Learning depth-3 circuits via quantum agnostic boosting

Srinivasan Arunachalam SRINIVASAN.ARUNACHALAM@IBM.COM
IBM Research, Silicon Valley Lab, CA, USA

Arkopal Dutt ARKOPAL@IBM.COM
IBM Research, Cambridge, MA, USA

Alexandru Gheorghiu AGHEORGHIU@IBM.COM
IBM Research, Cambridge, MA, USA

Michael de Oliveira MICHAEL.OLIVEIRA@INL.INT
International Iberian Nanotechnology Laboratory, Braga, Portugal.

Editors: Steve Hanneke and Tor Lattimore

Abstract

We initiate the study of *quantum agnostic learning* of phase states with respect to a function class $\mathcal{C} \subseteq \{c : \{0,1\}^n \to \{0,1\}\}$: given copies of an unknown n-qubit state $|\psi\rangle$ which has fidelity opt with a phase state $|\phi_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{c(x)} |x\rangle$ for some $c \in \mathcal{C}$, output $|\phi\rangle$ which has fidelity $|\langle \phi | \psi \rangle|^2 \geq \mathsf{opt} - \varepsilon$. To this end, we give agnostic learning protocols for the following classes:

1. Size-t decision trees which runs in time $\mathsf{poly}(n, t, 1/\varepsilon)$. This also implies k-juntas can be agnostically learned in time $\mathsf{poly}(n, 2^k, 1/\varepsilon)$.
2. s-term DNF formulas in time $\mathsf{poly}(n, (s/\varepsilon)^{\log\log(s/\varepsilon)\cdot\log(1/\varepsilon)})$.

Our main technical contribution is a *quantum agnostic boosting* protocol which converts a "weak" agnostic learner, which outputs a parity state $|\phi\rangle$ such that $|\langle \phi | \psi \rangle|^2 \geq \mathsf{opt}/\mathsf{poly}(n)$, into a "strong" learner which outputs a superposition of parity states $|\phi'\rangle$ such that $|\langle \phi' | \psi \rangle|^2 \geq \mathsf{opt} - \varepsilon$.

Using quantum agnostic boosting, we give a $n^{O(\log(n/\varepsilon)\cdot\log\log n)}$-time algorithm for ε-learning $\mathsf{poly}(n)$-sized depth-3 circuits (consisting of AND, OR, NOT gates) in the uniform PAC model given quantum examples. Classically, obtaining an algorithm with a similar complexity has been an open question in the PAC model and our work answers this given quantum examples.

Keywords: Quantum learning theory, agnostic learning, PAC learning, constant-depth circuits

Contents

1. Introduction

Learning classical circuits. A central goal in computational learning theory is to determine which natural classes of Boolean functions can be efficiently learned, both in the *Probably Approximately Correct* (PAC) model and in the more challenging *agnostic model*. Circuit classes of small depth provide a canonical test case since they are expressive enough to capture rich computational phenomena, yet structured enough that one might hope for efficient algorithms. The seminal work of Linial, Mansour and Nisan (Linial et al. (1993)) first showed that depth-d circuits on n-bit inputs, consisting of AND, OR, NOT gates (the class of AC^0 circuits) are learnable in time $n^{O(\log^{d-1} n)}$ in the uniform PAC model with only examples. While this provides a general guarantee, it leaves open the question of whether specialized *efficient* algorithms exist for concrete depths of $d = 2, 3, 4, 5$? By the influential work of Naor and Reingold (2004), it is believed that depth-5 circuits are hard to classically learn (*assuming* factoring is hard). This naturally shifts the attention to depths $2, 3, 4$. In particular, the status of learning depth-2 circuits has been a longstanding 30-year old open question, with the best-known algorithm in the PAC model running in time $n^{O(\log n)}$ (Verbeurgt (1998)). Analogous to classical examples in the PAC model, Bshouty and Jackson (1995) introduced *quantum examples* and the quantum PAC model and surprisingly showed that depth-2 circuits are learnable in *quantum polynomial time*, thus giving a separation between quantum PAC and the state-of-the-art (SOTA) classical PAC learning. The natural next frontier in quantum learning theory is then

Can we learn depth-3 circuits in the quantum PAC model efficiently?

Classically, a well-known idea to PAC learn depth-3 circuits is to consider the model of *agnostic learning*. Particularly, Feldman (2009) and Kalai et al. (2008b) showed agnostic learning depth-2 circuits, in particular DNF formulas, could yield learning algorithms for depth-3 circuits. This naturally motivates the need to understand learning DNFs in the quantum agnostic learning model.

Quantum agnostic learning. Tomography of quantum states (i.e., learning *quantum states* in the noise-free model) is well-studied in quantum computing. Quantum agnostic learning has gained traction only recently with the works of Grewal et al. (2024) and Chen et al. (2025), which considered learning stabilizer states. Subsequently, a few works considered stabilizer product states (Grewal et al. (2026)), high stabilizer-dimension states (Chen et al. (2025)) and product states (Bakshi et al. (2025)). In the pursuit of agnostic learning DNFs, we initiate the problem of agnostic learning *phase states* (which is incomparable to the works mentioned and discussed in more detail below). We now define the model of agnostic learning specialized to phase states. For the concept class $\mathcal{C} \subseteq \{c : \{0,1\}^n \to \{0,1\}\}$, we denote the phase state $|\phi_c\rangle$ corresponding to a function $c \in \mathcal{C}$ as

$$|\phi_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{c(x)} |x\rangle. \tag{1}$$

In quantum agnostic learning, an algorithm is given copies of an unknown $|\psi\rangle$ and the goal of an improper *strong agnostic learner* is to output a $|\phi'\rangle$ (not necessarily a phase state) such that

$$|\langle\psi|\phi'\rangle|^2 \geq \mathsf{opt} - \varepsilon,$$

where $\mathsf{opt} = \max_{c \in \mathcal{C}} |\langle\psi|\phi_c\rangle|^2$. The natural question at this point is: what classes of functions are agnostically learnable in this model? As far as we know, the agnostic learnability of classes such as parities, decision trees, DNFs have not yet been considered, motivating the question

Can we agnostically learn phase states corresponding to DNFs efficiently?

1.1. Main results

In this work, we make progress on both of the questions highlighted above. For the tasks of agnostically learning $\mathrm{poly}(n)$-sized DNFs, we give a $n^{O(\log\log n\cdot\log(1/\varepsilon))}$-time quantum algorithm and for PAC learning $\mathrm{poly}(n)$-sized depth-3 circuits, we give $n^{O(\log(n/\varepsilon)\cdot\log\log n)}$ time quantum algorithm. Below, we will discuss these results, starting with our main technical contribution, *quantum agnostic boosting*. Classically obtaining similar complexities given only classical examples is an open question and we compare both classical and quantum complexities below.

Quantum agnostic boosting. We denote the fidelity with respect to the concept class as

$$\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \max_{c\in\mathcal{C}} |\langle\psi|\phi_c\rangle|^2.$$

Similar to the definition of a strong agnostic learner above, we define a *weak agnostic learner* as one that outputs a state $|\phi''\rangle$ such that

$$|\langle\psi|\phi''\rangle|^2 \geq P(\mathsf{opt}/n),$$

for some function $P:\mathbb{R}^+\to\mathbb{R}^+$. We say a learner is *efficient* if the running time scales polynomially in the description size of the concept class in the (inverse of the) error parameter $1/\varepsilon$. Finally, we remark that the PAC model is defined just as above, except that the unknown $|\psi\rangle$ is promised to be $|\phi_c\rangle$ for an (unknown) $c\in\mathcal{C}$, in which case $\mathsf{opt}=1$. With this we are ready to state our main contributions.

We give a quantum boosting algorithm that, given access to a weak agnostic learner with a polynomial overhead, produces a strong agnostic learner for a concept class $\mathcal{C}$. To this end, we first define the class $\mathcal{C}$ of *parity functions*, i.e. $\chi_S(x)=\langle S,x\rangle$ for some $S\in\{0,1\}^n$. We refer to $\{|\chi_S\rangle = 2^{-n/2}\sum_x \chi_S(x)|x\rangle : S\in\{0,1\}^n\}$ as *parity states*. We summarize this in the theorem below.

Result 1 *Let $\mathcal{C}$ be a concept class and $|\psi\rangle$ be an unknown n-qubit state such that $\mathcal{F}_{\mathcal{C}}(|\psi\rangle)=\mathsf{opt}$. For every $\tau\geq 0$, let $\mathcal{A}_{\mathsf{WAL}}$ be a weak agnostic learner for $\mathcal{C}$, i.e., given copies of $|\varphi\rangle$ with $\mathcal{F}_{\mathcal{C}}(|\varphi\rangle)\geq\tau$, outputs a parity $|\chi_S\rangle$ such that $|\langle\varphi|\chi_S\rangle|^2\geq P(\tau/n)$ in time T_{WAL}. Then, there is a strong agnostic learner for $\mathcal{C}$, i.e., given copies of $|\psi\rangle$, runs in time $\mathrm{poly}(n,T_{\mathsf{WAL}},1/\varepsilon,1/P(\varepsilon/n))$ and outputs $|\widehat{\phi}\rangle$ with $|\langle\psi|\widehat{\phi}\rangle|^2\geq\mathsf{opt}-\varepsilon$.*

We formally state this theorem in Section B. To provide some context, classically, Freund and Schapire (Schapire (1990); Freund (1995); Freund and Schapire (1999)) proposed the boosting algorithm called *AdaBoost* that *efficiently* uses a *weak learner* as a black-box to construct a *strong learner* in the usual PAC model. The AdaBoost algorithm by Freund and Schapire was one of the first few theoretical boosting algorithms that was simple enough to be extremely useful and successful in practice (Schapire and Freund (2012)). Similarly, agnostic boosting has been considered by works of (Ben-David et al. (2001); Kalai et al. (2008b); Feldman (2009)) wherein they show similar results to boost weak agnostic learners to strong ones.

In the quantum setting, there are only a handful of works that have used boosting in the PAC model (Bshouty and Jackson (1995); Arunachalam and Maity (2020); Izdebski and de Wolf (2020)), and ours is the first work that demonstrates how to perform boosting in the harder model of *agnostic*

learning.[1] Apart from the context of learning Boolean functions, we believe that our quantum boosting algorithm could have utility for learning more general quantum states. Recently, Arunachalam and Dutt (2026) utilized boosting on top of a weak agnostic learner for stabilizer states to give tomography protocols of states promised to have structured stabilizer decompositions.

Agnostic learning decision trees, juntas and DNFs. Our second contribution involves applying the quantum boosting algorithm on top of quantum weak agnostic learners for interesting concept classes. In particular, we first observe that (strong) agnostic learning of parity states can be done efficiently. We then exploit properties of different classes – size-t decision trees, k-juntas and s-term DNF formulas[2]– in terms of their Fourier spectrum, which allow us to obtain agnostic learning algorithms for these concept classes as well, all based on quantum agnostic boosting. These quantum agnostic learners in particular use weak agnostic learners that output parity states. This result is summarized below.

Result 2 *Size-t decision trees and k-juntas are learnable in time* $\mathrm{poly}(n, t, 1/\varepsilon)$ *and* $\mathrm{poly}(n, 2^k, 1/\varepsilon)$ *respectively. Similarly, s-term DNF formulas are learnable in time* $\mathrm{poly}(n, (s/\varepsilon)^{\log\log s/\varepsilon \cdot \log(1/\varepsilon)})$.

