Journal of Computer and System Sciences 77 (2011) 728–737

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Almost-natural proofs

Timothy Y. Chow

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540, United States

ARTICLE INFO

Article history:
Received 1 April 2009
Received in revised form 31 May 2010
Accepted 18 June 2010
Available online 30 June 2010

Keywords:
Circuit lower bound
Natural proof

ABSTRACT

Razborov and Rudich have proved that, under a widely-believed hypothesis about pseudorandom number generators, there do not exist $P/poly$-computable Boolean function properties with density greater than $2^{-poly(n)}$ that exclude $P/poly$. This famous result is widely regarded as a serious barrier to proving strong lower bounds in circuit complexity theory, because virtually all Boolean function properties used in existing lower bound proofs have the stated complexity and density. In this paper, we show that under the same pseudorandomness hypothesis, there *do* exist nearly-linear-time-computable Boolean function properties with only slightly lower density (namely, $2^{-q(n)}$ for a quasi-polynomial function q) that not only exclude $P/poly$, but even separate NP from $P/poly$. Indeed, we introduce a simple, explicit property called *discrimination* that does so. We also prove *unconditionally* that there exist *non-uniformly* nearly-linear-time-computable Boolean function properties with this same density that exclude $P/poly$. Along the way we also note that by slightly strengthening Razborov and Rudich's argument, one can show that their "naturalization barrier" is actually a barrier to proving superquadratic circuit lower bounds, not just $P/poly$ circuit lower bounds. It remains open whether there is a naturalization barrier to proving superlinear circuit lower bounds.

1. Introduction

In a famous paper [6], Razborov and Rudich introduced the concept of a *natural combinatorial property* of a Boolean function. They showed on the one hand that almost all lower bounds in circuit complexity theory proved up to that time (specifically, all non-relativizing, non-monotone, superlinear lower bounds) had employed natural properties, and on the other hand that natural properties cannot be used to separate P from NP unless 2^{n^ϵ}-hard pseudorandom number generators do not exist. Their result is widely regarded as a serious barrier to proving strong circuit lower bounds.

In more detail, if Γ and Λ are complexity classes, then Razborov and Rudich say that a property of Boolean functions on n variables is *Γ-natural of density δ_n and useful against Λ* if (roughly speaking) the property is Γ-computable, holds for $2^{2^n}\delta_n$ Boolean functions, and contains no Λ-computable Boolean functions. (Here the complexity Γ is measured in terms of the size $N = 2^n$ of the truth table of a Boolean function.) They showed that if $\Gamma = \Lambda = P/poly$ and $\delta_n = \Omega(2^{-poly(n)})$, then no such properties exist unless 2^{n^ϵ}-hard pseudorandom number generators do not exist.

It follows that if we believe in hard pseudorandom number generators but still wish to prove circuit lower bounds, then we are led to ask just *how* complex and/or sparse a property needs to be in order to circumvent the so-called "naturalization barrier." Our main result is that only a slight decrease in the density is needed. Specifically, under the same 2^{n^ϵ}-hard pseudorandomness assumption made in the original Razborov–Rudich paper, we can explicitly exhibit a nearly-linear-time-computable property that separates NP from $P/poly$ and whose density is $2^{-q(n)}$ where q is a quasi-polynomial function (whose degree depends on ϵ and on the size of the pseudorandom number generator). Of course, the pseudorandomness

E-mail address: tchow@alum.mit.edu.

0022-0000/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcss.2010.06.017

hypothesis trivially implies the existence of constructive properties that separate *NP* from $P/poly$; for example, simply take an explicit family of *NP*-complete Boolean functions. However, this latter family has density $2^{-e(n)}$ for some function $e(n)$ that grows exponentially; this is far smaller than $2^{-q(n)}$.

The main idea of our proof is to exploit the *self-defeating nature* of natural proofs. Assume that natural, useful properties do not exist (for example, by assuming that 2^{n^ϵ}-hard pseudorandom number generators exist and invoking Razborov–Rudich). This means that every attempt to find a natural property that discriminates high-complexity functions from low-complexity functions fails. The key observation is that *a natural property is itself a low-complexity function* (a low-complexity function of a truth table, that is, but a truth table is just an arbitrary binary string). Therefore we have identified a feature that every low-complexity function has: It is no good at discriminating high-complexity functions from low-complexity ones. So if we consider the property of *discrimination*, i.e., the ability to distinguish high-complexity functions from low-complexity ones, then *discrimination is a useful property*—i.e., it excludes $P/poly$.[1] On the other hand, it turns out to be easy to show, unconditionally, that the discrimination property has the claimed complexity and density. It is also easy to describe explicitly an *NP* function that is discriminating. Thus, under our pseudorandomness assumption, discrimination separates *NP* from $P/poly$. (As we shall see later, the proof in fact separates a subclass of *NP* from $P/poly$.) This is our main result.

The key point is that the very assumption that natural, useful properties do not exist yields a useful property.

One can ask whether the above line of reasoning can be used to prove an *unconditional* result, just as Avi Wigderson has adapted Razborov and Rudich's argument to prove unconditionally that there is no natural proof that the discrete logarithm problem is hard. Indeed, this is possible, as we show below. We also show that this unconditional result can be proved using a direct counting argument.

After my talk at FOCS 2008, Salil Vadhan showed me a variant of the main result of this paper. Making a slightly weaker assumption, namely that SAT is not computable by circuits of size 2^{n^ϵ}, one can deduce that there exists a sublinear-natural property of density $2^{-q(n)}$ that separates *NP* from $P/poly$ (though not a subclass of *NP* as in our main result). With Vadhan's kind permission, his proof is included in this paper.

