Almost-natural Proofs

Timothy Y. Chow
Center for Communications Research
805 Bunn Drive
Princeton, NJ 08540
tchow@alum.mit.edu

Abstract

Razborov and Rudich have shown that so-called natural proofs *are not useful for separating P from NP unless hard pseudorandom number generators do not exist. This famous result is widely regarded as a serious barrier to proving strong lower bounds in circuit complexity theory.*

By definition, a natural combinatorial property satisfies two conditions, constructivity *and* largeness*. Our main result is that if the largeness condition is weakened slightly, then not only does the Razborov–Rudich proof break down, but such "almost-natural" (and useful) properties provably exist. Specifically, under the same pseudorandomness assumption that Razborov and Rudich make, a simple, explicit property that we call* discrimination *suffices to separate $P/poly$ from NP; discrimination is nearly linear-time computable and almost large, having density $2^{-q(n)}$ where q grows slightly faster than a quasi-polynomial function. For those who hope to separate P from NP using random function properties in some sense, discrimination is interesting, because it is constructive, yet may be thought of as a minor alteration of a property of a random function.*

The proof relies heavily on the self-defeating character of natural proofs. Our proof technique also yields an unconditional *result, namely that there exist almost-large and useful properties that are constructive, if we are allowed to call* non-uniform *low-complexity classes "constructive." We note, though, that this unconditional result can also be proved by a more conventional counting argument.*

1. Introduction

In a famous paper [4], 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 function on n variables is Γ-*natural of density* δ_n *and useful against* Λ if (roughly speaking) the property is Γ-computable (from the truth table of a given Boolean function), if it holds for $2^{2^n}\delta_n$ Boolean functions, and if it contains no Λ-computable Boolean functions. 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. Informally, if a property is *constructive* (Γ is sufficiently weak) and *large* (δ_n is sufficiently large), then it is not likely to be useful for proving strong circuit lower bounds.

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* non-constructive and/or small a property needs to be in order to circumvent the so-called "naturalization barrier." Rudich [6] has shown that if we allow ourselves to assume a stronger pseudorandomness hypothesis, then the naturalization barrier remains intact even if constructivity is weakened to $N\tilde{P}/poly$-constructivity. On the other hand, as pointed out by a referee 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).

In this paper we investigate the weakening of the largeness condition. The main result is that under the same 2^{n^ϵ}-hard pseudorandomness assumption of the original Razborov-Rudich paper, we can explicitly exhibit a nearly-linear-natural[1] property that is useful against $P/poly$ and whose density is $2^{-q(n)}$ where q grows slightly faster than a quasi-polynomial function. More precisely, let $\psi(n, g)$

[1] By this we mean that $\Gamma = DTIME(n(\log n)^c)$ for some constant c.

denote the number of Boolean functions of n variables that are computable by Boolean circuits with at most g gates. If 2^{n^ϵ}-hard pseudorandom number generators exist, then for any superpolynomial, subexponential function γ there exists a nearly-linear-natural property of density $\Omega(2^{-\psi(\log n, \gamma(\log n))})$ that separates NP from $P/poly$. Of course, the pseudorandomness 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 much lower density than $2^{-\psi(\log n, \gamma(\log n))}$.

The main idea of our proof is to exploit the "self-defeating nature" of natural proofs. Assume initially that natural, useful properties do not exist. This means that every attempt to find a natural property that discriminates nonconstructive functions from constructive ones is confounded by some constructive function that manages to slip in. The key observation is that *a natural property is itself just a constructive function* (a constructive 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 constructive function has: When we attempt to use it as a discriminator, it is always confounded by some (other) constructive function. So if we consider the property of *discrimination*, i.e., of "not being confounded by any constructive function," then *discrimination is a useful property.* It is easy to check that discrimination is constructive, and almost large.

The argument up to this point already allows us to deduce an unconditional theorem (Theorem 2 below): There exist (non-uniformly) constructive, useful, almost-large properties. For either our initial assumption was false and some constructive, useful, large properties exist, or the particular property of discrimination is constructive, useful, and almost large. We do not know which is the case, but either way, some constructive, useful, almost-large property exists.

If we now allow ourselves to assume the existence of 2^{n^ϵ}-hard pseudorandom number generators, then we can eliminate one horn of our dilemma and conclude that discrimination is natural and useful. Moreover, discrimination contains a function in NP, so discrimination separates NP from $P/poly$. This is our main result (Theorem 3 below).

Note that this argument is not just a simple counting or diagonalization argument, but exploits specifically the self-defeating character of natural proofs, in a way that is reminiscent of (though not quite the same as) Avi Wigderson's argument that there is no natural proof that the discrete logarithm is hard. Now it turns out, as we show later, that Theorem 2 can be proved—and even strengthened—using a more conventional counting argument. However, we do not know of any such way to prove Theorem 3.