We formally state this theorem for each class in Section C. In order to compare with classical results and for ease of exposition, let us consider the parameters above to take values of $2^k, t, s, 1/\varepsilon = \mathrm{poly}(n)$ (which in general are considered the most interesting settings of these parameters for learning). Classically, the SOTA algorithm for learning decision trees in the agnostic model (without membership queries) runs in $n^{O(\log n)}$ (Kalai et al. (2008a)) time and with membership queries scales as $\mathrm{poly}(n)$ (Gopalan et al. (2008b)).[3] The same results hold for juntas since k-juntas have size-2^k decision trees. In contrast, for DNF formulas, the SOTA algorithm in the agnostic model is $n^{O(\log^2 n)}$ (Kalai et al. (2008a); Gopalan et al. (2008a)). Our work shows that one can achieve an $n^{O(\log n)}$-time result with only quantum examples.

PAC-learning depth-3 circuits. Finally, using our quantum boosting algorithm, we also obtain a new quantum PAC learning algorithm for depth-3 circuits.

Result 3 *The class of size-s depth-3 circuits can be learned upto error ε in the quantum PAC model in time* $\mathrm{poly}(n, (s/\varepsilon)^{\log(s/\varepsilon)\cdot\log\log(s/\varepsilon)})$.

We formally state this theorem in Section C.4. Classically, it is a long-standing open problem to efficiently PAC learn *depth*-2 circuits of size s, wherein the state-of-the-art algorithm runs in time $n^{O(\log s)}$. In contrast, Bshouty and Jackson (1995) showed depth-2 circuits are quantumly learnable in time $\mathrm{poly}(n, s)$ and we further show that even depth-3 circuits exhibit a separation between quantum PAC and classical PAC learning. Classically the SOTA algorithm for learning $\mathrm{poly}(n)$-sized depth-3 circuits (without queries) scales as $n^{O(\log^2 n)}$ that comes via Fourier concentration bounds of Tal (2017). We summarize our main contributions in the table below.

1. We remark that Chatterjee et al. (2024) also discusses an agnostic quantum booster but their model assumes that the unknown quantum state is a *function state* whereas we make no assumption on our input state.
2. We refer the reader to Section A.2 for a definition of these classes.
3. By membership queries we mean that an algorithm can query an unknown $f : \{0,1\}^n \to \{0,1\}$ on an x of its choice. In the (uniform) agnostic model, by membership query we mean the following: for every distribution $D : \{0,1\}^{n+1} \to [0,1]$ whose marginal on the first n bits is uniform, the learner can query x and obtain a sample from $b \sim D(x, \cdot)$.

	Classical		**Quantum**
	Membership queries	*Random examples*	*Quantum examples*
Agnostic DNF	$n^{\log(1/\varepsilon)\log\log n}$ Gopalan et al. (2008a)	$n^{\log(1/\varepsilon)\log n}$ Kalai et al. (2008a)	$n^{\log(1/\varepsilon)\log\log n}$ ***This work***
PAC depth-3	$n^{\log(n/\varepsilon)\log\log n}$ Feldman (2009); Kanade and Kalai (2009)	$n^{\log(n/\varepsilon)\log n}$ Tal (2017)	$n^{\log(n/\varepsilon)\log\log n}$ ***This work***

Table 1: This gives a summary of the state-of-the-art results for agnostic learning $\mathrm{poly}(n)$-sized AC^0 circuits of depth-2 (i.e., DNFs) and PAC learning depth-3 circuits acting on n bits.

Apart from depth-3 circuits, we are able to learn TAC^0_2, i.e., *threshold of depth*-2 circuits (consisting of $\mathsf{AND}, \mathsf{OR}, \mathsf{NOT}$ gates). This class of circuits is compelling for two reasons. First, even quantum-efficiently learning thresholds of *threshold* gates would imply breakthrough classical circuit lower bounds (see Arunachalam et al. (2022) for more details). Second, as observed in Arunachalam et al. (2021), learning threshold circuits is equivalent to learning weights of feedforward neural networks. Thus, quantum efficient learnability of threshold circuits would translate into a dramatic advantage over classical computers for training neural networks, echoing Aaronson's "Ten Semi-Grand Challenges for Quantum Computing Theory" (Aaronson (2005)). Prior to our work, no results were known for PAC learning circuits consisting of any threshold gates; ours is the first to handle a single threshold on the top.

1.2. Prior works and concept challenges

We first discuss a few potential approaches that do not yield efficient algorithms. These ideas will, in turn, motivate the need for new learning algorithms.

1.2.1. IN THE QUANTUM SETTING

Often in quantum learning, the first class that one wants to learn is *parities*. If one can learn these, the next step is to learn depth-1 circuits (i.e., disjunctions/conjunctions), juntas and then depth-2 circuits (i.e., DNF formulas) – the key milestone en route to learning depth-3 circuits. Let us first discuss the applicability of recent algorithms to the problem of agnostic learning phase states corresponding to these concept classes.

1. Fourier/Bell sampling: The starting point of almost all quantum learning algorithms is Fourier sampling. Indeed, given copies of $|\phi_f\rangle = \frac{1}{\sqrt{2^n}}\sum_x f(x)|x\rangle$, one can simply apply the Hadamard transform and measure in order to sample from the Fourier distribution $\{\widehat{f}(S)^2\}_S$. In the agnostic model, when we do not have copies of $|\phi_f\rangle$, but rather copies of $|\psi\rangle$ that are promised to be τ-close[4] to $|\phi_f\rangle$, it is unclear whether Fourier sampling $|\psi\rangle$ would yield anything meaningful. It could very well be that $|\phi_f\rangle$ has one large Fourier coefficient S, but $|\psi\rangle$ puts 0 amplitude on $|S\rangle$ and

4. Throughout the paper, by "τ-close", we mean that the two states have squared overlap at least τ, i.e., $|\langle\psi|\phi_f\rangle|^2 \geq \tau$.

agrees with $|\phi_f\rangle$ elsewhere (so that it is τ-close to $|\phi_f\rangle$). It is therefore unclear if one can strongly learn the unknown f (i.e., learn f up to $\mathsf{opt} - \varepsilon$) given copies of $|\psi\rangle$.

Observe that Fourier sampling does work for parity states, denoted as $\mathcal{C}_{\mathsf{Par}} = \{\chi_S(x) = \langle S, x\rangle \text{ for all } S \in \{0,1\}^n\}$, since the Fourier spectrum of parity function χ_S is a point-mass on $|S\rangle$. In particular, this implies that if $|\psi\rangle$ is τ-close to $|\chi_S\rangle$, then must have a "large" amplitude on $|S\rangle$. Hence, strong learning via Fourier sampling can be achieved using $O(1/\tau^2)$ samples. But this no longer holds for other classes of states and, in particular, DNFs for which the Fourier spectrum does not enjoy such a "point-concentration" property. One can instead consider *Bell sampling*, which has been used in Grewal et al. (2026) to agnostically learn stabilizer product states (of which parity states are a subclass). Unfortunately, the results in Grewal et al. (2026) solve a more general problem than the one we are considering and the resulting time and sample complexity of their results is $\mathrm{poly}(n, 2^{1/\tau})$. As we are aiming for a polynomial scaling in $1/\tau$, this is unsatisfactory.

2. Stabilizer Bootstrapping: Another approach is to look at the recent work of Chen et al. (2025) for agnostic learning of stabilizer states. As with (Grewal et al. (2026)), however, they solve the more general task of agnostically learning states with *stabilizer dimension-t*, achieving sample and time complexity scaling $\mathrm{poly}(n, (1/\tau)^{\log 1/\tau}, 2^t)$. It is not hard to see that learning s-juntas or s-term DNFs reduces to agnostic learning states with stabilizer dimension $O(s)$, so their agnostic learning algorithm would scale as $\mathrm{poly}(n, (1/\tau)^{\log 1/\tau}, 2^s)$.

3. Product state learning: A third approach is to look at a recent work of Bakshi et al. (2025) who considered agnostic learning matrix product states (MPS): in particular, they show that agnostic learning n-qubit MPS with bond dimension r has complexity $\mathrm{poly}(n, r, 1/\varepsilon)$. The question then is: what is the bond dimension of junta states or DNF states?[5] We observe that k-junta states have bond dimension that scales as $2^{\lfloor k/2 \rfloor}$, so in particular this yields a quantum agnostic learning algorithm with time complexity $\mathrm{poly}(n, 2^k, 1/\varepsilon)$, which is already better than the previous two approaches that we mentioned. In fact, for disjunctions (i.e., depth-1 circuits) their bond dimension equals 2, so it yields a $\mathrm{poly}(n, 1/\varepsilon)$ algorithm. However, for s-term DNFs, the corresponding function states can be shown to have bond dimension that is at least 2^s. This in turn yields a running time of $\mathrm{poly}(n, 2^s, 1/\varepsilon)$, which is again too high.

1.2.2. IN THE CLASSICAL SETTING

In classical learning theory, agnostic learning decision trees (DT) and DNFs has received a lot of attention. Classically, the model of agnostic learning is defined as follows: a learner is given uniformly random $x \in \{0,1\}^n$ and $b \sim (1 + \phi(x)/2, 1 - \phi(x)/2)$ and the goal is to find a function f from the concept class which agrees with ϕ as well as possible. The SOTA algorithms for size-s DTs run in time polynomial in n, s but requires membership queries (Feldman (2009); Gopalan et al. (2008b)). They crucially use that the ℓ_1 norm of the Fourier coefficients of $f \in \mathsf{DT}(s)$ is at most s. However, DNFs do not enjoy the property of small ℓ_1 norm, but instead are only known to have sparse Fourier spectrum and at this point, it is even unclear classically how one can obtain a weak learner for DNFs (with examples) if ϕ is only promised to satisfy $\max_x |\phi(x)| \leq 1$. We show that this can be circumvented when given access to quantum examples and a weak agnostic learner can be naturally proposed with just the Fourier concentration promise.

5. In Appendix E.1 we show the bond dimension bounds that we claim next.

Our contributions. Although the three quantum approaches give new agnostic learning algorithms for parities, disjunctions and juntas, as we've mentioned these approaches eventually lead to agnostic algorithms for s-term DNFs with complexity that is exponential in s, and our goal is to ideally have a $\mathrm{poly}(n, s)$ algorithm for this class. Conceptually, the goal of these works is to solve a much harder problem, so they do not immediately yield results for the task that we are concerned with in this work (whose motivation comes more from quantum learning theory). As alluded to earlier, our main contribution is in obtaining an umbrella framework, that achieves two purposes: (i) unifies all the learning algorithms for different classes of phase states, and (ii) is simpler than the algorithms mentioned above (which solve a harder task). We achieve this via *quantum agnostic boosting*, which we describe in the next section, which could be of independent interest.

1.3. Technical overview

In this section, we give an overview of the proofs of our main results.

1.3.1. QUANTUM AGNOSTIC BOOSTING

Our quantum agnostic learner is inspired by the gradient-descent based algorithms for classical boosting proposed by the works of Kanade and Kalai (2009) and Feldman (2009). Below, we first give a high-level idea of the boosting algorithm before describing the iterations of the procedure.

