Evasiveness Through A Circuit Lens

[Extended Abstract] *

Raghav Kulkarni
Centre for Quantum Technologies, Singapore
Singapore
kulraghav@gmail.com

ABSTRACT

A function $f : \{0,1\}^n \rightarrow \{0,1\}$ is called *evasive* if its decision tree complexity is maximal, i.e., $D(f) = n$. The long-standing Anderaa-Rosenberg-Karp (ARK) Conjecture asserts that every non-trivial monotone graph property is evasive. The Evasiveness Conjecture (EC) is a generalization of ARK Conjecture from monotone graph properties to arbitrary monotone transitive Boolean functions.

In this paper we study a weakening of the Evasiveness Conjecture called Weak Evasivenss Conjecture (weak-EC). The weak-EC asserts that every non-trivial monotone transitive Boolean function must have $D(f) \geq n^{1-\epsilon}$, for every $\epsilon > 0$. The purpose of this note is to make some remarks on weak-EC that hint towards a plausible attack on EC.

First we observe that weak-EC is equivalent to EC. Further we observe that ruling out only certain simple (monotone-NC^1) counter-examples to weak-EC suffices to confirm EC in its whole generality. Finally we rule out some simple counter-examples to weak-EC (AC^0 : unconditionally; and monotone-TC^0 : under a conjecture of Benjamini, Kalai, and Schramm on their noise stability).

We also investigate an analogue of weak-EC for the stronger model of *parity decision trees* and provide a counter-example to this seemingly stronger version under a conjecture of Montanaro and Osborne.

Categories and Subject Descriptors

F.2.0 [**Theory of Computation**]: ANALYSIS OF ALGORITHMS AND PROBLEM COMPLEXITY—*General*; F.1.3 [**Theory of Computation**]: COMPUTATION BY ABSTRACT DEVICES—*Complexity Measures and Classes*

General Terms

Algorithms, Theory

Keywords

Decision Tree Complexity, Evasiveness Conjecture, Monotone Graph Properties, Circuit Complexity

1. INTRODUCTION

The *decision tree model* aka *query model* [3], perhaps due to its simplicity and fundamental nature, has been extensively studied over decades; yet it remains far from being completely understood.

Fix a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$. A deterministic decision tree D_f for f takes $x = (x_1, \ldots, x_n)$ as an input and determines the value of $f(x_1, \ldots, x_n)$ using queries of the form " is $x_i = 1$? ". Let $C(D_f, x)$ denote the cost of the computation, that is the number of queries made by D_f on input x. The *deterministic decision tree complexity* of f is defined as $D(f) = \min_{D_f} \max_x C(D_f, x)$.

The function f is called *evasive* if $D(f) = n$, i.e., one must query all the variables in worst case in order to determine the value of the function.

1.1 The Anderaa-Rosenberg-Karp Conjecture

A natural theme in the study of decision tree complexity is to exploit the structure within f to prove strong lower bounds on its query complexity. A classic example is the following conjecture attributed to Anderaa, Rosenberg, and Karp, asserting the *evasiveness* of monotone graph properties:

Conjecture 1.1 (ARK Conjecture). *(cf. [6]) Every non-trivial monotone graph property is evasive.*

Since its origin around 1975, the ARK Conjecture has caught the imagination of generations of researchers resulting in beautiful mathematical ideas; yet - to this date - remains unsolved. A major breakthrough on ARK Conjecture was obtained by Kahn, Saks, and Sturvevant [6] via their novel *topological approach.* They settled the conjecture when the number of vertices of the graphs is a power of prime number. The topological approach subsequently turned out useful for solving some other variants and speccial cases of the conjecture. For example: Yao confirms the

*Research at the Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation. No qubits were harmed during the preparation of this article. At the time of submission of this article the author was at LIAFA Paris 7, partially supported by the French ANR Defis program under contract ANR-08- EMER-012 (QRAC project) and the European Commission IST STREP Project Quantum Computer Science (QSC) 25596.

ITCS'13, January 9–12, 2012, Berkeley, California, USA.

variant of the conjecture for monotone properties of bipartite graphs [19]. More recently, building on Chakraborty, Khot, and Shi's work [4], Babai et. al. [1] show that under some well-known conjectures in number theory, *forbidden subgraph* property - containment of a fixed subgraph in the graph - is evasive.

