Abstract

The criticality of a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is the minimum real number $\lambda \geq 1$ such that

$$P \left[ DT_{\text{depth}}(f| R_p) \geq t \right] \leq (p\lambda)^t$$

for all $p \in [0, 1]$ and $t \in \mathbb{N}$, where $R_p$ is the $p$-random restriction and $DT_{\text{depth}}$ is decision-tree depth. Criticality is a useful parameter, as it implies an $O(2^{(1 - \frac{1}{2\lambda})n})$ bound on the decision-tree size of $f$, as well as bounds on the Fourier tails on $f$. In a recent unpublished note [11], we observed that AC$^0$ circuits of depth $d + 1$ and size $s$ have criticality at most $O(\log s)^d$ via a combination of Håstad’s switching and multi-switching lemmas [5, 6].

In the present paper, we establish a stronger $O(\frac{1}{d} \log s)^d$ bound for regular formulas (the class of AC$^0$ formulas in which all gates of the same height have the same fan-in). This result is based on: (1) a switching lemma for unbounded-width DNF formulas which uses a novel entropy argument, and (2) an extension of (1) which analyzes a canonical decision tree associated with an entire depth-$d$ formula. As corollaries of our improved criticality bound, we obtain a #SAT algorithm and a tight LMN Theorem for regular formulas which strengthen previous results for AC$^0$ circuits due to Impagliazzo, Matthews and Paturi [7] and Tal [17]. As a further corollary, we increase from $o\left(\frac{\log n}{\log \log n}\right)$ to $o(\log n)$ the number of quantifier alternations for which the QBF-SAT (quantified boolean formula satisfiability) algorithm of Santhanam and Williams [14] beats exhaustive search.

1 Introduction

For a boolean function $f$, we consider the random variable $DT_{\text{depth}}(f| R_p)$ (the decision-tree depth of $f$ under a $p$-random restriction) parameterized by $p \in [0, 1]$. For every $f$, there is a sufficiently small value of $p > 0$ such that $DT_{\text{depth}}(f| R_p)$ satisfies an exponential tail bound. This “sufficiently small” is quantified by the following notion of criticality.

Definition 1. For $\lambda \in \mathbb{R}_{\geq 1}$, we say that a boolean function $f$ is $\lambda$-critical if

$$P \left[ DT_{\text{depth}}(f| R_p) \geq t \right] \leq (p\lambda)^t$$

for all $p \in [0, 1]$ and $t \in \mathbb{N}$. The criticality of $f$ is the minimum $\lambda \in \mathbb{R}_{\geq 1}$ for which $f$ is $\lambda$-critical.

Criticality has been implicitly studied in previous works, although we are unaware if this parameter of boolean functions has been named before. Most notably, Håstad’s switching lemma [5] is equivalent to the statement that every width-$w$ CNF or DNF formula is $O(w)$-critical. Motivating our study of criticality is the observation that upper bounds on criticality imply upper bounds on decision-tree size.

Theorem 2. If $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is $\lambda$-critical, then $DT_{\text{size}}(f)$ is at most $O(2^{(1 - \frac{1}{2\lambda})n})$. 

*Supported by NSERC and a Sloan Research Fellowship
In light of Theorem 2, it is reasonable to expect upper bounds on the criticality of a class of boolean functions to yield (randomized) \#SAT algorithms.

In an unpublished manuscript [11], we observed that a combination of H˚astad’s switching lemma [5] and “multi-switching lemma” [6] can be used to show that \(AC^0\) circuits of depth \(d + 1\) and size \(s\) have criticality \(O(\log s)^d\). Via Theorem 2, this implies an essentially tight upper bound on the decision-tree size of \(AC^0\) circuits and yields a randomized \#SAT algorithm with parameters matching that of Impagliazzo, Matthews and Paturi [7]. In the present paper, we improve these results by giving a quantitatively stronger (and arguably simpler) upper bound on the criticality of regular \(AC^0\) formulas, where regular means that all gates at the same height have equal fan-in.

**Theorem 3.** Regular \(AC^0\) formulas of depth \(d + 1\) and size \(s\) have criticality \(O_{\lambda}(\log s)^d\) (specifically, at most \(60^d(\frac{1}{d} \ln s + 1)^d\)).

Theorem 3 unifies (and arguably simplifies) several of the main results on \(AC^0\) circuits, including bounds on decision-tree size and the Fourier spectrum and \#SAT algorithms. In addition, by obtaining quantitative stronger versions of these results for regular \(AC^0\) formulas, we improve an algorithm of Santhanam and Williams [14] for satisfiability of quantified boolean formulas with bounded-many quantifier blocks.

1.1 Known bounds on criticality

The following bounds on criticality are immediate or known from previous work.

(1) If \(f\) is a boolean function which depends on \(n\) variables, then it is \(n\)-critical. This follows from

\[
P\left[ DT_{\text{depth}}(f|R_p) \geq t \right] \leq P\left[ \text{Bin}(n,p) \geq t \right] \leq p^t \binom{n}{t} \leq (pn)^t.
\]

(2) If \(f\) has decision-tree depth \(k\), then \(f\) is \(k\)-critical. This follows from the folklore bound: for all \(t \geq 1\),

\[
P\left[ DT_{\text{depth}}(f|R_p) \geq t \right] \leq 2^{t-1} p^t \binom{k}{t} \leq \frac{2^{t-1}}{t!} (pk)^t \leq (pk)^t.
\]

(The first inequality is shown by induction on \(t\).)

(3) Showing that (1) and (2) are tight: the \(n\)-variable parity function has criticality exactly \(\lambda = n\). This follows from

\[
np(1 - p)^{n - 1} = P\left[ \text{Bin}(n,p) = 1 \right] \leq P\left[ DT_{\text{depth}}(\text{PARITY}_n|R_p) \geq 1 \right] \leq p\lambda.
\]

Therefore, \(\lambda \geq n(1 - p)^{n - 1}\) for all \(p \in (0, 1]\), hence \(\lambda \geq n\).

(4) H˚astad’s switching lemma [5] shows that every width-\(w\) CNF or DNF formula is \(O(w)\)-critical.

(5) An alternative switching lemma in [11] shows that every size-\(m\) CNF or DNF formula is \(O(\log m)\)-critical.

(6) By a combination of Hastad’s switching lemma [5] and multi-switching lemma [6], it is shown in [11] that every boolean function \(f\) computable by an \(AC^0\) circuit of depth \(d + 1\) and size \(s\) is \(O(\log s)^d\)-critical. The switching lemma is used to show

\[
P\left[ DT_{\text{depth}}(f|R_p) \geq t \right] \leq (p \cdot O(\log s)^d)^t
\]

for \(t \leq \log s\), while the multi-switching lemma establishes this inequality for \(t > \log s\).
1.2 Formulas vs. circuits

Every AC⁰ circuit of depth d + 1 and size s is equivalent to a regular AC⁰ formula of depth d + 1 and size at most s⁴. Theorem 3 therefore implies the O((log s)⁴) criticality bound for AC⁰ circuits.

The proof of our quantitatively stronger O(1/2 log s)d bound for regular AC⁰ formulas is based on a novel “depth-d switching lemma”. Previous switching lemmas analyze the so-called canonical decision tree of bounded-width depth-2 formula under a random restriction. In contrast, we analyze a certain canonical decision tree associated with a depth-d formula under a sequence of random restrictions. The bound we obtain is in terms of top fan-in, as opposed to width (i.e., bottom fan-in of a depth-2 formula).

While our proof of Theorem 3 relies on the assumption of regularity, we conjecture that the O(1/2 log s)d criticality bound applies to all AC⁰ formulas. In this connection, let us mention that a previous result of the author [12] implies that every boolean function f computed by a (not necessarily regular) AC⁰ formula of depth d + 1 and size s satisfies

$$P \left[ \text{DT}_{\text{depth}}(f|{R_p}) \geq t \right] \leq (p \cdot O(1/2 \log s)^d)^t$$

for all t ≤ log s. The method of [12] applies Håstad’s switching lemma to AC⁰ formulas in a more efficient way. However, this method encounters the same log s barrier mentioned in §1.1(6). We do not know how to establish criticality for non-regular AC⁰ formulas by proving the above inequality for t > log s.

2 Preliminaries

\(\mathbb{N}\) is the set of natural numbers \{0, 1, 2, \ldots\}. For \(n \in \mathbb{N}\), \([n]\) is the set \{1, \ldots, n\} (in particular, \([0]\) is the empty set). \(\ln(\cdot)\) is the natural logarithm and \(\log(\cdot)\) is the base-2 logarithm. We consistently use boldface for random objects.

Throughout this paper, we fix an arbitrary set \(V\) whose elements we call variable indices. Without loss of generality, \(V = [n]\); however, since the nature and number of variable indices plays no role in our switching lemma, we prefer to think of \(V\) as an abstract set. (The only time we assume \(V = [n]\) is when speaking of boolean functions \(f: \{0, 1\}^n \rightarrow \{0, 1\}\) in §3)

**Definition 4 (AC⁰ formulas).** A depth-0 formula is a constant 0 or 1 or a literal \(X_v\) or \(\overline{X}_v\) where \(v\) is a variable index. For \(d \geq 1\), a depth-d formula is a syntactic object of the form OR\((F_1, \ldots, F_m)\) or AND\((F_1, \ldots, F_m)\) where \(m \geq 1\) and \(F_1, \ldots, F_m\) are depth \(d - 1\) formulas.

We measure size of a formula by the number of depth-1 subformulas. Formally,

$$\text{size}(F) := \begin{cases} 0 & \text{if } F \text{ has depth 0}, \\ 1 & \text{if } F \text{ has depth 1}, \\ \sum_{\ell=1}^m \text{size}(F_\ell) & \text{if } F \text{ has depth } \geq 2 \text{ and is the } \text{OR or AND of } F_1, \ldots, F_m. \end{cases}$$

Up to a constant factor, size is equivalent to the number of gates in \(F\).

The (syntactic) support of a formula is the set of variable indices \(v\) such that the literal \(X_v\) or \(\overline{X}_v\) occurs as a depth-0 subformula. Throughout this paper, all definitions and proofs by induction are, first, with respect to depth, and second, with respect to support size.

If \(F\) is a formula, we write \(F \equiv 0\) (resp. \(F \equiv 1\)) if \(F\) computes the constant 0 function (resp. the constant 1 function).

A depth-d formula is regular if there exist integers \(m_2, \ldots, m_d \geq 1\) such that, for all \(i \in \{2, \ldots, d\}\), every depth \(i\) subformula has top fan-in \(m_i\). Note that such a formula has size \(\prod_{i=2}^d m_i\).

**Definition 5 (Restrictions and inputs).** A restriction is a partial function \(g\) from \(V\) to \(\{0, 1\}\), viewed as a subset of \(V \times \{0, 1\}\), whose elements we denote by \(v \mapsto b\). We write \(\text{Dom}(g)\) for the domain of \(g\), and we write \(\text{Stars}(g)\) for the set \(V \setminus \text{Dom}(g)\) of “unrestricted” variable indices.

An input is a restriction with domain \(V\) (i.e., a total function from \(V\) to \(\{0, 1\}\), as opposed to a string in \(\{0, 1\}^{|V|}\)).
Two restrictions $\rho$ and $\sigma$ are consistent (we also say that $\sigma$ is $\rho$-consistent) if $\rho(v) = \sigma(v)$ for all $v \in \text{Dom}(\rho) \cap \text{Dom}(\sigma)$. In this case, the union $\rho \cup \sigma$ is a restriction. We say that $\sigma$ is a refinement of $\rho$ if $\rho \subseteq \sigma$ (i.e., $\sigma$ extends $\rho$ by fixing additional variables).

If $F$ is a formula and $\rho$ is a restriction, we denote by $F|_\rho$ the formula obtained from $F$ by relabeling literals according to $\rho$ (we do not perform any simplification to $F$). Formally, we have the induction definition:

$$F|_\rho = \begin{cases} F & \text{if } F \text{ is a constant or a literal } X_v \text{ or } \overline{X}_v \text{ where } v \in \text{Stars}(\rho), \\
0 & \text{if } F = X_v \text{ and } \rho(v) = 0, \text{ or } F = \overline{X}_v \text{ and } \rho(v) = 1, \\
1 & \text{if } F = X_v \text{ and } \rho(v) = 1, \text{ or } F = \overline{X}_v \text{ and } \rho(v) = 0, \\
\text{OR/AND}(F_1|_\rho, \ldots, F_m|_\rho) & \text{if } F \text{ is OR/AND}(F_1, \ldots, F_m). \end{cases}$$

Note that the support of $F|_\rho$ equals the support of $F$ minus the domain of $\rho$.

