Approximate Degree-Weight and Indistinguishability

Xuangui Huang*  Emanuele Viola*
Northeastern University  Northeastern University
stslxg@ccs.neu.edu  viola@ccs.neu.edu

January 13, 2020

Abstract

We prove that the OR function on \(\{-1,1\}^n\) can be point-wise approximated with error \(\varepsilon\) by a polynomial of degree \(O(k)\) and weight \(2^{O(n \log(1/\varepsilon)/k)}\), for any \(k \geq \sqrt{n \log(1/\varepsilon)}\). This result is tight for \(k = (1 - \Omega(1))n\). Previous results were either not tight or had \(\varepsilon = \Omega(1)\).

In general we obtain a tight approximate degree-weight result for any symmetric function. Building on this we also obtain an approximate degree-weight result for bounded-width CNF. For these two classes no such result was known.

One motivation for such results comes from the study of indistinguishability. Two distributions \(P, Q\) over \(n\)-bit strings are \((k, \delta)\)-indistinguishable if their projections on any \(k\) bits have statistical distance at most \(\delta\). The above approximations give values of \((k, \delta)\) that suffice to fool OR, symmetric functions and bounded-width CNF, and the first result is tight for all \(k\) while the second result is tight for \(k = (1 - \Omega(1))n\). We also show that any two \((k, \delta)\)-indistinguishable distributions are \(O(n)^{k/2\delta}\)-close to two distributions that are \((k, 0)\)-indistinguishable, improving the previous bound of \(O(n)^k\delta\). Finally we present proofs of some known approximate degree lower bounds in the language of indistinguishability, which we find more intuitive.

1 Introduction

The idea of approximating boolean functions point-wise using real-valued polynomials of “low complexity” has been a powerful tool in theoretical computer science. A natural notion of complexity of the polynomial is its degree, extensively studied since the seminal work by Nisan and Szegedy [NS94]. We can also consider the weight of the approximating polynomial, that is the sum of absolute value of its coefficients, which was studied under the name “spectral norm” in [AFH12, AFK17] for polynomials over \(\{-1,1\}\). In this paper we study weight in conjunction with degree, and we will show that we can typically trade degree with weight for approximating several large classes of functions over some basis.

Bogdanov and Williamson [BW17] showed tight degree-weight tradeoffs for approximating OR on \(\{-1,1\}^n\) within constant error. To set context, recall that the approximate degree of OR is \(\Theta(\sqrt{n})\) [NS94]. They showed that OR can be approximated in degree \(O(k)\) and weight \(2^{O(n/k)}\) for \(k \geq \sqrt{n}\), and this is tight. Prior to their results, Servedio et al. [STT12] showed \(w = 2^{O(n/k)}\); Chandrasekaran et al. [CTUW14] showed \(w = 2^{O(n \log^2(1/\varepsilon)/k)}\) for error \(\varepsilon\) when \(k \geq \sqrt{n \log(1/\varepsilon)}\); Bun and Thaler [BT15] showed \(w = 2^{\Omega(n/k)}\). Apparently

*Supported by NSF CCF award 1813930.
little degree-weight tradeoff result was known for arbitrary symmetric functions and non-
symmetric functions.

Bounds on the weight of approximations have several applications, ranging from differential privacy [CTUW14], to attribute efficient learning [KS06 STT12], and to indistinguish-
ability [BW17].

1.1 Our results: approximate degree-weight

We prove a tight result for approximating the OR function. This refines the result in [BW17] by including the dependency on the error $\varepsilon$, and the upper bound improves on the result in [CTUW14] by getting a better dependence on $\log(1/\varepsilon)$ and removing the other log terms. Jumping ahead, this kind of improvement is critical to obtain our result for t-CNF, because we will need to set $\varepsilon$ exponentially small. However our improvements don’t seem to affect their applications mentioned above.

We state the upper and lower bounds as separate theorems. Note that in the lower bound for $k \leq \varepsilon n$ we have $2^{(c n/k - 1) \log(1/\varepsilon)} \geq 2^{c n \log(1/\varepsilon)/2k}$, so the upper bound is tight for $k = (1 - \Omega(1)) n$.

**Theorem 1.1.** For every $\varepsilon, n, k$ satisfying $\sqrt{n \log(1/\varepsilon)} \leq k \leq n$, OR$_n$ can be $\varepsilon$-approximated on $\{-1, 1\}^n$ in degree $O(k)$ and weight $2^O(n \log(1/\varepsilon)/k)$.

**Theorem 1.2.** There exists a constant $c < 1$ such that for every $\varepsilon, n, k \leq n$, if a polynomial $p$ $\varepsilon$-approximates OR$_n$ on $\{-1, 1\}^n$ in degree $k$, then its weight is at least $2^{(cn/k - 1) \log(1/\varepsilon)}$.

These theorems are special cases of the following results for symmetric functions. A function is symmetric if its value only depends on the Hamming weight of the input, i.e. the number of −1’s in the input on $\{-1, 1\}^n$. For a symmetric function $f_n$ with input length $n$, let $\tau(f_n)$ denote the smallest number $t \in [0, \frac{n}{2}]$ such that $f_n$ is constant on inputs of Hamming weight in $(t, n - t)$. For $0 \leq t \leq \frac{n}{2}$, let SYM$_{n,t}$ denote the class of symmetric functions $f_n$ with $\tau(f_n) = t$. To set context, the $\varepsilon$-approximate degree of any $f \in$ SYM$_{n,t}$ is $\Theta\left(\sqrt{n \log(1/\varepsilon)} + t\right)$ [Pa02, dW08].

Again we state the upper and lower bounds separately.

**Theorem 1.3.** For every $\varepsilon, n, t, k$ satisfying $\sqrt{n \log(1/\varepsilon)} + t \leq k \leq n$, every function $f \in$ SYM$_{n,t}$ can be $\varepsilon$-approximated on $\{-1, 1\}^n$ in degree $O(k)$ and weight $2^O(n \log(1/\varepsilon) + t)/k$.

**Theorem 1.4.** There exists a constant $c < 1$ such that for every $\varepsilon, n, t, k \leq \varepsilon n$ and $0 \leq t \leq \frac{\varepsilon n}{2}$, if a polynomial $p$ $\varepsilon$-approximates $f \in$ SYM$_{n,t}$ on $\{-1, 1\}^n$ in degree $k$, then its weight is at least $2^{O(n \log(1/\varepsilon) + t)/k}$.

Independently and concurrently, Bogdanov et al. [BMTW19] obtained a similar result with a weaker upper bound: degree $O(k)$ and weight $2^{O(n \log(1/\varepsilon) + t) \log^2 n/k}$ for $k \geq \sqrt{n \log_n(1/\varepsilon)} + t \log n$.

We then move to non-symmetric functions. A t-CNF is a CNF with clauses of size $t$. Sherstov [She18] proved that the $\varepsilon$-approximate degree of t-CNF is $O_t\left(n^{1/t} \log(1/\varepsilon)\right)^{1/t}$. For $t = 2$ and constant $\varepsilon$ this is $O(n^{2/3})$. We prove the following degree-weight approximation for t-CNF, which recovers [She18] and shows that the larger the degree $k$ the smaller the weight $w$ we can have, up to about $w = 2^{O(n^{1-1/t})}$. For $t = 2$ the latter is $2^{O(\sqrt{n})}$.

**Theorem 1.5.** For every $\varepsilon, n, t, k$ satisfying $n^{1/t} \log(1/\varepsilon) \leq k \leq n$, there exists constant $c_t$ depending on $t$ such that any t-CNF can be $\varepsilon$-approximated on $\{-1, 1\}^n$ in degree $c_t \cdot k$ and weight $2^{c_t \cdot n \log(1/\varepsilon) + t}/k^{1/t}$.
1.2 Fourier vs. Boolean basis, and our results for approximate degree-weight of EXACT and AND

In Section 1.1 we approximate the functions over the Fourier basis \([-1, 1]\), where 1 represents False and -1 represents True. Alternatively we can use 0 for False and 1 for True, called the Boolean basis. In some cases the Fourier basis is more convenient as negation of variables becomes negation of values; while in some other case the Boolean basis is more convenient as multiplication is equivalent to AND.

The degree of a polynomial is basis invariant, but the weight is not. The following lemma shows the direction from the Boolean basis to the Fourier Basis, proved in Section 2.

**Lemma 1.6.** For any polynomial \(f: \{0, 1\}^n \to \mathbb{R}\) on the Boolean input basis, we have a polynomial representing the same function on the Fourier basis with the same weight.

The other direction is not always true. For example, as shown in the following claims, PARITY and OR have large weights on \(\{0, 1\}^n\), even though PARITY has constant weight on \([-1, 1]^n\) with degree \(n\), and OR has much smaller weight for large degrees on \([-1, 1]^n\) as shown in Theorem 1.1. Claim 1.8 shows that it is impossible to get approximate degree-weight tradeoffs for OR over \(\{0, 1\}\). For completeness we present their proofs in Section 8.

**Claim 1.7.** For any \(\varepsilon \in (0, 1)\), the weight of any polynomial \(f\) that \(\varepsilon\)-approximates PARITY: \(\{0, 1\}^n \to \{-1, 1\}\) is at least \((1-\varepsilon)2^n\).

**Claim 1.8.** For any fixed \(\varepsilon \leq \frac{1}{3}\), the weight of any polynomial \(f\) that \(\varepsilon\)-approximates OR: \(\{0, 1\}^n \to \{0, 1\}\) is \(2^{\Omega(\sqrt{n})}\).

Therefore approximate degree-weight tradeoff upper bounds on \(\{0, 1\}^n\) are stronger than those on \([-1, 1]^n\). In fact, to prove Theorem 1.3 for symmetric functions on \([-1, 1]^n\), we actually prove the following stronger result on \(\{0, 1\}^n\) for \(\text{EXACT}_{n,n-t}\), where

\[
\text{EXACT}_{n,r}(x) = \begin{cases} 
1 & \text{if the Hamming weight of } x \text{ is } r, \\
0 & \text{otherwise.}
\end{cases}
\]

Note that both \(\text{EXACT}_{n,t}\) and \(\text{EXACT}_{n,n-t}\) belong to the class \(\text{SYM}_{n,t}\) for \(0 \leq t \leq \frac{n}{2}\), but on \(\{0, 1\}^n\) we can only prove the theorem for \(\text{EXACT}_{n,n-t}\) since \(\text{EXACT}_{n,t} = 1 - \text{OR}_n\) for \(t = 0\).

**Theorem 1.9.** For every \(\varepsilon, k, n, t\) such that \(\sqrt{n(\log(1/\varepsilon) + t)} \leq k \leq n\) and \(0 \leq t \leq \frac{n}{2}\), there is a polynomial \(p: \{0, 1\}^n \to \mathbb{R}\) that \(\varepsilon\)-approximates \(\text{EXACT}_{n,n-t}\) with degree \(O(k)\) and weight \(2^{O(n(\log(1/\varepsilon)+t)/k)}\).

A straightforward corollary using Lemma 1.6 is that the same parameters also work for \([-1, 1]^n\). In particular, as \(\text{AND}_n = \text{EXACT}_{n,n}\), we get the following approximate degree-weight tradeoff upper bound for AND with arbitrary accuracy on both basis, in contrast to OR. Note that \(\text{AND}_n\) has constant weight on \(\{0, 1\}^n\) with degree \(n\), matched by this result. Also note that by Theorem 1.2 and De Morgan’s rule this upper bound is tight over \([-1, 1]\) for \(k = (1 - \Omega(1))n\), thus also tight over \(\{0, 1\}\) for the same range of \(k\) by Lemma 1.6.

**Corollary 1.10.** For every \(\varepsilon, n, k\) satisfying \(\sqrt{n\log(1/\varepsilon)} \leq k \leq n\), \(\text{AND}_n\) can be \(\varepsilon\)-approximated on \(\{0, 1\}^n\) and on \([-1, 1]^n\) in degree \(O(k)\) and weight \(2^{O(n(\log(1/\varepsilon)/k)})\).

It is instructive to see why for OR we can only use OR \(\in \text{SYM}_{n,0}\) and thus the weaker result for \(\text{SYM}_{n,0}\) on \([-1, 1]^n\). The reason is that if we try to use De Morgan’s rule on \(\{0, 1\}^n\) from \(\text{AND}_n\), by substituting each \(x_i\) with \(1 - x_i\), the weight will be blown up to be exponential in the degree as Claim 2.2 will show, eliminating the potential degree-weight tradeoff.
1.3 Our results: \((k, \delta)\)-indistinguishability

One of our motivations for these approximation results comes from our interest in indistinguishability. Two distributions on \(n\) bits are called \(k\)-wise indistinguishable if the marginals on any \(k\) bits are identical. It seems natural to ask which functions are fooled by \(k\)-wise indistinguishability, or in other words cannot distinguish any two \(k\)-wise indistinguishable distributions. Linear programming duality shows that \(k\)-wise indistinguishability fools a function \(f\) if and only if the approximate degree of \(f\) is at most \(k\) \cite[Theorem 1.1]{BIVW16}. We will have more discussions about that in Section 1.4.