1.2 The Evasiveness Conjecture

The key feature of monotone graph properties is that they are sufficiently *symmetric*. In particular, they are *transitive* Boolean functions, i.e., there is a transitive group acting on the set of variables under which the function remains invariant. A natural question was raised: how much *symmetry* is necessary in order to guarantee the evasiveness? The following generalization (cf. [10]) of ARK Conjecture asserts that only transitivity suffices.

CONJECTURE 1.2 (EVASIVENESS CONJECTURE (EC)). *If f is a non-trivial monotone transitive Boolean function then f is evasive.*

The above conjecture is known to hold when the number of variables is a power of prime number [15]. The general case remains widely open.

1.3 The Weak Evasiveness Conjecture

'Whether or not one can save a single query?' might appear to some a bit obscure question as we are usually content with a loose bound on the complexity (say up to a constant or poly-logarithmic factor). The ARK Conjecture holds up to a constant factor [6] and one may raise the following:

CONJECTURE 1.3 (WEAK EVASIVENESS CONJECTURE). *If $\{f_n\}$ is a sequence of non-trivial monotone Boolean functions then for every $\epsilon > 0$*

$$D(f_n) \geq n^{1-\epsilon}.$$

The best known lower bond in this context is $D(f) \geq R(f) \geq n^{2/3}$, which follows from the work of O'Donell et. al. [14]. The purpose of this paper is to make some remarks on the weak-EC in connection with EC.

1.4 Our remarks on the Weak EC

Loosely speaking, we attempt to test the following hypothesis: *computationally simple* monotone transitive functions are *weakly evasive*. Our simple but crucial observation is that with an appropriate quantification of *computational simplicity* and of *weak evasiveness*, the above hypothesis becomes equivalent to the EC itself! Our main contribution is in formulating the above hypothesis in terms of circuit complexity and then verifying it partially. More concretely, we observe:

- The weak-EC is equivalent to the EC (Section 3).
- Furthermore, it suffices to prove weak-EC only for certain simple functions, namely monotone-NC^1 functions (Section 3).
- Finally, the weak-EC holds for AC^0 functions (Section 4); and for monotone-TC^0 functions (Section 5) assuming their noise-stability [2].

We note that the EC for AC^0 functions is widely open. The *forbidden subgraph* property is in AC^0 but it is only known to be evasive under some number theoretic conjectures [1].

2. PRELIMINARIES

Stronger variants of decision tree

A bounded error randomized decision tree R_f is a probability distribution over all deterministic decision trees such that for every input, the expected error of the algorithm is bounded by some fixed constant less than $1/2$. The cost $C(R_f, x)$ is the highest possible number of queries made by R_f on x, and the *bounded error randomized decision tree complexity* of f is $R(f) = \min_{R_f} \max_x C(R_f, x)$.

A *parity decision tree* may query " is $\sum_{i \in S} x_i \equiv 1 \pmod 2$? " for an arbitrary subset $S \subseteq [n]$. We call such queries *parity queries*. For a parity decision tree P_f for f, let $C(P_f, x)$ denote the number of parity queries made by P_f on input x. The *parity decision tree complexity* of f is

$$D_{\oplus}(f) = \min_{P_f} \max_x C(P_f, x).$$

Note that $D_{\oplus}(f) \leq D(f)$ as " is $x_i = 1$? " can be treated as a parity query.

Parity decision trees were introduced by Kushilevitz and Mansour [7] in the context of learning Boolean functions by estimating their Fourier coefficients. Recently they came in light in the study of the communication complexity of XOR functions [18].

Variance, influence, and average depth

Let μ_p denote the p-biased distribution on the Boolean cube, i.e., each co-ordinate is independently chosen to be 1 with probability p. The *variance* of a Boolean function is $\mathrm{Var}(f,p) := 4 \cdot \Pr_{x \leftarrow \mu_p}(f(x) = 0) \Pr_{x \leftarrow \mu_p}(f(x) = 1)$. The *influence* of the i^{th} variable under μ_p is $\mathrm{Inf}_i(f,p) := \Pr_{x \leftarrow \mu_p}(f(x) \neq f(x \oplus e_i))$. The *total influence* aka *average sensitivity* of f is $\mathrm{Inf}(f,p) := \sum_i \mathrm{Inf}_i(f,p)$.