Regarding the complexity Γ, Rudich [8] has shown that if we allow ourselves to assume a stronger pseudorandomness hypothesis, then the naturalization barrier remains intact even if Γ is taken to be $N\tilde{P}/qpoly$ (i.e., non-uniform, nondeterministic circuits of quasi-polynomial size). On the other hand, as pointed out by a referee of the FOCS 2008 extended abstract of this paper, for any fixed k there are properties computable in time $2^{n^{k+1}}$ that are useful against circuits of size n^k (simply use brute-force search).

We hope that these results will give some insight into how to bypass the naturalization barrier. If 2^{n^ϵ}-hard pseudorandom number generators do not exist, then of course the naturalization barrier evaporates. On the other hand, if such generators *do* exist, then our results show that there exists at least one property (namely, discrimination) that separates *NP* from $P/poly$ and that is both constructive and—as we shall see shortly—only a minor alteration of a random property.

2. Table of results

To help the reader acquire an overall picture of our results, we collect them together here in one place. For ease of comprehension, we do not state the results in their greatest generality here. The notation $NP[\log^k n]$ is due to Papadimitriou and Yannakakis and denotes the language accepted by nondeterministic polynomial time machines that make $O(\log^k n)$ nondeterministic moves.

- If there is a 2^{k^ϵ}-hard pseudorandom number generator in $SIZE(k^c)$, then there is no $1/2^{n^d}$-dense $P/poly$-natural property useful against $SIZE(n^e)$ whenever $e > 1 + cd/\epsilon$. (Theorem 1, essentially due to Razborov and Rudich.)
- If there is a 2^{k^ϵ}-hard pseudorandom number generator in $SIZE(k^c)$, then there is a $1/2^{qpoly(n)}$-dense nearly-linear-natural property useful against $P/poly$ that contains a language in $NP[\log^e n]$ (where $e > 1 + c/\epsilon$). In particular $NP[polylog(n)] \nsubseteq P/poly$. (Theorem 2.)
- If SAT is not in $SIZE[2^{k^\epsilon}]$, then there is a $1/2^{qpoly(n)}$-dense sublinear-natural property useful against $P/poly$ that contains SAT. In particular $NP \nsubseteq P/poly$. (Theorem 3.)
- Unconditionally, there is a $1/2^{qpoly(n)}$-dense $SIZE(N)$-natural property useful against $P/poly$. (Theorem 5.)

3. Preliminaries

We write $\mathbb{N}$ for the positive integers, and our logarithms are always base 2. All gates in our Boolean circuits are assumed to have just two inputs. We use the notation (x_n) to denote a sequence $x_1, x_2, \ldots,$ and whenever we refer to a sequence (f_n) of Boolean functions, we always understand that f_n is a function of n variables. Given a function $\lambda : \mathbb{N} \to \mathbb{N}$, we write $SIZE(\lambda)$ to denote the complexity class comprising all sequences (f_n) of Boolean functions for which there exists a constant c such that the minimum circuit size of f_n is at most $c\lambda(n)$ for all sufficiently large n. The following standard notation will also be convenient.

[1] See Definition 8 below for a precise definition of a *discriminating* function.

Definition 1. Given two functions $\gamma : \mathbb{N} \to \mathbb{N}$ and $\lambda : \mathbb{N} \to \mathbb{N}$, we write $\gamma(n) = \omega(\lambda(n))$ if for every constant $c > 0$ there exists n_0 such that $\gamma(n) > c\lambda(n)$ for all $n \geqslant n_0$. That is, γ eventually grows *strictly* faster than any constant times λ.

Now let us review some fundamental concepts from [6].

Definition 2. A *Boolean function property* (or just *property* for short) is a sequence $C = (C_n)$ where each C_n is a set of Boolean functions on n variables.

Definition 3. If Γ is a complexity class and (δ_n) is a sequence of positive real numbers, then a property (C_n) is *Γ-natural with density δ_n* if

1. (largeness) $|C_n| \geqslant 2^{2^n}\delta_n$ for all sufficiently large n; and
2. (constructivity) the problem of determining whether $f_n \in C_n$, given as input the full truth table of a Boolean function f_n on n variables, is computable in Γ.

Note that our definition of *natural* differs slightly from that of Razborov and Rudich; for them, a natural property is one which *contains* a large and constructive property. This difference will do no harm, because our results assert the *existence* of certain natural properties in our sense, and a property that is natural in our sense is also natural in Razborov and Rudich's sense.

Later on we will be particularly interested in the case of *nearly-linear-natural* properties, which we define to mean $\Gamma = \mathit{DTIME}(N(\log N)^c)$ for some constant c. Here we have used an uppercase N to emphasize that "nearly linear" means nearly linear in $N = 2^n$, the size of the truth table of f_n.

Next we recall the definition of a *useful* property.

Definition 4. If Λ is a complexity class, then a property (C_n) is *useful against Λ* if $(f_n) \notin \Lambda$ whenever (f_n) is a sequence (f_n) of Boolean functions satisfying $f_n \in C_n$ for infinitely many n.

For our purposes we also need a slightly weaker notion, which we shall call *quasi-usefulness*.

Definition 5. If Λ is a complexity class, then a property (C_n) is *quasi-useful against Λ* if $(f_n) \notin \Lambda$ whenever (f_n) is a sequence (f_n) of Boolean functions satisfying $f_n \in C_n$ for all sufficiently large n.

The difference between usefulness and quasi-usefulness is that there may be infinitely many n for which a quasi-useful property is easy to compute, whereas this cannot happen for a useful property.[2] However, a quasi-useful property retains the important characteristic of not containing any Λ-computable sequence of Boolean functions. So for the purpose of separating Λ from a higher complexity class, quasi-usefulness suffices.

Note that the only reason we introduce quasi-usefulness is to handle the slightly annoying technicality that the length of a truth table is not an arbitrary integer but is always a power of two. An alternative way around this technicality might be to pad out strings whose lengths are not powers of two, but we do not pursue that possibility here.