For $p \in [0, 1]$, the $p$-random restriction $R_p$ is the random restriction which independent maps each variable index $v$ to 0 or 1 with probability $\frac{1-p}{2}$, or leaves $v$ unrestricted with probability $p$. For a restriction $\rho$, a $p$-random refinement of $\rho$ is the random restriction $R_p$ conditioned on being an extension of $\rho$ (i.e., conditioned on $\rho \subseteq R_p$).

**Definition 6** (Sequences and bitstrings). For integers $s, t \in \mathbb{N}$ and arbitrary sequences $\alpha = \langle \alpha_1, \ldots, \alpha_s \rangle$ and $\beta = \langle \beta_1, \ldots, \beta_t \rangle$, we write $\alpha \circ \beta$ for the concatenated sequence $\langle \alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \rangle$. The unique sequence of length 0 is denoted by $\langle \rangle$. (Note that $\langle \rangle$ is the identity with respect to concatenation.)

We refer to sequences $a = \langle a_1, \ldots, a_s \rangle$ in the set $\{0, 1\}^s$ as bitstrings. (To avoid confusion, we regard inputs to formulas as total functions $V \to \{0, 1\}$ rather than as ordered bitstrings in the set $\{0, 1\}^{|V|}$.) For $t \geq s$, we write $\{0, 1\}_t^s$ for the set of bitstrings $q = \langle q_1, \ldots, q_t \rangle \in \{0, 1\}^t$ such that $q_1 + \cdots + q_t = s$. For bitstrings $a \in \{0, 1\}^s$ and $b \in \{0, 1\}^t$ and $q \in \{0, 1\}_t^s$, we write $b \leftarrow a$ for the bitstring $\langle c_1, \ldots, c_t \rangle$ defined by

$$c_j := \begin{cases} b_j & \text{if } q_j = 0, \\
a_i & \text{if } q_j = 1 \text{ and } q_1 + \cdots + q_{j-1} = i \text{ (i.e., } q_j \text{ is the } i^{th} \text{ 1-coordinate of } q). \end{cases}$$

That is, $b \leftarrow a$ overwrites $b$ with $a$ in the indices specified by $q$.

**Definition 7** (Ordered restrictions). An ordered restriction is a sequence $\beta = \langle v_1 \mapsto b_1, \ldots, v_t \mapsto b_t \rangle$ where $t \in \mathbb{N}$ and each $v_i \mapsto b_i$ is an ordered pair with $v_i \in V$ and $b_i \in \{0, 1\}$ such that $v_1, \ldots, v_t$ are distinct. As a matter of notation, we sometimes identify $\beta$ with its underlying (unordered) restriction $\{v_1 \mapsto b_1, \ldots, v_t \mapsto b_t\}$, for instance, by writing $\text{Dom}(\beta)$ for the set $\{v_1, \ldots, v_t\}$ or $F|_{\beta}$ for $F|_{\{v_1 \mapsto b_1, \ldots, v_t \mapsto b_t\}}$.

For an ordered restriction $\beta = \langle v_1 \mapsto b_1, \ldots, v_t \mapsto b_t \rangle$ and a set of variable indices $S \subseteq V$ and a bitstring $a = \langle a_1, \ldots, a_s \rangle \in \{0, 1\}^{\text{Dom}(\beta) \cap S}$, we write $b \leftarrow S a$ for the ordered restriction $\langle v_1 \mapsto c_1, \ldots, v_t \mapsto c_t \rangle$ where

$$c_j := \begin{cases} b_j & \text{if } v_j \notin S, \\
a_i & \text{if } v_j \text{ is the } i^{th} \text{ variable of } \text{Dom}(\beta) \cap S \text{ in the order given by } \beta. \end{cases}$$

In other words, $\langle c_1, \ldots, c_t \rangle = \langle b_1, \ldots, b_t \rangle \leftarrow S a$ where $q \in \{0, 1\}_t^s$ is the bitstring defined by $q_j = 1 :\iff v_j \in S$.

**Definition 8** (Decision trees). A decision tree is a finite rooted binary tree $T$ in which each non-leaf is labeled by a variable index $v$ and the two edges to its children are labeled by 0 and 1. We require the variable indices on any root-to-leaf branch are distinct; each root-to-leaf branch therefore corresponds to an ordered restriction. We measure size by the number of leaves and depth by the maximum number of non-leaves on a root-to-leaf path.

We say that a decision tree $T$ determines a boolean function $f$ if the restricted function $f|_\alpha$ is constant for each ordered restriction $\alpha$ corresponding to a branch of $T$. (We might also say that $T$ “computes” $f$, if we regard $T$ as having output values on leaves.) The decision-tree size (resp. decision-tree depth) of a boolean function $f$, denoted $\text{DT}_{\text{size}}(f)$ (resp. $\text{DT}_{\text{depth}}(f)$), is the minimum size (resp. depth) of a decision tree that determines $f$. 

Later on, it will be convenient to identify decision trees with the set of ordered restrictions corresponding to branches. From this perspective, a decision tree is a nonempty set $T^*$ of ordered restrictions such that, for all $(v_1 \mapsto a_1, \ldots, v_s \mapsto a_s) \in T^*$ and $i \in [s]$,

- if $(v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v'_i \mapsto a'_i)$ is an initial subsequence of any element of $T^*$, then $v'_i = v_i$,
- $(v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v_i \mapsto 1 - a_i)$ is an initial subsequence of some element of $T^*$.

### 2.1 Some inequalities

**Lemma 9.** For every integer $s \geq 1$ and $\varepsilon \in (0, 1$],

$$\sum_{t=s}^{\infty} (1 - \varepsilon)^t \left( \frac{t-1}{s-1} \right) = \left( \frac{1-\varepsilon}{\varepsilon} \right)^s.$$  

**Proof.** Let $X_1, X_2, \ldots$ be independent Bernoulli($\varepsilon$) random variables. Then

$$1 = \mathbb{P} \left[ \sum_{i=1}^{\infty} X_i \geq s \right] = \sum_{t=s}^{\infty} \mathbb{P} \left[ \sum_{t=s}^{t-1} X_i = s-1 \right] = \sum_{t=s}^{\infty} \varepsilon^t (1 - \varepsilon)^{t-s} \left( \frac{t-1}{s-1} \right).$$

The inequality follows by multiplying both sides by $((1 - \varepsilon)/\varepsilon)^s$. □

The next inequality also comes up in the AC$^0[2]$ formula lower bound of Rossman and Srinivasan [13].

**Lemma 10.** For all real numbers $a, b, c \geq 0$,

$$\left( \frac{a}{c} + 1 \right)^c (b+1) \leq \left( \frac{a+b}{c+1} + 1 \right)^{c+1}.$$  

**Proof.** The lemma is trivial if $c = 0$ (under the convention that $(a/0 + 1)^0 = 1$), so assume $c > 0$. Let $f(a, b, c) := \text{RHS} - \text{LHS}$. Then

$$\frac{\partial}{\partial b} f(a, b, c) = \left( \frac{a+b}{c+1} + 1 \right)^c - \left( \frac{a}{c} + 1 \right)^c.$$  

Note that this is an increasing function of $b$ with a zero at $b = a/c$. Therefore, $f(a, b, c)$ is minimal at $b = a/c$ where it takes value $f(a, a/c, c) = 0$. □

As a corollary, we get:

**Lemma 11.** For all integers $d, m_1, \ldots, m_d \geq 1$,

$$\prod_{i=1}^{d} (\ln m_i + 1) \leq \left( \frac{1}{d} \ln \left( \prod_{i=1}^{d} m_i \right) + 1 \right)^d.$$  

**Proof.** For each $j \in [d-1]$, Lemma 10 implies

$$\left( \frac{1}{j-1} \ln \left( \prod_{i=1}^{j-1} m_i \right) + 1 \right)^{j-1} (\ln m_j + 1) \leq \left( \frac{1}{j} \ln \left( \prod_{i=1}^{j} m_i \right) + 1 \right)^j.$$  

The lemma follows from these $d-1$ inequalities. □

The final inequality of this section plays a key role in our switching lemma analysis.
Lemma 12. Let $I$ be a set and suppose $\mu : I \to [0, 1]$ such that $\sum_{i \in I} \mu(i) \leq 1$. Then for every function $t : I \to \mathbb{N}$ and integer $s \geq 1$,

$$\sum_{i \in I} \left( \frac{t(i)}{s} \right) \mu(i) \leq e^s \left( \frac{1}{s} \ln \left( \sum_{i \in I} e^{t(i)} \mu(i) \right) + 1 \right)^s.$$ 

Proof. Let $\lambda := \sum_{i \in I} \mu(i)$ ($\in [0, 1]$) and let $\nu(i) := \mu(i)/\lambda$ ($\geq \mu(i)$). We have

$$\sum_{i \in I} \left( \frac{t(i)}{s} \right) \mu(i) \leq \lambda \sum_{i \in I} \left( \frac{et(i)}{s} \right) \nu(i) \leq \lambda e^s \sum_{i \in I} \left( \frac{1}{s} \ln(e^{t(i)}) + 1 \right)^s \nu(i)$$

by Jensen’s inequality since $a \mapsto \left( \frac{1}{s} \ln(a) + 1 \right)^s$ is concave over $a \in \mathbb{R}_{\geq 1}$

$$\leq \lambda e^s \left( \frac{1}{s} \ln \left( \sum_{i \in I} e^{t(i)} \nu(i) \right) + 1 \right)^s = \lambda e^s \left( \frac{1}{s} \ln \left( \sum_{i \in I} e^{t(i)} \mu(i) \right) + 1 - \frac{1}{s} \ln(\lambda) \right)^s \leq e^s \left( \frac{1}{s} \ln \left( \sum_{i \in I} e^{t(i)} \mu(i) \right) + 1 \right)^s$$

since $\lambda \mapsto \lambda(a - \frac{1}{s} \ln(\lambda))^s$ is increasing over $\lambda \in (0, 1]$ (hence maximal at $\lambda = 1$) for every $a \in \mathbb{R}_{\geq 1}$.

3 Implications of criticality

Before presenting our main result on regular $\text{AC}^0$ formulas, we give some general results on $\lambda$-critical functions. We begin with the following upper bound on decision-tree size, which is slightly stronger than Theorem 2.

Proposition 13. If $f : \{0, 1\}^n \to \{0, 1\}$ is $\frac{1}{2\varepsilon}$-critical, then $\text{DT}_{\text{size}}(f) \leq 2^n - \varepsilon n - \sqrt{\varepsilon n + \log(\varepsilon n)} + O(1)$.

Proof. We first note that the proposition is trivial if $\varepsilon > \frac{1}{2}$, since no non-constant boolean function has criticality $< 1$. If $n < 10$ or $\varepsilon < \frac{n}{2}$, then the bound $\text{DT}_{\text{size}}(f) \leq 2^n - \varepsilon n - \sqrt{\varepsilon n + \log(\varepsilon n)} + O(1)$ follows from the trivial bound $\text{DT}_{\text{size}}(f) \leq 2^n$ by choosing a large enough constant. We may therefore assume that $n \geq 10$ and $\varepsilon \in [\frac{1}{n}, \frac{1}{2}]$.

Let $p := \varepsilon - \frac{1}{n}$ and note that $p \in [\frac{1}{n}, \frac{1}{2}]$. We have

$$|E \left[ \text{DT}_{\text{size}}(f | R_p) \right] | \leq |E \left[ 2^{\text{DT}_{\text{depth}}(f | R_p)} \right] | = \sum_{t=0}^{\infty} 2^t P \left[ \text{DT}_{\text{depth}}(f | R_p) = t \right] \leq \sum_{t=0}^{\infty} 2^t \left( \frac{p}{2e} \right)^t = \sum_{t=0}^{\infty} \left( 1 - \frac{1}{e^p} \right)^t = \varepsilon n.$$ 

We next make use of the following facts:

- $P \left[ \text{Bin}(n, p) \geq pn + \sqrt{pn + 1} \right] > 0.05$

  (this bound holds for all $n \geq 10$ and $p \in [\frac{1}{n}, \frac{1}{2}]$, as can be shown using estimates in [19]),
\* \( \text{DT}_{\text{size}}(f) \leq \sum_{\mathcal{S} \to \{0,1\}} \text{DT}_{\text{size}}(f \mid \mathcal{S}) \) for every set of variable indices \( \mathcal{S} \subseteq [n] \).

