Poly-logarithmic independence fools AC^0 circuits

Mark Braverman
Microsoft Research New England

January 21, 2009

Abstract

We prove that poly-sized AC^0 circuits cannot distinguish a poly-logarithmically independent distribution from the uniform one. This settles the 1990 conjecture by Linial and Nisan [LN90]. The only prior progress on the problem was by Bazzi [Baz07, Baz09], who showed that $O(\log^2 n)$-independent distributions fool poly-size DNF formulas. Razborov [Raz08] has later given a much simpler proof for Bazzi's theorem.

1 Introduction

1.1 The problem

The main problem we consider is on the power of r-independence to fool AC^0 circuits. For a distribution μ on the finite support $\{0,1\}^n$, we denote by $\mathbf{E}_\mu[F]$ the expected value of F on inputs drawn according to μ. For an event X, we denote by $\mu[X]$ its probability under μ. When the distribution under consideration is the uniform distribution on $\{0,1\}^n$, we suppress the subscript and let $\mathbf{E}[F]$ denote the expected value of F, and $\mathbf{P}[X]$ the probability of X. A distribution μ is said to *ε-fool* a function F if

$$|\mathbf{E}_\mu[F] - \mathbf{E}[F]| < \varepsilon.$$

The distribution μ on $\{0,1\}^n$ is r-independent if every restriction of μ to r coordinates is uniform on $\{0,1\}^r$. AC^0 circuits are circuits with AND, OR and NOT gates, where the fan-in of the gates is unbounded. The depth of a circuit C is the maximum number of AND/OR gates between an input of C and its output. The problem we study is

Main Problem. *How large does $r = r(m,d,\varepsilon)$ has to be in order for every r-independent distribution μ on $\{0,1\}^n$ to ε-fool every function F that is computed by a depth-d AC^0 circuit of size $\leq m$?*

The original conjecture by [LN90] was that for a constant ε, $r(m,d,\varepsilon) = (\log m)^{d-1}$ suffices. The conjecture with these parameters turned out to be false [LV96], but it remained open whether $r(m,d,\varepsilon) = (\log m)^{O(1)}$ for a constant d and ε.

Prior to our work, Bazzi [Baz07, Baz09], in a proof that was later simplified by Razborov [Raz08], showed that a poly-logarithmic r is sufficient for $d = 2$ (i.e. when the F's are DNF or CNF formulas):

Theorem 1. *[Baz07, Raz08] $r(m,2,\varepsilon)$-independence ε-fools depth-2 circuits, where*

$$r(m,2,\varepsilon) = O\left(\log^2 \frac{m}{\varepsilon}\right).$$

Our main result is that for any constant d, $r(m,d,\varepsilon)$ is poly-logarithmic in m/ε. This gives a huge class of distributions that look random to AC^0 circuits. For example, as in [Baz09], it implies that linear codes with poly-logarithmic seed length can be PRGs for AC^0.

1.2 Main results

We prove the following:

Main Theorem. *Let $s \geq \log m$ be any parameter. Let F be a boolean function computed by a circuit of depth d and size m. Let μ be an r-independent distribution where*

$$r \geq r(s,d) = 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)},$$

then

$$|\mathbf{E}_\mu[F] - \mathbf{E}[F]| < \varepsilon(s,d),$$

where $\varepsilon(s,d) = 0.82^s \cdot (15m)$.

In particular, by taking $s = 5 \log \frac{15m}{\varepsilon}$, we get the following:

Corollary 2. *$r(m,d,\varepsilon)$-independence ε-fools depth-d AC^0 circuits of size m, where*

$$r(m,d,\varepsilon) = 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot \left(5 \log \frac{15m}{\varepsilon}\right)^{d(d+3)} = \left(\log \frac{m}{\varepsilon}\right)^{O(d^2)}.$$

Note that by choosing $\varepsilon = 2^{-n^\delta}$ for a small $\delta = \delta(d)$, one sees that polynomial independence fools AC^0 circuits up to an exponentially small error. The results carry some meaning for super-constant d's up to $d = \tilde{O}(\sqrt{\log m})$.

As in [Baz09], we can use [AGM02] to show that almost r-independent distributions also fool AC^0. A distribution μ is called a (δ, r)-approximation, if μ is δ-close to uniform for every r (distinct) coordinates. Thus an r-independent distribution is a $(0,r)$-approximation. We use the following theorem.