Definition 6. Fix $\epsilon > 0$. A family of functions $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ is a *2^{n^ϵ}-hard pseudorandom number generator* if for every circuit C with fewer than 2^{n^ϵ} gates,

$$\left|\mathrm{Prob}\big[C\big(G_n(\mathbf{x})\big) = 1\big] - \mathrm{Prob}\big[C(\mathbf{y}) = 1\big]\right| < 1/2^{n^\epsilon}.$$

Here $\mathbf{x}$ is chosen at random from $\{0,1\}^n$ and $\mathbf{y}$ is chosen at random from $\{0,1\}^{2n}$.

We are now ready for Razborov and Rudich's fundamental result. We need a slightly stronger version of the theorem than the one that appears in their paper. This strengthened version is of some independent interest, because by taking $c = d = 1$ and $\epsilon < 1$ in Theorem 1 below, we see that there is a naturalization barrier to proving superquadratic circuit lower bounds, not just $P/poly$ circuit lower bounds. It seems to be an open problem whether there is a naturalization barrier to proving *superlinear* circuit lower bounds.

Theorem 1 *(Razborov–Rudich). Fix $c \geqslant 1$, $d \geqslant 1$, and $\epsilon > 0$. Assume that there exists a 2^{k^ϵ}-hard pseudorandom number generator G_k in SIZE(k^c). Then for any $e > 1 + cd/\epsilon$, there is no $P/poly$-natural property with density greater than 2^{-n^d} that is useful against SIZE(n^e).*

[2] As pointed out by a referee, our distinction between *useful* and *quasi-useful* is the same as the distinction between *diagonalization a.e.* and *diagonalization i.o.* in [7].

Proof. Only minor changes to Razborov and Rudich's argument are needed, but for completeness we give a full proof.

Choose any $e > 1 + cd/\epsilon$. We use our pseudorandom *number* generator G to construct a pseudorandom *function* generator f. For every $k \geqslant 1$, let $G_k^0, G_k^1 : \{0,1\}^k \to \{0,1\}^k$ be the first and last k bits of G_k respectively. For the rest of the proof, we will write n for $\lfloor k^{\epsilon/d}/2 \rfloor$. For any k-bit string x, let $f(x)$ be the Boolean function that sends $y \in \{0,1\}^n$ to the first bit of

$$G_k^{y_n} \circ G_k^{y_{n-1}} \circ \cdots \circ G_k^{y_1}(x).$$

We claim that the family of functions $\{f(x)\}$ is in *SIZE*(n^e). This is because G_k is in *SIZE*(k^c) $\subseteq$ *SIZE*(n^{e-1}), and it is straightforward to build a circuit for $f(x)$ using n copies of G_k (with the ith bit of the input dictating which half of the ith copy of G_k to use).

Now assume towards a contradiction that there exists a $P/poly$-natural property (C_n) with density at least 2^{-n^d} that is useful against *SIZE*(n^e). Then for all sufficiently large k, none of the functions $f(x)$ are in C_n. Therefore if $\mathbf{f}_n$ denotes a randomly chosen Boolean function on n variables and $\mathbf{x}$ denotes a randomly chosen k-bit string, then

$$\bigl|\mathrm{Prob}\bigl[C_n\bigl(f(\mathbf{x})\bigr) = 1\bigr] - \mathrm{Prob}\bigl[C_n(\mathbf{f}_n) = 1\bigr]\bigr| \geqslant 2^{-n^d}. \tag{1}$$

Eq. (1) gives us a statistical test for $f(\mathbf{x})$, which we now convert into a statistical test for G_k. Let T be a binary tree of height n, having $2^n - 1$ internal nodes and 2^n leaves. Construct a labeling ℓ of the nodes of T by labeling the leaves with (distinct) n-bit binary strings and labeling the internal nodes with (distinct) numbers 1 to $2^n - 1$ in such a way that if u and v are internal nodes and u is a child of v, then $\ell(u) < \ell(v)$. If y is a leaf of T, then let $\ell(y)(j)$ denote the jth bit of $\ell(y)$. For $i \in \{0, 1, \ldots, 2^n - 1\}$, let T_i be the subforest of T induced by the set of internal nodes v with $\ell(v) \leqslant i$, together with all the leaves. If y is a leaf of T, then let $v_i(y)$ be the root of the subtree of T_i containing y, and let $h(i, y)$ be the distance between $v_i(y)$ and y (so for example $h(i, y) = 0$ if $v_i(y) = y$).

Now define independent random variables $\mathbf{x}(v)$, one for each node v of T, and each chosen uniformly from $\{0,1\}^k$. Define a random collection $\mathbf{f}_{i,n}$ by letting $\mathbf{f}_{i,n}(y)$ (for a leaf y of T) be the first bit of

$$G_k^{\ell(y)(n)} \circ G_k^{\ell(y)(n-1)} \circ \cdots \circ G_k^{\ell(y)(n-h(i,y)+1)}\bigl(\mathbf{x}\bigl(v_i(y)\bigr)\bigr).$$

Then $\mathbf{f}_{0,n}$ is $\mathbf{f}_n$ and $\mathbf{f}_{2^n-1,n}$ is $f(\mathbf{x})$, so Eq. (1) implies that for some i,

$$\bigl|\mathrm{Prob}\bigl[C_n(\mathbf{f}_{i-1,n}) = 1\bigr] - \mathrm{Prob}\bigl[C_n(\mathbf{f}_{i,n}) = 1\bigr]\bigr| \geqslant 2^{-n^d}/2^n \geqslant 2^{-2n^d}, \tag{2}$$

since $d \geqslant 1$. There must exist some assignment of the values of the $\mathbf{x}(v)$ for all roots v of subtrees of T_i except the root u with $\ell(u) = i$, such that Eq. (2) still holds when conditioned on this assignment. By fixing such an assignment, we obtain a statistical test that distinguishes between $G_k(\mathbf{x}(u))$ and $(\mathbf{x}(u'), \mathbf{x}(u''))$, where u' and u'' are the children of u, and that can be computed by circuits of size $2^{O(n)}$ (because $(C_n) \in P/poly$). But this contradicts the 2^{k^ϵ}-hardness of G_k, because for all sufficiently large k, k^ϵ is larger than $2n^d$ and also larger than any constant times n. □

For our final preliminary result we need the following definition.