Let \( \mathcal{S} \) be a \( p \)-random subset of \([n]\) (i.e., a uniform random subset of size \( \text{Bin}(n, p) \)), and let \( \mathcal{g} \) be a uniform random function \([n] \setminus \mathcal{S} \to \{0,1\} \). Note that \( \mathcal{g} \) is a \( p \)-random restriction.

For any \( c > 0 \), we have

\[
I[\text{DT}_{\text{size}}(f) > c2^{n-\varepsilon n}] \leq \mathbb{P}_S \left[ 2^{n-|S|} \mathbb{E}_\mathcal{g} \left[ \text{DT}_{\text{size}}(f \mid \mathcal{g}) \right] > c2^{n-\varepsilon n} \right] \\
\leq \mathbb{P}_S \left[ \left( |S| < pn + \sqrt{pn + 1} \right) \text{ or } \left( \mathbb{E}_\mathcal{g} \left[ \text{DT}_{\text{size}}(f \mid \mathcal{g}) \right] > c2^{p(n + \sqrt{pn + 1} - \varepsilon n)} \right) \right] \\
\leq \mathbb{P}_S \left[ |S| < pn + \sqrt{pn + 1} \right] + \mathbb{P}_S \left[ \mathbb{E}_\mathcal{g} \left[ \text{DT}_{\text{size}}(f \mid \mathcal{g}) \right] > c2^{\sqrt{\varepsilon n} - 1} \right] \\
\leq \mathbb{P} \left[ \text{Bin}(n, p) < pn + \sqrt{pn + 1} \right] + \frac{2}{c2^{\sqrt{\varepsilon n}}} \mathbb{E} \left[ \text{DT}_{\text{size}}(f \mid R_{p}) \right] \\
< 0.95 + \frac{2\varepsilon n}{c2^{\sqrt{\varepsilon n}}}. 
\]

Setting \( c := 40\varepsilon n/2^\sqrt{\varepsilon n} \), we have \( I[\text{DT}_{\text{size}}(f) > c2^{n-\varepsilon n}] < 1 \). We conclude that

\[
\text{DT}_{\text{size}}(f) \leq c2^{n-\varepsilon n} = 40 \cdot 2^{n-\varepsilon n - \sqrt{\varepsilon n + \log(\varepsilon n)}}.
\]

The following theorem (which includes Theorem 2) lists several consequences of criticality, which follow from Proposition 13 as well as results of Linial, Mansour and Nisan [9] and Tal [17] relating the Fourier spectrum of a boolean function to its degree under a \( p \)-random restriction.

**Theorem 14** (Implications of criticality). If \( f : \{0,1\}^n \to \{0,1\} \) is \( \lambda \)-critical, then

1. \( \text{DT}_{\text{size}}(f) \leq O(2^{(3-\frac{\lambda}{2})n}) \),
2. \( f \) agrees with \( \text{PARITY}_n \) on at most \( \frac{1}{2} + O(2^{-n/2\lambda}) \) fraction of inputs,
3. \( \mathbb{P}[\deg(f \mid R_{p}) \geq t] \leq (p\lambda)^t \) for all \( p \) and \( t \),
4. \( \sum_{S \subseteq [n] : |S| \geq k} \hat{f}(S)^2 \leq 2e \cdot e^{-k/\lambda} (= 2^{-\Omega(k/\lambda)}) \) for all \( k \),
5. \( \sum_{S \subseteq [n] : |S| = k} |\hat{f}(S)| \leq O(\lambda)^k \) for all \( k \).

**Proof.** (1) follows immediately from Proposition 13. Property (2) is a consequence of (1). Property (3) follows from the definition of criticality and the fact that \( \deg(\cdot) \leq \text{DT}_{\text{depth}}(\cdot) \). Linial, Mansour and Nisan [9] showed that (3) \( \Rightarrow \) (4). Tal [17] showed that (4) \( \Rightarrow \) (5) (and moreover that (4) \( \Rightarrow \) (3), i.e., properties (3) and (4) are equivalent up to constant in the \( O(\cdot) \)).

We conclude this section by observing that any exponential tail bound on \( \text{DT}_{\text{depth}}(f \mid R_{q}) \) implies an upper bound on criticality.

**Proposition 15.** Let \( f \) be a boolean function, let \( q, \varepsilon \in (0,1] \), and suppose \( \mathbb{P}[\text{DT}_{\text{depth}}(f \mid R_{q}) = t] \leq (1 - \varepsilon)^t \) for all \( t \in \mathbb{N} \). Then \( f \) is \( \frac{2}{\varepsilon q} \)-critical.
Proof. Let $0 \leq p \leq q$, let $\varrho_1$ be a $q$-random restriction over the variables of $f$, and let $\varrho_2$ be a $p/q$-random restriction over $\text{Stars}(\varrho_1)$. Then using [11.12] and Lemma 9, we have

$$
\Pr[\text{DT}_{\text{depth}}(f_i | R_p) \geq t] = \E_{\varrho_1} \left[ \Pr_{\varrho_2} \left[ \text{DT}_{\text{depth}}(f_i | \varrho_2) \geq t \right] \right]
$$

$$
= \sum_{k=t}^{\infty} \Pr_{\varrho_1} \left[ \text{DT}_{\text{depth}}(f_i | \varrho_2) = k \right] \E_{\varrho_1} \left[ \Pr_{\varrho_2} \left[ \text{DT}_{\text{depth}}(f_i | \varrho_2) \geq t \right] \right] \Pr_{\varrho_2} \left[ \text{DT}_{\text{depth}}(f_i | \varrho_2) = k \right]
$$

$$
\leq \sum_{k=t}^{\infty} \Pr_{\varrho_1} \left[ \text{DT}_{\text{depth}}(f_i | R_p) = k \right] \max_{g: \text{depth}(g) = k} \Pr_{\varrho_2} \left[ \text{DT}_{\text{depth}}(g | R_p/q) \geq t \right]
$$

$$
\leq \sum_{k=t}^{\infty} (1 - \varepsilon)^k \left( \frac{2p}{q} \right)^t \left( \frac{k}{t} \right) = \left( \frac{2p}{q} \right)^t \frac{(1 - \varepsilon)^t - 1}{\varepsilon^t} \leq \left( \frac{2p}{\varepsilon q} \right)^t. \quad \square
$$

4 The canonical decision tree of a depth-$d$ formula

In this section, we define the canonical decision tree of a depth-$d$ formula $F$ under a chain of restrictions $\varrho_1 \leq \cdots \leq \varrho_d$, denoted $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$. The primary definition, however, is of a richer object $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$.

Definition 16. For every $d \in \mathbb{N}$ and chain of restrictions $\varrho_1 \leq \cdots \leq \varrho_d$ and depth-$d$ formula $F$, we define a set of ordered restrictions $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$ as follows. In the base case $d = 0$, let

$$
\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F) := \begin{cases} \{ () \} & \text{if } F \text{ is a constant 0 or 1,} \\
\{ (v \mapsto 0), (v \mapsto 1) \} & \text{if } F \text{ is a literal } X_v \text{ or } \overline{X}_v.
\end{cases}
$$

For $d \geq 1$, the definition is inductive. Suppose $F = \text{OR}(F_1, \ldots, F_m)$ where each $F_i$ is a depth $d - 1$ formula. Assume that $\mathcal{T}_{\varrho_1, \ldots, \varrho_d-1}(F_i)$ is defined for all $i \in [m]$ and that $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F_i) = \mathcal{T}_{\varrho_1, \ldots, \varrho_d-1}(F_i)$ is defined for every restriction $\varrho$ whose domain includes at least one variable index in the support of $F$. We consider three cases:

(i) If $F_1 | \varrho_d \equiv \cdots \equiv F_m | \varrho_d \equiv 0$, then $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F) := \{ () \}$.

(ii) If $F_1 | \varrho_d \equiv \cdots \equiv F_{t-1} | \varrho_d \equiv 0$ and $F_t | \varrho_d \equiv 1$, then $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F) := \{ () \}$.

(iii) If $F_1 | \varrho_d \equiv \cdots \equiv F_{t-1} | \varrho_d \equiv 0$ and $F_t | \varrho_d$ computes a non-constant function, then $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$ is the set of ordered restrictions $\{ (v \mapsto a_1, \ldots, v_u \mapsto a_u) \}$ of length $u \geq 1$ such that there exist $t \in [u]$ and $b \in \{0, 1\}^t$ satisfying

- $\{ (v_1 \mapsto b_1, \ldots, v_t \mapsto b_t) \} \in \mathcal{T}_{\varrho_1, \ldots, \varrho_d-1}(F_t)$,
- $\{ (v_{t+1} \mapsto a_{t+1}, \ldots, v_u \mapsto a_u) \} \in \mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F_i | \{ v_1 \mapsto a_1, \ldots, v_t \mapsto a_t \})$, and
- for all $i \in [u]$, if $v_i \in \text{Dom}(\varrho_d)$, then $b_i = a_i$ if $F_i | \varrho_d \neq 0$, and $b_i = 1 - a_i$ if $F_i | \varrho_d \equiv 0$.

Finally, $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$ is defined in the same way if $F = \text{AND}(F_1, \ldots, F_m)$, but with the roles 0 and 1 exchanged.

Lemma 17. $\mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$ is nonempty and every $\alpha = \{ v_1 \mapsto a_1, \ldots, v_u \mapsto a_u \} \in \mathcal{T}_{\varrho_1, \ldots, \varrho_d}(F)$ satisfies:

(a) $\alpha$ is consistent with $\varrho_d$ (i.e., for all $i \in [u]$, if $v_i \in \text{Dom}(\varrho_d)$, then $a_i = \varrho_d(v_i)$),

(b) the support of $F$ contains $\text{Dom}(\alpha)$ (i.e., for all $i \in [u]$, the literal $X_{v_i}$ or $\overline{X}_{v_i}$ occurs as a depth-$0$ subformula of $F$).
(c) for all \( i \in [u] \), if \( v_i \in \text{Stars}(\varrho_d) \), then \( \langle v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v_i \mapsto 1 - a_i \rangle \) is an initial subsequence of some element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \).

(d) for all \( i \in [u] \) and every variable index \( v'_i \) and bit \( a'_i \in \{0, 1\} \), if \( \langle v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v'_i \mapsto a'_i \rangle \) is an initial subsequence of any element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \), then \( v'_i = v_i \).

(e) the function computed by \( F|_{\varrho_d, \ldots, \varrho_d} \) is constant (i.e., \( F|_{\varrho_d, \ldots, \varrho_d} \equiv 0 \) or \( F|_{\varrho_d, \ldots, \varrho_d} \equiv 1 \)).

Proof. Though the proof is straightforward from Definition \[16\] we include full details. Note that the lemma is trivial when \( d = 0 \) as well as in cases (i) and (ii) when \( d \geq 1 \). So we assume that \( F = \text{OR}(F_1, \ldots, F_m) \) falls under case (iii), as witnessed by \( t \in [m] \). By the induction hypothesis, we may assume that the lemma holds with respect to \( F_t \) as well as \( F|_{\gamma} \) for every restriction \( \gamma \) whose domain includes at least one variable index in the support of \( F \).

We first establish that \( T_{\varrho_1, \ldots, \varrho_d}(F) \) is nonempty. By the induction hypothesis, \( T_{\varrho_1, \ldots, \varrho_{d-1}}(F_t) \) is nonempty.

Since \( F_t|_{\varrho_d} \) is non-constant and \( F_t|_{\varrho_d} \) is constant for every \( \beta \in T_{\varrho_1, \ldots, \varrho_{d-1}}(F_t) \), there exists \( \beta \in T_{\varrho_1, \ldots, \varrho_{d-1}}(F_t) \) such that \( F_t|_{\varrho_d} \equiv 1 \). Let \( \beta = \langle v_1 \mapsto b_1, \ldots, v_t \mapsto b_t \rangle \) and note that \( t \geq 1 \). For all \( i \in [t] \), we have \( F_t|_{\varrho_d} \langle v_1 \mapsto b_1, \ldots, v_i \mapsto b_i \rangle \neq 0 \), since this is the same formula as \( F_t|_{\varrho_d} \langle v_1 \mapsto b_1, \ldots, v_i \mapsto b_i \rangle \) by \( \varrho_d \)-consistency of \( \beta \).