Let $f : \{0,1\}^n \to \{0,1\}$. Let T_f be a deterministic decision tree for f. Let $d(T_f, x)$ denote the number of queries that T_f makes on input x. The average depth of T is $\Delta(T_f, p) := \mathbb{E}_{x \leftarrow \mu_p} d(T_f, x)$, and the average depth of f under μ_p is $\Delta(f,p) := \min_{T_f} \Delta(T_f, p)$.

Critical probability and threshold interval

We say that f is *balanced with repect to* μ_p if:

$$1 - 1/3 \leq \mathrm{Var}(f,p) \leq 1 + 1/3.$$

We call f *balanced* if f is balanced with respect to $\mu_{1/2}$. The *critical probability* of f is $p_c(f) := p$ such that $\mathrm{Var}(f,p) = 1$, i.e., $\Pr_{x \leftarrow \mu_p}(f(x) = 1) = 1/2$. If f is a monotone Boolean function then $p_c(f)$ is well-defined. Moreover, the critical probability can not be too small:

PROPOSITION 2.1. *If f is a non-trivial monotone Boolean function on n variables then*

$$p_c(f) = \Omega(1/n).$$

The threshold interval of f is $I := \{q \in [0,1] \mid 1 - 1/3 \leq \mathrm{Var}(f,q) \leq 1 + 1/3\}$. Let p be the critical probability of f. The threshold window of f, denoted by $t(f)$, is the largest real number such that $[p-t, p+t]$ is contained in the threshold interval of f.

The threshold window can not be too small either:

PROPOSITION 2.2. *If f is a non-trivial monotone Boolean function on n variables then:*

$$t(f) = \Omega(1/n).$$

Polynomial degree and sparsity

Let $f_\pm : \{-1,1\}^n \to \{-1,1\}$ be represented by the following polynomial with real coefficients: $f_\pm(z_1,\ldots,z_n) = \sum_{S\subseteq[n]} \widehat{f}(S)\prod_{i\in S} z_i$. The above polynomial is unique and it is called the Fourier expansion of f. The $\widehat{f}(S)$ are called the Fourier coefficients of f. The *polynomial degree* of f is $\deg(f) := max\{|S| \mid \widehat{f}(S) \neq 0\}$. The *sparsity* of a Boolean function f is $||\widehat{f}||_0 := |\{S \mid \widehat{f}(S) \neq 0\}|$. It is known that $\deg(f) \leq D(f)$ and $\log||\widehat{f}||_0 \leq D_\oplus(f)$.

3. EQUIVALENCE OF WEAK-EC AND EC

OBSERVATION 3.1. *Conjecture 1.2 is equivalent to Conjecture 1.3.*

Proof: Firstly Conjecture 1.2 ⇒ Conjecture 1.3 is obvious as the later is a weakening of the former.

Now we prove Conjecture 1.3 ⇒ Conjecture 1.2 by contrapositive.

Suppose there is a counter-example $g : \{0,1\}^T \to \{0,1\}$ to Conjecture 1.2 then one can construct a counter-example $\{f_n\}$ to Conjecture 1.3.

For $n = T^k$, construct g_k recursively from g.

$$g_1 := g,$$

$$g_k := g(g_{k-1},\ldots,g_{k-1}).$$

Note that g_k is a non-trivial monotone transitive function on $n = T^k$ variables. Moreover: $D(g_k) \leq (T-1)^k = T^{k\cdot(\log(T-1)/\log T)} = n^{\log(T-1)/\log T}$. The first inequality follows because $D(g(h,\ldots,h)) \leq D(g)\cdot D(h)$.

Let $1-\delta := \log(T-1)/\log T$. Since T is a constant $\delta > 0$ is a constant. We have $D(g_k) \leq n^{1-\delta}$ for a constant $\delta > 0$.

Now our counter-example $\{f_n\}$ to the Weak Evasiveness Conjecture would be as follows: if $n = T^k$ for some k then choose $f_n = g_k$; otherwise choose f_n to be (say) the OR function on n variables.