Definition 7. We write $\psi(n, g)$ for the number of Boolean functions of n variables that can be computed by Boolean circuits with at most g gates.

We need an upper bound for $\psi(n, g)$. The result is essentially due to Shannon, though the version we quote here is Lemma 2.1 in [9].

Proposition 1. *For all $n \geqslant 1$ and $g \geqslant 1$, $\psi(n, g) < g^g e^{g+4n}$.*

4. The main result

Theorem 2. *Assume that, for some $\epsilon > 0$, there exists a 2^{n^ϵ}-hard pseudorandom number generator G in $P/poly$. Then there exists a quasi-polynomial function q and a nearly-linear-natural property of density $\Omega(2^{-q(n)})$ separating NP from $P/poly$.*

In fact, as will be apparent from the proof, the property we exhibit contains functions that are probably not *NP*-hard, so our separation is actually stronger than *NP* $\not\subseteq$ $P/poly$.

The main tool in our proof of Theorem 2 is the following concept.

Definition 8. Given $\gamma : \mathbb{N} \to \mathbb{N}$, we define a Boolean function f on n variables to be *γ-discriminating* if either of the following two conditions holds:

1. n is not a power of 2.
2. $n = 2^m$ for some m and
   (a) $f(x) = 1$ for at least $2^n/n$ values of (the n-digit binary string) x, and
   (b) $f(x) = 0$ if x is the truth table of a Boolean function on m variables that is computable by a Boolean circuit with at most $\gamma(m)$ gates.

If we let M_n^γ be the set of all γ-discriminating Boolean functions on n variables, then (M_n^γ) is a Boolean function property that we shall call *γ-discrimination.*

The following easy lemma shows that γ-discrimination is constructive, and gives a lower bound on its density.

Lemma 1. *Let $\gamma : \mathbb{N} \to \mathbb{N}$ be a time-constructible function satisfying $\gamma(m) \leqslant 2^m/m$ for all m. Then γ-discrimination is a nearly-linear-natural property with density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$.*

Proof. Let n denote the number of variables of our Boolean functions. If n is not a power of 2 then the lemma is trivial, so assume that $n = 2^m$.

First we note that, since $\gamma(m) \leqslant 2^m/m$, it is easy to deduce from Proposition 1 that the number of Boolean circuits with m inputs and at most $\gamma(m)$ gates is much less than $2^{2^m} = 2^n$.

Let us check constructivity. To verify that a given truth table is the truth table of a γ-discriminating function, we must check that the fraction of entries equal to 1 is at least $1/n$, and we must also check that the entries indexed by truth tables of functions computable by circuits with at most $\gamma(m)$ gates are 0. Let $N = 2^n$ be the size of the truth table. Counting 1's clearly takes time that is nearly linear in N, but to check the forced 0's we must first compute $\gamma(m)$, then run through each possible Boolean circuit in turn, computing its n truth table values, and checking that the corresponding entry of the given truth table is 0. Since γ is time-constructible, computing $\gamma(m)$ takes time $O(2^m)$, so evaluating γ at $m = \log\log N$ takes time at most polylogarithmic in N. Enumerating all the circuits is a straightforward process, and the total number of circuits to be enumerated is at most N, so the entire computation takes time at most N multiplied by some factors that are polylogarithmic in N.

It remains to estimate the density. If we were to ignore condition 2(a) in the definition of a γ-discriminating function, then we would simply be counting functions that must be 0 in certain positions and are unrestricted otherwise, so the total number of functions on n variables would be precisely $2^{2^n - \psi(m,\gamma(m))}$.From this we can get a lower bound for the true number of γ-discriminating functions by subtracting off the total number of Boolean functions on n variables whose truth tables have at most $2^n/n$ entries equal to 1. This latter quantity is

$$\sum_{i=0}^{2^n/n} \binom{2^n}{i}.$$

By Lemma 3,

$$\sum_{i=0}^{2^n/n} \binom{2^n}{i} = O\left(\binom{2^n}{2^n/n}\right) = 2^{O(2^n \log n)/n},$$

where the second equality is a routine application of Stirling's approximation. It follows that for some constant c, the number of γ-discriminating functions is at least

$$2^{2^n - \psi(m,\gamma(m))} - 2^{c(2^n \log n)/n} = 2^{2^n} 2^{-\psi(m,\gamma(m))}\left(1 - 2^{c(2^n \log n)/n - 2^n + \psi(m,\gamma(m))}\right).$$

Again, $\psi(m, \gamma(m))$ is vanishingly small compared to $2^{2^m} = 2^n$, so the density is indeed eventually lower-bounded by a constant times $2^{-\psi(m,\gamma(m))}$. □

We are now ready for the proof of our main result.

Proof of Theorem 2. By hypothesis, there exists $c \geqslant 1$ such that the pseudorandom number generator G_k is in *SIZE*(k^c). Choose some number $e > 1 + c/\epsilon$, and let γ be the function $\gamma(m) = m^e$. Then we claim that the desired property is simply γ-discrimination.

By Lemma 1 we know that γ-discrimination is nearly-linear-natural with density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$. Since γ is a polynomial function, Proposition 1 implies that this density is indeed $\Omega(2^{-q(n)})$ for some quasi-polynomial q.

