Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 134 (2012)

Real Advantage

Alexander Razborov* Emanuele Viola†

December 26, 2012

Abstract

We highlight the challenge of proving correlation bounds between boolean functions and integer-valued polynomials, where any non-boolean output counts against correlation.

We prove that integer-valued polynomials of degree $\frac{1}{2}\lg_2 \lg_2 n$ have correlation with parity at most zero. Such a result is false for modular and threshold polynomials. Its proof is based on a variant of an anti-concentration result by Costello, Tao, and Vu (Duke Math. J. 2006).

1 Introduction

The polynomial method has been one of the most successful tools in theoretical computer science. It has had many applications, for example, in complexity and learning theory. The surveys [Bei93, Vio09, She08] provide starting points to learn more about this method.

As is well-known, however, there are several problems about polynomials which have resisted decades of attacks. The purpose of this work is to highlight certain new basic problems about polynomials which appear to stand in the way of further progress, making some initial technical contributions along the way.

A challenge that we are interested in is that of proving correlation bounds. Specifically, for two functions $f, g : \{0,1\}^n \to R$, where R represents the set of real numbers, define their "correlation" to be the quantity:

$$\mathrm{Cor}_n(f,g) \stackrel{\text{def}}{=} \mathbf{P}_x[f(x) = g(x)] - 1/2,$$

where x is uniformly distributed over $\{0,1\}^n$.

Most of the research has so far concentrated on the case in which both f and g are boolean, and in order to incorporate into this framework arbitrary multivariate polynomials,

*University of Chicago, razborov@cs.uchicago.edu. Part of this work was done while the author was at Steklov Mathematical Institute, supported by the Russian Foundation for Basic Research, and at Toyota Technological Institute, Chicago

†Supported by NSF grant CCF-0845003. Email: viola@ccs.neu.edu

ISSN 1433-8092

one clearly has to convert them to boolean functions $b : \{0,1\}^n \to \{0,1\}$. Historically, there have been two prominent methods of doing this. The first applies to polynomials with integer coefficients and consists in declaring $b(x) = 1$ if $p(x)$ is divisible by a prescribed integer m, and 0 otherwise. We refer to these functions b as *modular polynomials*. The second declares $b(x) = 1$ if $p(x) > t$ for some prescribed threshold t, and 0 otherwise. (Here the involved polynomials may be also assumed to have integer coefficients without loss of generality [MTT61, Mur71].) We refer to these functions b as *threshold polynomials*.

It is an open problem to exhibit an explicit boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $\mathrm{Cor}_n(b, f) = o(1/\sqrt{n})$ for any modular polynomial b whose underlying polynomial has degree $\lg_2 n$, cf. [Vio09]. Interestingly, the same problem is open even for threshold polynomials.

These parallel developments make it very natural (and hopefully instructive) to consider the "universal", "umbrella" model of *real polynomials* where we just view the polynomial itself as computing a boolean function, and any output of the polynomial outside of $\{0,1\}$ is counted as an error. As it appears, this generic setting was considered before, but in a somewhat ad hoc way and mostly as a building block for other constructions (see e.g. [ABFR94, Section 5]). We are not aware of any previous attempts to study it independently, and, as a consequence, we are not aware of any lower bound techniques for real polynomials that are not derivative from modular or threshold case. In particular we highlight the following challenge:

Challenge 1.1. Exhibit an explicit boolean function $f : \{0,1\}^n \to \{0,1\}$ such that $\mathrm{Cor}_n(p, f) = o(1/\sqrt{n})$ for any real polynomial $p : \{0,1\}^n \to R$ of degree $\lg_2 n$.

Another motivation for considering real correlation in its unprocessed form comes from connections to matrix analysis. It is well-known that analogies between polynomial approximations and matrix approximations are extremely important and influential in Theory and other areas like Machine Learning (see e.g. [She08]). Viewed under this angle, our model is a straightforward analogy of matrix rigidity [Val77] (cf. [SV12]) that still remains one of the greatest unresolved mysteries in the modern Complexity Theory.

Note that the Parity function is a candidate for f in Challenge 1.1. We also note that solving Challenge 1.1 is a pre-requisite for solving the corresponding problem for threshold polynomials. Similarly, the special case of Challenge 1.1 when the polynomials have integer coefficients is a pre-requisite for solving the corresponding problem for modular polynomials.