By the definition of \( T_{\varrho_1, \ldots, \varrho_d}(F) \) in case (iii), it follows that \( \beta \circ \gamma \in T_{\varrho_1, \ldots, \varrho_d}(F) \) for every \( \gamma \in T_{\varrho_1, \ldots, \varrho_d}(F|_{\beta}) \).

Nonemptiness of \( T_{\varrho_1, \ldots, \varrho_d}(F) \) therefore follows from nonemptiness of \( T_{\varrho_1, \ldots, \varrho_d}(F|_{\beta}) \), which we know by the induction hypothesis applied to \( F|_{\beta} \) (noting that \( \text{Dom} (\beta) \) contains a variable index in the support of \( F \), namely \( v_1 \), which is in the support of \( F_t \) by the induction hypothesis applied to \( F_t \)).

Now consider any \( \alpha = \langle v_1 \mapsto a_1, \ldots, v_u \mapsto a_u \rangle \in T_{\varrho_1, \ldots, \varrho_d}(F) \), as witnessed by some \( t \in [u] \) and \( b \in \{0, 1\}^t \) in definition of case (iii). Let \( \gamma = \langle v_1 \mapsto a_1, \ldots, v_t \mapsto a_t \rangle \). We establish properties (a)–(e) in order.

(a): Suppose \( i \in [u] \) and \( v_i \in \text{Dom}(\varrho_d) \). If \( i \in \{1, \ldots, t\} \), then \( a_i = \varrho_d(v_i) \) by definition of \( T_{\varrho_1, \ldots, \varrho_d}(F) \) in case (iii). Otherwise, if \( i \in \{t + 1, \ldots, u\} \), then \( a_i = \varrho_d(v_i) \) by property (a) with respect to \( F|_{\gamma} \).

(b): From the induction hypothesis, we know that \( v_1, \ldots, v_t \) are in the support of \( F_t \) (hence also the support of \( F \)) and that \( v_{t+1}, \ldots, v_u \) are in the support of \( F|_{\gamma} \) (hence also the support of \( F \)).

(c): First note that \( \langle F_t|_{\varrho_d}\rangle|_{\{v_1 \mapsto b_1, \ldots, v_{i-1} \mapsto b_{i-1}\}} \neq 0 \) for all \( i \in [t] \), as easily shown by induction on \( i \). It then follows from the definition of case (iii) that for all \( i \in [t] \), if \( v_i \in \text{Stars}(\varrho_d) \), then \( \langle v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v_i \mapsto 1 - a_i \rangle \) is an initial subsequence of some element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \). The same conclusion for all \( i \in \{t + 1, \ldots, u\} \) follows from property (c) with respect to \( F|_{\gamma} \).

(d): If \( i \in [t] \) and \( \langle v_1 \mapsto a_1, \ldots, v_{i-1} \mapsto a_{i-1}, v'_i \mapsto a'_i \rangle \) is an initial subsequence of an element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \), then by definition of case (iii), \( \langle v_1 \mapsto b_1, \ldots, v_{i-1} \mapsto b_{i-1}, v'_i \mapsto a'_i \rangle \) is initial subsequence of an element of \( T_{\varrho_1, \ldots, \varrho_{d-1}}(F_t) \) and therefore \( v'_i = v_i \). For \( i \in \{t + 1, \ldots, u\} \), the conclusion follows from property (d) with respect to \( F|_{\gamma} \).

(e): Since \( \langle v_{t+1} \mapsto a_{t+1}, \ldots, v_u \mapsto a_u \rangle \in T_{\varrho_1, \ldots, \varrho_d}(F|_{\gamma}) \), the formula \( (F|_{\gamma})|_{\varrho_d, \{v_{t+1} \mapsto a_{t+1}, \ldots, v_u \mapsto a_u\}} \), which is the same formula as \( F|_{\varrho_d, \ldots, \varrho_d} \) by \( \varrho_d \)-consistency of \( \alpha \), computes a constant function by property (e) with respect to \( F|_{\gamma} \).

Definition 18. For \( \alpha = \langle v_1 \mapsto a_1, \ldots, v_u \mapsto a_u \rangle \in T_{\varrho_1, \ldots, \varrho_d}(F) \), let \( \alpha^* \) denote the subsequence \( \alpha^* := \langle v_{i_1} \mapsto a_{i_1}, \ldots, v_{i_s} \mapsto a_{i_s} \rangle \) for the unique \( 1 \leq i_1 < \cdots < i_s \leq u \) such that \( \{v_{i_1}, \ldots, v_{i_s}\} = \text{Dom}(\alpha) \cap \text{Stars}(\varrho_d) \).

Let \( T_{\varrho_1, \ldots, \varrho_d}(F) := \{ \alpha^* : \alpha \in T_{\varrho_1, \ldots, \varrho_d}(F) \} \).

Lemma 19. \( T_{\varrho_1, \ldots, \varrho_d}(F) \) is the set of branches of a decision tree determining \( F|_{\varrho_d} \). Moreover, each element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \) is a subsequence of a unique element of \( T_{\varrho_1, \ldots, \varrho_d}(F) \).

Proof. Straightforward from Lemma \[17\]
Definition 20. We call $T_{\varrho_1\ldots\varrho_d}(F)$ the canonical decision tree of $F$ under $\varrho_1,\ldots,\varrho_d$. For a bitstring $a \in \{0,1\}^*$ and an ordered restriction $\alpha$, we write “$T_{\varrho_1\ldots\varrho_d}(a) = \alpha$” if $a \in T_{\varrho_1\ldots\varrho_d}(F)$ and there exist variable indices $v_1,\ldots,v_s$ such that $\alpha^* = \langle v_1 \mapsto a_1, \ldots, v_s \mapsto a_s \rangle$. We say that “$T_{\varrho_1\ldots\varrho_d}(F)$ exists” if $T_{\varrho_1\ldots\varrho_d}(F) = \alpha$ for any $\alpha \in T_{\varrho_1\ldots\varrho_d}(F)$.

Note that, by Lemma 19, if $T_{\varrho_1\ldots\varrho_d}(F)$ exists then $T_{\varrho_1\ldots\varrho_d}(F) = \alpha$ for a unique $\alpha \in T_{\varrho_1\ldots\varrho_d}(F)$ (justifying our use of the equality symbol). We may regard $T_{\varrho_1\ldots\varrho_d}(F)$ as a partial function from bitstrings to elements of the set $T_{\varrho_1\ldots\varrho_d}(F)$.

5 Depth-d switching lemma

In this section, we consider a depth-$d$ formula $F = \text{OR}(F_1,\ldots,F_m)$ and study the branches of $T_{\varrho_1\ldots\varrho_d}(F)$ where $\varrho_1 \subseteq \cdots \subseteq \varrho_d$ is a chain of random restrictions where $\varrho_d$ is a $p$-random refinement of $\varrho_{d-1}$ and formulas $F_1,\ldots,F_m$ satisfy a certain hypothesis with respect to $\varrho_1,\ldots,\varrho_{d-1}$. This allows us to bound the probability that $T_{\varrho_1\ldots\varrho_d}(F)$ has an $a$-branch for any string $a \in \{0,1\}^*$. We refer to the main result of this section, Proposition 22, as the “depth-d switching lemma” since it analyzes the canonical decision tree of $F$ in a similar manner as Hastad’s switching lemma analyzes the canonical decision tree of a CNF or DNF formula.

Proposition 22 is in fact a special case of the slightly more general Proposition 25 (“serial depth-d switching lemma”), which we prove in the next section. The proofs are essentially the same, but with Proposition 22 we have fewer indices to keep track of. The next lemma unpacks the recursive definition of $T_{\varrho_1\ldots\varrho_d}(F)$ to obtain a more explicit characterization of its branches. This lemma associates $T_{\varrho_1\ldots\varrho_d}(F)$, whenever this exists, with certain data $(r,s,\ell,t,b,q)$.

Lemma 21 (Unpacking $T_{\varrho_1\ldots\varrho_d}(F)$). Let $F = \text{OR}(F_1,\ldots,F_m)$ be a depth-$d$ formula, let $\varrho_1 \subseteq \cdots \subseteq \varrho_d$ be restrictions, let $s \geq 1$, and let $a \in \{0,1\}^s$. If $T_{\varrho_1\ldots\varrho_d}(F)$ exists, then there exist

- integers $r \in [s]$ and $s_1,\ldots,s_r \geq 1$ with $s_1 + \cdots + s_r = s$,
- integers $1 \leq \ell_1 < \cdots < \ell_r \leq m$,
- integers $t_i \geq s_i$ and bitstrings $b_i \in \{0,1\}^{t_i}$ and $q_i \in \{0,1\}^{s_i}$ for each $i \in [r]$

with the property that there exist unique ordered restrictions $\beta_1,\ldots,\beta_r$ such that, for all $i \in [r]$,

(i) $(F_{\ell'}|_{\gamma_i})|_{\varrho_d} \equiv 0$ for all $1 \leq \ell' < \ell_i$,
(ii) $(F_{\ell_i}|_{\gamma_i})|_{\varrho_d} \not\equiv 0$,
(iii) $T_{\varrho_1\ldots\varrho_{d-1}}(F_{\ell_i}|_{\gamma_i}) = \beta_i$,
(iv) $\beta_i$ is $\varrho_d$-consistent and $(F_{\ell_i}|_{\gamma_i})|_{\varrho_d \cup \beta_i} \equiv 1$,
(v) “$q_i$ identifies Stars($\varrho_d$) within Dom($\beta_i$) \cap Stars($\varrho_{d-1}$)” in the following sense: for all $j \in [t_i]$,

$q_{i,j} = 1 \iff \text{Stars($\varrho_d$) contains the } j^{\text{th}} \text{ variable of Dom($\beta_i$) \cap Stars($\varrho_{d-1}$) in the order given by $\beta_i$.}$

where

$\gamma_i := (\beta_1 \circ \cdots \circ \beta_{i-1}) \leftarrow_{\text{Stars($\varrho_{d-1}$)}} c_i$,
$c_i := (b_1 \circ \cdots \circ b_{i-1}) \leftarrow_{\{0,1\}^{s_1} \cdots \{0,1\}^{s_{i-1}}} \{a_1,\ldots,a_{s_1}+\cdots+s_{i-1}\}$.

(Note that conditions (iii) and (v) imply that $|\text{Dom($\beta_i$)} \cap \text{Stars($\varrho_{d-1}$)}| = t_i$ and $|\text{Dom($\beta_i$)} \cap \text{Stars($\varrho_d$)}| = s_i$ and $\gamma_i = (\beta_1 \circ \cdots \circ \beta_{i-1}) \leftarrow_{\text{Stars($\varrho_d$)}} \{a_1,\ldots,a_{s_1}+\cdots+s_{i-1}\})$)

Proof. Straightforward from Definition 10 □

10
Proposition 22 ("Depth-d switching lemma"). Let $F = \text{OR}(F_1, \ldots, F_m)$ be a depth-$d$ formula. Suppose $\mathcal{Q}_1 \subseteq \cdots \subseteq \mathcal{Q}_{d-1}$ are random restrictions such that the following holds: for all integers $r \geq 1$ and $1 \leq \ell_1 \prec \cdots \prec \ell_r \leq m$ and $t_1, \ldots, t_r \geq 1$ and bitstrings $b_1, \ldots, b_r, c_1, \ldots, c_r$ where $b_i \in \{0,1\}^{t_i}$ and $c_i \in \{0,1\}^{t_1 + \cdots + t_{i-1}}$.

\[ \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_{d-1}} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that, for all } i \in [r], \right. \]
\[ \left. \begin{array}{l}
(i) (F_{\ell_i} \mid _{\gamma_i})_{\mathcal{Q}_d} \equiv 0 \text{ for all } 1 \leq \ell' < \ell_i \\
(ii) (F_{\ell_i} \mid _{\gamma_i})_{\mathcal{Q}_d} \neq 0 \\
(iii) T_{\mathcal{Q}_1, \ldots, \mathcal{Q}_{d-1}}^{(b_i)}(F_{\ell_i} \mid _{\gamma_i}) = \beta_i \\
(iv) \beta_i \text{ is } \mathcal{Q}_d\text{-consistent and } (F_{\ell_i} \mid _{\gamma_i})_{\mathcal{Q}_{d-1} \cup \beta_i} \equiv 1 \\
(v) q_i \text{ identifies Stars}(\mathcal{Q}_d) \text{ within Dom}(\beta_i) \cap \text{Stars}(\mathcal{Q}_{d-1}) \\
\end{array} \right] \]

By Lemma 21 and a union bound,

\[ \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d} \left[ T_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d}^{(a)}(F) \text{ exists} \right] \leq (4ep \ln m + 1)^{s}. \]

Proof. By Lemma 21 and a union bound,

\[ \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d} \left[ T_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d}^{(a)}(F) \text{ exists} \right] \leq \sum_{r, s_1, \ldots, s_r} \sum_{\ell_1, \ldots, \ell_r, \beta_1, \ldots, \beta_r, q_1, \ldots, q_r} \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that } (i) - (v) \text{ for all } i \in [r] \right]. \]

Henceforth, we fix $r, s_1, \ldots, s_r$ and bound the sum over $\ell, t, b, q$.