□

We note that the above construction fails to prove the equivalence of 'ARK and weak-ARK' as the recursive function no longer remains a graph property. However, the recursive construction still preserves the transitivity. A glance at the above proof also yields the following:

OBSERVATION 3.2. *If Conjecture 1.2 is false then there is a counter-example $\{f_n\}$ to Conjecture 1.3 such that $\{f_n\}$ is in monotone-NC^1.*

4. REFUTING AC^0 COUNTER-EXAMPLES TO WEAK-EC

The main ingredient of our proof is a well known inequality by O'Donell et. al. [14] that relates maximum influence to the average depth. The second ingredient that we use is another well known result by Linial, Mansour, and Nissan [9] that gives upper bound on the total influence of AC^0 functions (using the Switching Lemma). In order to make these two ingredients fit together in our context, we need (as a technicality) a simple but crucial transformation. Our transformation modifies a monotone Boolean function so that it becomes balanced with only constant increase in the depth. This allows us to derive a good (nearly linear) lower bound on the query complexity of balanced AC^0 functions. Then we infer the desired bound for non-balanced case via composition theorems for query complexity.

4.1 A transformation to balance the monotone functions

The idea is to *simulate* its critical probability by a monotone circuit and our crucial observation is that only a constant depth monotone circuit suffices. More specifically, we replace each variable of f by a read-once formula of depth 2 (OR of ANDs) that outputs 1 with probability sufficiently close to the critical probability of f so that the composed function is balanced.

Our construction works in two steps: first we make the function sufficiently unbalanced and then we balance the sufficiently unbalanced function.

Unbalancing the function only to help in balancing it later

Given a monotone Boolean function f on n variables we construct (A.1) another monotone Boolean function f_U on $N = n^3$ variables such that:

$$p_c(f_U) = O(\log N/N^{2/3}).$$

The function f_U is defined as follows:

$$f_U := f(g,\ldots,g),$$

where $g : \{0,1\}^{n^2} \to \{0,1\}$ is the OR function on n^2 variables:

$$g(y_1,\ldots,y_{n^2}) := \bigvee_{i=1}^{n^2} y_i.$$

Simulating the critical probability of unbalanced functions

Let f be a monotone Boolean function on n variables such that:

$$p_c(f) = o(1/\sqrt{n}).$$

We construct another balanced monotone Boolean function f_B as follows:

$$f_B := f(g,\ldots,g),$$

where

$$g((x_{ij})) := \bigvee_{i=1}^{m}\bigwedge_{j=1}^{k} x_{ij}$$

where $k = \lceil 3\log n\rceil$ and m is the integer minimizing $|p_c(f) - \frac{m}{2^k}|$.

Our goal is to show that g *approximates* the critical probability of f well enough so that the composite function $f_B = f(g,\ldots,g)$ is balanced.

More formally, let q be the probability that g outputs 1 under the uniform distribution. Our goal will be to show that $q \in [p_c(f) - t(f), p_c(f) + t(f)]$. The crucial fact that we use is that both the critical probability and the threshold window can not be too small.

First note that: $|p_c(f) - \frac{m}{2^k}| \leq 1/2^k$. Since $p_c(f) \geq 1/n$ and $k = \lceil 3\log n\rceil$, we have $1/2^k \leq p_c(f)^2$, and $m/2^k \leq p_c(f) + p_c(f)^2 \leq 2\cdot p_c(f)$.

Next note that: $q = 1-(1-1/2^k)^m = 1 - \frac{m}{2^k} \pm \epsilon$, where $\epsilon \leq (m/2^k)^2 \leq 4\cdot p_c(f)^2$.

Now we use the assumption $p_c(f) = o(1/\sqrt{n})$ together with Proposition 2.2 ($t(f) \geq 1/n$) to conclude: $\epsilon = o(t(f))$.

Since $m/2^k \leq p_c(f) + p_c(f)^2 = p_c(f) + o(t(f))$, we have: $q = p_c(f) \pm \gamma$, where $\gamma = o(t(f))$. Hence:

LEMMA 4.1. *If f is a monotone Boolean function on n variables such that $p_c(f) = o(1/\sqrt{n})$ then f_B is balanced.*

4.2 AC^0 transitive monotone functions are weakly evasive

THEOREM 4.2 (O'DONELL ET AL.). *(Corollary 1.2 in [14])*

$$\max_i \{\mathrm{Inf}_i(f,p)\} \geq \frac{\mathrm{Var}(f,p)}{\Delta(f,p)}.$$

COROLLARY 4.3. *If f is transitive then*

$$R(f) \geq \Delta(f,p) \geq \frac{\mathrm{Var}(f,p) \cdot n}{\mathrm{Inf}(f,p)}.$$

The first inequality follows from Yao's min-max principle.