Theorem 3. [AGM02] *Let μ be a (δ,r)-approximation over n variables. Then μ is $n^r \cdot \delta$-close to an r-independent distribution μ'.*

Theorem 3 and the Main Theorem immediately imply:

Corollary 4. *For every boolean circuit F of depth d and size m over n variables and any $s \geq \log m$, let*

$$r \geq r(s,d) = 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)}.$$

Then for any (δ, r)-approximation μ,

$$|\mathbf{E}_\mu[F] - \mathbf{E}[F]| < \varepsilon(s,d) + n^r \cdot \delta = 0.82^s \cdot (15m) + n^r \cdot \delta.$$

Corollary 4 in turn implies:

Corollary 5. *$(\delta, r(m,d,\varepsilon))$-approximations ε-fool depth-d AC^0 circuits of size m, where*

$$r(m,d,\varepsilon) = 4 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot \left(5 \log \frac{15m}{\varepsilon}\right)^{d(d+3)},$$

as long as δ is sufficiently small so that

$$\frac{\varepsilon}{\delta} > 2n^{r(m,d,\varepsilon)}.$$

1.3 Techniques and proof outline

As in [Baz09], our strategy is to approximate F with low degree polynomials over $\mathbb{R}$. The reason being that degree r-polynomials are completely fooled by r-independence.

Proposition 6. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a degree-r polynomial, and let μ be an r-independent distribution. Then f is completely fooled by μ:*

$$\mathbf{E}_\mu[f] = \mathbf{E}[f].$$

Proposition 6 is true since every term of f is a product of $\leq r$ variables, whose distribution is uniform under μ.

In our construction we combine two types of approximations of AC^0 circuits by low degree polynomials over $\mathbb{R}$. The first one is combinatorial in the spirit of [Raz87, Smo87, BRS91, Tar93] (for a comprehensive survey on polynomials in circuit complexity see e.g. [Bei93]). These approximating polynomials agree with F on all but a small fraction of inputs. Thus for such a polynomial f, $\mathbf{P}[f = F]$ is very close to 1. While essentially using the same construction as [BRS91, Tar93], utilizing tools from [VV85], we repeat the construction from scratch in Lemma 9, since we want to reason about details of the construction. We believe that any construction in this spirit would fit in our proof.

The second approximation is based on Fourier analysis and uses [LMN93] where it is shown that any AC^0 function G can be approximated by a low degree polynomial g so that the ℓ_2 norm $\|G - g\|_2^2$ is small. There is no guarantee, however, that g agrees with G on any input (most likely, it doesn't).

We use an approximation f of F of the first type as the starting point of our construction. Thus $\mathbf{P}[f \neq F]$ is very small. If we knew that $\|F-f\|_2^2$ is small we would be done by a simple argument similar to one that appeared in [Baz09]. Unfortunately, there are no guarantees that f is close to F *on average*, since f may deviate wildly on points where $f \neq F$ (in fact, it is likely untrue that $\|F - f\|_2^2$ is small).

Our key insight is that in the construction of f, the indicator function $\mathcal{E}$ of where f fails to agree with F is an AC^0 function itself. Thus $\mathcal{E} = 1$ whenever $f \neq F$, and $\mathbf{P}[\mathcal{E} = 1]$ is very small (since $f = F$ most of the time). We then use a low-degree approximation $\tilde{\mathcal{E}}$ of $\mathcal{E}$ of the second type so that $\|\tilde{\mathcal{E}} - \mathcal{E}\|_2^2$ is very small. We then take $f' := f \cdot (1 - \tilde{\mathcal{E}})$. The idea is that $1 - \tilde{\mathcal{E}} \approx 1 - \mathcal{E}$ will kill the values of f where it misbehaves (and thus $\mathcal{E} = 1$), while leaving other values (where $\mathcal{E} = 0$) almost unchanged. Note that the values where $f = 0$ remain completely unchanged, and thus f' is a semi-exact approximation of F. In Lemma 11 we show that $\|F - f'\|_2^2$ is small. We choose f' to "almost agree" with F against both the uniform distribution and the distribution μ, a property we use to finish the proof.

It should be noted that while an inductive proof on the depth d of F is a natural approach to the problem, a non-inductive construction appears to yield much better parameters for the theorem.

