A Composition Theorem for Conical Juntas

Mika Göös†  T.S. Jayram
University of Toronto  IBM Almaden

October 15, 2015

Abstract

We describe a general method of proving degree lower bounds for conical juntas (nonnegative combinations of conjunctions) that compute recursively defined boolean functions. Such lower bounds are known to carry over to communication complexity. We give two applications:

• **AND-OR trees.** We show a near-optimal \( \tilde{\Omega}(n^{0.753\ldots}) \) randomised communication lower bound for the recursive NAND function (a.k.a. AND-OR tree).

• **Majority trees.** We show an \( \Omega(2^{0.59^k}) \) randomised communication lower bound for the 3-majority tree of height \( k \). This improves over the state-of-the-art already in the context of randomised decision tree complexity.

†Work done while at IBM Research Almaden.
1 Conical Juntas?

Conical juntas are nonnegative linear combinations of conjunctions. Here are two examples, one computing the two-bit OR function $\text{OR}: \{0,1\}^2 \to \{0,1\}$ and another computing the three-bit majority function $\text{Maj}_3: \{0,1\}^3 \to \{0,1\}$:

\[
\begin{align*}
    h_1(x) &= \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_1x_2 + \frac{1}{4}x_1x_2, \\
    h_2(y) &= \frac{1}{3}y_1y_2 + \frac{1}{3}y_2y_3 + \frac{1}{3}y_1y_3 + \frac{2}{3}y_1y_2y_3 + \frac{2}{3}y_1y_2y_3 + \frac{2}{3}y_1y_2y_3.
\end{align*}
\]

The purpose of this work is to prove lower bounds on the degree $\deg(h)$ (maximum width of a conjunction in $h$) of any conical junta $h$ that computes—even approximately—a given boolean function $f: \{0,1\}^n \to \{0,1\}$. More precisely, we study the $\epsilon$-approximate conical junta degree of $f$, denoted $\deg_\epsilon(f)$, that is defined as the minimum degree of a conical junta $h$ satisfying

$$\forall x \colon |h(x) - f(x)| \leq \epsilon.$$ 

Communication complexity connection. A major motivation for studying conical junta degree comes from the works [CLRS13, GLM+15, LRS15] that connect conical juntas with nonnegative rank, a basic measure in communication complexity. Roughly speaking, lower bounds on approximate conical junta degree of $f$ can be translated into lower bounds on the approximate nonnegative rank of a certain two-party “lift” of $f$, and therefore into lower bounds against randomised protocols.

Related models. Conical juntas have been studied under such names as the (one-sided) partition bound for query complexity [JK10] and query complexity in expectation [KLDW15]. Another closely related model is that of randomised subcube partitions [FKW02, JLW15, KRS15]. Moreover, if we restrict the coefficients in a conical junta to be 0-1, we obtain the model of subcube partitions a.k.a. unambiguous DNFs [Sav02, Bel06, Göö15, GPW15, KRS15].

2 Our Results

Our main technical result is a Composition Theorem that makes it easy to prove conical junta degree lower bounds for functions that are defined from simpler functions via composition. If $f$ and $g$ are boolean functions on $n$ and $m$ bits, respectively, their composition $f \circ g^m$ is the function on $nm$ bits that maps an input $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ to the output

$$(f \circ g^m)(x) := f(g(x_1), \ldots, g(x_n)).$$

Define also $f^{\circ k} := f \circ (f^{\circ (k-1)})^n$ where $f^{\circ 1} := f$. The exact statement of the Composition Theorem is deferred to Section 4 as it is somewhat technical. It is phrased in terms of dual solutions (or certificates) to a linear program that captures a certain average version of conical junta degree (defined in Section 3). The theorem splits the task of proving lower bounds into two steps: we first need to find dual certificates for $f$ and $g$ (e.g., by solving an LP, either by inspection, or by using a computer), and then we can let the Composition Theorem construct a dual certificate for $f \circ g^m$ in a black-box fashion. We note that similar LP-based approaches have been extremely popular in analysing the degree of multivariate polynomials (see [She13, She14, BT15] for recent examples)—in short, this work develops such a framework for conical juntas, a nonnegative analogue of multivariate polynomials.

Setting these technical matters aside for a moment, let us illustrate the power the Composition Theorem by looking at some of its consequences.
Theorem 1. \( \deg_{\epsilon}(\text{NAND}^{\circ k}) \geq \Omega(n^{0.753\ldots}) \) for all \( \epsilon \leq 1/n \) where \( n := 2^k \).

Theorem 2. \( \deg_{\epsilon}(\text{Maj}_3^{\circ k}) \geq \Omega(2.59\ldots^k) \) for all \( \epsilon \leq 1/n \) where \( n := 3^k \).

**Discussion of Theorem 1.** The function \( \text{NAND}^{\circ k} \) is computed by a height-\( k \) binary tree consisting of \( \text{NAND} \) gates (a.k.a. \( \text{AND-OR} \) tree). A classical result [SW86, San95] states that any randomised decision tree needs to query \( \Omega(n^{0.753\ldots}) \) (here \( 0.753\ldots = \log(1 + \sqrt{33}) - 2 \)) many input bits in order to compute \( \text{NAND}^{\circ k} \) with high probability. This matches an upper bound due to Snir [Sni85]. Our Theorem 1 shows that the same lower bound holds even for conical juntas that approximate \( \text{NAND}^{\circ k} \) sufficiently well. This is a qualitative strengthening of the classical results since conical juntas are relaxations of decision trees. Indeed, a randomised decision tree of depth \( d \) that computes a function \( f \) to within error \( \epsilon > 0 \) can be converted into a degree-\( d \) \( \epsilon \)-approximate conical junta for \( f \) (the reason is the same as for multivariate polynomials [BdW02, Theorem 15]).

Note: A caveat with Theorems 1–2 is that we only know how to prove them for \( \epsilon \leq 1/n \). By contrast, one usually takes \( \epsilon = 1/3 \) when studying decision trees, and this is well-known to be w.l.o.g., because the error can be reduced below any \( \epsilon < 1/3 \) with only a factor \( O(\log(1/\epsilon)) \) increase in query complexity. Interestingly, for conical juntas, it is known [GLM+15] that \( \epsilon \) cannot always be efficiently reduced: for any constants \( \epsilon > \delta > 0 \) there exists a partial function \( f \) with \( \deg_{\epsilon}(f) = 1 \) but \( \deg_{\delta}(f) \geq \Omega(n) \). For total functions, it is still open whether efficient error reduction is possible (standard techniques [BdW02] at least show that \( \deg_{\epsilon}(f) \) is polynomially related to \( \deg_0(f) \)). In any case, Theorems 1–2 do indeed imply lower bounds for randomised decision trees with error \( \epsilon = 1/3 \): we simply have to reduce the error below \( 1/n \) first and only then convert the decision tree into a conical junta. This incurs a factor \( \Theta(\log n) \) loss in the value of the lower bound.