THEOREM 4.4 (LINIAL, MANSOUR, AND NISAN [9]). *If $\{f_n\}$ is a sequence of functions on n variables having circuits of size $M(n)$ and depth $d(n)$ then:*

$$\mathrm{Inf}(f, 1/2) = O((\log M)^d).$$

Thus from Corollary 4.3 we have:

LEMMA 4.5. *If $\{f_n\}$ is a sequence of balanced transitive Boolean function on n variables having circuit of size M and depth d then:*

$$R(f) = \Omega(n/(\log M)^d).$$

THEOREM 4.6. *If f is a monotone transitive Boolean function on n variables having a circuit of size M and depth d then:*

$$D(f) \geq R(f) \geq \Omega\left(\frac{n}{(\log M)^{d+4}}\right).$$

Proof: Let $F := (f_U)_B$, i.e., F is obtained from f by first making it unbalanced f_U and then making f_U balanced. Note that $F = f(g, \ldots, g)$ for some monotone transitive g on $K = n^{O(1)}$ variables. Thus: F has the following properties: (a) F is a monotone transitive function on $N = nK = n^{O(1)}$ variables, (b) F is balanced, and (c) F has a circuit of size $M \cdot n^{O(1)}$ and depth $d+3$. Thus from Lemma 4.5 we have: $R(F) = \Omega(N/(\log M + \log n)^{d+3})$. Since $R(f(g,\ldots,g)) \leq R(f) \cdot R(g) \cdot O(\log n)$, and $R(g) \leq K$ we get the desired lower bound on $R(f)$ and hence on $D(f)$. □

5. REFUTING TC^0 COUNTER-EXAMPLES

THEOREM 5.1 (O'DONELL ET AL.). *(Theorem A.1 in [14]) If $f : \{0,1\}^n \to \{-1,1\}$ is a Boolean function on n variables and $g : \{0,1\}^n \to \mathbb{R}$ is a function such that there is an anti-chain $\mathcal{S} \subseteq 2^{[n]}$ (no member is a subset of another) with $\widehat{g}(S) = 0$ for all $S \notin \mathcal{S}$; then*

$$\mathrm{Cov}[f,g]^2 \leq \mathrm{Var}(f) \cdot \sum_{i=1}^{n} \delta_i(\mathcal{T})\,\mathrm{Inf}_i(g),$$

where $\mathrm{Cov}[f,g] := \mathbb{E}[f \cdot g] - \mathbb{E}[f] \cdot \mathbb{E}[g]$, *$\delta_i$ is the probability (over the uniform distribution of the inputs) that the randomized decision tree $\mathcal{T}$ for f queries the variable i, and* $\mathrm{Inf}_i(g) := \sum_{i \in S} |S| \cdot \widehat{g}(S)^2$.

The *noise sensitivity* of f under noise μ_δ, denoted by $NS_\delta(f)$ is $\Pr(f(x) \neq f(x \oplus \eta))$, where η is drawn according to μ_δ and x is drawn uniformly at random. It is convenient to write $NS_\delta(f) = (1 - \mathrm{Stab}_{1-2\delta}(f))/2$, where $\mathrm{Stab}_{1-2\delta}(f)$ is called *noise stability* under δ noise. Moreover: $\mathrm{Stab}_{1-2\delta}(f) = \sum_S (1-2\delta)^{|S|} \widehat{f}(S)^2$. Benjamini, Kalai, and Schramm [2] conjecture:

CONJECTURE 5.2 (BKS CONJECTURE). *If f is computed by a monotone threshold circuit of size $M(n)$ and depth $d(n)$ then for $\delta(n) = (\log M(n))^{-\Omega(d(n))}$,*

$$\mathrm{Stab}_{1-2\delta(f)} \geq 2/3.$$

We can combine Conjecture 5.2 with Theorem 5.1 along the lines of the previous section to obtain the following (A.2):