1.4 Paper organization

The rest of the paper is organized as follows. In Section 2 we repeat the [LMN93] theorem on low-degree ℓ_2-approximation and state an additional simple property that we need in the proof. In Section 3 we develop low-degree approximation tools that are used in the proof of the main theorem. In Section 4 we prove the main theorem.

Acknowledgments

I am grateful to Louay Bazzi, Marek Karpinski, and Alex Samorodnitsky for stimulating discussions at the early stages of this work. I would like to thank Nina Balcan, Henry Cohn, Nick Harvey, Toni Pitassi, and Madhu Sudan for the many useful comments on the earlier versions of this manuscript.

2 ℓ_2-approximations by low-degree polynomials

We will make use of the [LMN93] bound:

Lemma 7. *([LMN93]) If $F : \{0,1\}^n \to \{0,1\}$ is a boolean function computable by a depth-d circuit of size m, then for every t there is a degree t polynomial $\tilde{f}$ with*

$$\|F - \tilde{f}\|_2^2 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |F(x) - \tilde{f}(x)|^2 \leq 2m \cdot 2^{-t^{1/d}/20}.$$

Specifically, $\tilde{f}$ is obtained as follows. Let $G : \{-1,+1\}^n \to \{-1,+1\}$ be the function corresponding to F:

$$G(x_1,\ldots,x_n) := 2F((x_1+1)/2,\ldots,(x_n+1)/2) - 1.$$

Let $\tilde{g}$ be the polynomial obtained by taking the Fourier coefficients of degree up to t of G. Then

$$\tilde{f}(x_1,\ldots,x_n) := (\tilde{g}(2x_1-1,\ldots,2x_n-1)+1)/2.$$

We make the following simple proposition:

Proposition 8. *For $m > 1$,*

$$\|\tilde{f}\|_\infty < m^t = m^{deg(\tilde{f})}.$$

Proof. Since all the Fourier coefficients $\hat{G}_S$ of G are bounded by the (trivial) bound of 1, and $n \le m$,

$$\|\tilde{f}\|_\infty < \|\tilde{g}\|_\infty \le \sum_{|S|\le t} |\hat{G}_S| < \#\{S \subset \{1,\ldots,n\},\ |S| \le t\} < n^t \le m^t.$$

□

3 Semi-exact approximations and error functions

In this section we prove the following lemma:

Lemma 9. *Let ν be any probability distribution on $\{0,1\}^n$. For a circuit of depth d and size m computing a function F, for any s, there is a degree $r = (s \cdot \log m)^d$ polynomial f and a depth $< d+3$ boolean function $\mathcal{E}_\nu$ of size $O(m^2 r)$ such that*

- *$\nu[\mathcal{E}_\nu(x) = 1] < 0.82^s m$, and*
- *whenever $\mathcal{E}_\nu(x) = 0$, $f(x) = F(x)$.*

Thus $\mathcal{E}_\nu$ tells us whether there is a mistake in f, and the weight of the mistakes as measured by ν is very small. Note that when there is a mistake, f does not have to be equal to $1 - F$, and can actually be quite large in absolute value.

Proof. We construct the polynomial f by induction on d, and show that w.h.p. $f = F$. The function $\mathcal{E}_\nu$ follows from the construction.

We will show how to make a step with an AND gate. Since the whole construction is symmetric with respect to 0 and 1, the step also holds for an OR gate. Let

$$F = G_1 \wedge G_2 \wedge \ldots \wedge G_k,$$

where $k < m$. For convenience, let us assume that $k = 2^\ell$ is a power of 2. We take a collection of $t := s\ell$ random Poisson subsets of $\{1,2,\ldots,k\}$: s of each of the $p = 2^{-1}, 2^{-2}, \ldots, 2^{-\ell} =$

$1/k$: $S_1, \ldots, S_t$ – we ignore empty sets. In addition, we make sure to include $\{1, \ldots, k\}$ as one of the sets. Let $g_1, \ldots, g_k$ be the approximating polynomials for $G_1, \ldots, G_k$. We set

$$f := \prod_{i=1}^{t} \left(\sum_{j \in S_i} g_j - |S_i| + 1 \right).$$

By the induction assumption, the degrees of g_j are $d' \leq (s \cdot \log m)^{d-1}$, hence the degree of f is bounded by $t \cdot d' \leq (s \cdot \log m)^d$. Next we bound the error $\mathbf{P}[f \neq F]$. It consists of two terms:

$$\nu[f \neq F] \leq \nu[g_j \neq G_j \text{ for some } j] + \nu \left[\prod_{i=1}^{t} \left(\sum_{j \in S_i} G_j - |S_i| + 1 \right) \neq \prod_{j=1}^{k} G_j \right]. \tag{1}$$