**Discussion of Theorem 2.** For the reasons discussed above, Theorem 2 implies a lower bound of \( \tilde{\Omega}(2.59\ldots^k) \geq \Omega(2.59^k) \) (here \( 2.59\ldots = \sqrt[3]{35/2} \)), and the \( \tilde{\Omega} \)-notation hides polylog\((n) \) factors) for the randomised query complexity of the recursive majority function \( \text{Maj}_3^{\circ k} \). This slightly improves over the previous bound of \( \Omega(2.57^k) \) that is the culmination of the line of work [JKS03, LNPV06, Leo13, MNS+15] wielding information theoretic tools. For comparison, a randomised zero-error decision tree of cost \( O(2.65^k) \) is known [MNS+15]. Even though our quantitative improvement in Theorem 2 is modest, the theorem nevertheless suggests that our new techniques are rather powerful: they are already competitive with highly optimised prior work, especially [MNS+15].

---

**Figure 1:** Examples of recursively defined boolean functions studied in this work.

2.1 Query complexity

We give applications for two well-studied recursively defined boolean functions; see Figure 1.

\[
\text{NAND}^{\circ k} = (\text{OR} \circ \text{AND})^{\circ 2} = \text{Maj}_3^{\circ 3}.
\]
2.2 Communication complexity

Using the machinery of [GLM+15] we can now translate Theorems 1–2 into analogous communication results. The translation incurs some polylog($n$) factor loss in parameters, which is suppressed by the $\tilde{\Omega}$-notation used below. Here $\text{BPP}^{cc}(F)$ stands for the bounded-error communication complexity of $F$ under a worst-case Alice–Bob bipartition of the input bits. For our functions, we may take the bipartition to be such that Alice gets the first bit of every bottom gate and Bob gets the rest.

**Theorem 3.** $\text{BPP}^{cc}(\text{NAND}^ok) \geq \tilde{\Omega}(n^{0.753...})$.

**Theorem 4.** $\text{BPP}^{cc}(\text{Maj}^ok) \geq \Omega(2.59^k)$.

**Discussion of Theorem 3.** Two independent works [JKR09, LS10] (building on [JKS03]) arrived at a lower bound of $\Omega(n/2^{O(k)})$ (or slightly worse $\Omega(n/k^{O(k)})$ in [JKR09]) for the randomised communication complexity of any height-$k$ unbounded fan-in alternating AND-OR tree (with fan-in 2 gates next to the inputs). While this lower bound is tight when $k = O(1)$, the bound becomes trivial in the setting of Theorem 3 where $k = \log n$. This shortcoming was partially addressed by [JKZ10] who showed, via a reduction from set-disjointness, a lower bound of $\tilde{\Omega}(\sqrt{n})$ for such AND-OR trees, independently of the height. Our Theorem 3 now gives an essentially optimal $\tilde{\Omega}(n^{0.753...})$ bound for the particular case of NAND$^ok$. It remains open whether this lower bound holds for all AND-OR trees (with the appropriate gates next to the inputs). For query complexity, Amano [Ama11a] has come close to settling this question, known as the Saks–Wigderson conjecture [SW86] for the class of read-once formulas (a more general version of the conjecture was recently disproved [ABB+15]).

**Discussion of Theorem 4.** The function $\text{Maj}^ok_3$ has not been studied in communication complexity previously—after all, even its randomised query complexity is not yet completely understood.

3 Definitions and Examples

We write $h = \sum w_C C$ for a generic conical junta, where the sum ranges over different conjunctions of literals $C: \{0, 1\}^n \rightarrow \{0, 1\}$ and $w_C \geq 0$ for each $C$. Note that $h: \{0, 1\}^n \rightarrow \mathbb{R}_\geq 0$. Let $|C|$ denote the width of a conjunction $C$, i.e., the number of literals in $C$. The degree of $h$, denoted $\deg(h)$, is defined as the maximum width of a conjunction $C$ with $w_C > 0$. Here, it is helpful to work with a more robust notion of degree that we call average degree. The average degree of $h$, denoted $\text{adeg}(h)$, is defined as the maximum over all inputs $x$ of

$$\text{adeg}_x(h) := \sum w_C |C| (x) = \sum w_C \text{adeg}_x(C).$$

In particular, $\text{adeg}(h) \leq \deg(h)$ in the natural setting where $h(x) \leq 1$ for all $x$. Our definition of average degree is in perfect analogy to the usual definition of cost for randomised zero-error decision trees, namely, charging for the expected number of queries made on a given input. Indeed, it is not hard to see that any zero-error decision tree of cost $d$ gives rise to a conical junta of average degree $d$ computing exactly the same boolean function as the decision tree.

For a boolean function $f: \{0, 1\}^n \rightarrow \{0, 1\}$ we define

- **Degree:** $\deg(f)$ is the minimum $\deg(h)$ over all conical juntas $h$ computing $f$.
- **Average degree:** $\text{adeg}(f)$ is the minimum $\text{adeg}(h)$ over all conical juntas $h$ computing $f$.
- **Approximate degree:** $\deg_\epsilon(f)$ is the minimum $\deg(h)$ over all conical juntas $h$ that compute $f$ to within error $\epsilon$, i.e., $h(x) \in f(x) \pm \epsilon$ for all $x$. 

3
3.1 Tame examples

For our conical juntas $h_1$ and $h_2$ from (1), we have $\text{adeg}(h_1) = \text{adeg}_{10}(h_1) = 3/2 < 2 = \deg(h_1)$ and $\text{adeg}(h_2) = \text{adeg}_{110}(h_2) = 8/3 < 3 = \deg(h_2)$. In fact, $h_1$ and $h_2$ are optimal:

$$\text{adeg}(\text{OR}) = 3/2 \quad \text{and} \quad \text{adeg}(\text{Maj}_3) = 8/3.$$ 

This can be seen by solving an LP whose value is $\text{adeg}(f)$, as is discussed shortly. Note that our degree measures are inherently \textit{one-sided}: $f$ and its negation $\neg f$ need not have the same degree. For example, we have $\text{adeg}(\neg \text{OR}) = 2$ (observe that $\bar{x}_1 \bar{x}_2$ is the only conical junta for $\neg \text{OR}$) even though $\text{adeg}(\text{OR}) = 3/2$. (More dramatic gaps can be demonstrated using variations of a function introduced in [GPW15].) By contrast, $\text{Maj}_3$ is \textit{self-dual}, $\neg \text{Maj}_3(x_1, x_2, x_3) = \text{Maj}_3(\neg x_1, \neg x_2, \neg x_3)$, so we automatically have $\text{adeg}(\text{Maj}_3) = \text{adeg}(\neg \text{Maj}_3)$.