We study a natural relaxation of indistinguishability \cite{BIVW16}, defined next.

**Definition 1.11.** Two distributions on \(n\) bits are \((k, \delta)\)-indistinguishable if the marginals on any \(k\) bits are \(\delta\)-close in statistical distance.

A function \(f : \{0,1\}^n \to \mathbb{R}\) is \(\varepsilon\)-fooled by \((k, \delta)\)-indistinguishability if for any two \((k, \delta)\)-indistinguishable distributions \(P\) and \(Q\) we have \(|\mathbb{E}[f(P)] - \mathbb{E}[f(Q)]| \leq \varepsilon\).

Actually in the aforementioned paper, Bogdanov and Williamson \cite{BW17} proved tradeoffs results in terms of \((k, \delta)\)-indistinguishability. They showed that if \(f\) can be \(\varepsilon\)-approximated on \([-1,1]^n\) in degree \(k\) and weight \(w\), then \(f\) is \(\varepsilon\)-fooled by \((k, \delta)\)-indistinguishability for \(\delta = \varepsilon / w\). Using this they showed that \(k \geq \sqrt{n}\), \((k, \delta)\)-indistinguishable fools \(\text{OR}\) for any \(\delta = 2^{-O(n/k)}\). They also show that this is tight. However, as mentioned before, they only consider fooling by constant error.

Using this connection in \cite{BW17} (see also Theorem 2.4), tradeoffs between degree and weight imply tradeoffs between \(k\) and \(\delta\). Therefore the following “fools” theorems for \(\text{OR}\), symmetric functions, and \(t\)-\text{CNF/DFN}\) follow from our degree-weight tradeoff upper bounds for approximating these functions.

**Theorem 1.12.** For every \(\varepsilon, n,\) and \(k\) satisfying \(\Omega\left(\sqrt{n \log(1/\varepsilon)}\right) \leq k \leq n, \ (k, 2^{-O(n \log(1/\varepsilon)/k)})\) -indistinguishability \(\varepsilon\)-fools \(\text{OR}_n\).

**Theorem 1.13.** For every \(\varepsilon, n, t,\) and \(k\) satisfying \(\Omega\left(\sqrt{n \log(1/\varepsilon) + t}\right) \leq k \leq n, \ (k, 2^{-O(n \log(1/\varepsilon) + t)/k)})\) -indistinguishability \(\varepsilon\)-fools any function \(f \in \text{SYM}_{n,t}\).

**Theorem 1.14.** For every \(\varepsilon, n, t,\) and \(k\) satisfying \(n^{1/t} (\log(1/\varepsilon))^{1/t} \leq k \leq n\), there exists constant \(c_t\) depending on \(t\) such that \((c_t \cdot k, 2^{-c_t \cdot n \log(1/\varepsilon)^{1/t}/k^{1/t}})\) -indistinguishability \(\varepsilon\)-fools \(t\)-\text{CNF/DFN}\) on \(n\) variables.

We also prove the following “does not fool” theorems, matching the first two “fools” results. Theorem 1.15 shows that Theorem 1.12 is tight for all \(k \leq n\), while Theorem 1.16 shows that Theorem 1.13 is tight for \(k = (1 - \Omega(1))n\). Using Theorem 2.4, they imply the degree-weight tradeoff lower bounds in Theorem 1.2 and 1.4. This is how the latter are proved in this paper.

**Theorem 1.15.** For every \(\varepsilon, n,\) and \(k, \ (k, 2^{-\Omega(n \log(1/\varepsilon)/k)})\) -indistinguishability doesn’t \(\varepsilon\)-fool \(\text{OR}_n\).

**Theorem 1.16.** There exists a constant \(c' < 1\) such that for every \(\varepsilon, n, t,\) and \(k\) with \(k \leq c' n\) and \(0 \leq t \leq \frac{n}{2}\), there exists function \(f \in \text{SYM}_{n,t}\) such that \((k, 2^{-\Omega(n \log(1/\varepsilon) + t)/k)})\) -indistinguishability doesn’t \(\varepsilon\)-fool \(f\).

The independent work by Bogdanov et al. \cite{BMTW19}, mentioned earlier, also obtained similar “does not fool” result for symmetric functions with constant \(\varepsilon\) (moreover, unlike ours, their distributions do not depend on \(k\)).
Finally, we improve the result in [BIVW16] about k-wise indistinguishability vs. (k, δ)-indistinguishability, analogous to the k-wise independence vs. almost k-wise independence results in [AGM03, Theorem 2.1]. [OZ18]. This result is tight because of the distributions given in [OD14, Theorem 1.2] when k is constant.

**Theorem 1.17.** If P and Q are (k, δ)-indistinguishable, then they are O(ε^k n^{k/2 δ})-close to P' and Q' that are k-wise indistinguishable.

### 1.4 Our results: reproving approximate degree lower bounds in the language of indistinguishability

We suggest that indistinguishability could be a more convenient framework to prove approximate degree lower bounds. To illustrate, we reprove (in Section 7) the following known approximate-degree lower bounds in the language of indistinguishability (for the first item, this presentation already appeared in lecture notes [Vio17, Lecture 8-9]). We find the proofs more intuitive than the originals.

**Claim 1.18.** Let \( \widehat{\deg}_\varepsilon(f) \) denote the \( \varepsilon \)-approximate degree of f over \{0, 1\}. Then

1. \( \widehat{\deg}_{1/3}(\AND_m \circ \OR_n) = \Omega(\sqrt{mn}) \) [BT13];
2. \( \widehat{\deg}_\varepsilon(\AND_m \circ \OR_n) = \Omega(\sqrt{n}) \) for \( \varepsilon = 1/2 - 2^{-\Theta(m)} \) [BT17];
3. \( \widehat{\deg}_\varepsilon(\text{GapMAJ}_m \circ f_n) = \Omega(\deg_{1/3}(f_n)) \) for \( \varepsilon = 1/2 - 2^{-\Theta(m)} \) [BCH+17] where \( \text{GapMAJ}_m \) is any function that outputs 1 on inputs of Hamming weight at least \( \varepsilon m \) and 0 on inputs of Hamming weight at most \( \varepsilon/2 m \);
4. \( \widehat{\deg}_{1/3}(g_m \circ f_n) = \Omega(\deg_{1/3}(g_m) \cdot \deg_{\varepsilon}(f_n)) \) for \( \varepsilon = 1/2 - 1/m^\alpha \) with \( \alpha > 1 \) [She13];
5. \( \widehat{\deg}_m(\XOR_m \circ f) = \Omega(m \cdot \deg_{\varepsilon}(f)) \) and \( \widehat{\deg}_m(\AND_m \circ f) = \Omega(m \cdot \deg_{\varepsilon}(f)) \) [She12].

It will be interesting to present the proofs of more advanced results, such as the AC^0 lower bound [BT17] and the surjectivity lower bound [BKT18], in this language.

### 1.5 Techniques

**Existence of low degree-weight polynomials.** As observed in [STT12, BW17], the Chebyshev polynomials \( T_d \) has degree d and weight \( 2^{O(d)} \), and by composing it with the monomial \( x^{k/d} \), which has high-degree but weight just one, we can get a polynomial \( T_d(x^{k/d}) \) with larger degree \( O(k) \), whose weight is only \( 2^{O(d)} \), and maintains some of the properties similar to those we are looking for from \( T_k(x) \). For example it is bounded on \([0,1]\) and has derivative \( \geq d^2 \cdot \frac{k}{2} \geq kd \) for \( x > 1 \).

At a high level, Theorem 1.9 follows by applying such an idea to the construction by Sherstov [She18] for EXACT_{n,n-t}. The crux of his construction is to first \( \varepsilon \)-approximate inputs of Hamming weight \{0, 1, \ldots, n - \ell \} \cup \{n - t\} with a number \( \ell \) that will be quite large for small \( \varepsilon \), by a simple application of Chebyshev polynomials. Then he multiplies this approximant with a set of auxiliary polynomials, each zeroing out the value of the approximant on inputs of one specific Hamming weight in \{n - t + 1, \ldots, n - t - 1\} \cup \{n - t + 1, \ldots, n\}, also using Chebyshev polynomials but with carefully designed “shifts”, i.e. \( T_k(ax + b) \) with suitable a and b. For the first part, we basically replace the usage of \( T_k(x) \) by \( T_d(x^{k/d}) \) to get degree-weight tradeoff for a suitable \( d \). For the second part, we use \( T_d(ax^{k/d} + b) \) instead, and we need to prove different bounds on a and b. It is also more involved to combine these two parts in our proof, as we have to carefully choose \( k \) for
each auxiliary polynomial to satisfy the degree and weight constraints. Finally Theorem 1.3 follows from Theorem 1.9 on \([-1,1]^n\) by writing symmetric functions as linear combinations of EXACTs, and in particular we get Theorem 1.1 as \(\text{OR}_n \in \text{SYM}_{n,0}\).

For Theorem 1.5 our proof is simpler than Sherstov’s for \(t\)-\text{CNF} [She08], as we are only considering approximating them on \([-1,1]^n\) instead of \([-1,1]^{m\leq n}\). The latter means that the Hamming weight is restricted to be at most \(n\) but the input length \(m\) could be much larger. Essentially his construction decomposes a \(t\)-\text{CNF} into an AND composed with \((t-1)\)-\text{CNFs} inductively for each \(t\). Therefore we use polynomials with degree-weight tradeoff as an outer approximation for the AND function and inner approximations for the \((t-1)\)-\text{CNFs}, and by tweaking the parameters we get a polynomial with degree-weight tradeoff. As mentioned earlier, we exploit the good dependence on \(\varepsilon\) in Corollary 1.10 for AND\(_n\) as we need to set \(\varepsilon\) exponentially small in the inner approximations.

**“Does not fool” theorems.** The notion of fooling by \((k,\delta)\)-indistinguishability does not seem to have a dual characterization, because there does not seem to be a way to express statistical tests in the dual LP. Indeed in Theorem 2.4 while we are considering the weight of the approximations in the dual, we are essentially restricting the statistical tests to the parity tests in the primal, which are not equivalent and can be separated easily for small-bias distributions [NN93]. Therefore degree-weight tradeoff lower bounds do not imply “does not fool” results. Instead we use a different method.

For Theorem 1.15 and 1.16 we reduce it to the case of \(k\)-wise indistinguishability (that is \(\delta = 0\)) by Lemma 5.1, generalizing the proof in [BW17]. By inserting 0’s into some random indices, we generate \((k,\delta)\)-indistinguishable distributions from \(k'\)-wise indistinguishable distributions while keeping their Hamming weight, for suitable settings of \(k,\delta,\) and \(k'\). Then the result follows from approximate degree lower bound of symmetric functions.

The proof of Theorem 1.17 follows the proof in [OZ18], which applies to independence rather than indistinguishability.

1.6 Organization

In Section 2 we provide useful facts about Chebyshev polynomials, weights, and its connection to \((k,\delta)\)-indistinguishability. In Section 3 we prove Theorem 1.17. In Section 4 we prove Theorem 1.3 for symmetric functions and in particular Theorem 1.1 for OR, thus also proving Theorem 1.13 and 1.12. We prove matching lower bounds (Theorem 1.2, 1.4, 1.15, 1.16) in Section 5. In Section 6 we prove Theorem 1.5 and 1.14 for \(t\)-\text{CNF}. We prove Claim 1.18 in Section 7 and we provide complementary proofs of Claim 1.7 and 1.8 in Section 8. Finally we list some open problems in Section 9.

2 Preliminaries

Let \([n]\) denote the set \(\{1,2,\ldots,n\}\).

**Weight of polynomials.** We denote the weight of polynomial \(p\) by \(\|p\|\). On \([-1,1]^n\), \(\|p\|\) is the \(\ell_1\) Fourier weight of \(p\) [O’D14]. It has the following properties.