High-level idea. Recall that we have a quantum state $|\psi\rangle$ satisfying $\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \mathsf{opt}$ and let $\varepsilon \in (0, 1)$. Consider a weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ that given copies of $|\varphi\rangle$ with $\mathcal{F}_{\mathcal{C}}(|\varphi\rangle) \geq \tau$, outputs a parity state $|\chi_S\rangle$ such that $|\langle\chi_S|\varphi\rangle|^2 \geq P(\tau/n)$ in time T_{WAL}. Our agnostic boosting algorithm then does the following: it first runs $\mathcal{A}_{\mathsf{WAL}}$ to find a parity state $|\chi_{S_1}\rangle$ that has $P(\mathsf{opt}/n)$-overlap with $|\psi\rangle$. After finding S_1, the algorithm "subtracts" $|\chi_{S_1}\rangle$ from $|\psi\rangle$ by constructing the state $|\psi_2\rangle = |\psi\rangle - \beta_1|\chi_{S_1}\rangle$ (ignoring the normalization for now). It then checks two things: (i) is $\||\psi_2\rangle\|_2 \leq \varepsilon$ and (ii) runs $\mathcal{A}_{\mathsf{WAL}}$ to check whether $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) \leq \varepsilon$ or not: if either of these conditions are met, the algorithm halts and outputs $|\widehat{\phi}\rangle \propto \beta_1|\chi_{S_1}\rangle$. Intuitively the former checks if we have done well on *tomography* (i.e. checking whether $\beta_1|\chi_{S_1}\rangle$ is close to $|\psi\rangle$), a harder task than agnostic learning, and the latter can be shown to be sufficient for the agnostic learning task (since it is checking whether, by subtracting $\beta_1|\chi_{S_1}\rangle$, we have moved the state far from $\mathcal{C}$). If neither is satisfied, the algorithm repeats the same procedure on $|\psi_2\rangle$. Again, this means running the weak learner on $|\psi_2\rangle$ to produce a parity state $|\chi_{S_2}\rangle$ which is "subtracted" along $|\chi_{S_1}\rangle$ from $|\psi\rangle$ and then the stopping conditions are checked. Eventually, after κ many iterations, the algorithm terminates producing a (suitably normalized) state $|\widehat{\phi}\rangle = \sum_i \beta_i|\chi_{S_i}\rangle$, which will be the output of the algorithm. We now discuss the iterations in more detail and why $|\widehat{\phi}\rangle$ accomplishes agnostic learning.

Iterations in the boosting algorithm. Our agnostic boosting algorithm will build a state $|\widehat{\phi}\rangle$ expressed as a linear combination of parity states

$$|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} \beta_i|\chi_{S_i}\rangle,$$

across κ iterations and stops when $|\widehat{\phi}\rangle$ achieves agnostic learning condition i.e., $|\langle\psi|\widehat{\phi}\rangle|^2 \geq \mathsf{opt} - \varepsilon$. Each parity state is learned sequentially in each iteration, as described above. Let us denote $|\widehat{\phi}^{(t)}\rangle$ as

a "running estimate" state at the end of iteration t. We also denote the parity states learned up to (and including) iteration $t \geq 1$ as $\{|\chi_{S_i}\rangle\}_{i\in[t]}$ and the corresponding span as $T(t) = \mathsf{span}(\{|\chi_{S_i}\rangle\}_{i\in[t]})$. We denote the orthogonal projector onto this span as $\Lambda_{T(t)}$. Lastly, we denote the inner products $\beta_i := \langle\psi|\chi_{S_i}\rangle$ and the norms $\alpha_{t+1} = \|(\mathbb{I} - \Lambda_{T(t)})|\psi\rangle\|_2$.

Initially, in iteration $t = 1$, the algorithm first runs the weak learner $\mathcal{A}_{\mathsf{WAL}}$ on copies of $|\psi\rangle$ to find a parity state $|\chi_{S_1}\rangle$ such that $|\langle\psi|\chi_{S_1}\rangle|^2 \geq P(\mathsf{opt}/n)$ (where P is the promise of $\mathcal{A}_{\mathsf{WAL}}$). The running estimate is then

$$|\widehat{\phi}^{(1)}\rangle = \beta_1|\chi_{S_1}\rangle,$$

where $\beta_1 = \langle\psi|\chi_{S_1}\rangle$.[6] Before proceeding to the next iteration, the algorithm checks if we would have accomplished state tomography i.e., $|\langle\psi|\widehat{\phi}^{(1)}\rangle|^2 \geq 1 - \varepsilon$ and stops if this is the case. This is done by checking if $|\alpha_2|^2 = 1 - |\beta_1|^2 < \varepsilon$. If not, the residual state is set to

$$|\psi_2\rangle := \big(\mathbb{I} - \Lambda_{T(1)}\big)|\psi\rangle = \big(\mathbb{I} - |\chi_{S_1}\rangle\langle\chi_{S_1}|\big)|\psi\rangle$$

up to renormalization, where $T(1) = \mathsf{span}(\{|\chi_{S_1}\rangle\})$. We now proceed to the next iteration.

In iteration $t = 2$, the boosting algorithm first checks if the running estimate $|\widehat{\phi}^{(1)}\rangle$ accomplishes the task of *agnostic learning* i.e., $|\langle\psi|\widehat{\phi}^{(1)}\rangle|^2 \geq \mathsf{opt} - \varepsilon$. To do this, the learner prepares copies of the residual state $|\psi_2\rangle$ and checks if $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) < \varepsilon$ or not. To accomplish this, the learner does the following: recall that if $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) \geq \varepsilon$, then running $\mathcal{A}_{\mathsf{WAL}}$ on $|\psi_2\rangle$, would produce a parity $|\chi_U\rangle$ such that $|\langle\psi_2|\chi_U\rangle|^2 \geq P(\varepsilon/n)$ (which can be checked by a SWAP test). By the contrapositive, if the output of $\mathcal{A}_{\mathsf{WAL}}$ does not output a parity for which $|\langle\psi_2|\chi_U\rangle|^2 \geq P(\varepsilon/n)$, then $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) < \varepsilon$ and we stop (hence we have implicitly used $\mathcal{A}_{\mathsf{WAL}}$ also as a tester for fidelity). It might seem counterintuitive to run a test on the residual state instead of directly checking the overlap of $|\psi\rangle$ with $|\widehat{\phi}^{(1)}\rangle$ via a SWAP test. However for the latter, we would need to know opt ahead of time, whereas we are assuming that opt is not known. Instead, we show that if $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) < \varepsilon$, then $|\widehat{\phi^1}\rangle$ (normalized) solves the task of agnostic learning.

If $\mathcal{F}_{\mathcal{C}}(|\psi_2\rangle) \geq \varepsilon$, the algorithm runs $\mathcal{A}_{\mathsf{WAL}}$ on copies of $|\psi_2\rangle$, to find a parity function $|\chi_{S_2}\rangle$ such that $|\langle\psi_2|\chi_{S_2}\rangle|^2 \geq P(\varepsilon/n)$. We then observe, by writing out $|\psi_2\rangle$, that

$$P(\varepsilon/n) \leq |\langle\chi_{S_2}|\psi_2\rangle|^2 = \frac{1}{|\alpha_2|^2}|\langle\chi_{S_2}|(|\psi\rangle - \beta|\chi_{S_1}\rangle)|^2 = \frac{1}{|\alpha_2|^2}|\langle\chi_{S_2}|\psi\rangle|^2 \implies |\langle\chi_{S_2}|\psi\rangle|^2 \geq \varepsilon\cdot P(\varepsilon/n),$$

where we have used $\langle\chi_{S_2}|\chi_{S_1}\rangle = 0$ in the last step before the implication and used the fact that $|\alpha_2|^2 \geq \varepsilon$ (as determined at the end of iteration $t = 1$) to give the implication. Our running estimate at this point is

$$|\widehat{\phi}^{(2)}\rangle = \beta_1|\chi_{S_1}\rangle + \beta_2|\chi_{S_2}\rangle$$

with the promise that $|\beta_1|^2 \geq P(\mathsf{opt}/n)$ and $|\beta_2|^2 \geq \varepsilon \cdot P(\varepsilon/n)$. Overall, this implies that

$$|\langle\widehat{\phi}^{(2)}|\psi\rangle|^2 \geq 2\varepsilon P(\varepsilon/n),$$

and thus have made progress towards the task of agnostic learning. As in the previous iteration, the learner now checks if $|\alpha_3|^2 = 1 - |\beta_1|^2 - |\beta_2|^2 < \varepsilon$. If not, the learner sets the residual state to

$$|\psi_3\rangle \propto (\mathbb{I} - \Lambda_{T(2)})|\psi\rangle = \big(\mathbb{I} - |\chi_{S_1}\rangle\langle\chi_{S_1}| - |\chi_{S_2}\rangle\langle\chi_{S_2}|\big)|\psi\rangle = |\psi\rangle - |\widehat{\phi}^{(2)}\rangle$$

6. In our boosting algorithm, we will not actually compute β_1 at this stage, and instead only keep $|\chi_{S_1}\rangle$.

up to normalization, with $T(2) = \mathsf{span}(|\chi_{S_1}\rangle, |\chi_{S_2}\rangle)$. The algorithm then moves to iteration $t = 3$ and continues until either $|\alpha_{t+1}|^2 < \varepsilon$ or $\mathcal{F}_{\mathcal{C}}(|\psi_{t+1}\rangle) < \varepsilon$ which can again be checked using the $\mathcal{A}_{\mathsf{WAL}}$. putting everything together, the algorithm stops when state tomography or agnostic learning has been achieved.

Overall our agnostic boosting algorithm can be divided into two stages, *structure learning* and *parameter learning*.[7] In structure learning, the goal is to learn the parities that constitute the elements of $|\widehat{\phi}^{(t)}\rangle$, so each iteration starts with structure learning. At multiple times, we mentioned that $|\widehat{\phi}^{(t)}\rangle$ is the state prepared at the tth iteration, but so far we only determined the parities present inside $|\widehat{\phi}^{(t)}\rangle$. Ideally, one could have let $|\widehat{\phi}^{(t)}\rangle$ be the projection $\Lambda_{T(t)}|\psi\rangle$ but that requires learning the coefficients β_i (including the phases). Estimating these coefficients β_is is referred to as parameter learning. To do so, one could compute $\beta_{t+1} = \langle\chi_{S_{t+1}}|\psi\rangle$ via the Hadamard test using the state preparation unitaries (and controlled versions) of $|\chi_{S_{t+1}}\rangle$ and $|\psi\rangle$. However, we avoid the need for a state preparation unitary and instead show that with just copies of $|\psi\rangle$, we can estimate β_i up to a global phase, and a valid proxy state $|\widehat{\phi}^{(t)}\rangle$ that is close to $\Lambda_{T(t)}|\psi\rangle$, hence is good at the task of agnostic learning.

What remains? The brief exposition above suppresses several subtleties: (i) an upper bound on the number of iterations κ[8], (ii) the correctness of the final state $|\widehat{\phi}^{(t)}\rangle$, (iii) the preparation of the residual states $|\psi_t\rangle$, (iv) the normalization factors in $|\psi_t\rangle$, (v) the circuit implementations of various subroutines in the algorithm and their complexity and finally (vi) the errors in the steps involving estimation and how they propagate in the algorithm. Our final boosting algorithm incorporates all these details and making it rigorous is the most technical part of our work.

1.3.2. LEARNING ALGORITHMS

In this section, we state the learning algorithms that are either used by the boosting procedure, or which the boosting procedure implies. Beginning with the former, we describe a weak learner for parity states. The subsequent algorithms are obtained by using the boosting procedure.

Weak learner. To agnostically learn parity states, we simply observe that, if $|\psi\rangle$ is τ-close to a parity $|\chi_S\rangle$, then we have that

$$|\langle\psi'|S\rangle|^2 = |\langle\psi|\mathsf{Had}\cdot\mathsf{Had}|\chi_S\rangle|^2 \geq \tau,$$

where $|\psi'\rangle = \mathsf{Had}|\psi\rangle$. Thus, if we measure $|\psi'\rangle$, $O(1/\tau^2)$ many times in the computational basis, we will recover S. Specifically, we record the measurement outcomes and check, via a SWAP test, which basis state has the highest fidelity with $|\psi'\rangle$. This will be the agnostic learner for parities.