3.2 A wild example!

What is the average degree of $\text{OR} \circ \text{Maj}_3^2$? We can obtain a conical junta for this function starting with the optimal conical juntas $h_1(x), h_2(y)$, $h_2(y) := h_2(y_1, y_2, y_3)$ computing $\text{OR}$, $\text{Maj}_3, \neg \text{Maj}_3$, respectively, as follows: Let $z^1 = (z_1^1, z_1^2, z_1^3)$ and $z^2 = (z_2^1, z_2^2, z_2^3)$ be fresh variables. Start with $h_1(x)$ and replace every positive literal $x_i$ by $b_2(z^i)$ and every negative literal $\bar{x}_i$ by $\bar{h}_2(z^i)$. This construction shows that

$$\text{adeg}(\text{OR} \circ \text{Maj}_3^2) \leq 3/2 \cdot 8/3 = 4.$$ 

It would be natural to conjecture that this is tight—\textit{but this conjecture is false}! There is in fact a more effective conical junta of average degree only $47/12 \approx 3.92$. An analogous phenomenon is well-known in the context of zero-error decision trees: so-called \textit{directional} decision trees need not be optimal for composed functions [SW86, Ver98, Ama11b].

**What of it?** This example shows that we cannot hope for a perfect composition theorem for average degree that would determine $\text{adeg}(f \circ g^n)$ solely in terms of $\text{adeg}(f)$, $\text{adeg}(g)$, and $\text{adeg}(\neg g)$, even assuming $\text{adeg}(g) = \text{adeg}(\neg g)$. Consequently, for our LP-based Composition Theorem, we will have to introduce \textit{some} technical assumptions: to enable the construction of a dual certificate for $\text{adeg}(f \circ g^n)$, we assume we have dual certificates of a special form for $\text{adeg}(f)$, $\text{adeg}(g)$, $\text{adeg}(\neg g)$. The rest of this section develops our LP formalism for average degree.

3.3 Generalised input costs

Let us first generalise the definition of $\text{adeg}(h)$ by allowing arbitrary costs $b_0, b_1 \geq 0$ to be assigned to reading the input bits. That is, for a conjunction $C$, we set $|C|_{b_0, b_1} := b_0 \cdot (\#\text{ of 0's read by } C) + b_1 \cdot (\#\text{ of 1's read by } C)$. In particular, $|C|_{1,1} = |C|$. Then $\text{adeg}(h; b_0, b_1)$ is defined as the maximum over all inputs $x$ of

$$\text{adeg}_x(h; b_0, b_1) := \sum w_C |C|_{b_0, b_1} C(x) = \sum w_C \text{adeg}_x(C; b_0, b_1).$$

We also introduce some “distributional” notation: for a distribution $D_1$ over $f^{-1}(1)$ we let

$$\text{adeg}_{D_1}(h; b_0, b_1) := \mathbb{E}_{x \sim D_1} [\text{adeg}_x(h; b_0, b_1)].$$

For a boolean function $f$: $(0,1)^n \rightarrow \{0,1\}$ we define

- $\text{adeg}(f; b_0, b_1)$ is the minimum of $\text{adeg}(h; b_0, b_1)$ over all conical juntas $h$ computing $f$. 

4
adeg_{D_1}(f; b_0, b_1) is the minimum of adeg_{D_1}(h; b_0, b_1) over all conical juntas h computing f.

It is clear that adeg(f; b_0, b_1) ≥ adeg_{D_1}(f; b_0, b_1) for all distributions D_1. (In fact, it can be shown using the minimax theorem that this inequality can be turned into an equality if we maximise over D_1 on the right hand side—however, we do not use this fact.)

### 3.4 An LP for average degree

We formulate adeg_{D_1}(f; b_0, b_1) as the optimum value of an LP—here the data f, D_1, b_0, b_1, is though of as fixed. We have a nonnegative variable \( w_C \geq 0 \) for each of the \( 3^n \) possible conjunctions \( C: \{0,1\}_n \rightarrow \{0,1\} \).

Here is the LP:

\[
\begin{align*}
\text{(Primal)} & \quad \text{min} & & \text{adeg}_{D_1}(\sum w_C C; b_0, b_1) \\
& \quad \text{subject to} & & \sum w_C C(x) = f(x), & \quad \forall x \\
& & & w_C \geq 0, & \quad \forall C
\end{align*}
\]

Here is the LP dual; the free variables are packaged into a function \( \Psi: \{0,1\}_n \rightarrow \mathbb{R} \).

\[
\begin{align*}
\text{(Dual)} & \quad \text{max} & & \langle \Psi, f \rangle \\
& \quad \text{subject to} & & \langle \Psi, C \rangle \leq \text{adeg}_{D_1}(C; b_0, b_1), & \quad \forall C \\
& & & \Psi(x) \in \mathbb{R}, & \quad \forall x
\end{align*}
\]

Since we are interested in proving lower bounds on average degree, we are only going to need the “weak” form of LP duality: Suppose \( h = \sum w_C C \) is an optimal solution to (Primal). Then any solution \( \Psi \) that is feasible for (Dual) witnesses a lower bound on adeg(f; b_0, b_1) like so:

\[
\begin{align*}
\text{adeg}(f; b_0, b_1) & \geq \text{adeg}_{D_1}(f; b_0, b_1) \\
& = \text{adeg}_{D_1}(h; b_0, b_1) \\
& = \sum w_C \text{adeg}_{D_1}(C; b_0, b_1) \\
& \geq \sum w_C \langle \Psi, C \rangle \\
& = \langle \Psi, \sum w_C C \rangle \\
& = \langle \Psi, f \rangle.
\end{align*}
\]

\[ (2) \]