**Claim 2.1 ([She18, Fact 2.7]).** For any polynomials \(p\) and \(q\),

- \(\|ap\| = |a| \cdot \|p\|\) for any \(a \in \mathbb{R}\);
- \(\|p + q\| \leq \|p\| + \|q\|\);
- \(\|p \cdot q\| \leq \|p\| \cdot \|q\|\).
Claim 2.2 ([BW17 Fact 8, 9]). For any univariate polynomial \( p \) of degree \( k \),

1. if \( q(x) = p(ax^2 + b) \) where \(|a| + |b| \geq 1 \) and \( t \geq 1 \), then \( \|q\| \leq (|a| + |b|)k\|p\| \);
2. if \( q(x_1, \ldots, x_n) = p(\sum_{i=1}^n x_i/n) \) then \( \|q\| \leq \|p\| \).

Change of basis. We present a sketch of proof for the change of basis theorem here.

Proof of Lemma 1.6. Define \( g : \{-1, 1\}^n \to \mathbb{R} \) by \( g(x) = f\left(\frac{1-x_1}{2}, \frac{1-x_2}{2}, \ldots, \frac{1-x_n}{2}\right) \), and the result follows from a multivariate version of Claim 2.2(i) with \(|a| + |b| = 1\). \(\square\)

Chebyshev polynomials. Chebyshev polynomials (c.f. [Che98]), denoted as \( T_d \) for each degree \( d \), is a sequence of orthogonal univariate polynomials that can be uniquely defined by \( T_d(\cos x) = \cos dx \) for each \( d \). Its value is given by \( T_d(x) = \frac{1}{2}\left((x + \sqrt{x^2 - 1})^d + (x - \sqrt{x^2 - 1})^d\right) \).

Claim 2.3 (c.f. [She18 BW17]). For degree-\( d \) Chebyshev polynomial \( T_d \), we have the following properties:

1. \( T_d(1) = 1 \);
2. \( T_d(\cos(\frac{2i-1}{2}\pi)) = 0 \), for \( i \in [d] \);
3. \( |T_d(z)| \leq 1 \) for \( z \in [-1, 1] \);
4. \( T'_d(t) \geq d^2 \) for \( t \in [1, \infty) \), so \( T_d \) is monotonically increasing on \([1, \infty)\);
5. \( T_d(1 + \delta) \geq 2^{d\delta - 1} \) for \( \delta \in [0, 1] \);
6. \( \|T_d\| \leq 2^{d^2} \).

Fooling by \((k, \delta)\)-Indistinguishability. The following theorem shows that low-degree low-weight approximation implies fooling by \((k, \delta)\)-indistinguishability.

Theorem 2.4 ([BW17]). Given any function \( f : \{-1, 1\}^n \to \mathbb{R} \), for any \( k \) and \( \delta \) we have

\[
\max_{P,Q: (k,\delta)\text{-indist.}} |\mathbb{E}[f(P)] - \mathbb{E}[f(Q)]| \leq \min_{g: \varepsilon\text{-approx. } f, \deg(g) \leq k} 2\varepsilon + 2\delta\|g\|.
\]

3 Proof of Theorem 1.17

More generally we are going to prove that for any \( k \leq n \), any two distributions \( P \) and \( Q \) on \( \{-1, 1\}^n \) are \( w \)-close to some \( k \)-wise indistinguishable distributions \( P' \) and \( Q' \), where \( w = e^k \sqrt{\sum_{|S| \leq k} (\mathbb{E}[\chi_S(P)] - \mathbb{E}[\chi_S(Q)])^2} \).

To prove this theorem, we need the following lemmas.

Lemma 3.1. Let \( \phi : \{-1, 1\}^n \to \mathbb{R}^{\geq 0} \) be a polynomial of degree at most \( k \). Then

\[
\|\hat{\phi}\|_2 = \sqrt{\sum_{|S| \leq k} \hat{\phi}(S)^2} \leq e^k\hat{\phi}(\emptyset).
\]

Proof. This lemma is essentially the same as Lemma 2.1 in [OZ18]. We have

\[
\|\hat{\phi}\|_2 = \mathbb{E}[\phi^2(x)] \leq e^k\mathbb{E}[|\phi(x)|] = e^k\mathbb{E}[\phi(x)] = e^k\hat{\phi}(\emptyset),
\]

where the first step comes from Parseval’s Theorem ([OD14 Section 1.4]), the second step holds by hypercontractivity ([OD14 Theorem 9.22]), the third step follows from the fact that \( \phi(x) \geq 0 \) for all \( x \), and the last step follows from standard Fourier analysis ([OD14 Proposition 1.8]). \(\square\)
Lemma 3.2 (Farkas’ Lemma). Let $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$. Then exactly one of the following two statements is true:

1. There exists an $x \in \mathbb{R}^n$ such that $Ax = b$ and $x \geq 0$.
2. There exists a $y \in \mathbb{R}^m$ such that $A^T y \geq 0$ and $b^T y < 0$.

Proof of Theorem 1.17. Given distributions $P$ and $Q$, let $b_S = \mathbb{E}[\chi_S(P)] - \mathbb{E}[\chi_S(Q)]$ for each $|S| \leq k$. We are going to find distributions $P''$ and $Q''$ such that for all $1 \leq |S| \leq k$,

$$\mathbb{E}[\chi_S(P'')] - \mathbb{E}[\chi_S(Q'')] = -\frac{b_S}{w}.$$

Suppose such $P''$ and $Q''$ exist, then we set $P' = \frac{P + wP''}{1+w}$ and $Q' = \frac{Q + wQ''}{1+w}$. Then the statistical distance $\Delta(P, P') \leq \frac{w}{1+w}$ and similarly for $Q$ and $Q'$. We also have

$$\mathbb{E}[\chi_S(P')] - \mathbb{E}[\chi_S(Q')] = \frac{1}{1+w} \left( \mathbb{E}[\chi_S(P)] - \mathbb{E}[\chi_S(Q)] + w(\mathbb{E}[\chi_S(P'')] - \mathbb{E}[\chi_S(Q'')]) \right) = 0,$$

for all $1 \leq |S| \leq k$, therefore $P'$ and $Q'$ are $k$-wise indistinguishable.

To prove the existence of $P''$ and $Q''$, we write it as an LP feasibility problem with variables $p(x)$ for $x \in \{-1, 1\}^n$ corresponding to $P''(x)$ and $q(x)$ for $Q''(x)$, and the following constraints.

\[
\begin{align*}
\sum_{x \in \{-1, 1\}^n} p(x) &= 1 \\
\sum_{x \in \{-1, 1\}^n} q(x) &= 1 \\
\sum_{x \in \{-1, 1\}^n} \chi_S(x)p(x) - \sum_{x \in \{-1, 1\}^n} \chi_S(x)q(x) &= -\frac{b_S}{w} & \text{for each } 1 \leq |S| \leq k \\
p(x) &\geq 0 & \text{for each } x \in \{-1, 1\}^n \\
q(x) &\geq 0 & \text{for each } x \in \{-1, 1\}^n
\end{align*}
\]

By Farkas’ Lemma, to prove that it is feasible is equivalent to prove that the following LP is infeasible, with unconstrained variables $y_\emptyset$, $y'_\emptyset$, and $y_S$ for $1 \leq |S| \leq k$.

\[
\begin{align*}
y_\emptyset + \sum_{1 \leq |S| \leq k} y_S \chi_S(x) &\geq 0 & \text{for each } x \in \{-1, 1\}^n \\
y'_\emptyset - \sum_{1 \leq |S| \leq k} y_S \chi_S(x) &\geq 0 & \text{for each } x \in \{-1, 1\}^n \\
y_\emptyset + y'_\emptyset - \frac{1}{w} \sum_{1 \leq |S| \leq k} y_S b_S &< 0
\end{align*}
\]

To prove that it is infeasible, it suffices to prove that any assignments satisfying the first two sets of constraints must violate the third one. Summing up the first set of constraints for all $x \in \{-1, 1\}^n$, we get $y_\emptyset \geq 0$, and similarly we have $y'_\emptyset \geq 0$. Now define a polynomial $\phi = y_\emptyset + \sum_{1 \leq |S| \leq k} y_S \chi_S$, then the degree of $\phi$ is at most $k$ and the first two sets of constraints become

$$\phi(x) \geq 0 \text{ for each } x \in \{-1, 1\}^n,$$

$$\phi(x) \leq y_\emptyset + y'_\emptyset \text{ for each } x \in \{-1, 1\}^n.$$

By Lemma 3.1 we have $\sqrt{\sum_{1 \leq |S| \leq k} y_S^2} \leq e^k y_\emptyset$, and we set $w = e^k \sqrt{\sum_{1 \leq |S| \leq k} b_S^2}$. Note that we have $w = O(e^k n^{k/2}/\delta)$ when $P$ and $Q$ are $(k, \delta)$-indistinguishable. Therefore

$$\frac{1}{w} \sum_{1 \leq |S| \leq k} y_S b_S \leq \frac{1}{w} \sum_{1 \leq |S| \leq k} |y_S||b_S| \leq \frac{1}{w} \sqrt{\sum_{1 \leq |S| \leq k} y_S^2} \sqrt{\sum_{1 \leq |S| \leq k} b_S^2} \leq e^k y_\emptyset \sqrt{\sum_{1 \leq |S| \leq k} b_S^2} = y_\emptyset \leq y_\emptyset + y'_\emptyset,$$

where the second inequality holds by Cauchy-Schwarz. This violates the third constraint thus completes our proof. □
4 Proofs of Theorem 1.1, 1.3, 1.12, 1.13, and 1.9

We prove Theorem 1.9 first, since it is the basis of all the other theorems in this section.

Warm-up for proving Theorem 1.9

Our goal is to construct a univariate polynomial $p^{*}$ to $\varepsilon$-approximate EXACT$_{n,n-t}$ such that $|p^{*}(\frac{i}{n}) - 1| \leq \varepsilon$ for $i = n - t$ and $|p^{*}(\frac{i}{n})| \leq \varepsilon$ for all $i \in [n] \setminus \{n - t\}$. Besides, $p^{*}$ must have the desired degree and weight.

We can already get a good approximation using Chebyshev polynomials. Let

$$\ell = \log \frac{2}{\varepsilon} + t, \quad d = \sqrt{n\ell}.$$ 

Without loss of generality assume $d \in \mathbb{N}$, define univariate polynomials $q_0$ and $p_0$ by

$$q_0(z) = T_d \left( \frac{n}{n - \ell} \cdot z \right), \quad p_0(z) = q_0 \left( \frac{n - t}{n} \right).$$

For $z \in [0, \frac{n - \ell}{n}]$, we have $\frac{n}{n - \ell} \cdot z \leq 1$ thus by Claim 2.3 (iii) we have $|q_0 \left( \frac{i}{n} \right)| \leq 1$ for all $i = 0, 1, \ldots, n - \ell$. The value of $q_0 \left( \frac{n - t}{n} \right)$ is also large enough, as by Claim 2.3 (iii) we have

$$q_0 \left( \frac{n - t}{n} \right) = T_{d} \left( 1 + \frac{\ell - t}{n - \ell} \right) \geq 2^{\sqrt{n\ell} - 1} \geq 2^{(\ell - t) - 1} = \frac{1}{\varepsilon},$$

where the third step uses $\frac{n - \ell}{n - \ell} \geq 1$ and $\ell \geq \ell - t$. Therefore $|p_0 \left( \frac{i}{n} \right)| \leq \varepsilon$ for all $i = 0, 1, \ldots, n - \ell$ and $p_0 \left( \frac{n}{n} \right) = 1$ for $i = n - t$, thus $p_0$ is a good approximation for these $i$’s. We have deg($p_0$) = $d$ and $\|p_0\| = 2^{O(d)}$, which are fixed by $n$, $t$, and $\varepsilon$.