In other words, to make a mistake, either one of the inputs has to be dirty, or the approximating function for the AND has to make a mistake. We will focus on the second term. The first term is bounded by union bound. We fix a vector of specific values $G_1(x), \ldots, G_k(x)$, and calculate the probability of an error over the possible choices of the random sets S_i.

Note that if all the $G_j(x)$'s are 1 then the value of $F(x) = 1$ is calculated correctly with probability 1. Suppose that $F(x) = 0$ (and thus at least one of the $G_j(x)$'s is 0). Let $1 \leq z \leq k$ be the number of zeros among $G_1(x), \ldots, G_k(x)$. And α be such that $2^\alpha \leq z < 2^{\alpha+1}$. Let S be a random Poisson set with $p = 2^{-\alpha-1}$. Our formula will work correctly if S hits exactly one 0 among the z zeros of $G_1(x), \ldots, G_k(x)$. The probability of this event is exactly

$$z \cdot p \cdot (1-p)^{z-1} \geq \frac{1}{2} \cdot (1-p)^{1/p-1} > \frac{1}{2e} > 0.18.$$

Hence the probability of being wrong after s such sets is bounded by 0.82^s. Since this is true for any value of x, we can find a collection of sets S_i such that the probability of error is at most 0.82^s. By making the same probabilistic argument at every node, we get an error of $< 0.82^s m$ by union bound.

Finally, if we know the sets S_i at every node, it is easy to check whether there is a mistake by checking that no set contains exactly one 0, thus yielding the depth $< (d+3)$ function $\mathcal{E}_\nu$. □

In addition, we have:

Proposition 10. *In Lemma 9,* $\|f\|_\infty < (2m)^{deg(f)-2} = (2m)^{t^d-2}$.

Proof. We prove the statement by induction on d. For $d = 1$, $deg(f) = t$ and the functions g_j are just 0/1-valued literals. Since $|S_i| \leq m$ for all i, we have for every x:

$$|f(x)| = \prod_{i=1}^{t} \left| \sum_{j \in S_i} g_j - |S_i| + 1 \right| \leq m^t < (2m)^{t-2}.$$

For the step, assuming the statement is true for $d-1 \geq 1$, we have

$$\|f\|_\infty \leq \prod_{i=1}^{t} \left| \sum_{j \in S_i} \|g_j\|_\infty + |S_i| - 1 \right| <$$

$$\prod_{i=1}^{t} \left| m \cdot (2m)^{t^{d-1}-2} + m \right| < \left((2m)^{t^{d-1}-1} \right)^t < (2m)^{t^d-2}.$$

□

Applying results from [LMN93] we can now take any shallow function F, modify it a little bit, so that the modified function would have a good one-sided-error approximation:

Lemma 11. *Let F be computed by a circuit of depth d and size m. Let s_1, s_2 be two parameters. Let μ be any probability distribution on $\{0,1\}^n$. Set*

$$\nu := \frac{1}{2}(\mu + U_{\{0,1\}^n}).$$

Let $\mathcal{E}_\nu$ be the function from Lemma 9 with $s = s_1$. Set $F' = F \vee \mathcal{E}_\nu$. Then there is a polynomial f' of degree $r_f \leq (s_1 \cdot \log m)^d + s_2$, such that

- $\mathbf{P}[F \neq F'] < 2 \cdot 0.82^{s_1} m$;
- $\mu[F \neq F'] < 2 \cdot 0.82^{s_1} m$;
- $\|F' - f'\|_2^2 < 0.82^{s_1} \cdot (4m) + 2^{2.9(s_1 \cdot \log m)^d \log m - s_2^{1/(d+3)}/20}$, *and*
- $f'(x) = 0$ *whenever* $F'(x) = 0$.