### 4 Statement of the Composition Theorem

We start by defining an \((a_0, a_1; b_0, b_1)\)-certificate for \( f \) as a special collection of certificates witnessing

\[
\begin{align*}
\text{adeg}(f; b_0, b_1) & \geq a_1, \\
\text{adeg}(\neg f; b_0, b_1) & \geq a_0.
\end{align*}
\]

\[ (3) \]

**Definition 5.** Call a function \( \Psi: \{0,1\}_n \rightarrow \mathbb{R} \) balanced if \( \sum_x \Psi(x) = 0 \), and also write \( X_{\geq 0} := \max\{X,0\} \) for short. An \((a_0, a_1; b_0, b_1)\)-certificate for a function \( f: \{0,1\}_n \rightarrow \{0,1\} \) consists of four balanced functions \( \{\Psi_v, \hat{\Psi}_v\}_{v=0,1} \) mapping \( \{0,1\}_n \rightarrow \mathbb{R} \) such that the following hold.
\begin{itemize}
  \item **Special form:** Functions $\Psi_0$ and $\Psi_1$ have the form
    \begin{equation}
      \Psi_v = a_v(D_v - D_{1-v}),
    \end{equation}
  \end{itemize}

  where $D_v$ is a distribution over $f^{-1}(v)$. Moreover, $\hat{\Psi}_v$ is supported on $f^{-1}(v)$.

  \item **Feasibility:** For all conjunctions $C$ and $v \in \{0,1\}$,
    \begin{equation}
      \langle \Psi_v, C \rangle_{\geq 0} + \langle \Psi_v, C \rangle \leq \text{adeg}_{D_v}(C; b_0, b_1).
    \end{equation}

\end{itemize}

**Theorem 6** (Composition Theorem). Suppose $f$ admits an $(a_0, a_1; b_0, b_1)$-certificate and $g$ admits a $(b_0, b_1; 1, 1)$-certificate. Then $f \circ g^n$ admits an $(a_0, a_1; 1, 1)$-certificate.

**Discussion.** First, we note that (5) actually packs together two linear inequalities; it would be equivalent to require that both $\Psi_v + \hat{\Psi}_v$ and $\hat{\Psi}_v$ are feasible for (Dual), namely that

\begin{equation}
  \begin{cases}
    \langle \Psi_v + \hat{\Psi}_v, C \rangle \leq \text{adeg}_{D_v}(C; b_0, b_1), \\
    \langle \hat{\Psi}_v, C \rangle \leq \text{adeg}_{D_v}(C; b_0, b_1).
  \end{cases}
\end{equation}

Here $\Psi_1 + \hat{\Psi}_1$ is the main attraction: it witnesses a lower bound of $\langle \Psi_1 + \hat{\Psi}_1, f \rangle = \langle \Psi_1, f \rangle + \langle \hat{\Psi}_1, f \rangle = a_1 + 0 = a_1$ for $\text{adeg}(f; b_0, b_1)$ as promised above (3); similarly, $\Psi_0 + \hat{\Psi}_0$ witnesses the complementary lower bound $\text{adeg}(-f; b_0, b_1) \geq a_0$.

The requirement that $\Psi_1 + \hat{\Psi}_1$ must be balanced is perhaps our most critical assumption. We use it to manoeuvre around the counterexample of Section 3.2: we have $\text{adeg}(\text{Maj}_3) = 8/3$, while the best balanced solution to (Dual) only witnesses the lower bound $\text{adeg}(\text{Maj}_3) \geq 5/2$ (see also Figure 3). The requirement that $\hat{\Psi}_v$ is feasible for (Dual) is merely a technical assumption that helps us in the upcoming proof (akin to a “strengthened induction hypothesis”); we do not know whether the theorem is true without this condition. Another technical assumption is (4), which allows us to assume that $\Psi_1$ and $\Psi_0$ have opposite signs: $\Psi_1 = -a_1/a_0 \cdot \Psi_0$.

Some simple certificates are illustrated in Figures 2–3. Their feasibility can be checked by hand. For more involved functions, certificates can in principle be found via a computer search (using computers is not uncommon even in “lower bounds” research [Ama14]). We will in fact use this approach for $\text{Maj}_{3k}$ in Section 6.

\section{Proof of the Composition Theorem}

Let $\{\Psi_v, \hat{\Psi}_v\}_{v=0,1}$ and $\{\Phi_v, \Psi_v\}_{v=0,1}$ be the certificates for $f$ and $g$, respectively. Our goal is to construct a certificate $\{\Upsilon_v, \Upsilon_v\}_{v=0,1}$ for $f \circ g^n$. We use the following notation:

\[
  \Psi_v := a_v(F_v - F_{1-v}), \quad \Phi_v := b_v(G_v - G_{1-v}), \quad \Upsilon_v := a_v(D_v - D_{1-v}).
\]

By assumption, the distribution $F_v$ is supported on $f^{-1}(v)$ and $G_v$ is supported on $g^{-1}(v)$. We will define $D_v$ to be supported on $(f \circ g^n)^{-1}(v)$. 

\section{Discussion}

First, we note that (5) actually packs together two linear inequalities; it would be equivalent to require that both $\Psi_v + \hat{\Psi}_v$ and $\hat{\Psi}_v$ are feasible for (Dual), namely that

\begin{equation}
  \begin{cases}
    \langle \Psi_v + \hat{\Psi}_v, C \rangle \leq \text{adeg}_{D_v}(C; b_0, b_1), \\
    \langle \hat{\Psi}_v, C \rangle \leq \text{adeg}_{D_v}(C; b_0, b_1).
  \end{cases}
\end{equation}

Here $\Psi_1 + \hat{\Psi}_1$ is the main attraction: it witnesses a lower bound of $\langle \Psi_1 + \hat{\Psi}_1, f \rangle = \langle \Psi_1, f \rangle + \langle \hat{\Psi}_1, f \rangle = a_1 + 0 = a_1$ for $\text{adeg}(f; b_0, b_1)$ as promised above (3); similarly, $\Psi_0 + \hat{\Psi}_0$ witnesses the complementary lower bound $\text{adeg}(-f; b_0, b_1) \geq a_0$.

The requirement that $\Psi_1 + \hat{\Psi}_1$ must be balanced is perhaps our most critical assumption. We use it to manoeuvre around the counterexample of Section 3.2: we have $\text{adeg}(\text{Maj}_3) = 8/3$, while the best balanced solution to (Dual) only witnesses the lower bound $\text{adeg}(\text{Maj}_3) \geq 5/2$ (see also Figure 3). The requirement that $\hat{\Psi}_v$ is feasible for (Dual) is merely a technical assumption that helps us in the upcoming proof (akin to a “strengthened induction hypothesis”); we do not know whether the theorem is true without this condition. Another technical assumption is (4), which allows us to assume that $\Psi_1$ and $\Psi_0$ have opposite signs: $\Psi_1 = -a_1/a_0 \cdot \Psi_0$.