To get approximations that have degree-weight tradeoff, we would decrease $d$ and increase the power of $\frac{n}{n - \ell} \cdot z$ inside $T_d$ accordingly. We use the same $\ell$, and for any $k \geq \sqrt{n\ell}$, let

$$d = \frac{n \ell}{k},$$

thus $d$ decreases when $k$ increases. Without loss of generality assume $d, \frac{k}{d} \in \mathbb{N}$, define

$$q_1(z) = T_d \left( \left( \frac{n}{n - \ell} \cdot z \right)^{\frac{k}{d}} \right), \quad p_1(z) = q_1 \left( \frac{n - t}{n} \right).$$

Similarly we have $|q_1 \left( \frac{i}{n} \right)| \leq 1$ for all $i = 0, 1, \ldots, n - \ell$. We also get

$$q_1 \left( \frac{n - t}{n} \right) = T_d \left( \left( 1 + \frac{\ell - t}{n - \ell} \right)^{\frac{k}{d}} \right) \geq T_d \left( 1 + \frac{\ell - t}{n - \ell} \cdot \frac{k}{d} \right) \geq 2^{\sqrt{\frac{k}{d} \cdot \frac{\ell - t}{n - \ell}} - 1} \geq 2^{(\ell - t) - 1} = \frac{1}{\varepsilon},$$

where the second step uses Bernoulli’s inequality and Claim 2.3 (iv), the third step uses Claim 2.3 (v), the fourth step uses $\sqrt{kd} = \sqrt{n\ell} \geq \sqrt{n(\ell - t)}$ and $\frac{n}{n - \ell} \geq 1$. Therefore $p_1$ is a good approximation for some $i$, namely

$$|p_1 \left( \frac{i}{n} \right)| \leq \varepsilon \quad \text{for all } i = 0, 1, \ldots, n - \ell, \quad (1)$$

$$p_1 \left( \frac{i}{n} \right) = 1 \quad \text{for } i = n - t. \quad (2)$$

The degree of $q_1$ and $p_1$ is $d \cdot \frac{k}{d} = k$. Now we are going to bound their weights. We can write $q_1(z) = T_d(a \cdot z^{k/d})$ with $a = \left( \frac{n}{n - \ell} \right)^{k/d}$, so by Claim 2.3 (vi) and Claim 2.1 (ii),

$$\|q_1\| \leq \|T_d\| \cdot a^d = 2^{O(d)} \cdot \left( 1 + \frac{\ell}{n - \ell} \right)^{k} \leq 2^{O(d)} \cdot \varepsilon^{n - \ell},$$

where
where the last step uses $1 + x \leq e^x$ for all $x \in \mathbb{R}$. We can assume $\ell \leq \frac{3}{5} n$, otherwise $\sqrt{\frac{nt}{n-\ell}} = \Omega(n)$ thus $d = \Omega(n)$ so we can simply use $p_0$. Thus we have $n(n-\ell) \geq \frac{1}{8} n^2 \geq \frac{1}{8} k^2$, so $\frac{kl}{n-\ell} = O\left(\frac{n^2}{k}\right) = O(d)$, therefore $\|q_1\| \leq 2^{O(d)}$, which is the same as $\|T_d\|$ up to the $O(\cdot)$ in the exponent. In other words, we can ignore effect of the scaling term $\frac{n}{n-\ell}$ to the weight.

Consequently,

$$\|p_i\| \leq \|q_1\| \cdot \varepsilon \leq 2^{O(d)} = 2^{O(n(\log(1/\varepsilon)+t)/k)}.$$ (3)

Therefore $p_1$ has the degree-weight tradeoff we need in Theorem 1.9.

The problem of $p_1$ is that for $i = n-\ell+1, \ldots, n-t-1$ and $n-t+1, \ldots, n$, we have no bound on its value. We need the following construction of auxiliary polynomials $T_{n,m}^{(k)}$ with degree-weight tradeoff that can be made zero on some specific points. Multiplying $p_1$ by such $T_{n,m}^{(k)}$, we can zero out the value on those $i$‘s and get the desired approximations.

Lemma 4.1. For every $n, m, k$ such that $0 \leq m < n$ and $\sqrt{\frac{n}{n-m}} \leq k \leq \frac{n}{n-m}$, there is a univariate polynomial $T_{n,m}^{(k)}$ of degree $O(k)$ and weight $2^{O\left(\frac{n}{m(n-m)}\right)}$ such that

$$T_{n,m}^{(k)}(1) = 1,$$ (4)

$$T_{n,m}^{(k)}(\frac{m}{n}) = 0,$$ (5)

$$\left|T_{n,m}^{(k)}(z)\right| \leq 1, \text{ for any } z \in [0, 1].$$ (6)

Our proof generalizes Sherstov’s in the sense that the above lemma for auxiliary polynomials already gives some degree-weight tradeoff via parameter $k$. The range of $k$ is chosen carefully such that the proof of this lemma works and it can also be used in the proof of Theorem 1.9. Building on the warm-up and assuming the lemma, we now present the proof of Theorem 1.9.

Proof of Theorem 1.9. Now we use the same $d$ and $\ell$ as discussed above, and define the following univariate polynomial $p^*$ by

$$p^*(z) = p_1(z) \prod_{m=m-n-\ell}^{n-t-1} T_{n-t,m}^{(k_m')}(\frac{n}{n-t} \cdot z) \prod_{m=m-n-t+1}^{n} 1 - (T_{m,n-t}^{(k_m'')}(\frac{n}{m} \cdot z))^2,$$

using the auxiliary polynomials from Lemma 4.1 where

$$k_m' = k \sqrt{\frac{n-t}{n\ell(n-t-m)}}, \text{ for } m = n-\ell, \ldots, n-t-1,$$

$$k_m'' = k \sqrt{\frac{m}{nt(m-n+t)}}, \text{ for } m = n-t+1, \ldots, n.$$

First, we need to show that our applications of Lemma 4.1 are legitimate.

- $\sqrt{\frac{n-t}{n-m-\ell}} \leq k_m' \leq \sqrt{\frac{n-t}{n-m-\ell}}$ for $m \in [n-t-1] \setminus [n-\ell-1]$: on one hand, we have $k \geq \sqrt{n\ell}$ so $k_m' \geq \sqrt{\frac{n-t}{n-m-\ell}}$; on the other hand, we have $n-m \leq \ell$ and $t < \ell \leq n$, so $\frac{n-t}{n-m-\ell} \leq \frac{n-t}{n-m} \leq \frac{n-t}{n-m-\ell}$, thus by $k \leq n$ we have $k_m' \leq \sqrt{\frac{n(n-t)}{\ell(n-t-m)}} \leq \frac{n-t}{n-m-\ell}$.

- $\sqrt{\frac{m}{m-n-t}} \leq k_m'' \leq \sqrt{\frac{m}{m-n-t}}$ for $m \in \mathbb{N} \setminus [n-t]$; on one hand, we have $k \geq \sqrt{n\ell}$ and $\ell \geq t$ so $k_m'' \geq \sqrt{\frac{m}{m-n-t}} \geq \sqrt{\frac{m}{m-n-t}}$; on the other hand, we have $n-m < t \leq n$, so $\frac{n-m}{t(n-m-t)} = \frac{m}{m-n-t}$, thus by $k \leq n$ we have $k_m'' \leq \sqrt{\frac{mn}{t(n-m-t)}} \leq \frac{m}{m-n-t}$. 

10
Second, we are going to show that $p^*$ is a good approximation. By Lemma 4.1 and Equation 11 we have

$$\left| p^* \left( \frac{i}{n} \right) \right| \leq \varepsilon \cdot \prod_{m=n-\ell}^{n-t-1} 1 \cdot \prod_{m=n-t+1}^{n} \left( 1 - 0^2 \right) = \varepsilon \quad \text{for all } i = 0, 1, \ldots, n - \ell - 1. \quad (7)$$

For all $i = n - \ell, \ldots, n - t - 1$, when $m = i$ we have $T^{(k_m')}_{n-t,m} \left( \frac{n}{n-t} \cdot \frac{i}{n} \right) = T^{(k_m')}_{n-t,m} \left( \frac{m}{n-t} \right) = 0$.

For all $i = n - t + 1, \ldots, n$, when $m = i$ we have $T^{(k_m'')}_{m,n-t} \left( \frac{m}{n} \cdot \frac{i}{n} \right) = T^{(k_m'')}_{m,n-t} \left( 1 \right) = 1$ thus $1 - \left( T^{(k_m'')}_{m,n-t} \left( \frac{m}{n} \cdot \frac{i}{n} \right) \right)^2 = 0$. We also have $T^{(k_m'')}_{n-t,m} \left( \frac{n}{n-t} \cdot \frac{i}{n} \right) = 1$ and $T^{(k_m'')}_{m,n-t} \left( \frac{m}{n} \cdot \frac{i}{n} \right) = 0$ when $i = n - t$. Therefore

$$p^* \left( \frac{i}{n} \right) = \begin{cases} 0 & \text{for all } i = n - \ell, \ldots, n - t - 1, \\ 1 \cdot \prod_{m=n-\ell}^{n-t-1} 1 \cdot \prod_{m=n-t+1}^{n} \left( 1 - 0^2 \right) = 1, & \text{for } i = n - t, \\ 0 & \text{for all } i = n - t + 1, \ldots, n. \end{cases} \quad (8)$$

Therefore $p^* \left( \frac{i}{n} \right) = 1$ for $i = n - t$ and $\left| p^* \left( \frac{i}{n} \right) \right| \leq \varepsilon$ otherwise.

Now we are going to bound the degree and weight of $p^*$. We have $k_m' = k \sqrt{\frac{n-t}{n(n-m)}} \leq k \frac{\sqrt{\ell}}{\sqrt{t(n-t)}}$ and $k_m'' = k \sqrt{\frac{n-t}{n(n-m)}} \leq k \frac{\sqrt{\ell}}{\sqrt{t(n-t)}}$. By Lemma 4.1

$$\deg(p^*) \leq k + \sum_{m=n-\ell}^{n-t-1} O(k_m') + \sum_{m=n-t+1}^{n} O(k_m'') \leq O \left( k + \frac{k}{\sqrt{\ell}} \sum_{m=n-\ell}^{n-t-1} \frac{1}{\sqrt{n-t-m}} + \frac{k}{\sqrt{t}} \sum_{m=n-t+1}^{n} \frac{1}{\sqrt{m-n+t}} \right)$$

$$= O \left( k + \frac{k}{\sqrt{\ell}} \sum_{i=1}^{\ell-t} \frac{1}{\sqrt{i}} + \frac{k}{\sqrt{t}} \sum_{i=1}^{\ell-t} \frac{1}{\sqrt{i}} \right) = O(k), \quad (9)$$

where in the last step we use $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} = O(\sqrt{n})$ for any $n \in \mathbb{N}$. Similar to the argument in the calculation of $\|q_1\|$, we can safely ignore effects of the scaling terms $\frac{n}{n-t}$ and $\frac{n}{m}$ to the weight of $p^*$. By (3) and Lemma 4.1 we have

$$\log \|p^*\| \leq O(d) + \sum_{m=n-\ell}^{n-t-1} O \left( \frac{n-t}{k_m'(n-t-m)} \right) + \sum_{m=n-t+1}^{n} O \left( \frac{n}{k_m''(m-n+t)} \right)$$

$$= O \left( \frac{n\ell}{k} + \sum_{m=n-\ell}^{n-t-1} \frac{\sqrt{n\ell(n-t)}}{k} \cdot \frac{1}{\sqrt{n-t-m}} + \sum_{m=n-t+1}^{n} \frac{\sqrt{n(t-m)}}{k} \cdot \frac{1}{\sqrt{m-n+t}} \right)$$

$$\leq O \left( \frac{n\ell}{k} + \frac{n\sqrt{\ell}}{k} \sum_{i=1}^{\ell-t} \frac{1}{\sqrt{i}} + \frac{n\sqrt{t}}{k} \sum_{i=1}^{\ell-t} \frac{1}{\sqrt{i}} \right) = O \left( \frac{n}{k} (\log(1/\varepsilon) + t) \right). \quad (10)$$

Finally, define $p: \{0,1\}^n \to \mathbb{R}$ by $p(x) = p^* \left( \frac{\sum_{i=1}^{n} x_i}{n} \right)$. The theorem follows from (7)-(10) and Claim 2.2 [ii].

Now we prove Theorem 1.3 and Theorem 1.13. We are working on the Fourier basis since we need to negate our input variables. Since $OR_n \in SYM_{n,0}$, we get Theorem 1.1 from Theorem 1.3 and Theorem 1.12 from Theorem 1.13.
Proof of Theorem 1.3. By Lemma 1.6 we can get the same results for EXACT on the Fourier basis as in Theorem 1.9. Then we can write \( f(x) \) as

\[
f(x) = c + \sum_{i=0}^{t} c_i' \cdot \text{EXACT}_{n,i}(x) + \sum_{i=0}^{t} c_i'' \cdot \text{EXACT}_{n,n-i}(x)
\]

\[
= c + \sum_{i=0}^{t} c_i' \cdot \text{EXACT}_{n,n-i}(\xi) + \sum_{i=0}^{t} c_i'' \cdot \text{EXACT}_{n,n-i}(x),
\]

where \( c, c_i' \)'s, and \( c_i'' \)'s are fixed reals, and \( \xi = (-x_1, \ldots, -x_n) \). Now let \( \varepsilon' = \frac{\varepsilon}{2n+2} \), then for \( 0 \leq i \leq t \), \( \sqrt{n(\log(1/\varepsilon') + i)} = O\left(\sqrt{n(\log(1/\varepsilon) + t)}\right) \) so we can ignore the constant factor difference and apply Theorem 1.9 with \( \varepsilon = \varepsilon' \) and the same \( k \) for each \( \text{EXACT}_{n,n-i} \). The degrees of the approximations for EXACT are \( O(k) \), so the total degree is also \( O(k) \). The weights of the approximations for EXACT are \( 2O(n(\log(1/\varepsilon') + i)/k) = 2O(n(\log(1/\varepsilon) + t)/k) \). By Claim 2.1, the total weight is \( O(t)2O(n(\log(1/\varepsilon) + t)/k) = 2O(n(\log(1/\varepsilon) + t)/k) \).