Agnostic learning for decision trees. As mentioned earlier, unlike parity states whose Fourier spectrum is concentrated on a single point, for decision trees, DNFs and juntas, we do not have this property. In fact, it is well-known (Kushilevitz and Mansour (1993)) that for a function f, computed by a size-s decision tree, we have that $\sum_T |\widehat{f}(T)| \leq s$. In particular, it is not not too hard to see that

7. The choice for these terms comes from the literature on learning *graphical models* where the goal is to learning the interactions and interaction strengths.
8. As part of our analysis, we show that we stop in $O(1/(\varepsilon P(\varepsilon/n))$ many iterations and the time complexity of the overall algorithm is then dictated by the promise P of $\mathcal{A}_{\mathsf{WAL}}$.

if $|\langle\psi|\phi_f\rangle|^2 \geq \tau$, then

$$\sqrt{\tau} \leq |\langle\psi|\phi_f\rangle| = \left|\sum_T \widehat{f}(T)\langle\psi'|T\rangle\right| \leq \sum_T |\widehat{f}(T)|\,|\langle\psi'|T\rangle| \leq O(s)\max_T |\langle\psi'|T\rangle|,$$

where in the first equality we applied Hadamard on both states and denoted $|\psi'\rangle = \mathsf{Had}|\psi\rangle$. We then used the triangle inequality and the fact that the ℓ_1 norm of the Fourier coefficients of f is at most $O(s)$. The above implies that there is a basis state in $|\psi'\rangle$ whose amplitude is $\Omega(\sqrt{\tau}/s)$. Finding it can be done by measuring $|\psi'\rangle$ several times and recording the statistics of the measurement outcomes. This serves as a weak learner and we then use our boosting algorithm to obtain a strong learner which outputs $|\phi\rangle$ (as a superposition over $\mathrm{poly}(s/\varepsilon)$ parity states) such that

$$|\langle\psi|\phi\rangle|^2 \geq \max_{c\in\mathsf{DT}(s)} |\langle\psi|\phi_c\rangle|^2 - \varepsilon. \tag{2}$$

The overall complexity is $\mathrm{poly}(n, s, 1/\varepsilon)$. At this point, we use the fact that k-juntas are decision trees of size 2^k, giving an algorithm with complexity $\mathrm{poly}(n, 2^k, 1/\varepsilon)$ for agnostic learning juntas.

Agnostic learning DNFs. The agnostic learner for DNFs is similar to the one for decision trees, except that we need to use Mansour's result (Mansour (1992); Lecomte and Tan (2022)) that shows that for size-s DNF formulas, the entire Fourier spectrum is concentrated on $s^{O(\log(1/\varepsilon)\cdot\log\log s)}$ coefficients. Using a similar argument as the one for deriving Eq. (2), one can show that if $|\psi\rangle$ is τ-close to a DNF phase state, then there exists a basis state $|\chi_T\rangle$ such that $|\langle\psi|\chi_T\rangle|^2 \geq \tau/s^{O(\log(1/\varepsilon)\cdot\log\log s)}$. Once again using our quantum boosting algorithm, we obtain a $\mathrm{poly}(n, s^{\log\log s\log(1/\varepsilon)})$ algorithm for agnostic learning size-s DNF formulas.

PAC learning depth-3 circuits. To learn these circuits, we employ our agnostic DNF learner. The key insight is that when the input state $|\psi_f\rangle$ is promised to correspond to a depth-3 circuit then state tomography is accomplished when agnostic learning against DNFs is accomplished, which was also observed classically (Feldman (2009)). This follows from using the seminal result of Hajnal et al. (1993) that says that if f is a threshold of m many DNF formulas $\{g_1, \ldots, g_m\}$ (each with size at most s), then $|\langle\psi_f|\psi_{g_i}\rangle| \geq 1/m$, for some $i \in [m]$, where $|\psi_f\rangle$ (in this section) equals $\frac{1}{\sqrt{2^n}}\sum_x f(x)|x\rangle$ since we are in the PAC learning setting. We can now use our agnostic DNF learner outputs a quantum state $|\phi\rangle$ which is at least opt/m^2 close to f. This will serve as our weak learner which we will then boost into a strong PAC learner. The boosting algorithm outputs a (classical description of a) quantum state $|\phi\rangle$ which is close to an unknown $|\psi_f\rangle$; we now *round* the final state $|\phi\rangle$ of the algorithm and show that it satisfies the requirement of PAC learning. Since the runtime of the DNF learner scales as $\mathrm{poly}(n, s^{\log(1/\varepsilon)\cdot\log\log s})$, the overall δ-error quantum PAC learning algorithm scales as $\mathrm{poly}(n, s^{\log(s/\delta)\cdot\log\log s})$.

1.3.3. LEARNING IN THE DISTRIBUTIONAL MODEL.

Finally, we remark that there are two natural definitions of quantum agnostic learning: the one defined in the introduction of this work, i.e., $|\psi\rangle$ is arbitrary and promised to be close to $|\phi_c\rangle$ (where $c \in \mathcal{C}$), or the one that was considered in (Arunachalam and De Wolf (2017); Caro et al. (2024)) wherein there is an unknown distribution $D : \{0,1\}^{n+1} \to [0,1]$ whose first n bits are uniform and the last bit is described by the marginal $\big((1+\phi(x))/2, (1-\phi(x))/2\big)$ where $\phi : \{0,1\}^n \to [-1,1]$

is an arbitrary function. The quantum algorithm is given copies of

$$|\psi_D\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes \Big(\sqrt{\frac{1+\phi(x)}{2}} |0\rangle + \sqrt{\frac{1-\phi(x)}{2}} |1\rangle \Big),$$

and the goal is to output a function $h : \{0,1\}^n \to \{0,1\}$ such that $\Pr_{(x,b)\sim D}[h(x) = b] \geq \mathsf{opt} - \varepsilon$ where $\mathsf{opt} = \max_{c \in \mathcal{C}} [c(x) = b]$. In contrast to the first model, in this distributional model the learning algorithm knows that the unknown quantum state $|\psi\rangle$ has the form of $|\psi_D\rangle$. However, the algorithm needs to output a *function* h, whereas in the first model it can output an arbitrary $|\varphi\rangle$. The two situations are therefore incomparable and interesting for different reasons. In Section D we show that if ϕ is "nice", i.e., $\mathbb{E}_x[\phi(x)^2] \leq \mathsf{opt}$, having a learning algorithm in the first model implies a learning algorithm in the second model. In particular, for these distributions, we also obtain quantum learning algorithms in the distributional model. We leave open the other direction.

Open questions. Our work opens up a number of interesting research directions.

1. ***Learning quantum objects***: In this work, We considered the learnability of depth-2 and depth-3 AC^0 circuits, what about learning depth-2 or depth-3 QAC^0 circuits with or without fanout gates? Recently, Foxman et al. (2025) proved the hardness of learning QAC^0 circuits, but their hard instances require depth that is a "large constant."

   Similarly, we could consider agnostic learning *low-degree* phase states. Tomography protocols (i.e., learning them exactly) for these class of states are known (Arunachalam et al. (2023)) but agnostic learning algorithms are unknown.

2. ***Learning in the distributional model***: We showed how to port learning algorithms from the state agnostic learning model to the standard distributional quantum agnostic model when the marginal function on the last bit $\phi : \{0,1\}^n \to [-1,1]$ satisfied $\mathbb{E}_x[\phi(x)^2] = 1/\operatorname{poly}(n)$. In this distributional model, can we learn even parities for all ϕ, or is it hard?

3. ***Learning more expressive circuits?*** Classically, it is believed that depth-5 circuits are hard to learn (*assuming* factoring is hard) (Naor and Reingold (2004)). Our work leaves opens the status of learning depth-4 circuits, which is the "only depth setting" for which we do not know any classical or quantum learning algorithms or hardness results.

   Similarly, classical works of Jackson et al. (2002) and Chen et al. (2021) considered the learnability of the class threshold of AC^0 gates, and Carmosino et al. (2016) looked at learning AC^0 augmented with $\bmod p$ gates, with membership queries. It would be interesting if one could learn threshold of $\mathsf{AC}^0[p]$ circuits using quantum examples (removing the use of classical queries).

4. ***Proper learning***: The agnostic learners presented in this work for decision trees, juntas, and DNFs are improper. A natural question is then: Could we obtain *proper* agnostic learners for these classes of phase states with similar time complexities? This has also remained open classically (Gopalan et al. (2008a)) and a quantum approach might lead to new insights.

Acknowledgments. SA thanks Matthias Caro, Alex Grilo and Ryan Sweke for an early discussion on agnostic learning. AD thanks Isaac Chuang and Kristan Temme for early discussions on agnostic learning phase states. We thank Igor Carboni, Gautam Chandrasekaran, Varun Kanade, and Adam Klivans for helpful clarifications on the classical SOTA algorithms. This work was done when MdO was an intern at IBM Quantum.

References

Scott Aaronson. Ten semi-grand challenges for quantum computing theory. https://www.scottaaronson.com/writings/qchallenge.html, 2005.

Srinivasan Arunachalam and Ronald De Wolf. Guest column: A survey of quantum learning theory. *ACM Sigact News*, 48(2):41–67, 2017.

Srinivasan Arunachalam and Arkopal Dutt. Learning stabilizer structure of quantum states. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*, STOC '26, page 1949–1959, New York, NY, USA, 2026. Association for Computing Machinery. ISBN 9798400725364. doi: 10.1145/3798129.3800900. URL https://doi.org/10.1145/3798129.3800900.

Srinivasan Arunachalam and Reevu Maity. Quantum boosting. In *International Conference on Machine Learning*, pages 377–387. PMLR, 2020.

Srinivasan Arunachalam, Alex Bredariol Grilo, and Aarthi Sundaram. Quantum hardness of learning shallow classical circuits. *SIAM Journal on Computing*, 50(3):972–1013, 2021.

Srinivasan Arunachalam, Alex B Grilo, Tom Gur, Igor C Oliveira, and Aarthi Sundaram. Quantum learning algorithms imply circuit lower bounds. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 562–573. IEEE, 2022.

Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal Algorithms for Learning Quantum Phase States. In *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, volume 266 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:24. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. ISBN 978-3-95977-283-9. doi: 10.4230/LIPIcs.TQC.2023.3.

Costin Badescu and Ryan O'Donnell. Improved quantum data analysis. In *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 1398–1411. ACM, 2021.

Ainesh Bakshi, John Bostanci, William Kretschmer, Zeph Landau, Jerry Li, Allen Liu, Ryan O'Donnell, and Ewin Tang. Learning the closest product state. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 1212–1221, New York, NY, USA, 2025. Association for Computing Machinery. ISBN 9798400715105. doi: 10.1145/3717823.3718207. URL https://doi.org/10.1145/3717823.3718207.

Shai Ben-David, Philip M Long, and Yishay Mansour. Agnostic boosting. In *International Conference on Computational Learning Theory*, pages 507–516. Springer, 2001.

Nader H Bshouty and Jeffrey C Jackson. Learning DNF over the uniform distribution using a quantum example oracle. In *Proceedings of the eighth annual conference on Computational learning theory*, pages 118–127, 1995.

Marco L Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Learning algorithms from natural proofs. In *31st Conference on Computational Complexity (CCC 2016)*, pages 10–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2016.