We do not know how to address Challenge 1.1. However, we can prove that the correlation with parity is zero for low degrees.

Theorem 1.2. $\mathrm{Cor}_n(p, \mathrm{parity}) \leq 0$ for every large enough n and every real polynomial $p : \{0,1\}^n \to R$ of degree $\leq \frac{1}{2} \lg_2 \lg_2 n$.

Theorem 1.2 follows easily from an anti-concentration result which is presented in §3 and is our main technical contribution. The proof of Theorem 1.2 is at the end of §3.

We note that the "zero behavior" in Theorem 1.2 does not hold for the other models mentioned earlier. Specifically, for threshold polynomials it follows from the results [ABFR94] of Aspnes, Beigel, Furst, and Rudich that increasing degree always increases correlation

with parity. For modular polynomials when the modulus is $m = 3$, it follows from Green's result [Gre04] that quadratic polynomials have better correlation with parity than linear polynomials. Thus, Theorem 1.2 appears to be the first authentic lower bound in our model.

Theorem 1.2 also raises the problem of determining the smallest degree for which the correlation with parity becomes strictly positive. Using standard techniques we note an $O(\sqrt{n})$ upper bound on this degree. In fact, the bound applies to any symmetric function, i.e., a function whose value only depends on the Hamming weight of the input. The same result obviously holds for threshold polynomials. The proof does not immediately apply to polynomials modulo m, because the coefficients may have denominators divisible by m. But a similar result for modular polynomials is obtained in Theorem 7 in [Vio09].

Fact 1.3. Let $f : \{0,1\}^n \to R$ be a real-valued, symmetric function. There exists a real polynomial $p : \{0,1\}^n \to R$ of degree $O(\sqrt{n})$ such that $\mathrm{Cor}_n(p, f) \geq 0.99$.

Proof. We construct a polynomial that computes f exactly on inputs of Hamming weight $n/2-c\sqrt{n}, \ldots, n/2+c\sqrt{n}$. For a suitable constant c, this yields the result by, say, Chebyshev's bound.

Denote by $h(w)$ the value of f on inputs of Hamming weight w. By interpolation, we can compute h on inputs in the above range by a univariate polynomial $p(w)$ of degree $2c\sqrt{n}$. The desired multivariate polynomial is then $p(\sum_i x_i)$.■

2 Notation

We let $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$, and $[n]^{\leq k} \stackrel{\text{def}}{=} \{\, S \subseteq [n] \,|\, |S| \leq k \,\}$. In this paper, we are interested in real-valued functions $f : \{0,1\}^n \longrightarrow R$. Every such function has a unique representation as a *multi-linear* polynomial $p(x_1, \ldots, x_n) = \sum_{S \subseteq [n]} c_S x_S$, where $c_S \in R$ and we have introduced the natural abbreviation $x_S \stackrel{\text{def}}{=} \prod_{i \in S} x_i$. $\mathrm{Supp}(p) \stackrel{\text{def}}{=} \{\, S \subseteq [n] \,|\, c_S \neq 0 \,\}$ corresponds to the set of non-zero coefficients.

Unless specifically noted otherwise, all probabilities and expectations in this paper are calculated w.r.t. the uniform distribution.

3 An anti-concentration result

In [CTV06], Costello, Tao and Vu proved the following remarkable result.

Proposition 3.1. Let k be a fixed positive integer, and $p(x_1, \ldots, x_n) = \sum_{S \in [n]^{\leq k}} c_S x_S$ be a multi-linear polynomial of degree $\leq k$. Then for any real interval I of length 1 we have $\mathbf{P}[p \in I] \leq O(m^{-a_k})$, where

$$m \stackrel{\text{def}}{=} \frac{1}{n^{k-1}} |\, \{\, S \in [n]^{\leq k} \,|\, |c_S| \geq 1 \,\}\, | \tag{1}$$

and

$$a_k \stackrel{\text{def}}{=} 2^{-(k^2+k)/2}. \tag{2}$$

In this paper, we are mostly interested in the following corollary easily obtainable by an indefinite scaling of the original polynomial.

Corollary 3.2. Under the same assumptions as in Proposition 3.1, for every fixed $h \in R$ we have the bound

$$\mathbf{P}[p = h] \leq O(s^{-a_k}),$$

where a_k is again given by (2) and

$$s \stackrel{\text{def}}{=} \frac{1}{n^{k-1}} |\text{Supp}(p)|. \tag{3}$$

Unfortunately, however, the size of the support does not behave well with respect to restrictions and thus can be hardly used for our purposes.