Let $\mathbf{x}$ be a uniform random completion of $\mathcal{Q}_d$. For each choice of $\ell, t, b, q$, we have the following key sequence of (in)equalities, which we state below and justify afterwards:

\[ \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d, \mathbf{x}} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that } (i) - (v) \text{ for all } i \in [r] \right] = 2^s \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d, \mathbf{x}} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that } (i) - (v) \text{ and } \beta_i \subseteq \mathbf{x} \text{ for all } i \in [r] \right] \]

\[ \leq 2^s \mathbb{P}_{\mathcal{Q}_1, \ldots, \mathcal{Q}_d, \mathbf{x}} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that, for all } i \in [r], \right. \]
\[ \left. \begin{array}{l}
(i') (F_{\ell_i} \mid _{\gamma_i})(\mathbf{x}) = 0 \text{ for all } 1 \leq \ell' < \ell_i \\
(ii') (F_{\ell_i} \mid _{\gamma_i})(\mathbf{x}) = 1 \\
(iii') T_{\mathcal{Q}_1, \ldots, \mathcal{Q}_{d-1}}^{(b_i)}(F_{\ell_i} \mid _{\gamma_i}) = \beta_i \\
(iv') \beta_i \subseteq \mathbf{x} \\
(v') q_i \text{ identifies Stars}(\mathcal{Q}_d) \text{ within Dom}(\beta_i) \cap \text{Stars}(\mathcal{Q}_{d-1}) \\
\end{array} \right. \]

\[ = (2p)^s(1 - p)^{(t_1 + \cdots + t_r - s)} \mu(\ell, t, b, q) \]

\[ \leq (2p)^s \mu(\ell, t, b, q) \]
where
\[
\mu(\vec{t}, \vec{b}, \vec{q}) := \mathbb{P}_{\vec{t}, \vec{b}, \vec{q} | x} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that (i')–(iv') for all } i \in [r] \right].
\]

The first equality follows from the independence of conditions (i)–(v) (which only depend on \(\varrho_1, \ldots, \varrho_d\)) and the event that \((\beta_1 \cup \cdots \cup \beta_r) \subseteq (\vec{x} \setminus \varrho_d)\) for any fixed \(\varrho_d\) in the support of \(\varrho_d\) (this event has probability \(2^{-s}\) since \((\text{Dom}(\beta_i) \cap \text{Stars}(\varrho_d)) = s_i\) for each \(i \in [r]\)). The subsequent inequality follows from the observation that conditions (i)–(v) together with \((\beta_1 \cup \cdots \cup \beta_r) \subseteq \vec{x}\) imply conditions (i')–(v'). The next equality follows from the independence of conditions (i')–(iv') and condition (v'). To see this, consider the following alternative way of generating \(\varrho_d\) and \(\vec{x}\) given \(\varrho_1, \ldots, \varrho_{d-1}\): first generate \(\vec{x}\) as a uniform random completion of \(\varrho_{d-1}\) (rather than of \(\varrho_d\)), then obtain \(\varrho_d\) from \(\vec{x}\) by randomly removing each pair \(v \mapsto x_v\) with \(v \in \text{Stars}(\varrho_{d-1})\) independently with probability \(1 - p\). The independence of conditions (i')–(iv') and condition (v') is now seen by observing that the former only depends on \(\varrho_1, \ldots, \varrho_{d-1}\) and \(\vec{x}\), while the latter only depends on \(\varrho_d\) (for any fixed \(\varrho_1, \ldots, \varrho_{d-1}, \vec{x}\) in the support of \(\varrho_1, \ldots, \varrho_{d-1}, \vec{x}\)). The probability of the latter event is precisely \(p^s(1 - p)^{(t_1 + \cdots + t_s)}\) since for each \(i \in [r]\), the set \(\text{Dom}(\beta_i) \cap \text{Stars}(\varrho_{d-1})\) contains \(t_i\) variables, of which \(\text{Stars}(\varrho_d)\) is required to include exactly the \(s_i\) variables specified by \(q_i\).

Combining the above inequalities, we have
\[
\mathbb{P}_{\varrho_1, \ldots, \varrho_d} \left[ T_{\varrho_1, \ldots, \varrho_d}(F) \text{ exists} \right] \leq (4p)^s \max_{r, \ell_1, \ldots, \ell_r} \sum_{t, \ell_1, \ldots, \ell_r} \mu(\vec{t}, \vec{b}, \vec{q}).
\]

We next turn to bounding both the individual probabilities \(\mu(\vec{t}, \vec{b}, \vec{q})\) and their sum \(\sum_{\vec{t}, \vec{b}, \vec{q}} \mu(\vec{t}, \vec{b}, \vec{q})\).

Ignoring conditions (i') and (ii'), we have
\[
\mu(\vec{t}, \vec{b}, \vec{q}) \leq \mathbb{P}_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that (iii') and (iv') for all } i \in [r] \right]
\]
\[
= \left( \frac{1}{2} \right)^{t_1 + \cdots + t_r} \mathbb{P}_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that (iii') for all } i \in [r] \right]
\]
\[
= \left( \frac{1}{2} \right)^{t_1 + \cdots + t_r} \mathbb{P}_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that, for all } i \in [r], \right.
\]
\[
\left. T_{\varrho_1, \ldots, \varrho_d}(F | (\beta_1 \circ \cdots \beta_{i-1}) \in \text{Stars}(\varrho_{d-1}) \cup \cdots \cup \text{Stars}(\varrho_{d-1})) = \beta_i \right]
\]
\[
= \left( \frac{1}{4c} \right)^{t_1 + \cdots + t_r}.
\]

The first equality follows from independence of conditions (iii') and (iv'). The second equality is a restatement of condition (iii'). The last inequality uses the hypothesis of the theorem concerning formulas \(F_1, \ldots, F_m\).

We next bound the sum \(\sum_{\vec{t}, \vec{b}, \vec{q}} \mu(\vec{t}, \vec{b}, \vec{q})\). We start out by observing that
\[
\sum_{\ell_1, \ldots, \ell_r, t_1, \ldots, t_r, s_1, \ldots, s_r, q_1, \ldots, q_r} \mathbb{P}_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_1, \ldots, \beta_r \text{ such that (i')–(v') for all } i \in [r] \right] \leq 1,
\]

since these events are mutually exclusive. To see why, consider any \(\varrho_1, \ldots, \varrho_d, \vec{x}\) in the support of \(\varrho_1, \ldots, \varrho_d, \vec{x}\) and notice that there is a unique process of uniquely determining \(\ell, \vec{t}, \vec{b}, \vec{q}\) (if any exist) such that conditions (i')–(v') hold. First, we find the unique \(\ell_1\) (if any exists) such that \(F_{\ell_1}(\vec{x}) = 1\) and \(F_{\ell'}(\vec{x}) = 0\) for all \(1 \leq \ell' < \ell_1\) (note that \(\gamma_1 = \) ). Next, let \(\beta_1\) be the unique branch of \(T_{\varrho_1, \ldots, \varrho_{d-1}}(F_{\ell_1})\) consistent with \(\vec{x}\), let \(b_1\) be the sequence of answers to the queried variable indices on this branch, and let \(t_1\) be the length of \(b_1\).

If \(F_{\ell_1}(\vec{x}) = 0\) or \(\text{Dom}(\beta_1) \cap \text{Stars}(\varrho_d) \neq s_1\), then the process fails; otherwise, let \(q_1 \in \{0, 1\}\) be the unique bitstring that identifies \(\text{Stars}(\varrho_d)\) within \(\text{Dom}(\beta_1) \cap \text{Stars}(\varrho_{d-1})\). Having uniquely determined \(\ell_1, \ell_1, b_1, q_1\), the process continues by finding the unique \(\ell_2\) (if any exists) such that \((F_{\ell_2} | q_2)(\vec{x}) = 1\) and \((F_{\ell'} | q_2)(\vec{x}) = 0\) for all \(1 \leq \ell' < \ell_1\) (note that \(\gamma_2\) is completed determined by previous data \(\beta_1, b_1, q_1\)). Continuing in this manner, we find unique \(t_2, b_2, q_2\), etc.
Note that condition (v') uniquely determines bitstrings \(q_1, \ldots, q_r\). This condition is omitted from the events in probabilities \(\mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q})\), which therefore are not mutually exclusive as the choice of \(q_i\in\{0,1\}\) is now free. However, we can restore mutual exclusivity as follows. For each \(i\in[r]\), let \(q_i^*\) range over functions associating each sequence of partial data \((\ell_1, t_1, b_1, \ldots, \ell_i, t_i, b_i)\) with an element \(q_i^*(\ell_1, t_1, b_1, \ldots, \ell_i, t_i, b_i)\in\{0,1\}\). Let

\[
\mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) := \mu(\vec{\ell}, \vec{t}, \vec{b}, (q_1^*(\ell_1, t_1, b_1), \ldots, q_r^*(\ell_1, t_1, b_1, \ldots, \ell_r, t_r, b_r))).
\]

For any choice of \(q_1^*, \ldots, q_r^*\), the events in probabilities \(\mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*)\) are mutually exclusive over \(\vec{\ell}, \vec{t}, \vec{b}\). (It is a subtle but important point that \(q_i^*\) is a function of \((\ell_1, t_1, b_1, \ldots, \ell_i, t_i, b_i)\) independent of any “future” data \(\ell_j, t_j, b_j\) for \(j > i\).) Therefore,

\[
\sum_{\ell_1, \ldots, \ell_r, \ell_1, \ldots, \ell_r, b_1, \ldots, b_r} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) \leq 1.
\]

We now have the bound

\[
\sum_{\ell_1, \ldots, \ell_r, \ell_1, \ldots, \ell_r, b_1, \ldots, b_r} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) \leq \sum_{\ell_1, \ell_1, b_1} \left( \frac{t_1}{s_1} \right) \max_{\ell_r, \ell_r, b_r} \sum_{\ell_r, \ell_r, b_r} \left( \frac{t_r}{s_r} \right) \max_{\ell_r, \ell_r, b_r} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*)
\]

\[
= \max_{q_1^*, \ldots, q_r^*} \sum_{\ell_1, \ell_1, b_1} \left( t_1 \right) \max_{\ell_r, \ell_r, b_r} \sum_{\ell_r, \ell_r, b_r} \left( t_r \right) \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*)
\]

\[
\leq \max_{q_1^*, \ldots, q_r^*} e^s \left( \frac{1}{s} \ln \left( \sum_{\ell_1, \ell_1, \ell_1, \ell_1, b_1, \ldots, b_r} e^{(t_1 + \cdots + t_r)} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) \right) + 1 \right)^s
\]

where the final inequality is by Lemma [12].

We next have \(\sum_{\ell, \ell, \ell, \ell, b} e^{(t_1 + \cdots + t_r)} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) \leq m^s\) as follows:

\[
\sum_{\ell_1, \ldots, \ell_r, \ell_1, \ldots, \ell_r, b_1, \ldots, b_r} e^{(t_1 + \cdots + t_r)} \mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}^*) \leq \sum_{\ell_1, \ldots, \ell_r, \ell_1, \ldots, \ell_r, b_1, \ldots, b_r} \left( \frac{1}{4} \right)^{t_1 + \cdots + t_r}
\]

\[
\leq \sum_{\ell_1, \ldots, \ell_r, t_1, \ldots, t_r, b_1, \ldots, b_r} \left( \frac{1}{4} \right)^t \sum_{t_1 + \cdots + t_r = t} 1
\]

\[
= \sum_{\ell_1, \ldots, \ell_r, t_1, \ldots, t_r} \left( \frac{1}{2} \right)^t \left( \frac{r - 1}{e} \right)
\]

\[
= \sum_{\ell_1, \ldots, \ell_r} 1 = m^r \leq m^s.
\]

The first inequality uses our bound \(\mu(\vec{\ell}, \vec{t}, \vec{b}, \vec{q}) \leq (1/8e)^{(t_1 + \cdots + t_r)}\) (which holds for any \(q_1, \ldots, q_r\), including \(q_i^*(\ell_1, t_1, b_1)\)). The first equality is due to the fact that there are \(t_1 + \cdots + t_r\) choices for integers \(t_1, \ldots, t_r \geq 1\) such that \(t_1 + \cdots + t_r = t\), and there are \(2^t\) choices for each bitstring \(b_1 \in \{0,1\}^t\). The second equality uses Lemma [9]. Finally, we use the fact that \(r \leq s\) since \(s_1, \ldots, s_r \geq 1\) are integers such that \(s_1 + \cdots + s_r = s\).