Matthias C Caro, Jens Eisert, Marcel Hinsche, Marios Ioannou, Alexander Nietner, and Ryan Sweke. Interactive proofs for verifying (quantum) learning and testing. *arXiv:2410.23969*, 2024.

Sagnik Chatterjee, SAPV Tharrmashastha, and Debajyoti Bera. Efficient quantum agnostic improper learning of decision trees. In *International Conference on Artificial Intelligence and Statistics*, pages 514–522. PMLR, 2024.

Lijie Chen, Zhenjian Lu, Xin Lyu, and Igor C Oliveira. Majority vs. approximate linear sum and average-case complexity below nc1. In *48th International Colloquium on Automata, Languages, and Programming (ICALP 2021)*, volume 198, page 51. Leibniz International Proceedings in Informatics, 2021.

Sitan Chen, Weiyuan Gong, Qi Ye, and Zhihan Zhang. Stabilizer bootstrapping: A recipe for efficient agnostic tomography and magic estimation. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 429–438, New York, NY, USA, 2025. Association for Computing Machinery. ISBN 9798400715105. doi: 10.1145/3717823.3718191. URL https://doi.org/10.1145/3717823.3718191.

Jeroen Dehaene and Bart De Moor. Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Phys. Rev. A*, 68:042318, Oct 2003. doi: 10.1103/PhysRevA.68.042318. URL https://link.aps.org/doi/10.1103/PhysRevA.68.042318.

Vitaly Feldman. Distribution-specific agnostic boosting. *arXiv:0909.2927*, 2009.

Ben Foxman, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. Random unitaries in constant (quantum) time. *arXiv:2508.11487*, 2025.

Y. Freund. Boosting a weak learning algorithm by majority. *Information and Computation*, 121(2): 256–285, 1995. Earlier in COLT'90.

Y. Freund and R. Schapire. A short introduction to boosting. *Journal-Japanese Society For Artificial Intelligence*, 14:771–780, 1999.

Héctor J García, Igor L Markov, and Andrew W Cross. On the geometry of stabilizer states. *Quantum Information & Computation*, 14(7&8):683–720, 2014.

Parikshit Gopalan, Adam Kalai, and Adam R Klivans. A query algorithm for agnostically learning DNF?. In *COLT*, pages 515–516, 2008a.

Parikshit Gopalan, Adam Tauman Kalai, and Adam R Klivans. Agnostically learning decision trees. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 527–536, 2008b.

Ben Green. Montreal lecture notes on quadratic Fourier analysis. *arXiv math/0604089*, 2006.

Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Improved stabilizer estimation via bell difference sampling. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 1352–1363, New York, NY, USA, 2024. Association for Computing Machinery. ISBN 9798400703836. doi: 10.1145/3618260.3649738. URL https://doi.org/10.1145/3618260.3649738.

Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Agnostic tomography of stabilizer product states. *Quantum*, 10:2027, 2026.

András Hajnal, Wolfgang Maass, Pavel Pudlák, Mario Szegedy, and György Turán. Threshold circuits of bounded depth. *Journal of Computer and System Sciences*, 46(2):129–154, 1993.

Adam Izdebski and Ronald de Wolf. Improved quantum boosting. *arXiv:2009.08360*, 2020.

Jeffrey C Jackson, Adam R Klivans, and Rocco A Servedio. Learnability beyond AC0. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 776–784, 2002.

Adam Tauman Kalai, Adam R Klivans, Yishay Mansour, and Rocco A Servedio. Agnostically learning halfspaces. *SIAM Journal on Computing*, 37(6):1777–1805, 2008a.

Adam Tauman Kalai, Yishay Mansour, and Elad Verbin. On agnostic boosting and parity learning. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 629–638, 2008b.

Varun Kanade and Adam Kalai. Potential-based agnostic boosting. *Advances in neural information processing systems*, 22, 2009.

Michael J Kearns, Robert E Schapire, and Linda M Sellie. Toward efficient agnostic learning. In *Proceedings of the fifth annual workshop on Computational learning theory*, pages 341–352, 1992.

Dain Kim, Anqi Li, and Jonathan Tidor. Cubic Goldreich-Levin. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 4846–4892. SIAM, 2023.

Eyal Kushilevitz and Yishay Mansour. Learning Decision Trees Using the Fourier Spectrum. *SIAM Journal on Computing*, 22(6):1331–1348, 1993. doi: 10.1137/0222080. URL https://doi.org/10.1137/0222080.

Victor Lecomte and Li-Yang Tan. Sharper bounds on the Fourier concentration of DNFs. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 930–941. IEEE, 2022.

Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. *Journal of the ACM (JACM)*, 40(3):607–620, 1993.

Yishay Mansour. An $O(n^{\log\log n})$ learning algorithm for DNF under the uniform distribution. In *Proceedings of the Fifth Annual workshop on Computational Learning Theory*, pages 53–61, 1992.

Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *Journal of the ACM (JACM)*, 51(2):231–262, 2004.

Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

Ketan N Patel, Igor L Markov, and John P Hayes. Efficient synthesis of linear reversible circuits. *arXiv quant-ph/0302002*, 2003.

R. E. Schapire. The strength of weak learnability. *Machine Learning*, 5:197–227, 1990. Earlier in FOCS'89.

R.E. Schapire and Y. Freund. *Boosting: Foundations and Algorithms*. MIT Press, 2012.

Avishay Tal. Tight bounds on the Fourier spectrum of AC0. In *32nd Computational Complexity Conference (CCC 2017)*, pages 15–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2017.

Madhur Tulsiani and Julia Wolf. Quadratic Goldreich–Levin Theorems. *SIAM Journal on Computing*, 43(2):730–766, 2014.

Leslie G. Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.

Karsten A Verbeurgt. Learning sub-classes of monotone DNF on the uniform distribution. In *Algorithmic Learning Theory: 9th International Conference, ALT'98 Otzenhausen, Germany, October 8–10, 1998 Proceedings 9*, pages 385–399. Springer, 1998.

Frank Verstraete and J Ignacio Cirac. Matrix product states represent ground states faithfully. *Physical Review B—Condensed Matter and Materials Physics*, 73(9):094423, 2006.

Appendix A. Preliminaries

A.1. Notation

Let $[n] = \{1, \ldots, n\}$. We define $\mathcal{B}_\infty^k$ as the unit complex ball, i.e., $x \in \mathcal{B}_\infty^k$ if $x_i \in \mathbb{C}$ for all $i \in [k]$ and $|x_i| \in (0, 1]$. For a set $S \subseteq [n]$ we denote $z \in \{0,1\}^S$ to be a bit-string of length $|S|$. For notational convenience, we will denote $|z_S, 0_{\overline{S}}\rangle$ to denote the quantum state where the i'th qubit is z_i if $i \in S$ and 0 otherwise. Similarly, by $|+\rangle_S|0\rangle_{\overline{S}}$, we mean qubit i equals $|+\rangle$ if $i \in S$ and $|0\rangle$ otherwise. For $\varepsilon \in (0, 1)$, we say $f(\varepsilon) = \mathrm{poly}(\varepsilon)$ if there exist constants $c_1, c_2 \geq 1$ such that $f(\varepsilon) = c_1\varepsilon^{c_2}$.[9]

Fact 4 *For every $x \in (-1, 1)$, by Taylor series expansion we have that*

$$1 + x/2 - x^2/2 \leq \sqrt{1+x} \leq 1 + x/2, \text{ and } 1 - x/2 - x^2/2 \leq \sqrt{1-x} \leq 1 - x/2.$$

Fourier analysis. We introduce the basics of Fourier analysis on the Boolean cube here, referring to O'Donnell (2014) for more. For functions $f, g : \{0,1\}^n \to \mathbb{R}$, define their inner product as

$$\langle f, g\rangle = \mathop{\mathbb{E}}_{x\in\{0,1\}^n}[f(x) \cdot g(x)],$$

where the expectation is with respect to the uniform distribution over $\{0,1\}^n$. For $S \in \{0,1\}^n$, the character function corresponding to S is given by $\chi_S(x) := (-1)^{S\cdot x}$, where the dot product $S \cdot x$ is $\sum_{i=1}^n S_i x_i$. Observe that the set of parity functions $\{\chi_S\}_{S\in\{0,1\}^n}$ forms an orthonormal basis for the space of all real-valued functions over the Boolean cube. In particular, every $f : \{0,1\}^n \to \mathbb{R}$ can be written uniquely as

$$f(x) = \sum_{S\in\{0,1\}^n} \widehat{f}(S)\chi_S(x) \quad \text{for all } x \in \{0,1\}^n,$$

where $\widehat{f}(S) = \langle f, \chi_S\rangle = \mathbb{E}_x[f(x)\chi_S(x)]$ is called a *Fourier coefficient* of f. A well-known result in Fourier analysis is Parseval's theorem that states that $\mathbb{E}_{x\in\{0,1\}^n}[f(x)^2] = \sum_S \widehat{f}(S)^2$. In particular, if $f : \{0,1\}^n \to \{-1, 1\}$, this implies that $\{\widehat{f}(S)^2\}_S$ forms a probability distribution.

A.2. Interesting concept classes

In this section, we introduce the main concept classes that we will be dealing with in this work.

Parities. This is the concept class defined as

$$\mathcal{C}_{\mathsf{Par}} = \{\chi_s : \chi_s(x) = \langle s, x\rangle\}_{s\in\{0,1\}^n}$$

where $\langle s, x\rangle = \sum_i s_i x_i \mod 2$.

Juntas. We say a Boolean function $c : \{0,1\}^n \to \{0,1\}$ is a k-junta if there exists $S = \{i_1, \ldots, i_k\} \subseteq [n]$ of size $|S| = k$ such that $c(x_1, \ldots, x_n) = g(x_{i_1}, \ldots, x_{i_k})$ where $g : \{0,1\}^k \to \{0,1\}$ is an arbitrary function on k bits. In relation to the class of disjunctions, note that OR_S is a $|S|$-junta.

9. In this paper, there are several polynomial factors that we have not explicitly optimized, so we use the convention $\mathrm{poly}(\varepsilon)$ to make the exposition easier to follow.

Decision trees. A decision tree (DT) on n Boolean variables is a binary tree such that the leaves have labels chosen from $\{0,1\}$ and the internal nodes of the tree have two children, the left child and the right child. On input $x \in \{0,1\}^n$, an algorithm traverses the binary tree from the root to a leaf by evaluating the node at the ith level as follows: if $x_i = 0$, go to the left child and if $x_i = 1$, go to the right child. The output of the DT is the label of the leaf that the algorithm reaches. The size of the decision tree is the total number of nodes in the tree.[10] We say that a function $c : \{0,1\}^n \to \{0,1\}$ is computed by a size-s decision tree, if there exists a size-s DT such that for every x, traversing this DT and outputting the label of the leaf yields $c(x)$.

Depth-2 circuits. Depth-2 circuits consisting of $\mathsf{AND}, \mathsf{OR}, \mathsf{NOT}$ gates are often referred to as *disjunctive normal form* (DNFs) formulas. One also refers to this concept class as AC^0_2. In particular, the class of s-term DNF formulas is defined as depth-2 circuits where the first layer consists of s AND gates, each with unbounded fanin (i.e., they take in as input an arbitrary subset of the variables in $x_1, \ldots, x_n$) and the second layer is a single OR gate of fanin s. The size of the circuit (or the DNF formula) is the total number of gates in the circuit, which in this case will be $s + 1$.