We next show that γ-discrimination is quasi-useful against *P/poly*. Given $f_n \in M_n^\gamma$, define the property (C_m) by letting a function with truth table x be in C_m if and only if $f_{2^m}(x) = 1$. Since f is a γ-discriminating function, it follows that (C_m) is useful against *SIZE*(m^e) and that (C_m) has density $\Omega(2^{-m})$. Invoking Theorem 1 with $d = 1$, we see that (C_m) cannot be *P/poly*-constructive. In other words, $(f_n) \notin$ *P/poly*, which means that γ-discrimination is indeed quasi-useful against *P/poly*.

Finally, let (f_n) be the sequence of γ-discriminating functions that are 0 only when forced to be by condition 2(b) and that are 1 otherwise. Then (f_n) is in *NP*, in the sense that the language L defined by

$$x \in L \quad \Longleftrightarrow \quad f_n(x) = 0$$

is in *NP*.[3] The reason is that, for n a power of 2, a Boolean circuit with truth table x is a certificate for membership in L, and such a circuit has size $\gamma(\log n)$, which is polynomial (even polylogarithmic) in n, the size of x. This completes the proof. □

Note that as we remarked earlier, the function (f_n) in the above proof is almost certainly not *NP*-complete; in fact, it is in $NP[\log^e n]$. So we have actually separated $P/poly$ from $NP[polylog(n)]$.

5. Vadhan's variation

Here we give the proof of Vadhan's variation mentioned in the introduction.

Theorem 3. *Assume that SAT is not computable by circuits of size 2^{n^ϵ}. Let γ be a function such that $\gamma(n) = \omega((\log n)^{1/\epsilon})$, and let $q(n) = 2^{\gamma(n)}$. Then there exists a sublinear-natural property of density $2^{-q(n)}$ that separates NP from $P/poly$.*

Proof. To ease notation, let $m = \gamma(n)$. Fix some way of encoding SAT instances as binary strings. Let C_n comprise all Boolean functions f of n variables with the following property. If the last $n - m$ bits of x are all zero, then $f(x)$ is 1 or 0 according to whether or not the first m bits of x encode a satisfiable instance of SAT. (If any of the last $n - m$ bits of x are nonzero, then $f(x)$ can be anything.) Then C_n has density $1/2^{2^m} = 2^{-q(n)}$. By our assumption on the hardness of SAT, functions in C_n cannot be computed by circuits of size 2^{m^ϵ}. Since m^ϵ grows faster than $d \log n$ for any fixed d, this shows that (C_n) is useful against $P/poly$. Checking membership in C_n can be done in time $poly(m) \cdot 2^m$, which is certainly sublinear in 2^n. □

6. An unconditional result

As we remarked in the introduction, the idea behind the proof of Theorem 2 can be adapted to prove a non-uniform version of the result that has no unproven hypotheses. Now, it turns out that this unconditional result can also be proven by a counting argument that does not use any self-reference. Since the two arguments are very different in flavor, we present both of them below.

First we need a non-uniform version of Lemma 1.

Lemma 2. *Let $\gamma : \mathbb{N} \to \mathbb{N}$ be a function satisfying $\gamma(m) \leqslant 2^m/m$ for all m. Then γ-discrimination is a non-uniformly linear-natural property with density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$.*

When we say "non-uniformly linear-natural property," we of course mean that membership can be decided by circuits whose size is linear in the size of the truth table.

Proof. The proof is the same as the proof of Lemma 1 except when it comes to Γ-constructivity.

Let $n = 2^m$ denote the number of variables of our Boolean functions. As we said before, to verify that a given truth table is the truth table of a γ-discriminating function, we must check that the fraction of entries equal to 1 is at least $1/n$, and we must also check that the entries indexed by truth tables of functions computable by circuits with at most $\gamma(m)$ gates are 0. Let $N = 2^n$ be the size of the truth table. We can count the number of 1's using $O(N)$ gates, for example by using carry-save addition. Also, for each n, the set of truth table entries that must be 0 is fixed, so this condition can be checked using a number of gates that is proportional to the number of forced 0's (even if γ is not time-constructible); this number is certainly $O(N)$. □

Theorem 4. *Let $\gamma, \lambda : \mathbb{N} \to \mathbb{N}$ be functions such that $\gamma(n) = \omega(\lambda(n))$ and such that $m \leqslant \gamma(m) \leqslant 2^m/m$ for all m. Let $\Gamma = SIZE(\gamma)$ and let $\Lambda = SIZE(\lambda)$. Then there exists a Γ-natural property (C_n) with density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$ that is quasi-useful against Λ.*

Proof. We argue by contradiction. Assume, as a reductio hypothesis, that there is no Γ-natural property (C_m) with density $\Omega(2^{-\psi(\log m, \gamma(\log m))})$ that is quasi-useful against Λ. Then we claim that γ-discrimination is quasi-useful against Λ.

To see this, pick an arbitrary sequence of functions $f_n \in M_n^\gamma$. Define a property (C_m) by letting a function of m variables with truth table x be in C_m if and only if $f_{2^m}(x) = 1$. Then by condition 2(a) in the definition of a γ-discriminating function, (C_m) has density $\Omega(2^{-m})$. By assumption, $\gamma(\log m) \geqslant \log m$, and it is easy to see that there are more than m distinct Boolean functions computable with $\log m$ gates and $\log m$ inputs, so the density of (C_m) is $\Omega(2^{-\psi(\log m, \gamma(\log m))})$. By condition 2(b),

[3] Technically, the language defined by $f_n(x) = 1$ is in co-*NP*, but we prefer to emphasize the *NP* side since there is a natural certificate. Alternatively, one can simply interchange the roles of 0 and 1 in Definition 8.

if $g_m \in C_m$ is any sequence of Boolean functions, then the minimum circuit size of g_m exceeds $\gamma(m)$, and hence $(g_m) \notin \Lambda$ since $\gamma(m) = \omega(\lambda(m))$. In other words, (C_m) is quasi-useful (in fact, useful) against Λ. Therefore, by our reductio hypothesis, membership in (C_m) is not Γ-computable. It follows that $(f_n) \notin \Gamma$, and a fortiori $(f_n) \notin \Lambda$. Therefore (f_n) is quasi-useful against Λ, as claimed.