Proof of Theorem 1.13. Apply Theorem 1.3, set \( \delta = \frac{\varepsilon}{2n} = 2 - O\left(\frac{e}{4}(\log(1/\varepsilon)+t)\right) \). Then it follows from Theorem 2.4.

4.1 Proof of Lemma 4.1

Let \( d = \frac{2n}{k(n-m)} \) so \( k = \frac{k^2(n-m)}{2n} \). As \( m < n \) we have \( d > 0 \) and \( \frac{k}{d} > 0 \). Without loss of generality assume \( d, \frac{k}{d} \in \mathbb{N} \), we can define

\[
T_{n,m}^{(k)}(z) = T_d\left(a \cdot z^{k/d} + b\right),
\]

where \( a, b \in \mathbb{R} \) are parameters to be set and \( T_d \) is the degree-\( d \) Chebyshev polynomial. We have \( \text{deg}(T_{n,m}^{(k)}) \leq d \cdot \frac{k}{d} = k \).

We set \( a, b \) such that

\[
a + b = 1, \tag{12}
\]

\[
a\left(\frac{m}{n}\right)^{k/d} + b = \cos\left(\frac{\pi}{2d}\right), \tag{13}
\]

then Property (4) follows from (12) and Claim 2.3 (ii), and Property (5) follows from (13) and Claim 2.3 (ii) with \( i = 1 \).

Our goal is to prove \( 0 \leq a \leq 1 \). Assume this is true. From (12) we have \( b \in [0,1] \). Hence \( a \cdot z^{k/d} + b \) is increasing in \( z \in [0,1] \), mapping \([0,1]\) to \([b,1]\) \subseteq [0,1]. Therefore Property (6) follows from Claim 2.3 (iii). Besides, we have \( |a| + |b| = a + b = 1 \), so by Claim 2.3 (vi) and Claim 2.2, we have \( \|T_{n,m}^{(k)}\| = 1 \cdot 2O(d) = 2O\left(\frac{n}{k(n-m)}\right) \). Therefore \( T_{n,m}^{(k)}(z) \) is the desired polynomial.

To see that \( a \in [0,1] \), we solve the linear equations (12) and (13) to get

\[
a = \frac{1 - \cos\left(\frac{\pi}{2k}\right)}{1 - \left(\frac{m}{n}\right)^{k/d}}, \tag{14}
\]

Because \( m < n \), we have \( \frac{m}{n} < 1 \), thus \( 1 - \left(\frac{m}{n}\right)^{k/d} > 0 \). We always have \( 1 - \cos\left(\frac{\pi}{2k}\right) \geq 0 \). Therefore from (14) we have \( a \geq 0 \). On the other hand, let \( u = \frac{n}{m} \), from (14) we can get

\[
a \leq \frac{1}{2} \left(\frac{\pi}{2k}\right)^2 \frac{k^2}{2n^2} \frac{1}{1 - e^{-\frac{k^2}{2n^2}}}, \tag{15}
\]
where the first step uses \( \cos x \geq 1 - \frac{1}{2}x^2 \) for \( x \in \mathbb{R} \) in the numerator, and the second step uses the value of \( d \) in the numerator and \( 1 + x \leq e^x \) for \( x \in \mathbb{R} \) in the denominator. Since 
\[
\sqrt{\frac{n}{n-m}} \leq k \leq \frac{n}{n-m} \quad \text{and} \quad m < n,
\]
we have \( 0 < \frac{k^2}{2m} \leq \frac{1}{2} \). Consider the function \( f(z) = \frac{z}{1-e^{-z}} \) on \( z \in (0, \frac{1}{2}] \). Its derivative \( f'(z) = \frac{e^z(e^z-z-1)}{(e^z-1)^2} > 0 \) for \( z \in (0,1] \), hence \( f(z) \) is increasing in \( (0, \frac{1}{2}] \), thus \( f(z) \leq f\left(\frac{1}{2}\right) \). From (15) we have \( a \leq \frac{n^2}{16}f\left(\frac{1}{2}\right) = \frac{\pi^2\sqrt{n}}{32(\sqrt{e}-1)} < 1 \), finishing our proof.

\[\square\]

5 Proofs of Theorem 1.2, 1.4, 1.15, and 1.16

First we generalize the proof in \[\text{[BWT]}\], reducing the problem into fooling by \( k \)-wise indistinguishability. We use \( \ell \) to deal with non-constant \( \varepsilon \) and symmetric functions with non-constant \( t \).

**Lemma 5.1.** Let \( c'' \) be any constant. For every \( n, k \) and \( \ell \) satisfying \( \frac{c''}{16}\sqrt{n\ell} \leq k \leq c'' n \), there exists \( n' \) with \( \ell \leq n' \leq n \) such that if there exist \( k' \)-wise indistinguishable distributions \( P', Q' \) on \( \{0,1\}^{n'} \) for \( k' = c''\sqrt{n\ell} \), then there exist distributions \( P, Q \) on \( \{0,1\}^n \) such that the Hamming weight distribution \( |P| \equiv |P'|, \; |Q| \equiv |Q'|, \) and \( P \) and \( Q \) are \( (k, 2^{-\Omega(n\ell/k)}) \)-indistinguishable.

**Proof.** To sample from \( P \), and \( Q \) respectively, we select \( n' \)-many indices from \( [n] \) uniformly at random as “active” indices and then fill in these \( n' \) indices using a random sample from \( P', \) and \( Q' \) respectively; for other indices we simply set them to be 0. Obviously this process keeps the Hamming weight of the samples.

Suppose \( P' \) and \( Q' \) are \( k' \)-wise indistinguishable with \( k' = c''\sqrt{n\ell} \) for some constant \( 0 < c'' < 1 \). For any \( k \) indices \( S \) of \( P \) and \( Q \), if there are at most \( k' \) active indices in \( S \), then their projections on \( S \) are identical by \( k' \)-wise indistinguishability. Therefore the probability that statistical test on \( k \) bits can distinguish \( P \) from \( Q \) is bounded by the probability that such event doesn’t happen. By tail bounds of hypergeometric distribution \[\text{[Hoe]}\], we have

\[
\Pr[\text{more than } k' \text{ active indices in } S] \leq e^{-kD\left(\frac{k'}{k}\|\frac{n'}{n}\right)} = 2^{-\Omega(kD\left(\frac{k'}{k}\|\frac{n'}{n}\right))},
\]

where \( D(a|b) = a \log \frac{a}{b} + (1-a) \log \frac{1-a}{1-b} \) is the Kullback-Leibler divergence. By a lower bound from Hellinger distance \( H \), for any \( p \) and any \( a \geq 16 \), we have

\[
D(ap||p) \geq 2H^2(ap||p) \geq (\sqrt{ap} - \sqrt{p})^2 = (\sqrt{a} - 1)^2p \geq \frac{1}{2}ap,
\]

where the last step comes from the fact that \( 2\sqrt{a} \leq \frac{a}{2} \) for \( a \geq 16 \). Now we set \( n' = \frac{c''^2 n^2 \ell}{16k} \), then we have \( k' = \frac{c''^2 n^2 \ell}{16k} \), thus \( k' / n' = 16 \), therefore we have

\[
2^{-\Omega(kD\left(\frac{k'}{k}\|\frac{n'}{n}\right))} \leq 2^{-\Omega(kk'/k)} = 2^{-\Omega(k'')} = 2^{-\Omega(n\ell/k)}.
\]

For \( \ell \leq n' \), we need \( \frac{c''^2 n^2 \ell}{16k} \geq 1 \) thus \( k \leq \frac{c''}{16} n \). For \( n' \leq n \), we need \( \frac{c''^2 n^2 \ell}{16k} \leq 1 \) thus \( k \geq \frac{c''}{16} \sqrt{n\ell} \).

Combining the following equivalence between approximate degrees and bounded indistinguishability, with the \( \varepsilon \)-approximate degree lower bound of symmetric functions due to Buhrman et al. \[\text{[BCdW]}\], improving \[\text{[Pat]}\], we can obtain \( k \)-wise indistinguishable distributions that don’t fool symmetric functions.
Theorem 5.2 ([BIVW16 Theorem 1.1]). For every $\varepsilon$, $n$, and $f: \{0,1\}^n \to \{0,1\}$ the following are equivalent:

1. $f$ is not $\varepsilon$-fooled by $k$-wise indistinguishability;
2. The $\varepsilon/2$-approximate degree of $f$ is bigger than $k$.

Theorem 5.3 ([BCdWZ99]). For any $f \in \text{SYM}_{n,t}$, $\deg_\varepsilon(f) = \Omega\left(\sqrt{n(\log(1/\varepsilon) + t)}\right)$.

Now we can prove Theorem 1.16 with $f = \text{EXACT}_{n,t} \in \text{SYM}_{n,t}$ for $0 \leq t \leq \frac{n}{2}$, and similarly for $f = \text{THR}_{n,t+1}$ where $\text{THR}_{n,r}$ is True iff the Hamming weight of its input is at least $\frac{r}{2}$. In particular for $\text{OR}_n = \text{THR}_{n,1}$ we get Theorem 1.15 by applying $t = 0$. Note that for $t = O(1)$ (in particular for OR), this theorem works for all $k$ as $(n, \varepsilon^{0.999})$-indistinguishability doesn’t $\varepsilon$-fool any non-constant function.

Proof of Theorem 1.16. We consider function $\text{EXACT}_{n,t}$. Let $\ell = \log(2/\varepsilon) + t$, $c''$ be the constant in $\Omega(\cdot)$ in Theorem 5.3. Set $c' = \frac{c''}{16}$.

For $k \leq c' \sqrt{n\ell}$, by Theorem 5.3 and Theorem 5.2 $k$-wise indistinguishability does not $\varepsilon$-fool $\text{EXACT}_{n,t}$, hence the theorem for $k \leq c' \sqrt{n\ell}$ as $2^{c''n\ell/k} \leq 2^{-k}$.

For $c'' \sqrt{n\ell} \leq k \leq \frac{c''}{16} n$, apply Lemma 5.1 to get $n'$ then Theorem 5.3 and Theorem 5.2 give us $k'$-wise indistinguishable distributions $P'$ and $Q'$ on $\{0,1\}^n$ that don’t $\varepsilon$-fool $\text{EXACT}_{n',t}$. The theorem follows by applying Lemma 5.1 again to get distributions $P, Q$. □

Theorem 2.4 shows that a polynomial $p$ that $(\varepsilon/2)$-approximates $f$ in degree $k$ must have weight at least $\varepsilon/\delta$ if $(k, \delta)$-indistinguishability does not $\varepsilon$-fool $f$. Let $c < 1$ be the constant in the $\Omega(\cdot)$ in Theorem 1.16. Then we get Theorem 1.2 from Theorem 1.15 and Theorem 1.3 from Theorem 1.16.

6 Proofs of Theorem 1.5 and 1.14

We first give a proof for $t = 2$, then generalize it for larger $t$.

Proof of Theorem 1.5 with $t = 2$. Given a 2-CNF $F$, we can first transform $F$ by the following procedure. For each $i \in [n]$, from $F$ we pick up all the terms that contain $x_i$ unnegated. Let $m_i$ be the number of such terms and $C_1^{(i)}, C_2^{(i)}, \ldots, C_{m_i}^{(i)}$ be these terms. We remove $x_i$ from them to get $C_1^{(i)}, C_2^{(i)}, \ldots, C_{m_i}^{(i)}$. If $m_i = 0$, define $f_i'(x) = \neg x_i$, otherwise define it as $\bigwedge_{j=1}^{m_i} C_j^{(i)}$. Remove all the original terms from $F$, continue for the next $i$ until $i = n$. Then we do this procedure on the remaining terms of $F$ for each $i \in [n]$ again, but this time we are collecting terms that contain $\neg x_i$ and defining $f_i''(x)$ similarly. At last we define

$$F_1(x) = \bigwedge_{i=1}^{n} x_i \lor f_i'(x),$$

$$F_2(x) = \bigwedge_{i=1}^{n} \neg x_i \lor f_i''(x),$$

and by distributive law we have $F = F_1 \land F_2$. Note that all the $f_i'$s and $f_i''$s are 1-CNFs, namely ANDs of literals.