Depth-3 circuits. In this work, we will consider two different notions of depth-3 circuits. The first is AC^0_3: these are depth-3 circuits where the gates are alternating layers of ANDs and ORs. For example, the top gate may be an AND that takes as input a collection of OR gates, each of which in turn takes as input a collection of AND gates. Another type of depth-3 circuit we consider is *threshold* of DNFs. To define this, we first define the threshold function.

Definition 5 *A threshold function has the form,*

$$T^m_k(y_1, .., y_m) = \begin{cases} 1, \text{ if } \sum_{i=1}^m y_i \geq k \\ 0, \text{ otherwise} \end{cases} . \tag{3}$$

Now, one can define the threshold-of-DNFs class as follows.

Definition 6 (Threshold-of-DNFs) *Define TAC^0_2 to be the class of depth 3 circuits on n bits where the top gate is a threshold function whose inputs are DNF formulas acting on n bits.*

For both definitions, AC^0_3 and TAC^0_2, the size of the corresponding circuit is the total number of $\mathsf{AND}, \mathsf{OR}, \mathsf{NOT}$ gates.

A.3. Function and state classes

For notational convenience, we will be explicit about the size in parenthesis, i.e., $\mathsf{DT}(s), \mathsf{AC}^0_3(s)$, $\mathsf{TAC}^0_2(s)$ will be size-s decision trees and circuits, respectively. Throughout the paper we will denote $\mathcal{C}_{\mathsf{Par}}$ as the class of parities, $\mathcal{C}_{\mathsf{DT}(s)}$ as the class of decision trees of size s, $\mathcal{C}_{\mathsf{Jun}(k)}$ as the class of k-juntas, $\mathcal{C}_{\mathsf{DNF}(s)}$ as the class of s-term DNF formulas, $\mathcal{C}_{\mathsf{AC}^0_3(s)}$ as the class of $\mathsf{AC}^0_3(s)$ circuits and $\mathcal{C}_{\mathsf{TAC}^0_2(s)}$ as the class of $\mathsf{TAC}^0_2(s)$ circuits.

10. We remark that there are some works that call the *number* of leaves as the DT size, but this is a factor 2 smaller than the way we define it here.

For every concept class $\mathcal{C}$, we will denote the phase state corresponding to a function $c \in \mathcal{C}$ as

$$|\phi_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{c(x)} |x\rangle, \tag{4}$$

and $\mathcal{S}_{\mathcal{C}}$ to be the corresponding *state class*, i.e.,

$$\mathcal{S}_{\mathcal{C}} = \left\{ |\phi_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{c(x)} |x\rangle : c \in \mathcal{C} \right\}. \tag{5}$$

Furthermore, we define the *fidelity* of an unknown $|\psi\rangle$ with respect to the class $\mathcal{S}_{\mathcal{C}}$ as $\mathcal{F}_{\mathcal{C}}$, i.e., a state $|\psi\rangle$ is said to have $\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \mathsf{opt}$, if

$$\max_{c \in \mathcal{C}} |\langle \phi_c | \psi \rangle|^2 = \mathsf{opt}.$$

A.4. Learning models

A.4.1. PAC LEARNING

Classical PAC learning. In his seminal paper, Valiant (1984) introduced the *Probably Approximately Correct* model of learning, often referred to as PAC learning. In this model, there is a *concept class* $\mathcal{C} \subseteq \{c : \{0,1\}^n \to \{0,1\}\}$ which is a collection of Boolean functions. The goal of the learning algorithm is to learn $\mathcal{C}$ in the following sense: The learner $\mathcal{A}$ obtains *labeled examples* $(x, c(x))$ where $x \in \{0,1\}^n$ is uniformly random and $c \in \mathcal{C}$ is the *unknown* target function promised to lie in $\mathcal{C}$.[11] The goal of an (ε, δ)-learner $\mathcal{A}$ is as follows: for every $c \in \mathcal{C}$, given labeled examples $\{(x^i, c(x^i))\}_i$, with probability $\geq 1 - \delta$ (over the randomness of the labeled examples and the randomness of the learner), output a *hypothesis* $h : \{0,1\}^n \to \{0,1\}$ such that $\Pr_x[c(x) = h(x)] \geq 1 - \varepsilon$. In other words, with *probability* $1 - \delta$, the hypothesis h *ε-approximates* c. The (ε, δ)-sample complexity of a learning algorithm $\mathcal{A}$ is the maximal number of labeled examples used for the hardest concept, i.e., maximized over all $c \in \mathcal{C}$. The (ε, δ)-sample complexity of learning $\mathcal{C}$ is the *minimal* sample complexity over all (ε, δ)-learners for $\mathcal{C}$. Similarly the (ε, δ)-time complexity of learning $\mathcal{C}$ is the total number of time steps used by an optimal (ε, δ)-learner for $\mathcal{C}$. We say a learner is *proper* if the output hypothesis h lies within the concept class $\mathcal{C}$ and otherwise it is referred to as *improper*. Throughout the paper, we present improper learners, with the exception of the parity learner, which is proper.

Quantum PAC learning. The quantum PAC model was introduced by Bshouty and Jackson (1995) wherein they allowed the algorithm access to quantum examples of the form

$$|\psi_c\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, c(x)\rangle.$$

In particular, the learner is given copies of $|\psi_c\rangle$ and is allowed to perform arbitrary measurements on them. Note that measuring $|\psi_c\rangle$ in the computational basis produces a classical labeled example,

11. In the general PAC learning model, there is an *unknown* distribution $D : \{0,1\}^n \to [0,1]$ from which x is drawn. In this paper we will only be concerned with uniform-distribution PAC learning, i.e., D is the uniform distribution.

so quantum examples are *at least* as strong as classical examples. Understanding the strengths and weaknesses of quantum examples has been looked at by several works (we refer an interested reader to the survey of Arunachalam and De Wolf (2017)). As with the classical complexities, one can similarly define the (ε, δ)-sample and time complexity for learning $\mathcal{C}$ as the quantum sample complexity (i.e., number of quantum examples $|\psi_c\rangle$ used) and quantum time complexity (i.e., number of one and two-qubit quantum gates used in the algorithm) of an optimal (ε, δ)-learner for $\mathcal{C}$.

A.4.2. CLASSICAL AGNOSTIC LEARNING

Let D be a distribution $D : \{0,1\}^n \to [0,1]$ and $\phi : \{0,1\}^n \to [-1,1]$. We say $A = (D, \phi)$ is a distribution on $\{0,1\}^{n+1}$ satisfying: the marginal on the first n bits of A is given by the distribution D and the distribution of the last bit is described by the distribution $(1 + \phi(x))/2, (1 - \phi(x)/2)$. More formally, for the distribution $A = (D, \phi)$, we have $D(z) = \Pr_{(x,b)\sim A}[x = z]$ and

$$\phi(z) = \mathop{\mathbb{E}}_{(x,b)\sim A}[b \mid z = x].$$

Formally, for a Boolean function h and a distribution D, we define

$$\Delta(A, h) = \Pr_{(x,b)\sim A}[h(x) \neq b].$$

Furthermore, we have the following simple equality

$$\Delta(D, h) = (1 - \langle \phi, h \rangle_D)/2 = (1 - \mathop{\mathbb{E}}_{x\sim D}[\phi(x)h(x)])/2. \tag{6}$$

For a concept class $\mathcal{C}$, define

$$\Delta(A, \mathcal{C}) = \min_{h\in\mathcal{C}}\{\Delta(A, h)\}$$

Now one can formally define agnostic learning as follows

Definition 7 (Kearns et al. (1992)) *An algorithm $\mathcal{A}$ agnostically learns a class $\mathcal{C} \subseteq \{h : \{0,1\}^n \to \{-1,1\}\}$ by a representation class H if for every $\varepsilon, \delta > 0$, distribution A over $\{0,1\}^n \times \{-1,1\}$, $\mathcal{A}$, given access to examples drawn randomly from A, outputs, with probability at least $1 - \delta$, a hypothesis $h \in H$ such that $\Delta(A, h) \leq \Delta(A, C) + \varepsilon$.*

As is often the case, we limit ourselves to the scenario in which the distribution on the first n bits is uniform. In that case, the goal of the learner is to output an $h : \{0,1\}^n \to \{-1,1\}$ such that

$$(1 - \mathop{\mathbb{E}}_x[\phi(x)h(x)])/2 \leq \min_{c\in\mathcal{C}}\{(1 - \mathop{\mathbb{E}}_x[\phi(x)c(x)])/2\} + \varepsilon \implies \mathop{\mathbb{E}}_x[\phi(x)h(x)] \geq \max_{c\in\mathcal{C}} \mathop{\mathbb{E}}_x[\phi(x)c(x)] - 2\varepsilon.$$

A.4.3. QUANTUM AGNOSTIC LEARNING

Distributional agnostic learning. Like in the classical model, let $A = (D, \phi)$ be a distribution on $\{0,1\}^n$. The quantum learning algorithm is given copies of

$$\sum_{(x,b)\in\{0,1\}^{n+1}} \sqrt{A(x,b)}|x, b\rangle.$$

In the case where D is the uniform distribution, one can view $A(x,b) = 2^{-n} \cdot (1 + (-1)^b \phi(x))/2$ in the expression above. Hence, the learning algorithm is given copies of

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes \Big(\sqrt{\frac{1+\phi(x)}{2}} |0\rangle + \sqrt{\frac{1-\phi(x)}{2}} |1\rangle \Big),$$

Like in the classical setting, the goal is to output a h such that

$$\mathop{\mathbb{E}}_x [\phi(x)h(x)] \geq \max_{c \in \mathcal{C}} \mathop{\mathbb{E}}_x [\phi(x)c(x)] - \varepsilon.$$

State agnostic learning. Here, the hypothesis class is a set of quantum state $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$.[12] The agnostic learning algorithm is given copies of an unknown $|\phi\rangle$ and the goal is to output an $|\phi'\rangle$ such that

$$|\langle \psi | \phi' \rangle|^2 \geq \max_{i \in [m]} |\langle \psi | \phi_i \rangle|^2 - \varepsilon.$$

The sample complexity of learning is the total number of copies used by the algorithm to satisfy the above guarantee and the time complexity is the total time. We say an algorithm is *sample and time efficient* these complexities scale polynomial in $n, 1/\varepsilon$ and the the description size of the class. If the learner outputs $|\psi'\rangle \in \mathcal{S}$, then the learner is called *proper*, else its an *improper* learner. As far as we are aware, there are only a handful of works that have considered quantum state agnostic learning (Chen et al. (2025); Badescu and O'Donnell (2021); Bakshi et al. (2025)) wherein they considered interesting classes of states such as stabilizer states, product states, matrix product states and proved results for this model. As we mentioned in the introduction, in this work, we will be concerned with the concept class of states being

$$\mathcal{S} = \Big\{ |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x c(x)|x\rangle : c \in \mathcal{C} \Big\},$$

where $\mathcal{C}$ is a Boolean-valued concept class of interest.

Appendix B. Quantum agnostic boosting

In this section, we introduce the framework of quantum agnostic boosting and prove one of our main theorems. To define the boosting algorithm, we first define weak agnostic learners.

Definition 8 (Weak agnostic leaner) *Let $\tau \in (0,1)$ and $\eta(\cdot)$ be a function of τ. Suppose $|\phi\rangle$ is an arbitrary n-qubit quantum state such that $\mathcal{F}_{\mathcal{C}}(|\phi\rangle) \geq \tau$. We say $\mathcal{A}_{\mathsf{WAL}}$ is a weak agnostic learner for $\mathcal{S}_{\mathcal{C}}$* with promise *$\eta(\cdot)$ if, given copies of $|\phi\rangle$, outputs $|\chi\rangle \in \mathcal{C}_{\mathsf{Par}}$ such that $|\langle \phi | \chi \rangle|^2 \geq \eta(\tau)$ with probability $\geq 1 - \delta$. Let S_{WAL} and T_{WAL} be the sample and time complexity of $\mathcal{A}_{\mathsf{WAL}}$ respectively.*[13]

We are now ready to state our main theorem which comments on obtaining a strong (improper) agnostic learner from a weak agnostic learner via boosting.