Putting together these inequalities, we get the desired bound

\[
P_{\varphi_1, \ldots, \varphi_d} \left[ \mathcal{T}_{\varphi_1, \ldots, \varphi_d}^{(a)}(F) \text{ exists} \right] \leq (4e\ln m + 1)^8.
\]
6 Serial depth-\(d\) switching lemma

We would like to prove Theorem 3 (our upper bound on the criticality of regular AC\(^0\) formulas) by applying Proposition 22 ("depth-\(d\) switching lemma") to each layer of a regular AC\(^0\) formula. Unfortunately, there is a mismatch between the hypothesis and the conclusion of Proposition 22: the hypothesis applies to a sequence of depth \(d - 1\) formulas, while the conclusion applies to single depth-\(d\) formula (and cannot therefore serve as the hypothesis for a depth \(d + 1\) formula).

In this section, we prove an extension of Proposition 22 which we require for Theorem 3. We call this result, Proposition 23, the "serial depth-\(d\) switching lemma", since it explore the canonical decision trees of a sequence of depth-\(d\) formulas \(F_1, \ldots, F_k\) in order. For integers \(s_1, \ldots, s_k \geq 1\) and bitstrings \(a_h \in \{0, 1\}^{s_h}\) \((h \in [k])\), we would like to bound the event that \(T_{\theta_1, \ldots, \theta_d}(F_1)\) has an \(a_1\)-branch, call it \(\alpha_1\), and that \(T_{\theta_1, \ldots, \theta_d}(F_2\|_{a_1})\) has an \(a_2\)-branch \(\alpha_2\), etc., and finally that \(T_{\theta_1, \ldots, \theta_d}(F_k\|_{a_1 \circ \cdots \circ a_{k - 1}})\) has an \(a_k\)-branch \(\alpha_k\).

However, in order for the conclusion of Proposition 22 to match the hypothesis, we need to consider a more general event where, instead of considering \(T_{\theta_1, \ldots, \theta_d}(F_k\|_{a_1 \circ \cdots \circ a_{k - 1}})\) in the \(h\)th stage, we instead apply the restriction \((a_1 \circ \cdots \circ a_{h - 1}) \leftarrow_{\text{Stars}(\theta_d)} c_h\) (overwriting \(a_1 \circ \cdots \circ a_{h - 1}\) on all previously queried variables) where \(c_h \in \{0, 1\}^{s_1 + \cdots + s_{h - 1}}\) is an arbitrary bitstring. Although this makes notation in Proposition 22 slightly more cumbersome, the probabilistic main argument is nearly identical to Proposition 22.

**Notation 23.** In what follows, we will consider integers \(k \geq 1\) and \(r_1, \ldots, r_k \geq 1\) and various indexed families \(\vec{w} = \{w_{h,i}\}_{h \in [k], i \in [r_h]}\). It is often convenient to regard \(\vec{w}\) as a sequence of length \(r_1 + \cdots + r_k\):

\[
\vec{w} = \langle w_{1,1}, \ldots, w_{1,r_1}, \ldots, w_{h,1}, \ldots, w_{h,r_h} \rangle.
\]

For \(h \in [k]\) and \(i \in [r_h + 1]\), notation "\(w_{1,1}, \ldots, w_{h,i-1}\)" shall refer to the initial subsequence of length \(r_1 + \cdots + r_{h-1} + i - 1\):

\[
\langle w_{1,1}, \ldots, w_{h,i-1} \rangle = \langle w_{1,1}, \ldots, w_{1,r_1}, \ldots, w_{h-1,1}, \ldots, w_{h-1,r_{h-1}}, w_{h,i}, \ldots, w_{h,i-1} \rangle.
\]

For example, if \(w_{h,i}\) are integers (or bitstrings, ordered restrictions, etc.), we will write "\(w_{1,1} + \cdots + w_{h,i-1}\)" (or "\(w_{1,1} \circ \cdots \circ w_{h,i-1}\)"") for the sum (or composition) of the first \(r_1 + \cdots + r_{h-1} + i - 1\) elements of \(\vec{w}\).

The following lemma plays the same role in Proposition 23 as Lemma 21 does in Proposition 22.

**Lemma 24.** Let \(F_1, \ldots, F_k\) be depth-\(d\) formulas where \(F_h = \text{OR}(F_{h,1}, \ldots, F_{h,m})\) for each \(h \in [k]\). Let \(\varrho_1 \subseteq \cdots \subseteq \varrho_d\) be restrictions. Let \(s_1, \ldots, s_k \geq 1\) and let \(a_h \in \{0, 1\}^{s_h}\) and \(c_h \in \{0, 1\}^{s_1 + \cdots + s_{h-1}}\) for each \(h \in [k]\). Suppose there exist ordered restrictions \(\alpha_1, \ldots, \alpha_k\) such that, for all \(h \in [k]\),

\[
T_{\theta_1, \ldots, \theta_d}(F_h\|_{(a_1 \circ \cdots \circ a_{h-1}) \leftarrow_{\text{Stars}(\theta_d)} c_h}) = \alpha_h.
\]

Then there exist

- integers \(r_h \in [s_h]\) and \(s_{h,1}, \ldots, s_{h,r_h} \geq 1\) with \(s_{h,1} + \cdots + s_{h,r_h} = s_h\) for each \(h \in [k]\),
- integers \(1 \leq \ell_{h,1} < \cdots < \ell_{h,r_h} \leq m\) for each \(h \in [k]\),
- integers \(t_{h,i} \geq s_{h,i}\) and bitstrings \(b_{h,i} \in \{0, 1\}^{t_{h,i}}\) and \(q_{h,i} \in \{0, 1\}^{s_{h,i}}\) for each \(h \in [k]\) and \(i \in [r_h]\)

with the property that there exist unique ordered restrictions \(\beta_{1,1}, \ldots, \beta_{h,r_h}\) such that, for all \(h \in [k]\) and \(i \in [r_h]\),

1. \((F_{h,l'}\|_{\gamma_{h,i}})\|_{\varrho_d} \equiv 0\) for all \(1 \leq l' < \ell_{h,i}\),
2. \((F_{h,\ell_{h,i}}\|_{\gamma_{h,i}})\|_{\varrho_d} \neq 0,
3. \(T_{\theta_1, \ldots, \theta_d-l}(F_{h,\ell_{h,i}}\|_{\gamma_{h,i}}) = \beta_{h,i},\n4. \beta_{h,i}\) is \(\varrho_d\)-consistent and \((F_{h,\ell_{h,i}}\|_{\gamma_{h,i}})\|_{\varrho_{d-1} \cup \beta_{h,i}} \equiv 1.\)
(v) \(^{\text{“}q_{h,i} \text{ identifies Stars}(\varrho_d) \text{ within } \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_{d-1})^{\text{“}}\text{ in the following sense: for all } j \in [t_{h,i}],\)
\[ q_{h,i,j} = 1 \iff \text{Stars}(\varrho_d) \text{ contains the } j^{\text{th}} \text{ variable of } \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_{d-1}) \text{ in the order given by } \beta_{h,i}. \]

where
\[ \gamma_{h,i} := (\beta_{1,1} \circ \cdots \circ \beta_{h,i-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ d_{h,i}, \]
\[ d_{h,i} := (b_{1,1} \circ \cdots \circ b_{h,i-1}) \leftarrow q_{1,1} \circ \cdots \circ q_{h,i-1} \ (c_h \circ (a_{h,1}, \ldots, a_{h,s,h,1+\cdots+s_{h-1}})). \]

(Note that conditions (iii) and (v) imply that \( \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_{d-1}) = t_{h,i} \) and \( \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_d) = s_{h,i} \) and \( \gamma_{h,i} = (\beta_{1,1} \circ \cdots \circ \beta_{h,i-1}) \leftarrow \text{Stars}(\varrho_d) \ (c_h \circ (a_{h,1}, \ldots, a_{h,s,h,1+\cdots+s_{h-1}})). \))

Proof. Straightforward from Definition \[16\] \( \square \)

**Proposition 25** ("Serial depth-\( d \) switching lemma"). Let \( k, m \geq 1 \), let \( F_1, \ldots, F_k \) be depth-\( d \) formulas where \( F_h = \text{OR}(F_{h,1}, \ldots, F_{h,m}) \) for each \( h \in [k] \). Suppose \( \varrho_1 \subseteq \cdots \subseteq \varrho_{d-1} \) are random restrictions such that, for all \( r_1, \ldots, r_k \geq 1 \) and \( 1 \leq \ell_{h,1} < \cdots < \ell_{h,r_h} \leq m \) and \( t_{h,i} \geq 1 \) and \( b_{h,i} \in \{0,1\}^{h-1} \) and \( a_{h,i} \in \{0,1\}^{h-1} \) \( h \in [k] \) and \( i \in [r_h] \),
\[ \Pr_{\varrho_1, \ldots, \varrho_{d-1}} \left[ \exists \beta_{1,1}, \ldots, \beta_{k,k} \right. \prod_{h \in [k]} \left( \bigwedge_{i \in [r_h]} \left( \text{Stars}(\varrho_{d-1}) \ (\beta_{1,1} \circ \cdots \circ \beta_{h,i-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ d_{h,i} \right) = \beta_{h,i} \right) \right] \leq \left( \frac{1}{2e} \right)^{t_{1,1} + \cdots + t_{h,r_h}}.
\]

Then for all integers \( s_1, \ldots, s_k \geq 1 \) and bitstrings \( a_h \in \{0,1\}^{s_h} \) and \( c_h \in \{0,1\}^{s_1+\cdots+s_{h-1}} \) \( h \in [k] \) and \( p \in [0,1] \), letting \( \varrho_d \) be a \( p \)-random refinement of \( \varrho_{d-1} \), we have
\[ \Pr_{\varrho_1, \ldots, \varrho_d} \left[ \exists \alpha_1, \ldots, \alpha_k \prod_{h \in [k]} \left( \bigwedge_{i \in [r_h]} \left( \text{Stars}(\varrho_{d-1}) \ (\alpha_{1,1} \circ \cdots \circ \alpha_{h-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ c_h \right) = \alpha_{h,i} \right) \right] \leq \left( 4ep(\ln m + 1) \right)^{s_1+\cdots+s_k}.
\]

Note that Proposition 22 is precisely the special case \( k = 1 \) of Proposition 25. The following proof closely parallels the proof of Proposition 22 (with a few more indices to keep track of). We omit the justifications of certain (in)equalities that would be redundant.

Proof. Fix \( s_1, \ldots, s_k \) and \( a_1, \ldots, a_k \) and \( c_1, \ldots, c_k \) and \( p \), and let \( s := s_1 + \cdots + s_k \).