We improve Corollary 3.2 by relaxing the density restriction to something more combinatorial, which makes our main technical contribution. Let us call the term x_S *significant* if $|S| = k$ (i.e., it has the highest possible degree) and $c_S \neq 0$. Choose a maximal possible set $\{x_{S_1}, \ldots, x_{S_r}\}$ of significant terms with *mutually disjoint sets of variables*. Then every term x_S with $c_S \neq 0$ either has degree $< k$ or contains at least one variable in common with one of the terms $x_{S_1}, \ldots, x_{S_r}$ which implies that $|\text{Supp}(p)| \leq kr \sum_{i=0}^{k-1} \binom{n}{i} \leq O(rn^{k-1})$. Thus, $r \geq \Omega(s)$ (as given by (3)) and we are going to prove that the existence of a large set of mutually disjoint significant terms is the *only* property necessary to derive the conclusion of Corollary 3.2. As a small by-product, we slightly improve their numerical bound.

Theorem 3.3. Let $p(x_1, \ldots, x_n) = \sum_{S \in [n]^{\leq k}} c_S x_S$ be a multi-linear polynomial of degree k, and assume that there exist r terms $x_{S_1}, \ldots, x_{S_r}$ of degree k each and with mutually disjoint sets of variables such that $c_{S_i} \neq 0$ $(1 \leq i \leq r)$. Then for any real h we have $\mathbf{P}[p = h] \leq O(r^{-b_k})$, where

$$b_k \stackrel{\text{def}}{=} (2k2^k)^{-1}. \tag{4}$$

Proof. We first condition (in the least advantageous way) on the values of all variables not appearing in the terms $x_{S_1}, \ldots, x_{S_r}$. Since these terms have maximal possible degree k, substitutions of other variables do not produce any effect on the coefficients $c_{S_1}, \ldots, c_{S_r}$. Thus, we may assume from the very beginning that our polynomial has precisely kr variables indexed by $S_1 \dot\cup \ldots \dot\cup S_r$. Renaming the variables, let, say

$$x_{S_j} = x_{1j} x_{2j} \ldots x_{kj},$$

where all variables x_{ij} $(i \in [k], j \in [r])$ are pairwise distinct.

Let us call a term t *cross-term* if it has degree k and, moreover, is of the form $x_{1j_1} \ldots x_{kj_k}$ for some function $j : [k] \longrightarrow [r]$. Cross-terms x_{S_j} themselves (i.e., those for which the function j is a constant) will be called *principal*. Our first task is to get rid of all terms that are not cross-terms (and this is where we suffer the enormous loss in the exponent in (4)); the proof is virtually identical to [CTV06] but we include it nonetheless for the sake of completeness.

Write $p = p(X_1, \ldots, X_k)$, where

$$X_i \stackrel{\text{def}}{=} \{ x_{ij} \mid j \in [r] \},$$

introduce an isomorphic set of variables $Y_1, \ldots, Y_k$ and form the alternating sum

$$\widehat{p}(X_1, \ldots, X_k, Y_1, \ldots, Y_k) \stackrel{\text{def}}{=} \sum_{a \in \{0,1\}^k} (-1)^{\sum_i a_i} p(W_1^{a_1}, \ldots, W_k^{a_k}), \tag{5}$$

where $W_i^a \stackrel{\text{def}}{=} \begin{cases} X_i & \text{if } a = 0 \\ Y_i & \text{if } a = 1. \end{cases}$

The Decoupling lemma [CTV06, Lemma 6.3] implies that

$$\mathbf{P}[p(X_1, \ldots, X_k) = h] \leq \mathbf{P}\left[\bigwedge_{a \in \{0,1\}^k} p(W_1^{a_1}, \ldots, W_k^{a_k}) = h \right]^{1/2^k} \leq \mathbf{P}[\widehat{p}(X_1, \ldots, X_k, Y_1, \ldots, Y_k) = 0]^{1/2^k}, \tag{6}$$

where $Y_1, \ldots, Y_k$ are picked from $\{0,1\}^r$ uniformly and independently of $X_1, \ldots, X_k$.