12. We remark that we define this model for pure states for simplicity since that is the focus of this work. One could similarly define a hypothesis class of mixed states $\{\rho_1, \ldots, \rho_m\}$.
13. We remark that in this work we only consider weak agnostic learners whose output class will be the class of parity states, hence why we define it this way.

Theorem 9 (Quantum agnostic boosting) *Let $\varepsilon, \delta, \eta_1 \in (0,1)$. Let $\eta_2 \geq 1$ be a universal constant and $\eta : [0,1] \to [0,1]$ be defined as $\eta(\tau) := \eta_1 \tau^{\eta_2}$. Let $\mathcal{C}$ be a concept class and $|\psi\rangle$ be an unknown n-qubit state with $\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \mathsf{opt}$.*

Let $\mathcal{A}_{\mathsf{WAL}}$ be a weak agnostic learner for $\mathcal{S}_{\mathcal{C}}$ with promise of $\eta(\cdot)$, with sample complexity S_{WAL} and time complexity T_{WAL}. Then, there is an algorithm $\mathcal{L}$ that with probability $\geq 1-\delta$, outputs a state $|\widehat{\phi}\rangle$ expressed as

$$|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} \beta_i |\chi_i\rangle,$$

where $\beta \in \mathcal{B}_\infty^k$, $\kappa \leq O(1/(\varepsilon^2 \cdot \upsilon))$ with $\upsilon = \eta(C\varepsilon^2/16)$, $C = (2/3)^{1/\eta_2+1}$ and $\{|\chi_i\rangle\}_{i\in[\kappa]}$ are parity states. Furthermore $|\widehat{\phi}\rangle$ satisfies

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon.$$

This algorithm $\mathcal{L}$ invokes $\mathcal{A}_{\mathsf{WAL}}$ κ times. The overall complexity of this algorithm is as follows

$$\textit{Sample complexity: } \widetilde{O}\Big(1/(\varepsilon^2\upsilon)\cdot S_{\mathsf{WAL}} + 1/(\varepsilon^{16}\upsilon^7)\log(1/\delta)\Big)$$
$$\textit{Time complexity: } \widetilde{O}\Big(1/(\varepsilon^2\upsilon)\cdot T_{\mathsf{WAL}} + n^2/(\varepsilon^{16}\upsilon^7)\log(1/\delta)\Big).$$

B.1. Useful subroutines and lemmas

In this section, we will provide a few definitions and lemmas that we use in our algorithm. As we mentioned in the high-level idea in the introduction (Section 1), the boosting algorithm will be executed across multiple iterations and at every iteration, we will apply projections of the quantum state in hand onto parity states. We now formally define these projections.

Projection. For a set of k states $\{|\chi_i\rangle\}_{i\in[k]}$, let its span be denoted as $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[k]})$. Let Λ_T be a projection onto T. The projection of $|\psi\rangle$ onto T is given by

$$\Lambda_T|\psi\rangle = \sum_{i=1}^{k} \beta_i|\chi_i\rangle \quad \text{s.t.} \quad \{\beta_i\}_{i\in[k]} = \underset{\alpha_1,\ldots,\alpha_k\in\mathbb{C}}{\operatorname{argmin}} \Big\||\psi\rangle - \sum_{i=1}^{k}\alpha_i|\chi_i\rangle\Big\|_2 \tag{7}$$

For the special case of parity states, the projection has a simpler expression. Given a set of parity states $\{|\chi_i\rangle\}_{i\in[k]}$ with $|\chi_i\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$, the projection is

$$\Lambda_T|\psi\rangle = \sum_{i=1}^{k} \beta_i|\chi_i\rangle \;\; s.t. \;\; \beta_i = \langle\chi_i|\psi\rangle, \tag{8}$$

where $T = \{|\chi_i\rangle\}_{i\in[k]}$ and using that the parity states are orthogonal to one another. In other words, we can represent the projector Λ_T in terms of the parity states $\{|\chi_i\rangle\}_{i\in[k]}$ as

$$\Lambda_T = \sum_{i=1}^{k} |\chi_i\rangle\langle\chi_i|, \tag{9}$$

and the solution to the optimization problem of Eq. (7) is when the coefficients are inner products of the basis elements and $|\psi\rangle$. Note that Λ_T is a projector, i.e., $(\Lambda_T)^2 = \Lambda_T$ since parity states are orthogonal. Additionally, we have the following fact regarding the residual $(\mathbb{I} - \Lambda_T)|\psi\rangle$, which we will use often in our analysis below.

Fact 10 *Let $\{|\chi_i\rangle\}_{i\in[k]}$ be a set of parity states and $T = \mathsf{span}(\{|\chi_i\rangle\}_i)$. Every state $|\psi\rangle$ can be written as $|\psi\rangle = \Lambda_T|\psi\rangle + \alpha|\phi^\perp\rangle$, where $\langle\phi^\perp|\chi_i\rangle = 0$ and $\alpha = \sqrt{1 - \sum_{i=1}^k |\langle\chi_i|\psi\rangle|^2}$.*

Proof We can express any arbitrary $|\psi\rangle$ as

$$|\psi\rangle = \Lambda_T|\psi\rangle + (\mathbb{I} - \Lambda_T)|\psi\rangle = \Lambda_T|\psi\rangle + \alpha|\phi^\perp\rangle, \tag{10}$$

where we have used that Λ_T is an orthogonal projector and $\alpha|\phi^\perp\rangle = (\mathbb{I} - \Lambda_T)|\psi\rangle$ with $\alpha \in \mathcal{B}_\infty$. Note that $|\phi^\perp\rangle$ is a valid quantum state orthogonal to $|\chi_i\rangle$ for all $i \in [k]$ since $\Lambda_T(\mathbb{I} - \Lambda_T) = 0$. Moreover, by Pythagoras' theorem, we have

$$1 = \| \, |\psi\rangle \, \|_2^2 = \| \, \Lambda_T|\psi\rangle \, \|_2^2 + |\alpha|^2 \cdot \| \, |\phi^\perp\rangle \, \|_2^2 = \sum_{i=1}^k |\langle\psi|\chi_i\rangle|^2 + |\alpha|^2 \implies \alpha = \sqrt{1 - \sum_{i=1}^k |\langle\psi|\chi_i\rangle|^2},$$

where we used that $|\phi^\perp\rangle$ is orthogonal to $\Lambda_T|\psi\rangle$ in the second equality, used Eq. (8) in the third equality along with the fact that parity states are orthogonal. ■

Subroutines. Before introducing the algorithm, we present a couple of useful subroutines and lemmas regarding stabilizer states that will be necessary, below.

Lemma 11 (SWAP test) *Let $\varepsilon, \delta \in (0, 1)$. Given two arbitrary n-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$, there is a quantum algorithm that estimates $|\langle\psi|\phi\rangle|^2$ up to error ε with probability at least $1 - \delta$ using $O(1/\varepsilon^2 \cdot \log(1/\delta))$ copies of $|\psi\rangle, |\phi\rangle$ and which runs in $O(n/\varepsilon^2 \cdot \log(1/\delta))$ time.*

Lemma 12 ((García et al., 2014, Lemma 2)) *Let $|\phi\rangle$ and $|\varphi\rangle$ be n-qubit stabilizer states such that $\langle\phi|\varphi\rangle \neq 1$. Then $(|\phi\rangle + i^\ell|\varphi\rangle)/\sqrt{2}$ for $\ell \in \{0, 1, 2, 3\}$ is a stabilizer state if and only if $\langle\phi|\varphi\rangle = 0$ and there exists an n-qubit Pauli operator P such that $|\varphi\rangle = P|\phi\rangle$.*

We use the following lemma that allows for the preparation of an arbitrary stabilizer state.

Lemma 13 (Clifford synthesis (Dehaene and De Moor (2003); Patel et al. (2003))) *Given the classical description of an n-qubit stabilizer state $|\phi\rangle$, there is a quantum algorithm that outputs a Clifford circuit C that prepares $|\phi\rangle$, using $O(n^2)$ single and two-qubit Clifford gates.*

B.2. Algorithm

In this section, we present our main boosting algorithm (Algorithm 1). We refer the reader to Section 1.3.1 for a high-level description and intuition regarding our approach. The algorithm has two stages: (i) *structure learning* in which we will learn a set of parities $\{|\chi_i\rangle\}_{i\in[\kappa]}$ across κ many iterations such that $|\langle\psi|(\Lambda_T|\psi\rangle)|^2 = \mathsf{opt}$ where $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[\kappa]})$, and (ii) *parameter learning* where we learn the coefficients corresponding to the parity states $|\chi_i\rangle$ and thereby learn a state which is a good approximation to $\Lambda_T|\psi\rangle$. We now describe the notation and execution of different steps in these two stages below before presenting their analysis.

Stage 1: Structure learning. In each iteration, we will denote the *residual vector* as

$$\Psi_{t+1} = |\psi\rangle - \Lambda_{T(t)}|\psi\rangle = |\psi\rangle - \sum_{i=1}^{t} \beta_i |\chi_i\rangle, \tag{11}$$

and the corresponding (normalized) state upon which we carry out agnostic learning as

$$|\psi_{t+1}\rangle = \Psi_{t+1}/\alpha_{t+1}, \tag{12}$$

where we have used $\alpha_{t+1} = \| \Psi_{t+1} \|_2$. Note that $|\psi_{t+1}\rangle$ is what we prepare during the course of Algorithm 1. Considering the unnormalized vector Ψ_{t+1} will, however, be useful for our *analysis*.

Stopping condition. First observe that we stop at the end of iteration $t \geq 1$ when either $|\alpha_{t+1}|^2 < \varepsilon$ or $\mathcal{F}_{\mathcal{C}}(|\psi_{t+1}\rangle) < \varepsilon$. This implies that

$$|\alpha_{t+1}|^2 \cdot \mathcal{F}_{\mathcal{C}}(|\psi_{t+1}\rangle) < \varepsilon. \tag{13}$$

If we do not stop and proceed with iteration $(t+1)$, then both $|\alpha_{t+1}|^2 \geq \varepsilon$ and $\mathcal{F}_{\mathcal{C}}(|\psi_{t+1}\rangle) \geq \varepsilon$.

State update. At each iteration, the state in consideration is $|\psi_t\rangle = (\mathbb{I} - \Lambda_{T(t-1)})|\psi\rangle/\alpha_t$. We now prepare the state $|\psi_{t+1}\rangle$ given copies of $|\psi\rangle$ as follows: consider the two-outcome measurement $\left\{\mathbb{I} - \Lambda_{T(t)}, \Lambda_{T(t)}\right\}$. The probability of this 2-outcome POVM giving the first outcome is given by

$$\langle\psi|\mathbb{I} - \Lambda_{T(t)}|\psi\rangle = \langle\psi|(\mathbb{I} - \sum_{i\in[t]} |\chi_i\rangle\langle\chi_i|)|\psi\rangle = 1 - \sum_{i\in[t]} |\langle\psi|\chi_i\rangle|^2 = 1 - \sum_{i\in[t]} \beta_i^2 = |\alpha_{t+1}|^2 \geq \varepsilon,$$

where the inequality used that we are in the tth iteration only if we did not exit the loop in the previous iterations, which occurs only if $|\alpha_{t+1}|^2 > \varepsilon$. Hence with probability ε we succeed in step (10) in preparing the quantum state corresponding to $|\psi_{t+1}\rangle$. Now, one can run the weak agnostic learner on copies of $|\psi_{t+1}\rangle$ to learn the next parity state $|\phi_{t+1}\rangle$ and update $\Lambda_{T(t)} \to \Lambda_{T(t+1)}$.

