Randomness buys depth for approximate counting. *Computational Complexity*, 23(3):479–508, 2014.

[Wat13] Thomas Watson. Pseudorandom generators for combinatorial checkerboards. *Computational Complexity*, 22(4):727–769, 2013.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il