1Note that $\text{THR}_{n,r} \in \text{SYM}_{n,r-1}$ for $r \leq \frac{n}{2} + 1$, equivalently $\text{THR}_{n,t+1} \in \text{SYM}_{n,t}$ for $t \leq \frac{n}{2}$.
2Indeed $(n, \delta)$-indistinguishability for any $\delta > \varepsilon$. 

14
We define \( F' : \{-1, 1\}^n \times \{-1, 1\}^{2n} \to \{0, 1\} \) by \( F'(x, y) = \bigwedge_{i=1}^{2n} y_i \lor f_i(x) \), where \( f_i = \begin{cases} f_i' & \text{for } i \in [n] \\ f_i'' & \text{for } i \in [2n] \setminus [n] \end{cases} \). If we set

\[
y_i = \begin{cases} x_i & \text{for } i \in [n] \\ -x_{i-n} & \text{for } i \in [2n] \setminus [n] \end{cases},
\]

we will have \( F(x) = F'(x, y) \) for all \( x \in \{-1, 1\}^n \) by (17) and (18). Therefore it suffices to prove this theorem for \( F'(x, y) \). Note here it is important to choose the input basis of \( F' \) to be the Fourier basis so we can negate the variables without increasing the weight.

Let \( N = 2n \) and \( B \in [N] \) be an integer to be determined later. Let \( S_1, \ldots, S_N \) be an even partition of \([N]\) into subsets of size \( B \). For each \( i \in [\frac{N}{B}] \) we can define \( h_i : \{-1, 1\}^n \times \{-1, 1\}^{S_i} \to \{0, 1\} \) by \( h_i(x, y) = \bigwedge_{j \in S_i} y_j \lor f_j(x) \) and we have \( F'(x, y) = \bigwedge_{i=1}^{\frac{N}{B}} h_i(x, y) = \bigwedge_{\frac{N}{B}} (h_1(x, y), \ldots, h_N(x, y)) \), where \( \bigwedge_{\frac{N}{B}} : \{0, 1\}^\frac{N}{B} \to \{0, 1\} \) is the AND function on \( \frac{N}{B} \) bits on the Boolean basis. Our goal is to approximate the outer AND function and the inner \( h_i \)'s carefully so that the total degree and weight can be bounded as we want.

For any subset \( T \subseteq S \subseteq [N] \), define the indicator function \( \mathbb{I}(; T, S) : \{-1, 1\}^N \to \{0, 1\} \) by

\[
\mathbb{I}(y; T, S) = \prod_{j \in T} \frac{y_j + 1}{2} \prod_{j \in S \setminus T} \frac{1 - y_j}{2},
\]

so it is 1 if and only if \( y \) represents \textit{False} on \( T \) and \textit{True} on \( S \setminus T \). Thus each \( h_i \) can be written using interpolation as

\[
h_i(x, y) = \sum_{T \subseteq S_i} \left( \bigwedge_{j \in T} f_j(x) \land \bigwedge_{j \in T} -y_j \land \bigwedge_{j \in S \setminus T} y_j \right)
= \sum_{T \subseteq S_i} \left( \bigwedge_{j \in T} f_j(x) \cdot \mathbb{I}(y; T, S_i) \right).
\]  

Now suppose we have a polynomial \( p : \{0, 1\}^\frac{N}{B} \to \mathbb{R} \) that \( \varepsilon_{\text{out}} \)-approximates the outer \( \text{AND}_N \) function within degree \( d_{\text{out}} \) and weight \( w_{\text{out}} \), where \( \varepsilon_{\text{out}}, d_{\text{out}}, \) and \( w_{\text{out}} \) are parameters to be set later. We called this \( p \) the outer approximation. We can write it as

\[
p(z) = \sum_{U \subseteq \left[ \frac{N}{B} \right]} a_U \prod_{i \in U} z_i,
\]

where \( a_U \in \mathbb{R} \), and \( \sum_{U} |a_U| = w_{\text{out}} \) by definition. Define \( F'' : \{-1, 1\}^n \times \{-1, 1\}^{2n} \to \mathbb{R} \) by substituting the outer \( \text{AND}_N \) function in \( F' \) by \( p : F''(x, y) = p(h_1(x, y), \ldots, h_N(x, y)) \).

Since \( p \) is a point-wise approximation, we have

\[
\|F'' - F'\|_\infty \leq \|p - \text{AND}_N\|_\infty = \varepsilon_{\text{out}}.
\]

On the other hand, we can expand \( F'' \) as

\[
F''(x, y) = \sum_{U \subseteq \left[ \frac{N}{B} \right]} a_U \prod_{i \in U} h_i(x, y)
\]

15
and the third step uses (27), (28). What remains to bound is the degree and weight of \( \tilde{\epsilon} \).

\[
\begin{align*}
&= \sum_{U \subseteq \mathbb{N}} a_U \prod_{i \in U} \sum_{T \subseteq S_i} \left( \bigwedge_{j \in T} f_j(x) \cdot \mathbb{I}(y; T, S_i) \right) \\
&= \sum_{U \subseteq \mathbb{N}} a_U \sum_{T: U \rightarrow \mathcal{P}([N]) \ni i \in U} \prod_{T(i) \subseteq S_i, \forall i \in U} \left( \bigwedge_{j \in T(i)} f_j(x) \right) \left( \prod_{i \in U} \mathbb{I}(y; T(i), S_i) \right) \\
&= \sum_{U \subseteq \mathbb{N}} a_U \sum_{T: U \rightarrow \mathcal{P}([N])} \left( \bigwedge_{i \in \text{img}(T)} f_j(x) \cdot \mathbb{I}(y; \text{img}(T), U_i \in U; S_i) \right).
\end{align*}
\]

where \( \text{img}(T) \) denotes the image of function \( T: U \rightarrow \mathcal{P}([N]) \) and \( \mathcal{P}([N]) \) is the powerset of \( [N] \), the first step uses \([22]\), the second step uses \([21]\), the third step exchanges the product with the sum, the fourth step uses properties of multiplication, and the last step uses the fact that multiplication on the Boolean basis is equivalent to \( \text{AND} \). It is important that we set the input basis of the outer approximation \( p \) (thus the output basis of \( \bigwedge_{i \in \text{img}(T)} f_j(x) \cdot \mathbb{I}(y; \text{img}(T), U_i \in U; S_i) \)) to be the Boolean basis even though the input basis of the whole function is the Fourier basis; otherwise the last step doesn’t hold.

Each \( \bigwedge_{j \in \text{img}(T)} f_j(x) \) is a 1-CNF (i.e. \( \text{AND} \)) since \( f_j(x) \) is 1-CNF. Suppose we can approximate \( \bigwedge_{j \in \text{img}(T)} f_j(x) \)'s within error \( \varepsilon_{\text{in}}, \) degree \( d_{\text{in}}, \) and weight \( w_{\text{in}}, \) where \( \varepsilon_{\text{in}}, d_{\text{in}}, \) and \( w_{\text{in}} \) are parameters to be set later. We called these \( \bigwedge_{j \in \text{img}(T)} f_j(x) \)'s the inner approximations. Then we can define \( \mathcal{F}'': \{-1,1\}^n \times \{-1,1\}^{2n} \rightarrow \mathbb{R} \) by

\[
\mathcal{F}''(x, y) = \sum_{U \subseteq \mathbb{N}} a_U \sum_{T: U \rightarrow \mathcal{P}([N])} \left( \bigwedge_{i \in \text{img}(T)} f_j(x) \cdot \mathbb{I}(y; \text{img}(T), U_i \in U; S_i) \right).
\]

Observe that for any \( y \in \{-1,1\}^N \), for any \( U \subseteq \mathbb{N} \) with \( |U| \leq d_{\text{out}} \), there is only one \( T: U \rightarrow [N] \) with \( T(i) \subseteq S_i, \forall i \in U \) such that \( \mathbb{I}(y; \text{img}(T), U_i \in U; S_i) = 1 \): it is uniquely determined by the value of \( y \) on \( U_i \in U; S_i \); all other summands will vanish. Therefore we have

\[
\| \mathcal{F}'' - \mathcal{F}' \|_{\infty} \leq \sum_{U \subseteq \mathbb{N}} a_U \varepsilon_{\text{in}} \leq \sum_{U \subseteq \mathbb{N}} |a_U| \varepsilon_{\text{in}} = w_{\text{out}} \varepsilon_{\text{in}}.
\]

Hence if we set

\[
\varepsilon_{\text{out}} = \frac{\varepsilon}{2},
\]

\[
\varepsilon_{\text{in}} = \frac{\varepsilon}{2w_{\text{out}}},
\]

then \( \mathcal{F}'' \varepsilon \)-approximates \( F' \) since \( \| \mathcal{F}'' - F' \|_{\infty} \leq \| \mathcal{F}'' - \mathcal{F}' \|_{\infty} + \| \mathcal{F}' - F' \|_{\infty} \leq w_{\text{out}} \varepsilon_{\text{in}} + \varepsilon_{\text{out}} = \varepsilon \), where the first steps uses the triangular inequality, the second step uses \([23]\) and \([26]\), and the third step uses \([27]\). \([28]\). What remains to bound is the degree and weight of \( \mathcal{F}'' \).
Denote the degree of $\widetilde{F}^i$ as $d$, and the weight of $\widetilde{F}^i$ as $w$. Note that by \((20)\) we have
\[
\deg(\Pi(\cdot; \mathrm{img}(T), \bigcup_{i \in U} S_i)) = |\bigcup_{i \in U} S_i| = |U|B \leq d_{out}B, \tag{29}
\]
\[
\|\Pi(\cdot; \mathrm{img}(T), \bigcup_{i \in U} S_i)\| \leq 1. \tag{30}
\]
For each $U$, there are at most $2^{|\bigcup_{i \in U} S_i|} \leq 2^{d_{out}B}$ $T$’s, since $T$ satisfies that $T(i) \subseteq S_i, \forall i \in U$. Therefore we have
\[
d \leq d_{out}B + d_{in} \tag{31}
\]
\[
\log w \leq \log \left( \sum_{U \subseteq \left[ \frac{N}{2} \right]} a_U 2^{d_{out}B} w_{in} \right) \leq \log w_{out} + d_{out}B + \log w_{in}, \tag{32}
\]
where the first inequality comes from \((25)\) and \((29)\), and the second inequality follows from \((25)\), \((30)\), Claim 2.1, and the observation above. What remains is to set $d_{in}, w_{in}, d_{out},$ and $w_{out}$ to get the desired bounds on $d$ and $w$.

By assumption $k$ satisfies $n^2 (\log(1/\varepsilon))^{1/3} \leq k \leq n$. For convenience we will ignore the difference between $N$ and $n$, and use them interchangeably, as they are the same up to a multiplicative factor of 2. Set
\[
B = \frac{N}{k}, \tag{33}
\]
\[
k_{in} = k, \tag{34}
\]
\[
k_{out} = \sqrt{k \log(1/\varepsilon)}, \tag{35}
\]
where $k_{in}$ and $k_{out}$ are numbers to be used later as the $k$’s for the inner approximations and the outer approximation, respectively.

For the outer approximation, from \((33)\) and \((35)\) we have
\[
\sqrt{\frac{N}{B}} \log \frac{1}{\varepsilon_{out}} = \sqrt{k \log(1/\varepsilon)} = k_{out} \leq k = \frac{N}{B},
\]
where the first equality follows from \((27)\) and ignoring the constant factor, the inequality comes from $k \geq N^{2/3} (\log(1/\varepsilon))^{1/3}$ and the fact that $\log(1/\varepsilon) \leq N$ (otherwise we can get all the bounds trivially). This means we can apply Corollary 1.10 over $\{0, 1\}$ with $\varepsilon = \varepsilon_{out}, k = k_{out},$ and $n = \frac{N}{B}$ to get the outer approximating polynomial $p$ with the following parameters:
\[
d_{out} = O(k_{out}) = O\left(\sqrt{k \log(1/\varepsilon)}\right), \tag{36}
\]
\[
\log w_{out} = O\left(\frac{N}{Bk_{out}} \log \frac{1}{\varepsilon_{out}}\right) = O\left(\sqrt{k \log(1/\varepsilon)}\right), \tag{37}
\]
using \((27)\), \((33)\), and \((35)\).