But since $n \leqslant \gamma(n) \leqslant 2^n/n$, Lemma 2 tells us that (M_n^λ) is Γ-natural with density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$. Combined with the quasi-usefulness against Λ that we just proved, this fact contradicts our reductio hypothesis, so the theorem is proved. □

Observe that a curious feature of the above proof is that it is highly ineffective. The natural property whose existence is asserted is not explicitly exhibited, nor can an explicit example be extracted from the proof, which is intrinsically a proof by contradiction. Note also that a *SIZE*(γ)-natural property is not necessarily "constructive" in the intuitive sense even if γ is polynomial, because *SIZE*(γ) is a *non-uniform* complexity class. Nevertheless, we feel that Theorem 4 remains of some interest because it is an unconditional result.

Next we present the promised counting argument, which in fact yields a stronger result than Theorem 4. The basic idea is very simple, and the reader is encouraged to skip ahead directly to Theorem 5 below and read the first paragraph of the proof, which contains the essence of the argument. Everything else in the rest of this section consists of technicalities needed to make that argument rigorous.

For the proof of Theorem 5, we need a lower bound on $\psi(n, g)$ (Proposition 2 below). The proof of the lower bound in turn relies on a couple of facts about binomial coefficients. These facts are well known to experts, but for completeness we give the proofs. The first fact is an elementary large-deviation result.

Lemma 3. *If $k \leqslant (1/2 - \epsilon)N$, then there is a constant $c > 0$ (depending on ϵ but not on N or k) such that*

$$\sum_{i=0}^{k} \binom{N}{i} \leqslant c\binom{N}{k}. \tag{3}$$

Proof. Let S denote the sum on the left-hand side of (3). The ratio between consecutive terms in S is $i/(N - i + 1)$, and since $i \leqslant k \leqslant (1/2 - \epsilon)N$, it follows that

$$\frac{i}{N - i + 1} \leqslant \frac{(1/2 - \epsilon)N}{(1/2 + \epsilon)N + 1}. \tag{4}$$

The right-hand side of (4) is bounded by some constant strictly less than one. Therefore S is bounded by a convergent geometric series, and this proves the lemma. □

Lemma 4. *Assume that $k \leqslant N/2$. If $\log\binom{N}{k} \leqslant N/2$, then $k \leqslant N/4$.*

As the proof below makes clear, Lemma 4 remains true if we replace "$N/2$" by "$(1 - \epsilon)N$," provided we replace "$N/4$" by a suitable constant times N and require that N be sufficiently large. We do not need this extra generality, so we have stated Lemma 4 with specific constants to make it easier to read.

Proof. If $k = 0$ then the result is trivial, so assume that $k \neq 0$. Let $H(x) := -x\log x - (1 - x)\log(1 - x)$ be the entropy function. The basic reason why the lemma is true is that $\log\binom{N}{k} \approx N \cdot H(k/N)$. More precisely, by Stirling's approximation,

$$\begin{aligned}\log\binom{N}{k} &\geqslant N \cdot H(k/N) + \frac{1}{2}\log\frac{N}{k(N-k)} - \frac{1}{2}\log 2\pi - \left(\frac{1}{12k} + \frac{1}{12(N-k)}\right)\log e \\ &\geqslant N \cdot H(k/N) + \frac{1}{2}\log\frac{N}{k(N-k)} - 2.\end{aligned}$$

So if $\log\binom{N}{k} \leqslant N/2$, then

$$H(k/N) \leqslant \frac{1}{2} - \frac{1}{2N}\log\frac{N}{k(N-k)} + \frac{2}{N}.$$

The expression $N/k(N - k)$ is minimized when $k = N/2$, and by elementary calculus we find that $(1/2x)\log(4/x)$ is minimized when $x = 4e$ (remember that in this paper, our logarithms are base 2). Therefore, provided $N \geqslant 10$,

$$H(k/N) \leqslant \frac{1}{2} + \frac{\log e}{8e} + 0.2 \leqslant 0.8.$$

It follows that if $N \geqslant 10$, $k/N \leqslant H^{-1}(0.8) \leqslant 1/4$ as desired. If $N < 10$, then the lemma can be checked by direct computation. □

Now we are ready to prove our lower bound on $\psi(n, g)$.

Proposition 2. *Let $\gamma : \mathbb{N} \to \mathbb{N}$ be a function such that $\gamma(n) \leqslant 2^{n-2}/n$ and such that $\gamma(n) = \omega(n \log n)$. Then for any fixed d, $\psi(n, \gamma(n)) \geqslant n^d \psi(n, \gamma(n)/2)$ for all sufficiently large n.*

Proof. Let $N = 2^n$. We are trying to find a lower bound on how many more Boolean functions we can compute with $\gamma(n)$ gates than we can compute with only $\gamma(n)/2$ gates. Our main observation is that by using $O(n)$ extra gates, we can change any single entry of the truth table of any given Boolean circuit: Simply use the $O(n)$ gates to test if the input equals a specific n-bit value, and flip the output of the circuit if it does.