Some simple certificates are illustrated in Figures 2–3. Their feasibility can be checked by hand. For more involved functions, certificates can in principle be found via a computer search (using computers is not uncommon even in “lower bounds” research [Ama14]). We will in fact use this approach for $\text{Maj}_{3k}$ in Section 6.

\section{Proof of the Composition Theorem}

Let $\{\Psi_v, \hat{\Psi}_v\}_{v=0,1}$ and $\{\Phi_v, \Psi_v\}_{v=0,1}$ be the certificates for $f$ and $g$, respectively. Our goal is to construct a certificate $\{\Upsilon_v, \Upsilon_v\}_{v=0,1}$ for $f \circ g^n$. We use the following notation:

\[
  \Psi_v := a_v(F_v - F_{1-v}), \quad \Phi_v := b_v(G_v - G_{1-v}), \quad \Upsilon_v := a_v(D_v - D_{1-v}).
\]

By assumption, the distribution $F_v$ is supported on $f^{-1}(v)$ and $G_v$ is supported on $g^{-1}(v)$. We will define $D_v$ to be supported on $(f \circ g^n)^{-1}(v)$. 

Figure 2: A \((2b_1, b_0 + \frac{1}{2}b_1; b_0, b_1)\)-certificate for NAND: \(\{0, 1\}^2 \rightarrow \{0, 1\}\) that is valid for all \(b_0, b_1 \geq 0\). The 1-inputs \(\text{NAND}^{-1}(1)\) are highlighted in gray. For feasibility, there are 6 equivalence classes (see Section 6.2) of conjunctions to check: \(\{***, *0, *1, 00, 10, 11\}\).

Figure 3: A \(\left(\frac{5}{2}, \frac{5}{2}; 1, 1\right)\)-certificate for Maj_3: \(\{0, 1\}^3 \rightarrow \{0, 1\}\). The 1-inputs \(\text{Maj}_3^{-1}(1)\) are highlighted in gray. Only \(\Psi_1, \hat{\Psi}_1\) are shown as \(\Psi_0, \hat{\Psi}_0\) are defined via self-duality. Here \(D_v\) is uniform on inputs of Hamming weight \(v + 1\). For feasibility, there are 10 equivalence classes of conjunctions to check: \(\{***, **1, *0, *10, *11, 000, 100, 110, 111\}\). Note that for any \(\alpha \geq 0\), we can obtain an \(\left(\frac{5}{2}\alpha, \frac{5}{2}\alpha; \alpha, \alpha\right)\)-certificate by simply scaling the functions \(\Psi_v, \hat{\Psi}_v\) by \(\alpha\).
5.1 Construction

Lifts. Let \( \Gamma : \{0, 1\}^n \to \mathbb{R} \) and suppose that for each \( y \in \{0, 1\}^n \) we have a function \( H_y : \{0, 1\}^m \to \mathbb{R} \) supported on \((g^n)^{-1}(y) = g^{-1}(y_1) \times \cdots \times g^{-1}(y_n)\). The lift of \( \Gamma \) by \( H \) is

\[
\Gamma^H := \sum_{y \in \{0, 1\}^n} \Gamma(y) \cdot H_y.
\]

In particular, if \( \Gamma \) and the \( H_y \)'s are probability distributions, so is \( \Gamma^H \). Note also that if \( \Gamma \) is supported on \( f^{-1}(v) \), then \( \Gamma^H \) is supported on \( (f \circ g^n)^{-1}(v) \).

New certificate. Write \( G_y := G_{y_1} \times \cdots \times G_{y_n} \) for the canonical product distribution on \((g^n)^{-1}(y)\). We also need a modified version of \( G_y \), denoted \( (G \downarrow \hat{\Phi})_y \) where \( i \in [n] \), that has a copy of \( \hat{\Phi}_{y_i} \) in place of \( G_{y_i} \); more formally

\[
(G \downarrow \hat{\Phi})_y(x) := \hat{\Phi}_{y_i}(x_i) \cdot \prod_{j \neq i} G_{y_j}(x_j).
\]

Note that \( (G \downarrow \hat{\Phi})_y \) is a balanced function supported on \((g^n)^{-1}(y)\). We now define \( \{ \Upsilon_v, \hat{\Upsilon}_v \}_{v=0,1} \) by

\[
\Upsilon_v := \Psi^G_v, \quad \hat{\Upsilon}_v := \hat{\Psi}^G_v + \sum_{i=1}^n F^G \downarrow \hat{\Phi}.
\]

Since \( \Psi^G_v = a_v(F^G_v - F^G_{1-v}) \), we have \( D_v = F^G_v \). It is also easy to check that \( \hat{\Upsilon}_v \) is a balanced function supported on \((f \circ g^n)^{-1}(v)\). Hence \( \{ \Upsilon_v, \hat{\Upsilon}_v \}_{v=0,1} \) is of the special form required of an \((a_0, a_1; 1, 1)\)-certificate for \( f \circ g^n \). The interesting part is to verify the feasibility condition (5).

5.2 Feasibility

Fix a conjunction \( C \) in the domain of \( f \circ g^n \). Our goal is to show

\[
\langle \Psi^G_v, C \rangle_{\geq 0} + \langle \hat{\Psi}^G_v + \sum_i F^G \downarrow \hat{\Phi}, C \rangle \leq \text{ade}g_{D_v}(C). \tag{7}
\]

Extracting a conical junta from \( C \). Our analysis will be centered around a conical junta \( h(y) \), defined below, that computes the acceptance probability \( \Pr_{x \sim G_y}[C(x) = 1] = \mathbb{E}_{x \sim G_y}[C(x)] = \langle G_y, C \rangle \). In a certain sense, \( h \) serves as a projection of \( C \) to the domain of \( f \). Write \( C(x) = \prod_{i=1}^n C_i(x_i) \) where \( C_i \) is a conjunction depending only on \( x_i \). Since \( G_y \) is a product distribution,

\[
\langle G_y, C \rangle = \prod_i \langle G_{y_i}, C_i \rangle = \prod_i p_{i,y_i},
\]

where we wrote \( p_{i,y_i} := \langle G_{y_i}, C_i \rangle \in \mathbb{R}_{\geq 0} \) for short. Fix \( y^* \in \{0, 1\}^n \) such that \( p_{i,y_i^*} \geq p_{i,1-y_i^*} \) for all \( i \). We now define \( h(y) \) that computes \( \langle G_y, C \rangle \):

\[
h(y) := \prod_{i=1}^n (p_{i,1-y_i^*} + (p_{i,y_i^*} - p_{i,1-y_i^*}) \cdot \ell_i) \quad \text{where literal } \ell_i \text{ is } \begin{cases} y_i & \text{if } y_i^* = 1, \\ \bar{y}_i & \text{if } y_i^* = 0. \end{cases} \tag{8}
\]

This product expression can be expanded into a conical combination of conjunctions, \( h = \sum w_T T \), in the natural way, but the above “implicit” form is more concise.