THEOREM 5.3. *If f is a monotone transitive function on n variables computed by a monotone threshold circuit of size $M(n)$ and depth $d(n)$ then assuming Conjecture 5.2 we have*

$$D(f) \geq R(f) \geq \Omega(n/(\log M(n))^{100 d(n)}).$$

6. A STRONGER VERSION OF WEAK-EC

Our results for AC^0 and TC^0 functions in fact hold for the randomized decision trees complexity. However the 'weak-EC for $R(f)$' is false as demonstrated by the recursive ternary majority function [16], which is in monotone-NC^1. So far we are unable to extend our results in the previous sections to monotone-NC^1 for deterministic decision trees (hence to settle the weak-EC). This motivates us to explore the stronger deterministic variants of weak-EC in the hope of finding a counter-example. In this section we consider a stronger deterministic model of decision trees called *parity decision trees*. The model is certainly more powerful than the ordinary decision trees as demonstrated by the parity function. In the case of monotone functions, the majority on 3 bits has parity decision tree of depth 2 whereas the ordinary decision tree must query all 3 variables. [1]However it is unclear whether or not the parity queries help significantly under the restriction of monotonicity. In this light we explore:

CONJECTURE 6.1 (PARITY-WEAK-EC). *If $\{f_n\}$ is a sequence of non-trivial monotone transitive Boolean functions on n variables then for every $\epsilon > 0$,*

$$D_\oplus(f) \geq \Omega(n^{1-\epsilon}).$$

The best known lower bound is $D_\oplus(f) \geq n^{1/2}$. We provide a counter-example to the above conjecture assuming the following:

[1]In fact, [5] shows that the majority on n variables requires exactly $n - \nu(n) + 1$ parity queries, where $\nu(n)$ is the number of 1s in the binary representation of n.

Conjecture 6.2 (Montanaro and Osborne). *(cf. Conjecture 7 in [11]) For any Boolean function f,*

$$D_{\oplus}(f) = O(\log ||\widehat{f}||_0).$$

Our main observation is the following lemma (A.3):

Lemma 6.3. *There exists a non-trivial monotone transitive evasive Boolean function on n variables such that*

$$\deg(f) \leq n^{1-\Omega(1)}.$$

Now we use the folklore fact: $\log ||\widehat{f}||_0 = O(\deg(f))$ to conclude that assuming Conjecture 6.2, the Conjecture 6.1 is false.

7. OPEN ENDS

7.1 Conditional/unconditional extensions

It seems that we are able to translate the circuit lower bound tools for certain classes (e.g. upper bound on the average sensitivity of AC^0) to lower bound their query complexity using monotonicity and transitivity. Would it be possible to do the same for other tools (e.g. Karchmer-Wigderson games) may be using the topological consequences of non-evasiveness?

If one can refute TC^0 counter-examples to weak-EC unconditionally then disproving EC would be at least as difficult as separating NC^1 from TC^0.

7.2 EC $\equiv$ weak-EC - with further restrictions

The equivalence of weak-EC and EC holds even under suitable restrictions and this equivalence may be useful. For example: for the functions that are transitive under some solvable group. Another example is when the number of distinct prime factors on n is bounded by a constant.

7.3 Gap between CC and Log-rank for monotone functions

To the best of our knowledge, we note the first monotone function with a super-linear gap between $D(f)$ and $\deg(f)$. Nissan and Wigderson [13] used earlier such examples for non-monotone functions [12] to produce a super-linear gap between the communication complexity and the log-rank. No such super-linear gap is noted for monotone functions. Does our example help in finding such a gap? Or does montonicity not allow such a gap?

7.4 The weak-parity-EC for AC^0 functions

In [8] it is shown that the Fourier spectrum of AC^0 functions is *dense*, i.e., $\log ||\widehat{f}||_0 = \widetilde{\Omega}(\deg(f))$. [2] A consequence is that for AC^0 transitive (possibly non-monotone) functions $D_{\oplus}(f) \geq n^{\Omega(1)}$. Is $D_{\oplus}(f) = \widetilde{\Omega}(n)$, more strongly: if f is non-trivial AC^0 transitive function on n variables then $\deg(f) \stackrel{?}{=} \widetilde{\Omega}(n)$.