If B denotes the set of truth tables of functions computable with at most $\gamma(n)/2$ gates, then our main observation implies that if we are allowed up to $\gamma(n)/2 + O(n)$ gates, then at minimum we can also compute all the functions on the *boundary* $G(B)$ of B, i.e., the truth tables whose Hamming distance from B is 1. We know very little about the structure of B, but we do have an estimate of its volume, so we can obtain a lower bound on the size of its boundary by appealing to a discrete isoperimetric inequality. In particular, it follows from standard results[4] that if we choose k so that

$$\sum_{i=0}^{k} \binom{N}{i} \leqslant |B| < \sum_{i=0}^{k+1} \binom{N}{i}, \tag{5}$$

then $|G(B)| \geqslant \binom{N}{k+1}$. We claim that there is some constant c such that $|B| < c|G(B)|$ for all large n. To see this, note that since $\gamma(n) \leqslant N/4n$, Proposition 1 implies that for large n,

$$\log|B| \leqslant \frac{N}{4n} \log \frac{N}{4n} + \left(\frac{N}{4n} + 4n\right) \log e \leqslant \frac{2N}{4n} \log \frac{N}{4n} = \frac{N}{2}\left(1 - \frac{\log 4n}{n}\right) \leqslant N/2.$$

But (5) yields the lower bound $|B| \geqslant \binom{N}{k}$, so by Lemma 4, $k \leqslant N/4$. This fact, together with the upper bound on $|B|$ given by (5), implies (by Lemma 3) that $|B|$ is bounded by a constant times $\binom{N}{k+1}$. Since $|G(B)| \geqslant \binom{N}{k+1}$, our claim is proved.

So when an additional $O(n)$ gates are allowed, the number of computable functions is multiplied by at least some constant factor $K > 1$. Now in fact we have $\gamma(n)/2$ additional gates at our disposal, and $\gamma(n)/2 = \omega(n \log n)$, so the multiplicative factor is greater than $K^{c \log n}$ for any constant c, and this eventually grows faster than n^d for any fixed d. □

Theorem 5. *Let $\gamma, \lambda : \mathbb{N} \to \mathbb{N}$ be functions such that $\lambda(n) = \Omega(n \log n)$, $\gamma(n) = \omega(\lambda(n))$, and $\gamma(n) \leqslant 2^{n-2}/n$ for all n. Let Λ = SIZE(λ). Then there exists a non-uniformly linear-natural property with density at least $1/\psi(n, \gamma(n))$ that is useful against Λ.*

Proof. Let us first give a somewhat informal proof that conveys the essential idea. Let $N = 2^n$. As usual, think of Boolean functions on n variables as represented by their truth tables. Let G_n be the set of Boolean functions on n variables computable by circuits of size $\gamma(n)/2$. For each $g \in G_n$, imagine a Hamming ball of volume $2^N/\psi(n, \gamma(n))$ centered at g (by a *Hamming ball centered at g* we mean the set of all Boolean functions within a certain Hamming distance from g). There are $\psi(n, \gamma(n)/2) < \psi(n, \gamma(n))$ such balls, so the total volume of these balls is less than 2^N. Therefore there must exist a function f_n outside all of these balls. It follows that there is a Hamming ball B_n of volume $2^N/\psi(n, \gamma(n))$ around f_n that is disjoint from G_n. Then since $\gamma(n) = \omega(\lambda(n))$, (B_n) is a property that is useful against Λ. Its density is $1/\psi(n, \gamma(n))$. Moreover, testing for membership in B_n amounts to computing Hamming distance from f_n, which can be done with circuits of linear size.

This completes the informal proof. The only point that is not entirely rigorous is the assumption that there exists a Hamming ball whose volume is exactly $2^N/\psi(n, \gamma(n))$; this may not be true because the volume of a Hamming ball is necessarily a sum of consecutive binomial coefficients. For a rigorous argument, we choose our Hamming balls to have radius r, where r is chosen so that

$$\sum_{i=0}^{r-1} \binom{N}{i} < \frac{2^N}{\psi_n} \leqslant \sum_{i=0}^{r} \binom{N}{i}, \tag{6}$$

where we have abbreviated $\psi(n, \gamma(n))$ to ψ_n to ease notation. Then the property of being in B_n certainly has density at least $1/\psi_n$, so all that needs to be checked is that $\psi(n, \gamma(n)/2)$ such Hamming balls have total volume strictly less than 2^N, i.e., that

[4] See for example Bezrukov's survey paper [2]. Bezrukov states an isoperimetric inequality for the *inner* boundary $\Gamma(B)$, but this can be converted into an inequality for $G(B)$ as follows. In the notation of Bezrukov's paper, we may assume that B is an optimal set L_m^N for some m. Then the radius-$(k+1)$ Hamming ball $S_{k+1}^N(0) \subseteq B \cup G(B)$, so if we let $b = |B \cup G(B)|$, it follows that as long as $k+1 < N/2$,

$$\left|\Gamma\left(B \cup G(B)\right)\right| \geqslant \left|\Gamma\left(L_b^N\right)\right| \geqslant \left|\Gamma\left(S_{k+1}^N(0)\right)\right| = \binom{N}{k+1}.$$

On the other hand, $\Gamma(B \cup G(B)) \subseteq G(B)$ so $|\Gamma(B \cup G(B))| \leqslant |G(B)|$.

$$\psi\bigl(n,\gamma(n)/2\bigr)\sum_{i=0}^{r}\binom{N}{r}<2^N. \tag{7}$$

To prove this, observe that we just need to show that the ratio $(\sum_{i=0}^{r}\binom{N}{i})/(\sum_{i=0}^{r-1}\binom{N}{i})$ is bounded by a polynomial function of n, because then (7) will follow from (6) and Proposition 2. Now

$$\frac{\sum_{i=0}^{r}\binom{N}{i}}{\sum_{i=0}^{r-1}\binom{N}{i}}=\frac{\binom{N}{r}}{\sum_{i=0}^{r-1}\binom{N}{i}}+1\leqslant\frac{\binom{N}{r}}{\binom{N}{r-1}}+1=\frac{N+1}{r}.$$