Proof. The first two properties follow from Lemma 9 directly, since

$$\mathbf{P}[\mathcal{E}_\nu = 1], \mu[\mathcal{E}_\nu = 1] \leq 2 \cdot \nu[\mathcal{E}_\nu = 1] < 2 \cdot 0.82^{s_1} m.$$

Let f be the approximating polynomial for F from that lemma, so that $F = F' = f$ whenever $\mathcal{E}_\nu = 0$, and thus $f = 0$ whenever $F' = 0$. By Proposition 10 we have

$$\|f\|_\infty < (2m)^{(s_1 \cdot \log m)^d} < 2^{1.4(s_1 \cdot \log m)^d \log m}.$$

We let $\tilde{\mathcal{E}}_\nu$ be the low degree approximation of $\mathcal{E}_\nu$ of degree s_2. By [LMN93] (Lemma 7), we have

$$\|\mathcal{E}_\nu - \tilde{\mathcal{E}}_\nu\|_2^2 < O(m^3) \cdot 2^{-s_2^{1/(d+3)}/20}.$$

Let

$$f' := f \cdot (1 - \tilde{\mathcal{E}}_\nu).$$

Then $f' = 0$ whenever $F' = 0$. It remains to estimate $\|F' - f\|_2^2$.

$$\|F' - f'\|_2^2 \leq 2 \cdot \|F' - f \cdot (1 - \mathcal{E}_\nu)\|_2^2 + 2 \cdot \|f \cdot (1 - \mathcal{E}_\nu) - f'\|_2^2 = 2 \cdot \|\mathcal{E}_\nu\|_2^2 + 2 \cdot \|f \cdot (\mathcal{E}_\nu - \tilde{\mathcal{E}}_\nu)\|_2^2 \leq$$

$$2 \cdot \mathbf{P}[\mathcal{E}_\nu = 1] + 2 \cdot \|f\|_\infty^2 \cdot \|\mathcal{E}_\nu - \tilde{\mathcal{E}}_\nu\|_2^2 < 0.82^{s_1}(4m) + 2^{2.9(s_1 \cdot \log m)^d \log m - s_2^{1/(d+3)}/20},$$

which completes the proof. □

4 Main Theorem

Lemma 11 implies the following:

Lemma 12. *For every boolean circuit F of depth d and size m and any $s \geq \log m$, and for any probability distribution μ on $\{0,1\}$ there is a boolean function F' and a polynomial f'_l of degree less than*

$$r_f = 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)}$$

such that

- $\mu[F \neq F'] < \varepsilon(s,d)/3$,
- $\mathbf{P}[F \neq F'] < \varepsilon(s,d)/3$,
- $f'_l \leq F'$ *on* $\{0,1\}^n$, *and*
- $\mathbf{E}[F' - f'_l] < \varepsilon(s,d)/3$,

where $\varepsilon(s,d) = 0.82^s \cdot (15m)$.

Proof. Let F' be the boolean function and let f' be the polynomial from Lemma 11 with $s_1 = s$ and $s_2 \approx 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)}$. The first two properties follow directly from the lemma. Set

$$f'_l := 1 - (1 - f')^2.$$

It is clear that $f'_l \leq 1$ and moreover $f'_l = 0$ whenever $F' = 0$, hence $f'_l \leq F'$. Finally, $F'(x) - f'_l(x) = 0$ when $F'(x) = 0$, and is equal to

$$F'(x) - f'_l(x) = (1 - f'(x))^2 = (F'(x) - f'(x))^2$$

when $F'(x) = 1$, thus

$$\mathbf{E}[F' - f'_l] \leq \|F' - f'\|_2^2 < 0.82^s \cdot (5m) = \varepsilon(s,d)/3,$$

by Lemma 11. To finish the proof we note that the degree of f'_l is bounded by

$$2 \cdot ((s_1 \cdot \log m)^d + s_2) < 2.5 \cdot s_2 < r_f.$$

□

Lemma 12 implies the following:

Lemma 13. *Let $s \geq \log m$ be any parameter. Let F be a boolean function computed by a circuit of depth d and size m. Let μ be an r-independent distribution where*

$$r \geq 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)},$$

then

$$\mathbf{E}_\mu[F] > \mathbf{E}[F] - \varepsilon(s,d),$$

where $\varepsilon(s,d) = 0.82^s \cdot (15m)$.