On the other hand, (5) defines a linear mapping from the space of multi-linear polynomials in kr variables, and on every term $t = t_1(X_1) \ldots t_k(X_k)$ it produces $(t_1(X_1) - t_1(Y_1))(t_2(X_2) - t_2(Y_2)) \ldots (t_k(X_k) - t_x(Y_k))$. Which implies that this mapping vanishes on all terms that are not cross-terms (as for them there exists an i such that $t_i = 1$), and on every cross-term the mapping acts simply as the substitution $x_{ij} \mapsto z_{ij} \stackrel{\text{def}}{=} x_{ij} - y_{ij}$. Thus,

$$\widehat{p}(X_1, \ldots, X_k, Y_1, \ldots, Y_k) = q(Z_1, \ldots, Z_k),$$

where q is the polynomial p from which we have erased all terms that are not cross-terms. Random variables z_{ij} are i.i.d, and for every individual variable z_{ij}, $\mathbf{P}[z_{ij} = 1] = \mathbf{P}[z_{ij} = -1] = 1/4$, and $\mathbf{P}[z_{ij} = 0] = 1/2$.

Definition 3.4. A polynomial $q(Z_1, \ldots, Z_k)$ (where $Z_j = \{z_{j1}, \ldots, z_{jr}\}$) is a (k, r)-*polynomial* if it is *multi-linear in* $Z_1, \ldots, Z_k$, meaning that every monomial appearing in q may contain at most one variable from each of these groups, and, moreover, the coefficient in front of all r principal terms is not zero.

It follows that a (k, r) polynomial has degree exactly k.

Note that q is a (k, r)-polynomial. Whereas q only contains terms of degree k, a (k, r) polynomial is allowed to have terms of smaller degree (we will need this for induction).

Claim 3.5. For any (k, r)-polynomial q, $\mathbf{P}[q(Z_1, \ldots, Z_k) = 0] \leq C_1 3^k r^{-1/(2k)}$, where $C_1 > 0$ is an absolute constant.

To complete the proof of Theorem 3.3, employ (6), and apply Claim 3.5 to our alternating sum $\widehat{p}(X_1, \ldots, X_k, Y_1, \ldots, Y_k) = q(Z_1, \ldots, Z_k)$.■

Proof of Claim 3.5. The proof is by induction on k.

Base case $k = 1$ follows from the Littlewood-Offord lemma [LO43, Erd45]. We state it here at the level of generality appropriate to our purposes.

Proposition 3.6 ([LO43, Erd45])**.** Let $z_1, \ldots, z_r$ be i.i.d. random variables such that $\mathbf{P}[z_i = 1] = \mathbf{P}[z_i = -1] = 1/4$, $\mathbf{P}[z_i = 0] = 1/2$. Let $c_1, \ldots, c_r$ be non-zero. Then for every real h,

$$\mathbf{P}[c_1 z_1 + \cdots + c_r z_r = h] \leq C_0/\sqrt{r},$$

for an universal constant C_0.

Strictly speaking, this result is stated in [Erd45] only for Rademacher (that is, $\{\pm 1\}$-valued) random variables, but since every z_i is a sum of two such variables, Proposition 3.6 follows.

Inductive step. Assume now that $k \geq 2$, and that Claim 3.5 is already established for $(k-1, r')$-polynomials, for arbitrary r'. Expand our (k, r)-polynomial q as

$$q(Z_1, \ldots, Z_k) = q_0(Z_1, \ldots, Z_k) + \sum_{j=1}^{r} z_{1j} z_{2j} \ldots z_{(k-1)j} R_j(Z_k),$$

where terms in $q_0(Z_1, \ldots, Z_k)$ are not divisible by any of $z_{1j} z_{2j} \ldots z_{(k-1)j}$, and

$$R_j(Z_k) = c_{j1} z_{k1} + \cdots + c_{jr} z_{kr} + c_j$$

is an affine form in the variables Z_k such that $c_{jj} \neq 0$.

What we need to prove for the inductive step is that after we assign $Z_k = \{z_{k1}, \ldots, z_{kr}\}$ at random (according to their distribution), then with high probability $R_j(Z_k) \neq 0$ for many j. Indeed, note that after we assign A_k to Z_k we obtain a multi-variate polynomial of degree $k-1$, and the coefficient of the j-th principal term is $R_j(A_k)$, because terms in q_0 cannot contribute to principal terms. Assigning further (in an arbitrary way) all those variables z_{ij} ($i \in [k-1]$) for which $R_j(A_k) = 0$, we arrive at $(k-1, r')$-polynomials, and we can apply the inductive assumption. This last assignment may give rise to terms of degree $< k-1$, and this is precisely why we had to forsake homogeneity in Definition 3.4.