For the inner approximations, we have $k_{in} = k \leq N$, and we also have
\[
\sqrt{N \log \frac{1}{\varepsilon_{in}}} = O\left(\sqrt{N \log \frac{w_{out}}{\varepsilon}}\right) = O\left(\sqrt{N \sqrt{k \log(1/\varepsilon)}}\right) \leq O(k) = O(k_{in}), \tag{38}
\]
where the first step uses \((28)\), the second step uses \((37)\), and the third step uses $k \geq N^{2/3} (\log(1/\varepsilon))^{1/3}$. Therefore we can invoke Corollary 1.10 over $\{-1, 1\}$ with $\varepsilon = \varepsilon_{in}, k = k_{in},$ and $n = N$ to get the inner approximations $\wedge_{j \in \mathrm{img}(T)} f_j(x)$ with the following parameters:
\[
d_{in} = O(k_{in}) = O(k), \tag{39}
\]
\[ \log w_{in} = O\left( \frac{N}{k_{in}} \log \frac{1}{\varepsilon_{in}} \right) = O\left( \frac{N}{k} \log w_{out} \right) = O\left( \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon)} \right), \quad (40) \]

using (28), (34), and (37).

Finally, combining (31), (33), (36) and (39), we get

\[ d = O\left( \frac{N}{k} \sqrt{k \log(1/\varepsilon) + k} \right) = O\left( \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon) + k} \right) = O(k), \]

where the last step follows from \( k \geq N^{2/3}(\log(1/\varepsilon))^{1/3} \). Combing (32), (33), (36), (37), and (40), we get

\[ \log w = O\left( \sqrt{k \log(1/\varepsilon)} + \frac{N}{k} \sqrt{k \log(1/\varepsilon) + \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon)} + \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon) + k} \right) = O\left( \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon)} \right), \]

since \( k \leq N \) implies \( \frac{N}{\sqrt{k}} \sqrt{\log(1/\varepsilon)} \geq \sqrt{k \log(1/\varepsilon)} \).

**Proof of Theorem 1.15** By induction on \( t: t = 1 \) is Corollary 1.10 for AND. Now assume the theorem holds for \((t-1)\)-CNF, and we want to prove it for \( t\)-CNF. Similarly to the proof for \( t = 2\), Equations (17)-(32) remain the same. The outer function is still AND \( \frac{N}{B} \), while the inner functions \( \wedge_{j \in \text{img}(T)} f_j(x) \)’s become \((t-1)\)-CNFs. What remains is to set \( d_{in}, w_{in}, d_{out}, \text{and } w_{out} \) to get the desired bounds on \( d \) and \( w \).

By assumption \( k \) satisfies \( n^{1/t}(\log(1/\varepsilon))^{1/t} \leq k \leq n \). Set

\[ B = \frac{N}{k^{2/t}}, \]

\[ k_{in} = k, \]

\[ k_{out} = k^{1/t}(\log(1/\varepsilon))^{1/t}. \]

For the outer approximation, it’s not hard to verify that \( \sqrt{\frac{N}{B} \log \frac{1}{\varepsilon_{out}}} = k_{out} \leq \frac{N}{B} \), so we can apply Corollary 1.10 to get

\[ d_{out} = O(k_{out}) = O\left( k^{1/t} (\log(1/\varepsilon))^{1/t} \right), \]

\[ \log w_{out} = O\left( \frac{N}{B k_{out}} \log \frac{1}{\varepsilon_{out}} \right) = O\left( k^{1/t} (\log(1/\varepsilon))^{1/t} \right). \]

For the inner approximation, it’s not hard to verify that \( N^{1/(t-1)} (\log \frac{1}{\varepsilon_{in}})^{1/(t-1)} \leq k_{in} \leq N \), so we can use the induction hypothesis for \((t-1)\)-CNF to get

\[ d_{in} \leq c_{t-1} \cdot k_{in} = c_{t-1} \cdot k, \]

\[ \log w_{in} \leq c_{t-1} \cdot \frac{N}{k_{in}^{1/(t-1)}} \left( \log \frac{1}{\varepsilon_{in}} \right)^{1/(t-1)} \leq c'_{t-1} \cdot \frac{N}{k^{1/t}} (\log(1/\varepsilon))^{1/t}, \]

where \( c'_{t-1} \) is some constant depending on \( c_{t-1} \).

Combining all these bounds, for some constant \( c_t \) (depending only on \( t \)) we get

\[ d = O\left( \frac{N}{k^{1/t}} (\log(1/\varepsilon))^{1/t} \right) + c_{t-1} \cdot k \leq c_t \cdot k, \]

\[ \log w = O\left( k^{1/t} (\log(1/\varepsilon))^{1/t} \right) + c_{t-1} \cdot \frac{N}{k^{1/t}} (\log(1/\varepsilon))^{1/t} \leq c_t \cdot \frac{N}{k^{1/t}} (\log(1/\varepsilon))^{1/t}. \]

**Proof of Theorem 1.14** Use Theorem 1.5 and Theorem 2.4.
7 Proof of Claim 1.18

First, we have the following lemma for compositions of indistinguishable distributions. Essentially it is equivalent to the dual block composition method in [BT13], but we find it more intuitive and easier to prove.

**Lemma 7.1 ([Vi17] Lecture 6-7).** Suppose that distributions $A^0, A^1$ over $\{0,1\}^{n_A}$ are $k_A$-wise indistinguishable; and distributions $B^0, B^1$ over $\{0,1\}^{n_B}$ are $k_B$-wise indistinguishable. For $b \in \{0,1\}$, define $C^b$ over $\{0,1\}^{n_A+n_B}$ by first drawing a sample $x \in \{0,1\}^{n_A}$ from $A^b$, then replacing each bit $x_i$ by a sample of $B^{x_i}$ independently. Then $C^0$ and $C^1$ are $(k_A \cdot k_B)$-wise indistinguishable.

**Proof.** Consider any set $S \subseteq \{1,\ldots,n_A \cdot n_B\}$ of $k_A \cdot k_B$ bit positions. We will show that they have the same distribution in $C^0$ and $C^1$.

View the $n_A \cdot n_B$ as $n_A$ blocks of $n_B$ bits. Call a block $K$ of $n_B$ bits heavy if $|S \cap K| > k_B$; call the other blocks light. There are at most $k_A$ heavy blocks by assumption, so that the distribution of the (entire) heavy blocks are the same in $C^0$ and $C^1$ by $k_A$-wise indistinguishability of $A^0$ and $A^1$. Furthermore, conditioned on any outcome for the $A^b$ samples in $C^b$, those bit positions in the light blocks have the same distribution in both $C^0$ and $C^1$ by $k_B$-wise indistinguishability of $B^0$ and $B^1$ and independence between blocks.

Therefore $C^0$ and $C^1$ are $k_A \cdot k_B$-wise indistinguishable. \(\square\)

Also observe that we can only consider disjoint distributions for indistinguishability.

**Claim 7.2 ([Vi17] Lecture 8-9).** For any function $f$, and for any $k$-wise indistinguishable distributions $A^0$ and $A^1$, if $f$ can distinguish with probability $\varepsilon$ then there are distributions $B^0$ and $B^1$ with the same property and disjoint supports. (By disjoint support we mean for any $x$ either $\Pr[B^0 = x] = 0$ or $\Pr[B^1 = x] = 0$.)

**Proof.** Let distribution $C$ by the “common part” of $A^0$ and $A^1$. That is to say, we define $C$ such that $\Pr[C = x] := \min\{\Pr[A^0 = x], \Pr[A^1 = x]\}$ divided by some constant that normalize $C$ into a distribution. We can write $A^0$ and $A^1$ as

$$A^0 = pC + (1-p)B^0,$$

$$A^1 = pC + (1-p)B^1,$$

where $p \in (0,1)$, $B^0$ and $B^1$ are two distributions. Clearly $B^0$ and $B^1$ have disjoint supports.

Then we have

$$\mathbb{E}[f(A^0)] - \mathbb{E}[f(A^1)] = p\mathbb{E}[f(C)] + (1-p)\mathbb{E}[f(B^0)] - p\mathbb{E}[f(C)] - (1-p)\mathbb{E}[f(B^1)]$$

$$= (1-p)((\mathbb{E}[f(B^0)] - \mathbb{E}[f(B^1)])$$

$$\leq \mathbb{E}[f(B^0)] - \mathbb{E}[f(B^1)].$$

Similarly, for all $S \neq \emptyset$ such that $|S| \leq k$, we have $\mathbb{E}[\chi_S(A^0)] - \mathbb{E}[\chi_S(A^1)] = (1-p)(\mathbb{E}[\chi_S(B^0)] - \mathbb{E}[\chi_S(B^1)])$, so $\mathbb{E}[\chi_S(B^0)] - \mathbb{E}[\chi_S(B^1)] = 0$.

Thus if $f$ can distinguish $A^0$ and $A^1$ with probability $\varepsilon$ then it can also distinguish $B^0$ and $B^1$ with such probability. Besides, $B^0$ and $B^1$ are $k$-wise indistinguishable. \(\square\)

Now we can prove approximate degree lower bounds using indistinguishability.
Proof of Claim 1.18. (i) We know that \( \deg_{1/3}(\text{AND}_m) = \Omega(\sqrt{m}) \) and \( \deg_{1/3}(\text{OR}_n) = \Omega(\sqrt{n}) \). By standard error reduction techniques (c.f. [BNRDW07]) \( \deg_e(f) = \Theta(\deg_{1/3}(f)) \) for all constant \( \varepsilon \in (0, \frac{1}{2}) \). By Theorem 5.2 we get \( \Omega(\sqrt{m}) \)-wise indistinguishable distributions \( A^0, A^1 \) s.t. \( \Pr[\text{AND}_m(A^1) = 1] \geq \Pr[\text{AND}_m(A^0) = 1] + 0.99 \), and similarly we have \( B^0, B^1 \) for \( \text{OR}_n \). By Claim 7.2, \( A^0, A^1 \) have disjoint supports, and same for \( B^0, B^1 \). Compose them by Lemma 7.1 to get \( \Omega(\sqrt{mn}) \)-wise indistinguishable distributions \( C^0, C^1 \). It remains to show that \( \text{AND}_m \circ \text{OR}_n \) can distinguish them:

- \( C^0 \): First \( A^0 \) is sampled. As there exists unique \( x = 1^m \) such that \( \text{AND}_m(x) = 1 \), \( \Pr[A^1 = x] > 0 \) thus by disjointness of support \( \Pr[A^0 = x] = 0 \). Therefore we get a string with at least one “0”. But then this “0” is replaced with sample from \( B^0 \). We have \( \Pr[B^0 = 0^n] \geq 0.99 \), and when it happens, \( \text{AND}_m \circ \text{OR}_n \) will return 0.

- \( C^1 \): First \( A^1 \) is sampled, and we know that \( A^1 = 1^m \) with probability at least 0.99. Each bit “1” is replaced by a sample from \( B^1 \), and we know that \( \Pr[B^1 = 0^n] = 0 \) by disjointness of support since \( \Pr[B^0 = 0^n] > 0 \), thus in this case \( \text{AND}_m \circ \text{OR}_n \) will return 1.

Therefore \( \text{AND}_m \circ \text{OR}_n \) is not 0.98-fooled by \( C^0, C^1 \). By Theorem 5.2 and standard error reduction techniques we have \( \deg_{1/3}(\text{AND}_m \circ \text{OR}_n) = \Omega(\sqrt{mn}) \).

(ii) Similarly, we have \( \Omega(\sqrt{n}) \)-wise indistinguishable distributions \( B^0, B^1 \) s.t. \( \Pr[\text{OR}_n(B^1) = 1] \geq \Pr[\text{OR}_n(B^0) = 1] + 0.99 \), thus \( \Pr[\text{OR}_n(B^0) = 1] \leq 0.01 \). We define \( C^b \) as \( m \) independent copies of \( B^b \) for \( b \in \{0, 1 \} \). Obviously \( C^0, C^1 \) are \( \Omega(\sqrt{n}) \)-wise indistinguishable. For \( C^1 \), every copy of \( B^1 \) satisfies \( \Pr[B^1 = 0^n] = 0 \) by disjointness of support, thus \( \Pr[\text{AND}_m \circ \text{OR}_n(C^1) = 1] = 1 \). For \( C^0 \), we have \( \Pr[\text{AND}_m \circ \text{OR}_n(C^0) = 1] \leq 0.01^m = 2^{-9(m)} \). Therefore \( \text{AND}_m \circ \text{OR}_n \) is not \((1 - 2^{-\Theta(m)})\)-fooled by \( C^0, C^1 \), thus by Theorem 5.2 we are done.