Next, we record two properties of \( h \) that will suffice for the remaining analysis.

Lemma 7. \( \text{ade}g_y(h; b_0, b_1) = \sum_i \langle \Phi_{y_i}, C_i \rangle_{\geq 0} \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \).
Proof. Write $h = \sum w_T T$. We compute the average degree by summing together the weights $\sum_{T \ni \ell_i} w_T T(y)$ contributed by each of the $n$ literals $\ell_i$, i.e.,

$$\text{adeg}_y(h; b_0, b_1) = \sum_i |\ell_i|_{b_0, b_1} \cdot \sum_{T \ni \ell_i} w_T T(y).$$

If $i$ is such that $y_i \neq y_i^*$, we have $\ell_i(y) = 0$ and so $T(y) = 0$ for all $T \ni \ell_i$; hence $\ell_i$ contributes no weight in this case. Suppose then that $i$ is such that $y_i = y_i^*$; here we can write

$$h(y) = p_i,1 - y_i \prod_{j \neq i} p_{j,y_j} + \ell_i \cdot (p_i,y_i - p_i,1 - y_i) \prod_{j \neq i} p_{j,y_j}.$$ The conjunctions $T$ underlying the first term do not involve $\ell_i$, so they contribute no weight for $\ell_i$. The conjunctions $T$ underlying the second term all involve $\ell_i$ and contribute a total weight of $(p_i,y_i - p_i,1 - y_i) \prod_{j \neq i} p_{j,y_j}$. Altogether we get

$$\text{adeg}_y(h; b_0, b_1) = \sum_i |\ell_i|_{b_0, b_1} \cdot \sum_{T \ni \ell_i} w_T T(y)
= \sum_i b_i(y_i, y_i^*) (p_i, y_i - p_i,1 - y_i) \prod_{j \neq i} p_{j,y_j}
= \sum_i b_i (p_i, y_i - p_i,1 - y_i,1) \prod_{j \neq i} (G_{y_j}, C_j)
= \sum_i (p_i, y_i, C_i) \prod_{j \neq i} (G_{y_j}, C_j).$$

Lemma 8. $\langle \Gamma, h \rangle = \langle \Gamma^G, C \rangle$ for all $\Gamma: \{0, 1\}^n \rightarrow \mathbb{R}$.

Proof. We calculate

$$\langle \Gamma, h \rangle = \sum_y \Gamma(y) h(y) = \sum_y \Gamma(y) \langle G_y, C \rangle = \sum_y \Gamma(y) \left[ \sum_x G_y(x) C(x) \right]
= \sum_x \left[ \sum_y \Gamma(y) G_y(x) \right] C(x) = \sum_x \Gamma^G(x) C(x) = \langle \Gamma^G, C \rangle.$$ 

Analysis. Let us expand the right hand side of the desired inequality (7):

$$\text{adeg}_{D_v}(C) = |C| \cdot \langle F^G_v, C \rangle
= E_{y \sim F_v} \left[ |C| \cdot \langle G_y, C \rangle \right]
= E_{y \sim F_v} \left[ \sum_i |C_i| \cdot \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \right]
= E_{y \sim F_v} \left[ \sum_i |C_i| \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \right]
= E_{y \sim F_v} \left[ \sum_i \text{adeg}_{G_{y_j}}(C_i) \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \right].$$

Substituting our hypothesis $\text{adeg}_{G_{y_j}}(C_i) \geq \langle \Phi_{y_i}, C_i \rangle \geq 0 + \langle \Phi_{y_i}, C_i \rangle$ into the above, we obtain

$$\text{adeg}_{D_v}(C) \geq \underbrace{E_{y \sim F_v} \left[ \sum_i \langle \Phi_{y_i}, C_i \rangle \geq 0 \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \right]}_{(I)} + \underbrace{E_{y \sim F_v} \left[ \sum_i \langle \Phi_{y_i}, C_i \rangle \prod_{j \neq i} \langle G_{y_j}, C_j \rangle \right]}_{(II)}.$$ For the first term,

$$(I) = E_{y \sim F_v} \left[ \text{adeg}_y(h; b_0, b_1) \right] \quad \text{(Lemma 7)}$$

$$= \text{adeg}_{F_v}(h; b_0, b_1)
\geq \langle \Psi_v, h \rangle \geq 0 + \langle \Phi_v, h \rangle \quad \text{(Feasibility of \{\Psi_v, \Phi_v\} and (2))}
= \langle \Psi^G_v, C \rangle \geq 0 + \langle \Psi^G_v, C \rangle. \quad \text{(Lemma 8)}$$
For the second term,
\[
(\Pi) = \mathbf{E}_{y \sim F_y} \left[ \sum_i \langle (G^{\frac{1}{2}} f)_{y}, C \rangle \right] \\
= \langle \sum_i F^G_{v} f^{\frac{1}{2}} \rangle, C \rangle.
\]
Combining these yields (7). This concludes the proof of Theorem 6.

6 Approximate Degree Lower Bounds

In this section we prove Theorems 1–2 using the Composition Theorem. We begin by observing that \((a_0, a_1; b_0, b_1)-certificates \{\Psi_v, \hat{\Psi}_v\}_{v=0,1}\) also yield lower bounds for approximate degree, if the 1-norm \(\|\hat{\Psi}_v\|_1\) is not too large. We call \(\{\Psi_v, \hat{\Psi}_v\}_{v=0,1}\) an \((a_0, a_1; b_0, b_1; c)-certificate\) if \(\max_v \|\hat{\Psi}_v\|_1 \leq c\).