Set

$$s \stackrel{\text{def}}{=} \frac{1}{20} r^{1/k},$$

and let us call the form R_j *large* if the number of indices $j' \in [r]$ such that $c_{jj'} \neq 0$ is $\geq s$, and *small* otherwise.

Case 1. *At least $r/2$ forms are large.* This case is analyzed similarly to [CTV06]. Assume w.l.o.g. that the large forms are $R_1, \ldots, R_{r/2}$. For every large form R_j, Proposition 3.6

implies that $\mathbf{P}[R_j(Z_k) = 0] \leq C_0 s^{-1/2}$. Picking at random $j \in_U [r/2]$, and applying Markov's inequality, we obtain

$$\mathbf{P}_{Z_k}\left[\mathbf{P}_{j\in_U[r/2]}[R_j(Z_k) = 0] \geq 1/2\right] \leq 2C_0 s^{-1/2}.$$

For every individual assignment A_k to the variables Z_k such that $\mathbf{P}_{j\in_U[r/2]}[R_j(A_k) = 0] < 1/2$ (followed by additionally assigning the variables z_{ij} with $i \in [k-1]$ and $R_j(A_k) = 0$) we are left with a $(k-1, r')$-polynomial for $r' \geq r/4$. Hence we have, by the inductive assumption:

$$\mathbf{P}[q(Z_1, \ldots, Z_k) = 0] \leq 2C_0 s^{-1/2} + C_1 3^{k-1}(r/4)^{-1/(2k-2)} \leq C_1 3^k r^{-1/(2k)},$$

as long as the constant C_1 is large enough relative to C_0. The last inequality uses that $(r/4)^{-1/(2k-2)} \leq 2r^{-1/(2k)}$ for $k \geq 2$.

Case 2. *At least $r/2$ forms are small.* Again, assume w.l.o.g. that the small forms are $R_1, \ldots, R_{r/2}$. Arrange coefficients $c_{jj'}$ $(j, j' \in [r/2])$ in the form of an $r/2 \times r/2$ square matrix C. Note the first row corresponds to the first small form, and every diagonal element c_{jj} of this matrix satisfies $c_{jj} \neq 0$.

The total number of non-zero entries in C is $\leq sr/2$. Hence, there are at most $r/4$ columns of C with more than $2s$ non-zero entries. So we have $\geq r/2 - r/4 = r/4$ columns with $\leq 2s$ non-zero entries. Let J be the corresponding indexes.

Now consider the following greedy procedure to select a subset $J' \subseteq J$ of these columns. While there are columns left, pick any column j. Exclude all other columns $j' \neq j$ such that $c_{jj'}$ or $c_{j'j}$ are non-zero. Note we exclude each time $\leq 2s + s = 3s$ columns. Hence we can guarantee $\geq (r/2)/(3s) \geq r/(6s)$ columns. Let J' be the corresponding indices; this set defines a principal diagonal sub-matrix with non-zero diagonal entries.

Fix in the least advantageous way any variable that does not correspond to one of these columns, i.e., z_{kj} for any $j \notin J'$.

We are left with $\geq r/(6s)$ forms R_j, $j \in J'$, whose values, over the choice of the remaining variables, are independent. Moreover, each form takes value 0 with probability $\leq 1/2$ (recall $1/2$ is the maximum probability that our variables take any value).

Applying Chernoff's bound, we have that

$$\mathbf{P}_{Z_k}\left[|\{j \in J' \mid \ R_j(Z_k) \neq 0\}| \leq \frac{r}{20s}\right] \leq 2^{-\epsilon r/s}$$

for a fixed constant $\epsilon > 0$, and in the good (i.e., when $|\{j \in J' \mid R_j(Z_k) \neq 0\}| \geq \frac{r}{20s}$) case we, as before, are left with a $(k-1, \frac{r}{20s})$-polynomial. Noting that $r/(20s) = r^{1-1/k}$ and that $r^{-(1-1/k)/(2k-2)} = r^{-1/(2k)}$, by inductive assumption we get

$$\mathbf{P}[q(Z_1, \ldots, Z_k) = 0] \leq 2^{-\epsilon r/s} + C_1 3^{k-1}\left(\frac{r}{20s}\right)^{-1/(2k-2)} \leq C_1 3^k r^{-1/(2k)},$$

again, provided the constant C_1 is large enough.