7.5 Parity trees for monotone functions

Does there exist a monotone Boolean function f with super-linear gap between $D(f)$ and $D_{\oplus}(f)$? A negative answer disproves the conjecture of Montantaro and Osborne [11].

[2]The $\widetilde{\Omega}$ hides the multiplicative poly-logarithmic factor in Ω notation.

8. REFERENCES

[1] László Babai, Anandam Banerjee, Raghav Kulkarni, Vipul Naik: Evasiveness and the Distribution of Prime Numbers. STACS 2010: 71-82

[2] Itai Benjamini, Gil Kalai, and Oded Schramm: Noise sensitivity of Boolean functions and its application to percolation

[3] Harry Buhrman, Ronald de Wolf: Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci. 288(1): 21-43 (2002)

[4] Amit Chakrabarti, Subhash Khot, Yaoyun Shi: Evasiveness of Subgraph Containment and Related Properties. SIAM J. Comput. 31(3): 866-875 (2001)

[5] Thomas P. Hayes, Samuel Kutin, Dieter van Melkebeek: The Quantum Black-Box Complexity of Majority. Algorithmica 34(4): 480-501 (2002)

[6] Jeff Kahn, Michael E. Saks, Dean Sturtevant: A topological approach to evasiveness. Combinatorica 4(4): 297-306 (1984)

[7] Eyal Kushilevitz, Yishay Mansour: Learning Decision Trees Using the Fourier Spectrum. SIAM J. Comput. 22(6): 1331-1348 (1993)

[8] Raghav Kulkarni, Miklos Santha: Query complexity of matroids. Electronic Colloquium on Computational Complexity (ECCC) 19: 63 (2012)

[9] Nathan Linial, Yishay Mansour, Noam Nisan: Constant Depth Circuits, Fourier Transform, and Learnability. J. ACM 40(3): 607-620 (1993)

[10] Frank H. Lutz: Some Results Related to the Evasiveness Conjecture. Comb. Theory, Ser. B 81(1): 110-124 (2001)

[11] Ashley Montanaro, Tobias Osborne: On the communication complexity of XOR functions CoRR abs/0909.3392: (2009)

[12] Noam Nisan, Mario Szegedy: On the Degree of Boolean Functions as Real Polynomials. Computational Complexity 4: 301-313 (1994)

[13] Noam Nisan, Avi Wigderson: On Rank vs. Communication Complexity. Combinatorica 15(4): 557-565 (1995)

[14] Ryan O'Donnell, Michael E. Saks, Oded Schramm, Rocco A. Servedio: Every decision tree has an influential variable. FOCS 2005: 31-39

[15] Ronald L. Rivest, Jean Vuillemin: On Recognizing Graph Properties from Adjacency Matrices. Theor. Comput. Sci. 3(3): 371-384 (1976)

[16] Michael E. Saks, Avi Wigderson: Probabilistic Boolean Decision Trees and the Complexity of Evaluating Game Trees FOCS 1986: 29-38

[17] Yaoyun Shi, Zhiqiang Zhang: Communication Complexities of XOR functions CoRR abs/0808.1762: (2008)

[18] Zhiqiang Zhang, Yaoyun Shi: On the parity complexity measures of Boolean functions. Theor. Comput. Sci. 411(26-28): 2612-2618 (2010)

[19] Andrew Chi-Chih Yao: Monotone Bipartite Graph Properties are Evasive. SIAM J. Comput. 17(3): 517-520 (1988)

APPENDIX

A.

A.1 Unbalancing

PROPOSITION A.1.

$$p_c(f_U) = O(\log N / N^{2/3}).$$

Proof: Let

$$\alpha_p := \Pr_{x \leftarrow \mu_p}(f_U(x) = 1).$$

Since f_U is monotone increasing, $\alpha_0 = 0$ and $\alpha_1 = 1$. Moreover: α_p is a monotone increasing function of p.

Let g_i denote a copy of g so that we can write $f_U = f(g_1, \ldots, g_n)$.

Since f is monotone increasing, we have:

$$\alpha_p \geq \Pr_{x \leftarrow \mu_p}[(\forall i)(g_i = 1)].$$

In other words:

$$\alpha_p \geq 1 - \Pr_{x \leftarrow \mu_p}[(\exists i)(g_i = 0)].$$

Applying the union bound, we get:

$$\alpha_p \geq 1 - n \cdot \Pr_{x \leftarrow \mu_p}(g = 0).$$

In particular, for $q := \ln(2n)/n^2$, we have: $\alpha_q \geq 1/2$. Since α_p is monotone increasing, the critical probability is at most q.