Lemma 9. Suppose \(f\) admits an \((a_0, a_1; 1, 1; c)-certificate\). If \(\epsilon \leq 1/4\) and \(c \cdot \epsilon \leq a_1/4\), then
\[
\deg_{\epsilon}(f) \geq \Omega(a_1).
\]

Proof. Fix a certificate \(\{\Psi_v, \hat{\Psi}_v\}_{v=0,1}\) for \(f\) and suppose \(\deg_{\epsilon}(f) = \deg(h)\) where \(h\) is a conical junta with \(\|h - f\|_1 \leq \epsilon\). Since \(h(x) \leq 1 + \epsilon\) for all \(x\), we have \(\deg(h) \geq (1 + \epsilon)^{-1} \deg(h) \geq \Omega(\deg(h))\).

Now we calculate
\[
\deg(h) \geq \langle \Psi_1 + \hat{\Psi}_1, h \rangle \geq \langle \Psi_1 + \hat{\Psi}_1, f \rangle + \langle \Psi_1 + \hat{\Psi}_1, h - f \rangle \\
\geq a_1 - \|\Psi_1 + \hat{\Psi}_1, h - f\|_1 \\
\geq a_1 - \|\Psi_1 + \hat{\Psi}_1\|_1 \cdot \|h - f\|_\infty \\
\geq a_1 - (\|\Psi_1\|_1 + \|\hat{\Psi}_1\|_1) \cdot \epsilon \\
\geq a_1 - (2a_1 + c) \cdot \epsilon \\
\geq a_1 / 4. \quad \square
\]

We use the following version of the Composition Theorem where the bounds on 1-norms (following immediately from the definition (6)) are made explicit.

Theorem 10. Suppose \(f\) admits an \((a_0, a_1; b_0, b_1; c)-certificate\) and \(g\) admits a \((b_0, b_1; 1, 1; d)-certificate\). Then \(f \circ g^n\) admits an \((a_0, a_1; 1, 1; c + nd)-certificate\).

6.1 Proof of Theorem 1

We iteratively apply Theorem 10 as follows.

1. Assume we have an \((\alpha_k, \beta_k; 1, 1; \gamma_k)-certificate\) for NAND\(^{\alpha_k}\) where \(\gamma_k \geq \alpha_k, \beta_k\).
2. Obtain a \((2\beta_k, \alpha_k + \frac{1}{2} \beta_k; \alpha_k, \beta_k; \beta_k)-certificate\) for NAND from Figure 2.
3. Compose the above to get an \((\alpha_{k+1}, \beta_{k+1}; 1, 1; \gamma_{k+1})\)-certificate for NAND\(^{\alpha_{k+1}}\) where
\[
\alpha_{k+1} := 2\beta_k, \\
\beta_{k+1} := \alpha_k + \beta_k / 2, \\
\gamma_{k+1} := \beta_k + 2\gamma_k.
\]

Note that \(\alpha_{k+1}, \beta_{k+1} \leq \gamma_{k+1} \leq 3\gamma_k\). Starting with \(\alpha_0 = \beta_0 = \gamma_0 = 1\) these recurrences (famously [SW86]) evaluate to \(\alpha_k, \beta_k = \Theta(n^{0.753\cdot})\) where \(n := 2^k\). In addition, \(\gamma_k \leq 3^k \leq n^{1.6}\). Now take \(\epsilon \leq 1/n\) in Lemma 9 to prove Theorem 1.
Function | Class representative | Class size | $\Psi_1$ | $\hat{\Psi}_1$ | $\Psi_1 + \hat{\Psi}_1$
---|---|---|---|---|---
Maj$_3^{\circ 1}$ | (0, 0, 1) | 3 | $-5/2$ | 0 | $-5/2$
| (0, 1, 1) | 3 | $5/2$ | $1/2$ | 3
| (1, 1, 1) | 1 | 0 | $-1/2$ | $-1/2$
| All others | 0 | 0 | 0 | 0

Maj$_3^{\circ 2}$ | (001, 001, 011) | 81 | $-20/3$ | 0 | $-20/3$
| (001, 011, 011) | 81 | 20/3 | $7/3$ | 9
| (000, 011, 011) | 27 | 0 | $-1/3$ | $-1/3$
| (001, 011, 111) | 54 | 0 | $-2/3$ | $-2/3$
| (011, 011, 011) | 27 | 0 | $-4/3$ | $-4/3$
| All others | 0 | 0 | 0 | 0

Maj$_3^{\circ 3}$ | (112, 112, 122) | 1594323 | $-35/2$ | 0 | $-35/2$
| (112, 122, 122) | 1594323 | 35/2 | $19/2$ | 27
| (122, 122, 122) | 531441 | 0 | $-7/2$ | $-7/2$
| (112, 122, 222) | 1062882 | 0 | $-2$ | $-2$
| (112, 122, 123) | 2125764 | 0 | $-4/3$ | $-4/3$
| (112, 122, 022) | 1062882 | 0 | $-2/3$ | $-2/3$
| (111, 122, 122) | 531441 | 0 | $-5/6$ | $-5/6$
| (113, 122, 122) | 531441 | 0 | $-1/2$ | $-1/2$
| (012, 122, 122) | 1062882 | 0 | $-2/3$ | $-2/3$
| All others | 0 | 0 | 0 | 0

Table 1: Certificates for Maj$_3^{\circ \ell}$ for heights $\ell = 1, 2, 3$. The table lists $(\alpha_\ell, \alpha_\ell; 1, 1)$-certificates with values $\alpha_1 = 5/2$ (also illustrated in Figure 3), $\alpha_2 = 20/3$, and $\alpha_3 = 35/2$. Only $\Psi_1, \hat{\Psi}_1$ are shown as $\Psi_0, \hat{\Psi}_0$ are defined dually. We give the total weight for each equivalence class of inputs; the functions are uniform on each class. For height $\ell = 3$ we represent the inputs to the bottom-most Maj$_3$ gates by their Hamming weight, e.g., 001 $\sim 1$, 011 $\sim 2$, etc.

6.2 Computer search for certificates

Iteratively composing (scaled versions of) the $(5/2, 5/2; 1, 1)$-certificate given in Figure 3 would yield only an $\Omega(2^{0.5k})$ lower bound for Maj$_3^{\circ k}$. This is the best possible for our approach if we were to just compose certificates for individual Maj$_3$ functions. To obtain a better lower bound, we can instead directly find a certificate for Maj$_3^{\circ \ell}$, where $\ell$ is a small constant, and then compose that certificate. Table 1 gives certificates for Maj$_3^{\circ \ell}$ for height up to $\ell = 3$. We used a computer to solve the dual LP (Dual), with the additional restriction that $\Psi (= \Psi_1 + \hat{\Psi}_1)$ should be balanced. The best balanced $\Psi$ happened to satisfy the other conditions required by our Definition 5.