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. Background definitions

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.

Now let us review some fundamental concepts from [4].

Definition 1. 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 2. 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) $|C_n| \geq 2^{2^n}\delta_n$ 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 $\Gamma = SIZE(N \log N)$ in the non-uniform case and $\Gamma = DTIME(N(\log N)^c)$ for some constant c in the uniform case. 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 3. If Λ is a complexity class, then a property (C_n) is *useful against* Λ if for every sequence (f_n) of

Boolean functions satisfying $f_n \in C_n$ for infinitely many n, $(f_n) \notin \Lambda$.

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

Definition 4. If Λ is a complexity class, then a property (C_n) is *quasi-useful against* Λ if for every sequence (f_n) of Boolean functions satisfying $f_n \in C_n$ for all sufficiently large n, $(f_n) \notin \Lambda$.

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.

Definition 5. 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,

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

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

The fundamental result of Razborov and Rudich is the following.

Theorem 1 (Razborov–Rudich)**.** *Fix $d > 1$. If 2^{n^ϵ}-hard pseudorandom number generators exist, then there is no $P/poly$-natural property with density $2^{-O(n^d)}$ that is useful against $P/poly$.*

Note that in Razborov and Rudich's paper, they prove the above theorem only for $d = 1$, but it is easy to check that their proof goes through for any fixed $d > 1$.

For our last piece of background, recall from the introduction that we let $\psi(n, g)$ denote the number of Boolean functions of n variables that can be computed by Boolean circuits with at most g gates. The value of the density δ_n in our results is dictated by Shannon's familiar upper bound on $\psi(n, g)$ (see for example [7, Chapter 4, Lemma 2.1]).

Proposition 1. *$\psi(n, g) \le (g + n + 1)^{2g} 16^g g/g!$ for all n and g. In particular, if $g \ge n$ then for all sufficiently large g, $\psi(n, g) < g^{2g}$.*

[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 [5].

3. The main result

In an earlier version of this paper, we considered both Theorems 2 and 3 to be main results. Later, we discovered a simpler proof of Theorem 2, which we shall sketch below in Section 4. Nevertheless, we have decided to keep the original statement and proof of Theorem 2 intact because we feel that it helps clarify the "self-defeating" nature of our proof technique.

Given two functions $\gamma : \mathbb{N} \to \mathbb{N}$ and $\lambda : \mathbb{N} \to \mathbb{N}$, we say that γ *outstrips* λ if for every constant $c > 0$ there exists n_0 such that $\gamma(n) > c\lambda(n)$ for all $n \ge n_0$.

Theorem 2. *Let $\gamma, \lambda : \mathbb{N} \to \mathbb{N}$ be functions such that γ outstrips λ and such that $m \log m \le \gamma(m) \le 2^m/m$ 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.*

The main tool in our proofs of Theorems 2 and 3 is the following concept.

Definition 6. 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.

We remark that the fraction $2^n/n$ in part 2(a) of the above definition is not tight; it could be made slightly larger or smaller, but $2^n/n$ is a convenient choice that suffices for our needs.

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. *If $\gamma : \mathbb{N} \to \mathbb{N}$ satisfies $\gamma(m) \le 2^m/m$ for all m, then γ-discrimination is a nearly-linear-natural property with density $\Omega(2^{-\psi(\log n,\, \gamma(\log n))})$. If γ is time-constructible then γ-discrimination is a* uniformly *nearly-linear-natural property.*

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 $\gamma(m) \leq 2^m/m$, 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. In the non-uniform case, counting the number of 1's can be done using N additions and one comparison of n-bit numbers, which can be done using $O(N \log N)$ gates. Also, for each n, the set of truth table entries that must be 0 is fixed, so in a non-uniform model of computation, this condition can be checked using a number of gates that is proportional to the number of forced 0's, and this is certainly $O(N \log N)$ (even $O(N)$).

In a uniform model of computation, counting 1's clearly takes nearly linear time, 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. If γ is time-constructible then computing $\gamma(m)$ takes time $O(2^m)$, so evaluating γ at $m = \log\log N$ takes time at most polylogarithmic in N. The total number of circuits we must enumerate 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

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

using standard estimates (large deviations, Stirling's formula). This means that for some constant c, the number of γ-discriminating functions is at least

$$\begin{aligned}&2^{2^n - \psi(m,\, \gamma(m))} - 2^{c(2^n \log n)/n} \\ &\quad = 2^{2^n} 2^{-\psi(m,\, \gamma(m))}(1 - 2^{c(2^n \log n)/n - 2^n + \psi(m,\, \gamma(m))}).\end{aligned}$$

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 can now prove Theorem 2.