Proof. Let F' be the boolean function and let f'_l be the polynomial from Lemma 12. The degree of f is $< r$. We use the fact that since μ is r-independent, $\mathbf{E}_\mu[f'_l] = \mathbf{E}[f'_l]$ (see Proposition 6 above):

$$\begin{aligned}\mathbf{E}_\mu[F] \geq \mathbf{E}_\mu[F'] - \mu[F \neq F'] \geq \mathbf{E}_\mu[f'_l] - \varepsilon(s,d)/3 = \mathbf{E}[f'_l] - \varepsilon(s,d)/3 = \\ \mathbf{E}[F'] - \mathbf{E}[F' - f'_l] - \varepsilon(s,d)/3 > \mathbf{E}[F'] - 2\varepsilon(s,d)/3 \geq \\ \mathbf{E}[F] - \mathbf{P}[F' \neq F] - 2\varepsilon(s,d)/3 > \mathbf{E}[F] - \varepsilon(s,d).\end{aligned}$$

□

The dual inequality to Lemma 13 follows immediately by applying the lemma to the negation $\overline{F} = 1 - F$ of F. We have $\mathbf{E}_\mu[\overline{F}] > \mathbf{E}[\overline{F}] - \varepsilon(s,d)$, and thus

$$\mathbf{E}_\mu[F] = 1 - \mathbf{E}_\mu[\overline{F}] < 1 - \mathbf{E}[\overline{F}] + \varepsilon(s,d) = \mathbf{E}[F] + \varepsilon(s,d).$$

Together, these two statements yield the main theorem:

Main Theorem. *Let $s \geq \log m$ be any parameter. Let F be a boolean function computed by a circuit of depth d and size m. Let μ be an r-independent distribution where*

$$r \geq r(s,d) = 3 \cdot 60^{d+3} \cdot (\log m)^{(d+1)(d+3)} \cdot s^{d(d+3)},$$

then

$$|\mathbf{E}_\mu[F] - \mathbf{E}[F]| < \varepsilon(s,d),$$

where $\varepsilon(s,d) = 0.82^s \cdot (15m)$.

References

[AGM02] N. Alon, O. Goldreich, and Y. Mansour, *Almost k-wise independence versus k-wise independence*, Electronic Colloquium on Computational Complexity. Report TR02-048, 2002.

[Baz07] L. M. J. Bazzi, *Polylogarithmic independence can fool DNF formulas*, Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07), IEEE Computer Society Washington, DC, USA, 2007, pp. 63–73.

[Baz09] ———, *Polylogarithmic independence can fool DNF formulas*, SIAM Journal on Computing (SICOMP) (2009), to appear.

[Bei93] R. Beigel, *The polynomial method in circuit complexity*, Proceedings of the 8th IEEE Structure in Complexity Theory Conference, 1993, pp. 82–95.

[BRS91] R. Beigel, N. Reingold, and D. Spielman, *The perceptron strikes back*, Proceedings of the Sixth Annual Structure in Complexity Theory Conference, 1991, pp. 286–291.

[LMN93] N. Linial, Y. Mansour, and N. Nisan, *Constant depth circuits, Fourier transform, and learnability*, Journal of the ACM (JACM) **40** (1993), no. 3, 607–620.

[LN90] N. Linial and N. Nisan, *Approximate inclusion-exclusion*, Combinatorica **10** (1990), no. 4, 349–365.

[LV96] M. Luby and B. Veličković, *On deterministic approximation of DNF*, Algorithmica **16** (1996), no. 4, 415–433.

[Raz87] A. A. Razborov, *Lower bounds on the size of bounded-depth networks over a complete basis with logical addition*, Math. Notes Acad. Sci. USSR **41** (1987), no. 4, 333–338.

[Raz08] ———, *A simple proof of Bazzi's theorem*, Electronic Colloquium on Computational Complexity. Report TR08-081, 2008.

[Smo87] R. Smolensky, *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, Proceedings of the nineteenth annual ACM Symposium on Theory of Computing (STOC'87), ACM New York, NY, USA, 1987, pp. 77–82.

[Tar93] J. Tarui, *Probabilistic polynomials, AC^0 functions and the polynomial-time hierarchy*, Theoretical computer science **113** (1993), no. 1, 167–183.

[VV85] L. G. Valiant and V. V. Vazirani, *NP is as easy as detecting unique solutions*, Proceedings of the seventeenth annual ACM Symposium on Theory of Computing (STOC'85), ACM New York, NY, USA, 1985, pp. 458–463.