This completes the proof of Claim 3.5.■

Proof. [Of Theorem 1.2] Suppose the hypothesis of Theorem 3.3 is satisfied with $r = \sqrt{n}$. Then the probability that the polynomial outputs a boolean value is

$$O\left(1/\sqrt{n}^{1/(2k2^k)}\right) \leq 1/2$$

when $k \leq \frac{1}{2}\lg_2 \lg_2 n$. This proves the theorem.

Otherwise, we can cover all the degree-k terms by $\leq k\sqrt{n}$ variables. Fix these variables in the most disadvantageous way (this reduces the degree of the polynomial), and iterate.

After $\leq k$ iterations either the hypothesis of Theorem 3.3 is satisfied with $r = \sqrt{n}$, in which case we reason as above, or else we end up with a polynomial of degree 0 with $n - \sqrt{n}k^2 \geq 1$ variables, in which case the theorem is again true.∎

4 Open Questions

Even if our bound (4) provides a slight improvement over the original bound (2) from [CTV06], it still decays exponentially in k. It remains open whether this dependence can be made (inverse) linear or polynomial. Such an improvement would immediately give rise to better bounds in our main result, Theorem 1.2, although we believe that in order to attain the logarithmic bound from Challenge 1.1, some essentially new ideas will be needed. Nguyen and Vu [NV13] mildly conjecture that in Corollary 3.2 one can actually take $a_k = 1/2$, so that the only dependence on k will be hidden in the assumed multiplicative constant. While this conjecture may look a bit bold, let us note that its partial case $k = 2$ has been verified by Costello [Cos09].

The first version of our paper claimed the result analogous to Theorem 3.3 in the "small ball" version (when anti-concentration is measured w.r.t. a unit interval, and the principal coefficients c_{S_i} are known to satisfy $|c_{S_i}| \geq 1$), but the proof contained a gap. Thus, the question whether such a common generalization of Proposition 3.1 and Theorem 3.3 is possible also remains open.

References

[ABFR94] James Aspnes, Richard Beigel, Merrick Furst, and Steven Rudich. The expressive power of voting polynomials. *Combinatorica*, 14(2):135–148, 1994.

[Bei93] Richard Beigel. The polynomial method in circuit complexity. In *8th Structure in Complexity Theory Conference*, pages 82–95. IEEE, 1993.

[Cos09] Kevin P. Costello. Bilinear and quadratic variants on the Littlewood-Offord problem. `http://arxiv.org/abs/0902.1538`, to appear in *Israel Journal of Mathematics*, 2009.

[CTV06] Kevin P. Costello, Terence Tao, and Van Vu. Random symmetric matrices are almost surely nonsingular. *Duke Math. J.*, 135(2):395–413, 2006.

[Erd45] Paul Erdős. On a lemma of Littlewood and Offord. *Bull. Amer. Math. Soc.*, 51:898–902, 1945.

[Gre04] Frederic Green. The correlation between parity and quadratic polynomials mod 3. *J. of Computer and System Sciences*, 69(1):28–44, 2004.

[LO43] John Littlewood and Albert Offord. On the number of real roots of a random algebraic equation. *III. Rec. Math. [Mat. Sbornik] N.S.*, 12:277–286, 1943.

[MTT61] Saburo Muroga, Iwao Toda, and Satoru Takasu. Theory of majority decision elements. *J. Franklin Inst.*, 271:376–418, 1961.

[Mur71] Saburo Muroga. *Threshold logic and its applications*. Wiley-Interscience, New York, 1971.

[NV13] Hoi H. Nguyen and Van Vu. Small probability, inverse theorems, and applications. Manuscript prepared for the Erdös Centennial Conference, 2013.

[She08] Alexander A. Sherstov. Communication lower bounds using dual polynomials. *Bulletin of the EATCS*, 95:59–93, 2008.

[SV12] Rocco A. Servedio and Emanuele Viola. On a special case of rigidity. Available at http://www.ccs.neu.edu/home/viola/, 2012.

[Val77] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *6th Symposium on Mathematical Foundations of Computer Science*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977.

[Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de