Let \( \tilde{r} = \{ r_h \} \) and \( \tilde{s} = \{ s_h \} \) and \( \tilde{t} = \{ t_{h,i} \} \) and \( \tilde{t}' = \{ t_{h,i}' \} \) and \( \tilde{b} = \{ b_{h,i} \} \) and \( \tilde{q} = \{ q_{h,i} \} \) (where \( h \in [k] \) and \( i \in [r_h] \)) range over data satisfying the bullet items of Lemma 24 We have
\[ \Pr_{\varrho_1, \ldots, \varrho_{d-1}} \left[ \exists \alpha_1, \ldots, \alpha_k \prod_{h \in [k]} \left( \bigwedge_{i \in [r_h]} \left( \text{Stars}(\varrho_{d-1}) \ (\alpha_{1,1} \circ \cdots \circ \alpha_{h-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ c_h \right) = \alpha_{h,i} \right) \right] \leq \sum_{\tilde{r}, \tilde{s}, \tilde{t}, \tilde{t}', \tilde{b}, \tilde{q}} \Pr_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_{1,1}, \ldots, \beta_{k,k} \right. \prod_{h \in [k]} \left( \bigwedge_{i \in [r_h]} \left( \text{Stars}(\varrho_{d-1}) \ (\beta_{1,1} \circ \cdots \circ \beta_{h,i-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ d_{h,i} \right) = \beta_{h,i} \right) \right]
\]
\[ \leq \sum_{\tilde{r}, \tilde{s}, \tilde{t}, \tilde{t}', \tilde{b}, \tilde{q}} \Pr_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_{1,1}, \ldots, \beta_{k,k} \text{ such that } \begin{cases} (i) \ (F_h, t'_{h,i}[\gamma_{h,i}])_{\varrho_d} = 0 \text{ for all } 1 \leq \ell' < t_{h,i} \\ (ii) \ (F_h, t_{h,i}[\gamma_{h,i}])_{\varrho_d} \neq 0 \\ (iii) \ T_{\varrho_1, \ldots, \varrho_{d-1}}(F_h, t_{h,i}[\gamma_{h,i}]) = \beta_{h,i} \\ (iv) \ \beta_{h,i} \text{ is } \varrho_{d-1}\text{-consistent and } (F_h, t_{h,i}[\gamma_{h,i}])_{\varrho_{d-1} \cup \beta_{h,i}} = 1 \\ (v) \ q_{h,i} \text{ identifies Stars}(\varrho_{d-1}) \text{ within } \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_{d-1}) \text{ where } \gamma_{h,i} = (\beta_{1,1} \circ \cdots \circ \beta_{h,i-1}) \leftarrow \text{Stars}(\varrho_{d-1}) \ d_{h,i}, \ d_{h,i} := (b_{1,1} \circ \cdots \circ b_{h,i-1}) \leftarrow q_{1,1} \circ \cdots \circ q_{h,i-1} \ (c_h \circ (a_{h,1}, \ldots, a_{h,s,h,1+\cdots+s_{h-1}})) \end{cases} \right]
\]
\[ \leq 2^s \max_{\tilde{r}, \tilde{s}} \sum_{\tilde{t}, \tilde{t}', \tilde{b}, \tilde{q}} \Pr_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_{1,1}, \ldots, \beta_{k,k} \text{ such that } (i)-(v) \text{ for all } h \in [k] \text{ and } i \in [r_h] \right]. \]
Letting \( \mathbf{x} \) be a uniform random completion of \( \varrho_d \), we have

\[
P_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that (i)--(v) for all } h \in [k] \text{ and } i \in [r_h] \right]
= 2^s \sum_{\varrho_1, \ldots, \varrho_d, \mathbf{x}} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that (i)--(v) and } \beta_{h,i} \subseteq \mathbf{x} \text{ for all } h \in [k] \text{ and } i \in [r_h] \right]
\leq 2^s \sum_{\varrho_1, \ldots, \varrho_d, \mathbf{x}} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that, for all } h \in [k] \text{ and } i \in [r_h],
(i') \quad (F_{h,i} \mid \gamma_{h,i})(x) = 0 \text{ for all } 1 \leq i' < \ell_{h,i},
(ii') \quad (F_{h,i} \mid \gamma_{h,i})(x) = 1
(iii') \quad \tau^{(b_{h,i})}_{\varrho_1, \ldots, \varrho_{d-1}}(F_{h,i} \mid \gamma_{h,i}) = \beta_{h,i}
(iv') \quad \beta_{h,i} \subseteq \mathbf{x}
(v') \quad q_{h,i} \text{ identifies } \text{Stars}(\varrho_d) \text{ within } \text{Dom}(\beta_{h,i}) \cap \text{Stars}(\varrho_{d-1})
\right]
\leq (2p)^s (1 - p)^{(t_1 + \cdots + t_k, s)} \mu(\tilde{\ell}, \tilde{t}, \tilde{b}, \tilde{q})
\]

where

\[
\mu(\tilde{\ell}, \tilde{t}, \tilde{b}, \tilde{q}) := \sum_{\varrho_1, \ldots, \varrho_d, \mathbf{x}} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that (i')--(iv') for all } h \in [k] \text{ and } i \in [r_h] \right]
\]

Ignoring conditions (i') and (ii'), we have

\[
\mu(\tilde{\ell}, \tilde{t}, \tilde{b}, \tilde{q}) \leq \sum_{\varrho_1, \ldots, \varrho_d, \mathbf{x}} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that (i)'} \text{ and (iv')} \text{ for all } h \in [k] \text{ and } i \in [r_h] \right]
= \left( \frac{1}{2} \right)^{t_1 + \cdots + t_k, r_k} \sum_{\varrho_1, \ldots, \varrho_d} \left[ \exists \beta_{1, \ldots, \beta_{k,r_k}} \text{ such that (i)'} \text{ for all } h \in [k] \text{ and } i \in [r_h] \right]
\leq \left( \frac{1}{2} \right)^{t_1 + \cdots + t_k, r_k}
\]

For each \( h \in [k] \) and \( i \in [r_h] \), let \( q^{t_{h,i}}_{\varrho,i} \) range over functions associating each sequence \((\ell_{1,1}, t_{1,1}, b_{1,1}, \ldots, \ell_{h,i}, t_{h,i}, b_{h,i})\) with an element \( q^*_{h,i}(\ell_{1,1}, t_{1,1}, b_{1,1}, \ldots, q^*_{k,r_k}(\ell_{1,1}, t_{1,1}, b_{1,1}, \ldots, \ell_{k,r_k}, t_{k,r_k}, b_{k,r_k})) \).
For every choice of $q_1^k, \ldots, q^k_{r_k}$, we have $\sum_{\ell, t, b} \mu(\ell, \bar{t}, \bar{b}, \bar{q}^*) \leq 1$. Therefore, using Lemma 9,

$$
\sum_{\ell, t, b, \bar{q}} \mu(\ell, \bar{t}, \bar{b}, \bar{q}) \leq \sum_{\ell_1, \bar{t}_1, \bar{b}_1} \left( t_{1, 1} \max \cdots \max \right)_{q_1, 1} \sum_{t_{k, r_k}, \bar{t}_{k, r_k}, \bar{b}_k, r_k} \left( t_{k, r_k} \right)_{s_k, r_k} \mu(\ell, \bar{t}, \bar{b}, \bar{q})
$$

$$
= \max_{\bar{q}^*} \sum_{\ell, t, b} \left( t_{1, 1} \cdots t_{k, r_k} \right) \mu(\ell, \bar{t}, \bar{b}, \bar{q}^*)
$$

$$
\leq \max_{\bar{q}^*} \sum_{\ell, t, b} \left( t_{1, 1} + \cdots + t_{k, r_k} \right) \mu(\ell, \bar{t}, \bar{b}, \bar{q}^*)
$$

$$
\leq \max_{\bar{q}^*} e^s \left( \frac{1}{s} \ln \left( \sum_{\ell, t, b} e^{(t_{1, 1} + \cdots + t_{k, r_k})} \mu(\ell, \bar{t}, \bar{b}, \bar{q}^*) \right) + 1 \right)^s.
$$

Finally, we have

$$
\sum_{\ell, t, b} e^{(t_{1, 1} + \cdots + t_{k, r_k})} \mu(\ell, \bar{t}, \bar{b}, \bar{q}^*) \leq \sum_{\ell, t, b} \left( \frac{1}{4} \right)^{t_{1, 1} + \cdots + t_{k, r_k}}
$$

$$
\leq \sum_{\ell} \sum_{t=r_1 + \cdots + r_k}^{\infty} \left( \frac{1}{4} \right)^t \sum_{t_{1, 1} + \cdots + t_{k, r_k} = t} 1
$$

$$
= \sum_{\ell} \sum_{t=r_1 + \cdots + r_k}^{\infty} \left( \frac{1}{2} \right)^t \left( r_1 + \cdots + r_k - 1 \right)
$$

$$
= \sum_{\ell} 1 = \left( \frac{m}{r_1} \right) \cdots \left( \frac{m}{r_k} \right) \leq m^{r_1 + \cdots + r_k} \leq m^s.
$$

Putting together these inequalities, we get the desired bound

$$
P_{\varrho_1, \ldots, \varrho_d} \left[ \exists \alpha_1, \ldots, \alpha_k \wedge \left( T_{\varrho_1, \ldots, \varrho_d}^{(\alpha_k)}(F_h |_{(\alpha_1 \circ \cdots \circ \alpha_{h-1}) \leftarrow \text{Stars}(\varrho_h)_{c_h}}) = \alpha_h \right) \right] \leq (4ep \ln m + 1)^s.
$$

\[\square\]

\section{Proof of Theorem 3}

The following lemma is required for the analysis of depth-1 subformulas in the proof of Theorem 3.

\textbf{Lemma 26.} Let $\varrho$ be a $p$-random restriction. Let $F_1, \ldots, F_k$ be depth-1 formulas, let $s_1, \ldots, s_k \geq 1$, and let $a_h \in \{0, 1\}^{s_h}$ and $c_h \in \{0, 1\}^{s_1 + \cdots + s_h - 1}$ for each $h \in [k]$. Then

$$
P_{\varrho} \left[ \exists \alpha_1, \ldots, \alpha_k \wedge \left( T_{\varrho}^{(\alpha_k)}(F_h |_{(\alpha_1 \circ \cdots \circ \alpha_{h-1}) \leftarrow \text{Stars}(\varrho)_{c_h}}) = \alpha_h \right) \right] \leq (2p)^{s_1 + \cdots + s_k}.
$$

\textbf{Proof.} Assume $F_1 |_{\varrho}$ computes a non-constant function, since otherwise $T_{\varrho}^{(\alpha_1)}(F_1)$ does not exist (note that $\alpha_1 = ()$). Let $V_1$ be the set of variable indices occurring in literals of $F_1$. Observe that $T_{\varrho}^{(\alpha_1)}(F_1)$ exists if, and only if, $|V_1 \cap \text{Stars}(\varrho)| = s_1$ and $\varrho$ gives the unique assignment to variables in $V_1 \cap \text{Dom}(\varrho)$ such that $F_1 |_{\varrho}$ is non-constant. This happens with probability $\left( \frac{|V_1|}{s_1} \right) p^{s_1} \left( \frac{1-p}{2} \right)^{|V_1| - s_1}$, which is at most $(2p)^{s_1}$. Also note that this event only depends $\varrho |_{V_1}$ (i.e., the partial function $\varrho$ restricted to $\text{Dom}(\varrho) \cap V_1$). If this event holds, then we have $T_{\varrho}^{(\alpha_1)}(F_1) = \alpha_1$ for the unique ordered restriction $\alpha_1$ with $\text{Dom}(\alpha_1) = V_1 \cap \text{Stars}(\varrho)$ whose values are given by $a_1$. 

17
Next let $F'_2 := F_2 \mid_{\alpha_1 \leftarrow \text{Stars}(F_1) \cap}$ and assume that $F'_2 \mid_{\varrho}$ computes a non-constant function, since otherwise $T_{\varrho}^{(a_2)}(F'_2)$ does not exist. Let $V_2$ be the set of variable indices occurring in literals of $F'_2$, and note that $V_1 \cap V_2 = \emptyset$. Observe that $T_{\varrho}^{(a_2)}(F'_2)$ exists if, and only if, $|V_2 \cap \text{Stars}(\varrho)| = s_2$ and $\varrho$ gives the unique assignment to variables in $V_2 \cap \text{Dom}(\varrho)$ such that $F'_2 \mid_{\varrho}$ is non-constant. Conditioned on the value of $\varrho \mid_{V_1}$, this second event happens with probability $(|V_2|) p^{s_2} (\frac{1 - p}{2})^{|V_2| - s_2}$, which is at most $(2p)^{s_2}$. Moreover, this second event only depends on $\varrho \mid_{V_2}$.

Continuing in this manner, we conclude that the event in question holds with probability at most $(2p)^{s_1 + \cdots + s_k}$.

**Proof of Theorem 3.** Let $F$ be a regular formula of depth $d + 1$ and size $s$. For $i \in \{2, \ldots, d + 1\}$, let $m_i$ be the top fan-in of depth-$i$ subformulas of $F$. Let

$$\lambda := \prod_{i=2}^{d+1} 8e^2 (\ln m_i + 1).$$

Note that $s = m_2 \cdots m_{d+1}$ and therefore by Lemma 11

$$\lambda \leq (8e^2)^d \left( \frac{1}{d} \ln s + 1 \right).$$

We claim that $F$ is $\lambda$-critical. To see this, consider any $p \in [0, \frac{1}{2}]$. Let $\varrho_1 \subseteq \cdots \subseteq \varrho_{d+1}$ be a sequence of random restrictions where

- $\varrho_1$ is a $\frac{1}{4e}$-random restriction,
- $\varrho_i$ is a $\frac{1}{8e^2(\ln m_i + 1)}$-random refinement of $\varrho_i$ for each $i \in \{2, \ldots, d\}$,
- $\varrho_{d+1}$ is a $\frac{p\lambda}{16e(\ln m_{d+1} + 1)}$-random refinement of $\varrho_d$.