(iii) Define \( \text{GapMAJ}_m' \) as the partial function version of \( \text{GapMAJ}_m \) with an extra requirement that it is undefined on inputs of Hamming weight in \( (\frac{1}{2}m, \frac{2}{3}m) \). For a partial function \( g \) with domain \( D \subset \{0, 1\}^m \), define the bounded approximate degree \( \deg_e(g) \) as the minimum degree of polynomial \( p \) such that \( |p(x) - g(x)| \leq \varepsilon \) for \( x \in D \) and \( |p(x)| \leq 1 + \varepsilon \) for \( x \not\in D \). It is easy to see that \( \deg_e(\text{GapMAJ}_m \circ f_n) \geq \deg_e(\text{GapMAJ}_m' \circ f_n) \), so it remains to prove the lower bound for the latter.

Analogous to Theorem 5.2, it is necessary and sufficient to give two \( \Omega(\deg_{1/3}(f_n)) \)-wise indistinguishable distributions \( C^0, C^1 \) such that

\[
\mathbb{E}_{x \sim C^1} \text{GapMAJ}_m' \circ f_n(x) - \mathbb{E}_{x \sim C^0} \text{GapMAJ}_m' \circ f_n(x) - \sum_{x \in D} (C^1(x) + C^0(x)) \geq 2\varepsilon, \tag{41}
\]

where \( D \) is the domain of \( \text{GapMAJ}_m' \circ f_n \), i.e. the distinguishing advantage of \( \text{GapMAJ}_m' \circ f_n \) on \( D \) minus the probability mass of \( C^0 \) and \( C^1 \) outside of \( D \) must be at least \( 2\varepsilon \).

Let \( k = \deg_{1/3}(f_n) \). Similarly as before we can get \( \Omega(k) \)-wise indistinguishable distributions \( B^0, B^1 \) s.t. \( \Pr[f_n(B^1) = 1] \geq \Pr[f_n(B^0) = 1] + 0.99 \). Now for \( b \in \{0, 1\} \), we still define \( C^b \) as \( m \) independent copies of \( B^b \), thus \( C^0, C^1 \) are \( \Omega(k) \)-wise indistinguishable. We have \( \Pr[f_n(B^1) = 1] \geq 0.99 \) and \( \Pr[f_n(B^1) = 0] \leq 0.01 \). Hence in expectation more than 0.99 fraction of the \( m \) independent copies of \( B^1 \) will make \( f_n \) return 1. Therefore by Chernoff bound, on \( C^1 \) the probability that \( \text{GapMAJ}_m' \) gets an input of

\footnote{Indeed by making them disjoint \( A^0, A^1 \) and \( B^0, B^1 \) witness the one-sided approximate degree [KT14] lower bounds of \( \text{AND}_m \) and \( \text{OR}_n \), respectively.}
Hamming weight less than $\frac{2}{3}m$ is at most $2^{-\Theta(m)}$. Similarly on $C^0$ the probability that GapMAJ$_m$ gets an input of Hamming weight larger than $\frac{1}{2}m$ is at most $2^{-\Theta(m)}$. Therefore Inequality $[41]$ holds for $2e = 1 - 2^{-\Theta(m)}$, and we finish the proof.

(iv) Similarly as before we get $A^0, A^1$ for $g_m$ and $B^0, B^1$ for $f_n$. Composing them by Lemma 7.1 gives $\Omega\left(\deg_{1/3}(g_m) \cdot \deg_\epsilon(f_n)\right)$-wise indistinguishable distributions $C^0, C^1$.

Note that now we have $\Pr[f_n(B^0) = 1] \geq \Pr[f_n(B^0) = 1] + (1 - \frac{2}{m^2})$, thus we have $\Pr[f_n(B^0) \neq b] \leq \frac{2}{m^2}$ for both $b \in \{0,1\}$, i.e. $B^b$ errs with probability at most $\frac{2}{m^2}$. Then by union bound, $\Pr[g_m \circ f_n(C^1) = 1] \geq 1 - \frac{1}{3} - m \cdot \frac{2}{m^2} = \frac{2}{3} - o(1)$, and similarly $\Pr[g_m \circ f_n(C^0) = 0] = \frac{2}{3} - o(1)$, thus $g_m \circ f_n$ is not $\frac{1}{6}$-fooled by $C^0, C^1$ and we finish the proof similarly.

(v) The $(m - 1)$-wise indistinguishable distributions $A^0, A^1$ for XOR$_m$ can be explicitly obtained by defining $A^0$ to be the uniform distribution over all strings of $\{0,1\}^m$ with parity 0, and $A^1$ for parity 1. Similarly as before we have $\Omega(\deg_\epsilon(f_n))$-wise indistinguishable distributions $B^0, B^1$ s.t. $\mathbb{E}[f_n(B^1)] = \mathbb{E}[f_n(B^0)] \geq 2\epsilon$. Composing them by Lemma 7.1 gives $\Omega(m \cdot \deg_\epsilon(f_n))$-wise indistinguishable distributions $C^0, C^1$.

Alternatively we can define $C^0, C^1$ inductively by:

- $C^0_1 = B^0, C^1_1 = B^1$;
- for each $k > 1$, for $C^0_k$ first randomly draw $z \in \{0,1\}$, then sample from $B^zC^z_{k-1}$ as result; for $C^1_k$ first randomly draw $z \in \{0,1\}$, then sample from $B^zC^z_{k-1}$.

It is easy to see that $C^0 = C^0_m$ and $C^1 = C^1_m$. For simplicity we convert the output basis from $\{0,1\}$ to $\{-1,1\}$, so XOR$_m \circ f_n$ becomes products of $f_n$’s. Under this basis we have $\mathbb{E}[f_n(B^0)] - \mathbb{E}[f_n(B^1)] \geq 2\epsilon$. Then

$$\mathbb{E}[\text{XOR}_m \circ f_n(C^0_m)] - \mathbb{E}[\text{XOR}_m \circ f_n(C^1_m)]$$

$$= \frac{1}{4} \sum_{z,z' \in \{0,1\}} \mathbb{E}[f_n(B^z) \cdot \text{XOR}_{m-1} \circ f_n(C^z_{m-1})] - \mathbb{E}[f_n(B^{z'}) \cdot \text{XOR}_{m-1} \circ f_n(C^{z'}_{m-1})]$$

$$= \frac{1}{4} \sum_{z,z' \in \{0,1\}} \mathbb{E}[f_n(B^z)] \mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^z_{m-1})] - \mathbb{E}[f_n(B^{z'})] \mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^{z'}_{m-1})]$$

$$= \frac{1}{2} (\mathbb{E}[f_n(B^0)] - \mathbb{E}[f_n(B^1)]) (\mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^0_{m-1})] - \mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^1_{m-1})])$$

$$\geq \frac{1}{2} \cdot 2\epsilon \cdot (\mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^0_{m-1})] - \mathbb{E}[\text{XOR}_{m-1} \circ f_n(C^1_{m-1})]).$$

Therefore by induction we have $\mathbb{E}[\text{XOR}_m \circ f_n(C^0_m)] - \mathbb{E}[\text{XOR}_m \circ f_n(C^1_m)] \geq 2\epsilon^m$, thus $\deg_\epsilon(\text{XOR}_m \circ f_n) = \Omega(m \cdot \deg_\epsilon(f_n))$ by Theorem 5.2.

For AND$_m$, use the same $A^0, A^1$ if $m$ is odd, and switch their roles if $m$ is even. The remaining proof follows similarly except that we keep the output basis to be $\{0,1\}$.

\[\square\]

8 Proofs of Claim 1.7 and 1.8

Proof of Claim 1.7. Suppose $f: \{0,1\}^n \rightarrow \mathbb{R}$ $\epsilon$-approximates PARITY and minimizes the weight. On one hand, we have $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x) \text{PARITY}(x) \in [1 - \epsilon, 1 + \epsilon]$. On the other hand, write $f$ as $f = \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i$, then

$$\sum_{x \in \{0,1\}^n} f(x) \text{PARITY}(x) = \sum_{T \subseteq [n]} (-1)^{|T|} \sum_{S \subseteq T} c_S \sum_{S \subseteq [n]} c_S \sum_{T \supseteq S} (-1)^{|T|} = (-1)^n c_{[n]},$$
where the last step comes from the fact that whenever $S \subseteq [n]$ we have $\sum_{T \supseteq S} (-1)^{|T|} = 0$ as we can arrange such $T$’s into matching pairs that has exactly opposite value of $(-1)^{|T|}$.

Therefore we have $\|f\| \geq |c_{[0]}| \geq (1 - \varepsilon)2^n$. \hfill \qed

**Proof of Claim 1.8** Let $f$ be the polynomial that $\varepsilon$-approximates OR and minimizes the weight. Let $w = \|f\|$. By a sampling argument (c.f. [Zha14], [CMS18]) we can get a polynomial $g : \{0,1\}^n \rightarrow \mathbb{R}$ such that $g \frac{1}{2}$-approximates OR and $g$ has $O(w^2n)$ monomials. Now define $h : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{R}$ by $h(x_1 \cdots x_n, y_1 \cdots y_n) = 1 - g(x_1y_1, \ldots, x_ny_n)$, then $h \frac{1}{3}$-approximates the set disjointness function DISJ, where $x_1 \cdots x_n$ and $y_1 \cdots y_n$ are interpreted as indicators of two sets $X,Y \subseteq [n]$ respectively and $\text{DISJ}(X,Y) = 1$ iff $X \cap Y = \emptyset$. Now $h$ also has $O(w^2n)$ monomials. By Theorem 8 in [BdW01] we get $w = 2^{\Omega(\sqrt{n})}$. \hfill \qed

9 Discussion and Open Problems

An obvious open question is to prove approximate degree-weight tradeoffs for more functions. A central function in the area is Surjectivity. For this it would suffice to have a polynomial approximating OR on the domain $\{-1,1\}_{\leq n}^m$, in which the Hamming of the input is restricted to be at most $n$. [Shi18] showed that the degree of such a polynomial depends on $n$ instead of $m$ as if we are working on $\{-1,1\}^n$. It is natural to ask if the same holds for weight. The answer is negative. To show this, note that the proof of Theorem 1.16 actually gives us $(k,\delta)$-indistinguishable distributions with bounded Hamming weight that don’t fool OR. In particular, for any $\varepsilon, n, m, k$ satisfying $\varepsilon^c \sqrt{\frac{m}{k} \log(1/\varepsilon)} \leq k \leq \frac{\varepsilon}{16} m$ and $n = \varepsilon^2 \frac{m^2 \log(1/\varepsilon)}{k^2}$, we have distributions that are $(k, 2^{-\Omega(m \log(1/\varepsilon)/k)})$-indistinguishable on $\{-1,1\}_{\leq n}^m$ but cannot $\varepsilon$-fool OR. For $m > n$, we have $2^{-\Omega(m \log(1/\varepsilon)/k)} < 2^{-\Omega(n \log(1/\varepsilon)/k)}$ for fixed $k$ and $\varepsilon$. This also means that we need other methods for Surjectivity.

Another open problem is to show tight degree-weight tradeoffs for OR on $\{-1,1\}_{\leq n}^m$. Chandrasekaran et al. [CTUW14 Corollary 5.2] proved that it requires weight roughly at least $(\frac{m}{k\sqrt{n}})^{\sqrt{n}}$ for constant $\varepsilon$, so when $k\sqrt{n} \leq (1 - \Omega(1))m$ it requires $2^{\Omega(\sqrt{n})}$.

Another open problem is to understand how the approximate weight of a symmetric function $f$ changes when $k = \Theta(n)$. In [AFH12], [AFK17] they showed that when $k = n$ for constant error it is very close to $2^{O(\tau(f))}$, where $\tau(f)$ is the smallest number $t' \in [0, \frac{n}{2}]$ such that $f$ or $f \cdot \text{PARITY}$ is constant on inputs of Hamming weight in $(t', n - t')$. Our results show tight bounds of $2^{O(\tau(f))}$ for $k = \Theta(n)$, but $\tau(f)$ could be much larger than $\tau'(f)$ as in the case of PARITY. What happens in between? Can we get a better upper or lower bound?

We also lack a matching “does not fool” result for $t$-CNF as tight approximate degree and weight are not known even for 2-CNF (without promise on the input). The open problem here is to prove lower bounds matching our results for $t$-CNF.

**Acknowledgment**

The authors thank Lijie Chen for showing the idea for proving Claim 1.8. Chin Ho Lee for pointing out the paper [OZ18], and Justin Thaler for pointing out the line of works [STT12], [CTUW14], [BT15]. The authors also thank Mark Bun and Avishay Tal for useful discussions, and anonymous reviewers for valuable feedback. Part of this work was done during the authors’ visit to the Simons Institute for the Theory of Computing.
References