□

A.2 monotone-TC^0

To refute the monotone-TC^0 counter examples to weak-EC we procede as follows: given a transitive function in monotone-TC^0, first we transform it into a balanced function F (as in the previous section) by simulating its critical probability by an OR-AND function. We will need a stronger guarantee, namely: $\Pr(F = 1) = 1/2 \pm \alpha$ where $\alpha = o((\log n)^{-100d})$, which can be obtained by the same method described in previous section.

Now let $G := T_{1-2\delta}(F) := \sum_S (1-2\delta)^{|S|} \widehat{F}(S)$. Note that for $\delta = (1/\log n)^{d+4}$, we have: $\mathbb{E}[F \cdot G] = \operatorname{Stab} F \geq 2/3$ by Kalai's conjecture.

In order to apply Theorem 5.1 we need the Fourier spectrum of G to be supported on an anti-chain. For this we consider $G^* = \sum_{|S|=k} \widehat{G}(S)$, where k is such that $\mathbb{E}[F \cdot G^*] \geq (\log n)^{2d}$. Note that such a k exists because G has $\Omega(1)$ Fourier weight on the first $(\log n)^{2d}$ layers.

Now note that $\mathbb{E}[F] = \mathbb{E}[G^*] = O(\alpha)$ and $\operatorname{Cov}[F, G^*] \geq 1/(\log n)^{2d} - \alpha^2 = \Omega(1/(\log n)^{2d})$.

Now from Theorem 5.1 we have: $\max_i \delta_i(F) \cdot \sum_i \operatorname{Inf}_i(G^*) \geq \Omega(1/(\log n)^{2d})$.

It is easy to see that $\sum_i \operatorname{Inf}_i(G^*) = O((\log n)^{2d}$ since the higher Fourier coefficients of G become negligible. Moreover: since F is transitive we can assume: $\max_i \delta_i = \Delta/N$ where N is the number of variables of F. This gives a nearly linear (up to poly logarithmic factor) lower bound on $\Delta(F)$. In the same manner as the one used for the AC^0 functions, we can now infer nearly linear lower bound on the randomized query complexity of f from here.

Benjamini, Kalai, and Schramm [2] conjecture the noise stability for monotone functions computed by (not necessarily monotone) TC^0 circuits as well. However they comment that the conjecture for monotone-TC^0 is more believable.

A.3 Gap between $D(f)$ and $\deg(f)$ for monotone functions

We use a specific example of Lutz [10] together with a theorem of Kahn, Saks, and Sturtevant [6] that show that non-trivial monotone graph properties of 6-vertex graphs are evasive.

PROPOSITION A.2 (LUTZ, FIG. 2 IN [10]). *There is a non-trivial monotone graph property $f : \{0,1\}^{\binom{6}{2}} \to \{0,1\}$ of 6-vertex graphs such that $\widehat{f}([n]) = 0$, i.e., $\deg(f) < 15$.*

THEOREM A.3 (KAHN, SAKS, AND STURTEVANT [6]). *If $f : \{0,1\}^{\binom{6}{2}} \to \{0,1\}$ is a non-trivial monotone graph property of 6-vertex graphs then $D(f) = 15$.*

Combining Proposition A.2 with Theorem A.3 we have:

COROLLARY A.4. *There exists a monotone Boolean function f on 15 variables such that*

$$D(f) = 15 \text{ and } \deg(f) \leq 14.$$

THEOREM A.5. *There exists a monotone Boolean function f on $n = 15^k$ variables such that:*

$$n = D(f) = \deg(f)^{1+\Omega(1)}.$$

Proof: Construct $f (= f_k)$ recursively from g.

$$f_1(\cdot) = g(\cdot),$$

$$f_k(\cdot) = g(f_{k-1}(\cdot), \ldots, f_{k-1}(\cdot)).$$

It is easy to see that $\deg(f) \leq 14^k$; whereas $D(f) = 15^k$ follows from $D(g(h, \ldots, h)) = D(h) \cdot D(g)$. □