Note that $\varrho_{d+1}$ is a $p$-random restriction.

For all integers $k \geq 1$ and $s_1, \ldots, s_k \geq 1$ and bitstrings $a_h \in \{0, 1\}^{s_h}$ and $c_h \in \{0, 1\}^{s_1 + \cdots + s_{h-1}}$ ($h \in [k]$), we have:

- for all depth-1 subformulas $F_1, \ldots, F_k$ of $F$, Lemma 26 implies
  $$\mathbb{P}_{\varrho_1} \left[ \exists \alpha_1, \ldots, \alpha_k \right. \bigwedge_{h \in [k]} \left( T_{\varrho_1}^{(a_h)}(F_h \mid_{(\alpha_1 \circ \cdots \alpha_{h-1}) \leftarrow \text{Stars}(\varrho_1) \cap c_h}) = \alpha_h \right) \bigg] \leq \left( \frac{1}{2e} \right)^{s_1 + \cdots + s_k},$$
- for all $i \in \{2, \ldots, d\}$ and depth-$i$ subformulas $F_1, \ldots, F_k$ of $F$, Proposition 25 implies
  $$\mathbb{P} \left[ \exists \alpha_1, \ldots, \alpha_k \right. \bigwedge_{h \in [k]} \left( T_{\varrho_i \cdots \varrho_i}^{(a_h)}(F_h \mid_{(\alpha_1 \circ \cdots \alpha_{h-1}) \leftarrow \text{Stars}(\varrho_i) \cap c_h}) = \alpha_h \right) \bigg] \leq \left( \frac{1}{2e} \right)^{s_1 + \cdots + s_k},$$
- finally, Proposition 22 (or Proposition 23) implies
  $$\mathbb{P} \left[ \exists \alpha_1 \right. \bigwedge_{\varrho_1, \ldots, \varrho_{d+1}} \left( T_{\varrho_1 \cdots \varrho_{d+1}}^{(a_1)}(F) \right. \text{ exists} \right] \leq \left( \frac{p\lambda}{4} \right)^{s_1}.$$
Therefore, for all $t \geq 1$, we have
\[
P \left[ \text{DT}_{\text{depth}}(F|R_p) \geq t \right] \leq \sum_{u=t}^{\infty} P \left[ \mathcal{T}^{(a)}_{\varrho_1,\ldots,\varrho_{d+1}}(F) \text{ has depth } u \right]
\leq \sum_{u=t}^{\infty} \sum_{a \in \{0,1\}^u} P \left[ \mathcal{T}^{(a)}_{\varrho_1,\ldots,\varrho_{d+1}}(F) \text{ exists } \right]
\leq \sum_{u=t}^{\infty} 2^u \left( \frac{p \lambda}{4} \right)^u \leq (p \lambda)^t.
\]
This shows that $F$ is $\lambda$-critical, and since $\lambda = O\left(\frac{1}{\varepsilon} \log s\right)^d$, the theorem is proved. 

\section{Satisfiability algorithms}

The next theorem gives a randomized #SAT algorithm for regular $AC^0$ formulas. For $AC^0$ circuits of size $\Omega(n^2)$ (after converting to regular formulas), this matches the runtime of the #SAT algorithm of Impagliazzo, Matthews and Paturi \cite{IMP}.

\begin{theorem}
There is a randomized, zero-error algorithm which, given a regular $AC^0$ formula $F$ of depth $d+1$ and size $s$ on $n$ variables, outputs a decision tree for $F$ of size $O(sn \cdot 2^{(1-\varepsilon)n})$ where $\varepsilon = 1/O(\frac{1}{\varepsilon} \log s)^d$.

This algorithm also solves the #SAT problem, that is, it counts the number of satisfying assignments for $F$.

\end{theorem}

\begin{proof}
First we require a lemma that $|\mathcal{T}_{\varrho_1,\ldots,\varrho_d}(F)| \leq |\mathcal{T}_{\varrho_1,\ldots,\varrho_d}(F)|$ for any depth-$d$ formulas $F$, restrictions $\varrho_1 \subseteq \cdots \subseteq \varrho_d$ and $\varrho_d$-consistent restriction $\gamma$. This is straightforward from Definition \ref{def:gamma-consistent} of $\mathcal{T}_{\varrho_1,\ldots,\varrho_d}(\cdot)$, but requires a careful argument (by induction on a stronger statement) to make precise. We omit the details.

Accepting this claim, we can extract from Definition \ref{def:gamma-consistent} an algorithm which, given any depth-$d$ formula $F$ and restrictions $\varrho_1 \subseteq \cdots \subseteq \varrho_d$, computes the set $\mathcal{T}_{\varrho_1,\ldots,\varrho_d}(F)$ in time $O(n) \cdot \sum_{i=1}^{d} \sum_{|\varrho_i|} |\mathcal{T}_{\varrho_1,\ldots,\varrho_i}(F_i)|$ where $F_i$ ranges over depth-$i$ subformulas of $F$.

If we are now given a regular $AC^0$ formula $F$ of depth $d+1$ and size $s$ on $n$ variables, we can compute a decision tree for $F$ as follows. Consider any sets $D_1 \subseteq \cdots \subseteq D_{d+1} \subseteq [n]$ and let $D := D_{d+1}$. We get a decision tree for $F$ by querying all variables in $D$, receiving answers $\varrho : D \to \{0,1\}$, and then proceeding as the decision tree $\mathcal{T}(\varrho_1,\ldots,\varrho_{d+1})(F)$ where $\varrho_i$ is the restriction of $\varrho$ to domain $D_i$. The time required to construct this decision tree is $O(n) \cdot \sum_{i=1}^{d+1} \sum_{|\varrho_i|} |\mathcal{T}_{\varrho_1,\ldots,\varrho_i}(F_i)|$. If $\varrho$ is a uniform random restriction with domain $D$ and $|D| \leq (1-\varepsilon)n$ (for a choice of $\delta > 0$ to be determined), then this bound is $O(n \cdot 2^{(1-\delta)n}) \cdot \sum_{i=1}^{d+1} \sum_{|\varrho_i|} E |\mathcal{T}_{\varrho_1,\ldots,\varrho_i}(F_i)|$.

Let us now randomly generate sets $D_1 \subseteq \cdots \subseteq D_{d+1} \subseteq [n]$ as follows:

- $D_1$ is a $1 - \frac{1}{8\varepsilon}$-random subset of $[n]$ (i.e., $D_1$ includes each variable index in $[n]$ independently with probability $1 - \frac{1}{8\varepsilon}$),

- for each $i \in \{2, \ldots, d+1\}$, $D_i$ is the union of $D_{i-1}$ and a $1 - \frac{1}{8\varepsilon^i(ln m_i + 1)}$-random subset of $[n] \setminus D_{i-1}$ where $m_i$ is the top fan-in of depth-$i$ subformulas of $F$ (equivalently: $[n] \setminus D_i$ is a $1 - \frac{1}{8\varepsilon^i(ln m_i + 1)}$-random subset of $[n] \setminus D_{i-1}$).

Note that $D := D_{d+1}$ is a $(1 - \frac{1}{8\varepsilon})$-random subset of $[n]$ where $\lambda = O\left(\frac{1}{\varepsilon} \log s\right)^d$. The proof of Theorem \ref{thm:randomized-sat} shows that, for every $i \in [d+1]$ and depth-$i$ subformula $F_i$,
\[
E |\mathcal{T}_{\varrho_1,\ldots,\varrho_i}(F_i)| = \sum_{t=0}^{\infty} \sum_{a \in \{0,1\}^t} P \left[ \mathcal{T}^{(a)}_{\varrho_1,\ldots,\varrho_i}(F_i) \text{ exists } \right] \leq 1 + \sum_{t=1}^{\infty} 2^t (1/2e)^t = \frac{1}{1 - (1/e)}.
\]

We may assume that $\lambda \leq n/2$, since otherwise the theorem is trivial. We then have $P \left[ |D| \leq (1 - \frac{1}{8\varepsilon})n \right]$ with probability $\Omega(1)$ (and in fact $1-o(1)$ when $\lambda \ll n$). It follows that, with at least this probability, our algorithm constructs a decision tree for $F$ in time $O(sn \cdot 2^{(1-\varepsilon)n})$.
\end{proof}
As a corollary, we improve the parameters of an algorithm of Santhanam and Williams [14] for the satisfiability problem for $q$-QB-CNF and $q$-QB-DNF, the class of quantified CNF and DNF formulas with $q$ quantifier blocks (i.e., $q$ quantifier alternations).

Corollary 28. Satisfiability of $q$-QB-CNF (resp. $q$-QB-DNF) with $n$ variables and poly($n$) clauses (resp. disjuncts) can be solved probabilistically with zero error in time $\text{poly}(n) \cdot 2^{n-O(qn^{1/(q+1)})+O(q)}$.

The proof of Corollary 28 is adapted straightforwardly from [14], using Theorem 27 in place of the AC$^0$-circuit satisfiability algorithm of Impagliazzo, Matthews and Paturi [7]. Corollary 28 extends from $o(\log n \log \log n)$ to $o(\log n)$ the range of $q$ for which the algorithm of [14] beats exhaustive search (i.e., poly($n$) time). We remark that a second algorithm in [14] running time $\text{poly}(n) \cdot 2^{n-\Omega(q)}$, which beats exhaustive search when $q = \omega(\log n)$. The range of $q$ where $q$-QB-CNF and $q$-QB-DNF is not known to beat exhaustive search by a factor of at least $n^k$ is therefore reduced to between $c_1 \log n$ and $c_2 \log n$ for constants $c_1(k) < c_2(k)$.

9 Open questions

It is an open problem to remove the assumption of regularity in Theorem 3.

Conjecture 29. All (not necessarily regular) AC$^0$ formulas of depth $d+1$ and size $s$ have criticality at most $O(\frac{1}{d} \log s)^d$.

Since $\deg(f) \leq DT_{\text{depth}}(f)$ for all boolean functions $f$, it follows that $\lambda$-criticality implies $\lambda$-degree-criticality, that is, the bound $\mathbb{P}[\deg(f \mid R_p) \geq t] \leq (p\lambda)^t$. One can ask whether a converse is true.

Question 30. Does degree-criticality $\lambda$ imply criticality $O(\lambda)$?

Tal [16] showed that DeMorgan formulas of size $L$ have degree-criticality $O(\sqrt{L})$. As a special case of Question 30, one can ask:

Question 31. Do DeMorgan formulas of size $L$ have criticality $O(\sqrt{L})$?

Finally, we ask a question that would potentially yield a much simpler and more aesthetic proof of Theorem 3. We will say that a boolean function $f$ is hereditarily $\lambda$-critical if every subfunction of $f$ is $\lambda$-critical (i.e., $f \mid _\varrho$ is $\lambda$-critical for every restriction $\varrho$).

Question 32. Suppose $f$ is the disjunction of boolean functions $f_1 \lor \cdots \lor f_m$ where each $f_i$ is hereditarily $\lambda$-critical. Is $f$ necessarily $O(\lambda \ln(n+1))$ critical?

A positive answer to Question 32 implies Theorem 3. If Question 32 could be answered affirmatively, we may then consider the following generalization:

Question 33. Suppose $f$ is the disjunction of boolean functions $f_1 \lor \cdots \lor f_m$ where each $f_i$ is hereditarily $\lambda_1$-critical. Let $\lambda \geq \max\{\lambda_1, \ldots, \lambda_m\}$ such that $\sum_{i=1}^m e^{-(\lambda_i/\lambda)} \leq 1$. Is $f$ necessarily $O(\lambda)$ critical?

A positive answer to Question 33 would be very interesting as it implies Conjecture 29.

Acknowledgements

I am grateful to Prahladh Harsha, Shrikanth Srinivasan, Siddharth Bhandari and Tulasi Molli for valuable feedback on a preliminary version of this paper.
References


[18] Patrick Traxler. Variable influences in conjunctive normal forms. In *Theory and Applications of Satis-
ifiability Testing-SAT 2009: 12th International Conference, SAT 2009, Swansea, UK, June 30-July 3,