Notes on implementation. For computational efficiency, it is useful to prune the search space by eliminating symmetries. The symmetries of Maj$_3^{\circ \ell}$ (permutations of input coordinates that do not change the value of the function) are the symmetries of the underlying height-$\ell$ ternary tree. These symmetries partition the set of inputs and the set of conjunctions into equivalence classes: two inputs/conjunctions are “equivalent” if one can be mapped to the other by a symmetry. The set of feasible solutions to the LP is also invariant under these symmetries. It follows that we may look w.l.o.g. for a $\Psi$ that is invariant, i.e., uniform on each equivalence class. (Indeed, if $\Psi$ is any feasible solution, we obtain an invariant solution by averaging $\Psi$ over all the symmetries.) Thus we
need only maintain one variable in the LP per equivalence class \( X \subseteq \{0, 1\}^n \) recording the total weight \( \sum_{x \in X} \Psi(x) \) of that class. Also, for such invariant \( \Psi \), we need only check the LP feasibility constraint \( \langle \Psi, C \rangle \leq \text{adeg}_{D_1}(C; b_0, b_1) \) for a single representative \( C \) from each class of conjunctions.

The optimal height-2 certificate happens to have the same support as the certificate produced by our Composition Theorem starting with two height-1 certificates. Inspired by this, in order to speed up the search for height 3, we only optimised over those \( \Psi \) whose support coincides with that coming from the Composition Theorem—this LP has only 9 variables (i.e., equivalence classes of inputs), but well over 100,000 constraints (i.e., equivalence classes of conjunctions).

It is open to analyse height 4. Is there an efficient separation oracle for \((\text{Dual})\)?

### 6.3 Proof of Theorem 2

Table 1 defines a certificate for \( \text{Maj}_{3}^{\circ3} \) with parameters \((35/2, 35/2; 1, 1; 19)\) and we may scale the certificate by any scalar \( \alpha \geq 0 \) to obtain one with parameters \(( (35/2)^k/3, (35/2)^k/3; \alpha, \alpha; 19\alpha) \). Using Theorem 10 iteratively as in Section 6.1, we get a certificate for \( \text{Maj}_{3}^{\circ k} \) with parameters \(( (35/2)^{k/3}, (35/2)^{k/3}; 1, 1; 28^{k/3} \cdot 19) \).

Here \((35/2)^{k/3} \geq n^{0.8} \) and \( 28^{k/3} \cdot 19 \leq n^{1.1} \) where \( n := 3^k \). Hence we may apply Lemma 9 with \( \epsilon \leq 1/n \) to conclude an \( \epsilon \)-approximate degree lower bound of \( \Omega((35/2)^{k/3}) = \Omega(2^{0.59\ldots k}) \).

### 7 Communication Lower Bounds

In this section we prove Theorems 3–4 by applying the main result of [GLM+15]: a simulation of randomised communication protocols by conical juntas. To this end, let \( \text{IP}_b: \{0, 1\}^b \times \{0, 1\}^b \rightarrow \{0, 1\} \) be the two-party (Alice has \( x \), Bob has \( y \)) inner-product function given by \( \text{IP}_b(x, y) := \langle x, y \rangle \mod 2 \).

Let \( \text{BPP}_{\epsilon}^c(F) \) denote the randomised \( \epsilon \)-error communication complexity of \( F: \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\} \). The following is a corollary of [GLM+15, Theorem 31] (the original formulation there talks about \( \text{WAPP}_{\epsilon}^d(f) \) which is the same as \( \text{deg}_\epsilon(f) \); moreover, the result is stated for \( \epsilon = \Theta(1) \), but the theorem is true more generally for \( \epsilon = 2^{-\Theta(b)} \)).

**Theorem 11 ([GLM+15]).** Let \( \epsilon := 1/n \) and \( b := \Theta(\log n) \) (with a large enough implicit constant). For any \( f: \{0, 1\}^n \rightarrow \{0, 1\} \) we have

\[
\text{BPP}_{\epsilon/2}^c(f \circ \text{IP}_b^n) \geq \Omega(\text{deg}_\epsilon(f) \cdot b).
\]

Let us prove Theorem 3 (a similar argument works for Theorem 4). A key observation (also made in [JKZ10, §3]) is that \( \text{IP}_b = \text{XOR}_b \circ \text{AND}^b \) reduces to computing a binary NAND tree on \( O(b^2) \) bits. To see this, think of the \( b \)-bit parity function \( \text{XOR}_b \) as a height-(\( \log b \)) binary tree of XOR gates. Each such XOR gate can be rewritten as a height-2 NAND tree (with some negations on inputs):
In the binary XOR tree, replace the top XOR gate with this NAND tree (this involves making copies of some subtrees), push the negations to inputs, and repeat recursively. This gives us a height-\((2 \log b)\) NAND tree. Moreover, the bottom layer of AND gates in IP\(_b\) is also easily simulated by NAND gates. Consequently, for some \(N := \Theta(nb^2)\), the communication matrix of NAND\(^{\log n} \circ \text{IP\(_b\)}\) appears as a submatrix of NAND\(^{\log N}\) (relative to some bipartition of the input given by the reduction).

We can now derive Theorem 3—here \(\epsilon\) and \(b\) are defined as in Theorem 11, and \(\gtrsim\) means that we ignore polylog\((N)\) factors.

\[
\begin{align*}
BPP_{\epsilon/3}^{cc}(\text{NAND}\circ \log N) & \gtrsim BPP_{\epsilon/2}^{cc}(\text{NAND}\circ \log N) & \text{(Error reduction)} \\
& \gtrsim BPP_{\epsilon/2}^{cc}(\text{NAND}\circ \log n \circ \text{IP\(_b\)}^n) & \text{(Key observation)} \\
& \gtrsim \deg_\epsilon(\text{NAND}\circ \log n) & \text{(Theorem 11)} \\
& \gtrsim n^{0.753\ldots} & \text{(Theorem 1)} \\
& = \tilde{\Theta}(N^{0.753\ldots}).
\end{align*}
\]

Acknowledgements

Many thanks to Thomas Watson for a careful perusal of the manuscript and to Li-Yang Tan for correspondence.

References