So we are reduced to showing that $(N+1)/r$ is bounded by a polynomial function of n. To prove this, remember that by assumption $\gamma(n)<N/n$, so Proposition 1 implies that $\psi_n\leqslant(N/n)^{N/n}e^{N/n+4n}$. Taking logarithms and dividing by N, we deduce that

$$\frac{\log\psi_n}{N}\leqslant\frac{1}{n}\log\frac{N}{n}+\left(\frac{1}{n}+\frac{4n}{N}\right)\log e=1-\frac{\log n}{n}+\left(\frac{1}{n}+\frac{4n}{N}\right)\log e.$$

The $(\log n)/n$ term in this expression dominates, so for large n,

$$1-\frac{\log\psi_n}{N}\geqslant\frac{\log n}{2n}. \tag{8}$$

On the other hand, from (6) we have

$$\frac{2^N}{\psi_n}\leqslant\sum_{i=0}^{r}\binom{N}{i}\leqslant\sum_{i=0}^{r}N^i=\frac{N^{r+1}-1}{N-1}\leqslant N^{r+1}.$$

Taking logarithms, we get $N-\log\psi_n\leqslant(r+1)\log N$, which combined with (8) implies that for large n,

$$\frac{r+1}{N}\geqslant\frac{1-(\log\psi_n)/N}{\log N}\geqslant\frac{\log n}{2n^2}.$$

We are now done, because $N/(r+1)$ and $(N+1)/r$ are within a constant factor of each other. □

7. Final remarks

It is natural to ask if our results give any new hope for proving strong circuit lower bounds.[5] It is probably difficult to prove unconditionally that, say, $n^{\log n}$-discrimination is useful against a strong complexity class Λ, not only because that would separate *NP* from Λ, but also because γ-discrimination is closely related to the circuit minimization problem, whose complexity is known to be difficult to get a handle on; see [4].

However, even as a *potential* candidate for an almost-natural proof of $NP\not\subseteq P/poly$, γ-discrimination has an illuminating feature. Namely, the only thing that prevents a γ-discriminating function from looking like a random function is the presence of certain forced 0's in the truth table. Moreover, the proportion of forced 0's goes to zero fairly rapidly as n goes to infinity. This illustrates the fact that largeness can be destroyed by imposing what seems intuitively to be a relatively small amount of "structure" on a random function. Therefore, the intuition that there is some constructive property of random functions that suffices to prove strong circuit lower bounds is not completely destroyed by the Razborov–Rudich results; a minor alteration of a random property may still work.

It is also worth noting that existing circuit lower bound proofs might still be mined for ideas to break the naturalization barrier. Some linear lower bounds, such as those of Blum [3] and Lachish and Raz [5], do not relativize and are not known to naturalize. Even proofs that are known to naturalize are not necessarily devoid of useful ideas. For example, in the course of analyzing a proof by Smolensky, Razborov and Rudich identify three properties $C_1\subseteq C_2\subseteq C_3$ that are implicit in the proof, and show that C_2, and a fortiori C_3, are natural. However, C_1 is constructive but not known to be large, so it is conceivable (though admittedly unlikely) that C_1 is only *almost* large and is actually useful. Of course, one would still need to identify and use some feature of C_1 that is not shared by C_2 in order to prove a stronger circuit lower bound than Smolensky's, but the point is that the usefulness of C_1 is not *automatically* ruled out by the fact that Smolensky's argument naturalizes. In theory, it could still be fruitful to study C_1.

Finally, recall that as evidence that largeness is hard to circumvent, Razborov and Rudich showed that any formal complexity measure automatically yields a large property. Knowing that almost-natural proofs exist, we could perhaps try to come up with something that is almost, but not quite, a formal complexity measure. Unfortunately, as of now, this tempting idea remains purely speculative.

[5] For a survey of other possible approaches to breaking the naturalization barrier, see [1].

Acknowledgments

I thank Salil Vadhan for allowing me to include his proof in this paper. I would also like to thank Bob Beals, Steve Boyack, Sandy Kutin, Avi Wigderson for helpful discussions and encouragement, and the anonymous referees for useful suggestions and comments.

References

[1] Eric S. Allender, Cracks in the defenses: Scouting out approaches on circuit lower bounds, in: Edward A. Hirsch, et al. (Eds.), Computer Science—Theory and Applications: Third International Computer Science Symposium in Russia, CSR 2008, Moscow, Russia, June 2008, Proceedings, in: Lect. Notes Control Comput. Sci., vol. 5010, Springer, 2008, pp. 3–10.

[2] Sergei L. Bezrukov, Isoperimetric problems in discrete spaces, in: Extremal Problems for Finite Sets, Visegrád, 1991, in: Bolyai Soc. Math. Stud., vol. 3, János Bolyai Math. Soc., 1994, pp. 59–91.

[3] Norbert Blum, A Boolean function requiring $3n$ network size, Theoret. Comput. Sci. 28 (1984) 337–345.

[4] Valentine Kabanets, Jin-Yi Cai, Circuit minimization problem, Proc. Symp. Theory Comput. (2000) 73–79.

[5] Oded Lachish, Ran Raz, Explicit lower bound of $4.5n - o(n)$ for Boolean circuits, Proc. 33rd ACM Symp. Theory Comput. (STOC 2001) (2001) 399–408.

[6] Alexander A. Razborov, Steven Rudich, Natural proofs, J. Comput. System Sci. 55 (1997) 24–35.

[7] Kenneth W. Regan, D. Sivakumar, Jin-Yi Cai, Pseudorandom generators, measure theory, and natural proofs, Proc. 36th IEEE Symp. Found. Comput. Sci. (FOCS 1995) (1995) 26–35.

[8] Steven Rudich, Super-bits, demi-bits, and $N\tilde{P}/qpoly$-natural proofs, in: Randomization and Approximation Techniques in Computer Science, in: Lect. Notes Control Comput. Sci., vol. 1269, Springer, 1997, pp. 85–93.

[9] Petr Savický, Alan R. Woods, The number of Boolean functions computed by formulas of a given size, Random Structures Algorithms 13 (1998) 349–382.