Proof of Theorem 2. 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 (M_n^γ) 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, $\gamma(\log m) \geq \log m \log\log m$, and it is easy to see that there are more than m distinct Boolean functions computable with $\log m \log\log m$ gates and $\log m$ inputs, so the density of (C_m) is $\Omega(2^{-\psi(\log m,\, \gamma(\log m))})$. By condition 2(b), 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 γ outstrips λ. In other words, (C_m) is quasi-useful (in fact, useful) against Λ. Therefore, by our reductio hypothesis, $(C_m) \notin \Gamma$. 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 $n \log n \leq \gamma(n) \leq 2^n/n$, Lemma 1 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. □

Now for our main result.

Theorem 3. *Assume that, for some $\epsilon > 0$, 2^{n^ϵ}-hard pseudorandom number generators exist. Let γ be any superpolynomial, subexponential, time-constructible function. Then γ-discrimination is a (uniformly) nearly-linear-natural property of density $\Omega(2^{-\psi(\log n,\, \gamma(\log n))})$ separating NP from $P/poly$.*

Proof. We know from Lemma 1 that γ-discrimination is nearly-linear-natural with density $\Omega(2^{-\psi(\log n,\, \gamma(\log n))})$. To see that γ-discrimination is quasi-useful against $P/poly$, we argue as in the proof of Theorem 2: Given $f_n \in M_n^\gamma$, we define the property (C_m) by letting a function with truth table x be in C_m if and only if $f_{2^m}(x) = 1$. Because γ is superpolynomial, (C_m) is useful[3] against $P/poly$. Also C_m has density $\Omega(2^{-m})$, which is large enough for Razborov and Rudich's result to apply. That is, since we have assumed that 2^{n^ϵ}-hard pseudorandom number generators exist, we can conclude that (C_m) cannot be $P/poly$-constructive. Therefore $(f_n) \notin P/poly$, so 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 by condition 2(b)

[3]Here we need usefulness and not merely quasi-usefulness, since we want to quote the Razborov–Rudich result.

and that are 1 otherwise. Then (f_n) is in NP, in the sense that the language L defined by

$$x \in L \iff f_n(x) = 0$$

is in NP.[4] 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 in n, the size of x, since γ is subexponential. □

Note that the density of γ-discrimination is less than $2^{-q(n)}$ for every quasi-polynomial q, because γ is superpolynomial and therefore $\log \psi(\log n,\, \gamma(\log n))$ is not quite polylogarithmic. However, if we choose γ to be a slowly growing superpolynomial function, then the density is not much less than $2^{-q(n)}$ for quasi-polynomial q. For example, if γ is quasi-polynomial then the density is $2^{-Q(n)}$ where

$$Q(n) = \exp\exp poly(\log\log n).$$

4. Theorem 2 improved

In this section we present a simple counting argument that improves the bound in Theorem 2.

Theorem 4. *Let $\gamma, \lambda : \mathbb{N} \to \mathbb{N}$ be functions such that γ outstrips λ and such that $\gamma(n) \le 2^n/n$ for all n. Let $\Lambda = SIZE(\lambda)$. Then there exists a non-uniformly nearly-linear-natural property with density $1/\psi(n,\, \gamma(n))$ that is useful against Λ.*

Proof. We give a sketch; complete details will appear in the full version of this paper.

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 $2^{2^n}/\psi(n,\, \gamma(n))$ 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^{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 $2^{2^n}/\psi(n,\, \gamma(n))$ around f_n that is disjoint from G_n. Then since γ outstrips λ, (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 non-uniformly in nearly-linear time. □

It would be interesting to know if the density bound in Theorem 3 can also be improved.

[4] Some authors might prefer to say that (f_n) is in co-NP, but since we could have chosen to interchange the roles of 0 and 1 in the definition of γ-discrimination, this distinction is of no importance.

5. Final remarks

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 [2].

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.

Finally, it is 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 [1] and Lachish and Raz [3], 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.

6. Acknowledgments

I would like to thank Bob Beals, Steve Boyack, Sandy Kutin, and Avi Wigderson for helpful discussions.

References

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

[2] Valentine Kabanets and Jin-Yi Cai, Circuit minimization problem, *Proc. Symp. Theory Comput.* 2000, 73–79.

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

[4] Alexander A. Razborov and Steven Rudich. Natural proofs, *J. Comput. Sys. Sci.* 55:24–35, 1997.

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

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

[7] Ingo Wegener, *The Complexity of Boolean Functions*, Wiley, 1987.