Stage 2: Parameter learning. In the previous stage we learned the new parity function, but in order to update our current state $|\widehat{\phi}^{(t)}\rangle = \sum_{i\in[t]} \beta_i|\chi_i\rangle$ to $|\widehat{\phi}^{(t+1)}\rangle = \sum_{i\in[t+1]} \beta_i|\chi_i\rangle$, we also need to learn the coefficient β_{t+1}. To do so, one could compute $\beta_{t+1} = \langle\phi_{t+1}|\psi\rangle$ via the Hadamard test using the state preparation unitaries (and their controlled versions) of $|\phi_{t+1}\rangle$ and $|\psi\rangle$. However, we show that we can avoid the need for state preparation unitary access and accomplish the task of agnostic learning by determining $\Lambda_{T(t)}|\psi\rangle$ up to a global phase, using only copies of $|\psi\rangle$. This is formally stated in Lemma 18. We present this as stage 2 in Algorithm 1 below.

Algorithm 1: Quantum agnostic boosting

Input : $\varepsilon \in (0,1)$, copies of $|\psi\rangle$, weak learner $\mathcal{A}_{\mathsf{WAL}}$ (Def. 8) with promise $\eta(\tau) = \eta_1 \tau^{\eta_2}$.

Output: List of parity states $L = \{|\chi_i\rangle\}_{i\in[\kappa]}$, coefficients $B = \{\beta_i\}_{i\in[\kappa]}$.

Set error parameters $\varepsilon_s = (2/3)^{1/\eta_2+1}\varepsilon^2/16$ and $\varepsilon_p = \varepsilon/2$.

`/* Stage 1: Structure learning (Theorem 14) */`

Set $|\psi_1\rangle = |\psi\rangle$, $\alpha_1 = 1$, $L = \varnothing$.

Set parameter $\eta = \eta(\varepsilon_s)$ with $\eta(\cdot)$ being the promise of $\mathcal{A}_{\mathsf{WAL}}$ (Theorem 9).

Set $t_{\max} = 4/(\varepsilon_s \eta(\varepsilon_s))$, $\delta' = \delta/(3t_{\max})$, $\kappa = 0$.

for $t = 1$ **to** $t_{\max}$ **do**

- Run the weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ on S_{WAL} copies of $|\psi_t\rangle$ to learn a parity state $|\chi_t\rangle$.
- Run SWAP test on $O(1/\eta^2 \log(t_{\max}/\delta))$ copies of $|\psi_t\rangle, |\chi_t\rangle$ such that with probability $\geq 1-\delta'$, one obtains an $\eta/2$ approximation of $|\langle\psi_t|\chi_t\rangle|^2$. Call the estimate ν_t.
- **if** $\nu_t < \eta$ **then** break loop.
- Update $L \leftarrow L \cup \{|\chi_t\rangle\}$ and $\kappa \leftarrow \kappa + 1$.
- Set $\Lambda_{T(t)} = \sum_{i=1}^{t} |\chi_i\rangle\langle\chi_i|$.
- Let $\widehat{\alpha}_{t+1}^2$ be an $\varepsilon_s/2$ approximation of $\alpha_{t+1}^2 := \| (\mathbb{I} - \Lambda_{T(t)})|\psi\rangle \|_2^2$ by measuring $|\psi\rangle$ in the basis $\{\mathbb{I} - \Lambda_{T(t)}, \Lambda_{T(t)}\}$, $O(1/\varepsilon_s^2 \log(1/\delta'))$ many times.
- **if** $\widehat{\alpha}_{t+1}^2 < \varepsilon_s$ **then** break loop.
- Prepare S_{WAL} copies of $|\psi_{t+1}\rangle = (\mathbb{I} - \Lambda_{T(t)})|\psi\rangle/\alpha_{t+1}$ by measuring $O(S_{\mathsf{WAL}}/\varepsilon_s \log(1/\delta'))$ copies of $|\psi\rangle$ in the basis $\{\mathbb{I} - \Lambda_{T(t)}, \Lambda_{T(t)}\}$ and post-selecting for the first outcome.

`/* Stage 2: Parameter learning (Theorem 19) */`

Set error parameters $\upsilon_1 = (\varepsilon_p \cdot \eta)/(63\kappa)$, $\upsilon_2 = (\varepsilon_p \cdot \sqrt{\eta})/(18\kappa)$, $\upsilon' = (\varepsilon_p \cdot \sqrt{\eta})/(36\kappa)$.

Estimate ξ_1 of $|\langle\psi|\chi_1\rangle|$ using the SWAP test up to error υ_1.

Estimate ξ_j of $|\langle\psi|\chi_j\rangle|$ for all $j \geq 2$ using the SWAP test up to error υ_2.

for $j = 2$ **to** κ **do**

- Prepare copies of $|\chi_j^R\rangle = (|\chi_1\rangle + |\chi_j\rangle)/\sqrt{2}$ and $|\chi_j^I\rangle = (|\chi_1\rangle + i|\chi_j\rangle)/\sqrt{2}$ which are promised to be stabilizer states, using Lemma 13.
- Estimate γ_j^R of $|\langle\chi_j^R|\psi\rangle|$ using SWAP test up to error υ'.
- Estimate γ_j^I of $|\langle\chi_j^I|\psi\rangle|$ using SWAP test up to error υ'.
- Set
$$a_j = \frac{2(\gamma_j^R)^2 - \xi_1^2 - \xi_j^2}{2\xi_1}, \quad \text{and} \quad b_j = \frac{2(\gamma_j^I)^2 - \xi_1^2 - \xi_j^2}{2\xi_1}.$$
- Set $\widehat{\beta}_j = a_j + ib_j$.

Set $\widehat{\beta}_j \leftarrow \widehat{\beta}_j/\beta$, where $\beta = \| \widehat{\beta} \|_2$.

return List of κ parity states $L = \{|\chi_i\rangle\}_i$ and their coefficients $B = \{\widehat{\beta}_i\}_i$.

B.3. Structure learning

In this section, we will analyze *structure learning*, which is step 1 of Algorithm 1, and prove the following theorem.

Theorem 14 (Structure learning) *Let $\varepsilon_s, \eta_1, \delta \in (0,1)$ and $\eta_2 \geq 1$. Let $\mathcal{C}_{\mathsf{Par}}$ be the class of parities and let $\mathcal{C}$ be a specified function class. Suppose $|\psi\rangle$ is an unknown n-qubit state such that $\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \mathsf{opt}$.*

Let $\mathcal{A}_{\mathsf{WAL}}$ be a weak agnostic learner as defined in Theorem 9 with sample complexity S_{WAL}, time complexity T_{WAL}, and the corresponding $\eta : [0,1] \to [0,1]$ be defined as $\eta(\tau) = \eta_1 \tau^{\eta_2}$. Then, there exists an algorithm that with probability $\geq 1-\delta$ determines a list of $\kappa \leq 4/(\varepsilon_s \cdot \eta(\varepsilon_s))$ parity states $\{|\chi_i\rangle\}_{i\in[\kappa]}$ such that $|\langle \chi_i|\psi\rangle|^2 \geq \varepsilon_s \cdot \eta(\varepsilon_s)/4$ for all $i \in [\kappa]$ and $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \Lambda_T|\psi\rangle + \alpha_{\kappa+1}|\psi_{\kappa+1}\rangle \quad \textit{where} \quad |\alpha_{\kappa+1}|^2 \cdot \mathcal{F}_{\mathcal{C}}(|\psi_{\kappa+1}\rangle) < \varepsilon_s',$$

where $T = \mathsf{span}\big(\{|\chi_i\rangle\}_{i\in[\kappa]}\big)$, $|\psi_{\kappa+1}\rangle$ is orthogonal to each parity state $|\chi_i\rangle$, and $\varepsilon_s' = (3/2)^{1/\eta_2+1}\varepsilon_s$. Additionally, the state $|\widehat{\phi}\rangle := \Lambda_T|\psi\rangle / \| \Lambda_T|\psi\rangle \|$ satisfies

$$|\langle \widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - 2\sqrt{\varepsilon_s'}. \tag{14}$$

The overall complexity of this algorithm is as follows

$$\textit{Sample complexity: } \kappa S_{\mathsf{WAL}} + \widetilde{O}(\kappa/\eta(\varepsilon_s)^2 \log(1/\delta)),$$
$$\textit{Time complexity: } \kappa T_{\mathsf{WAL}} + \widetilde{O}(\kappa n/\eta(\varepsilon_s)^2 \log(1/\delta)).$$

The algorithm corresponding to Theorem 14 is stage 1 of Algorithm 1 that we presented above. The proof follows the analysis in Arunachalam and Dutt (2026) which showed how to learn structured stabilizer decompositions of quantum states, and which itself is inspired by the analysis from structured decomposition results from additive combinatorics (Green (2006); Tulsiani and Wolf (2014); Kim et al. (2023)). This can also be viewed as bringing arguments from Feldman's work on classical agnostic boosting (Feldman (2009)), applicable to Boolean functions, to the quantum setting.

We break down the proof of the theorem into two parts: we first provide an upper bound on the number of iterations the algorithm runs for, and then we prove Eq. (14), the main guarantee of the structure learning theorem.

Iterations. We need to upper bound the maximum number of iterations κ, the boosting algorithm runs for. To this end, we have the following observations regarding the promise of the parity state $|\chi_i\rangle$ learned in each iteration, and the residual vectors (Eq. (12)) across consecutive iterations before we stop.

Claim 15 *Consider the context of Theorem 14. Let $\delta' \in (0,1)$ be the failure probability of any iteration in Algorithm 1. Using a sample complexity of $O(1/\eta(\varepsilon_s)^2 \log(1/\delta'))$ for the SWAP test in step 7 and $O(1/\varepsilon_s^2 \log(1/\delta'))$ for estimating probability of preparing ψ_t in step 11, we ensure that for each $t \leq \kappa$, we have*

$$|\beta_t|^2 = |\langle \chi_t|\psi\rangle|^2 \geq \varepsilon_s \cdot \eta(\varepsilon_s)/4,$$

with probability $\geq 1-\delta'$.

Proof Consider iteration $t \geq 1$. We obtain an estimate of $|\langle\phi_t|\psi_t\rangle|^2$, denoted via ν_t, up to error $\eta(\varepsilon_s)/2$ with probability $\geq 1-\delta'/2$ using the SWAP with $O(1/\eta(\varepsilon_s)^2\log(1/\delta'))$ sample complexity and $O(n/\eta(\varepsilon_s)^2\log(1/\delta'))$ time. We also obtain an estimate of $\alpha_t := \| (\mathbb{I}-\Lambda_{T(t-1)})|\psi\rangle \|_2$, denoted by $\widehat{\alpha}_t$, up to error $\varepsilon_s/2$ with probability $1-\delta'/2$ using $O(1/\varepsilon_s^2\log(1/\delta'))$ samples and $O(n/\varepsilon_s^2\log(1/\delta'))$ time. By a union bound, we thus ensure with probability $\geq 1-\delta'$ that

$$\left||\widehat{\alpha}_t| - |\alpha_t|\right| \leq \varepsilon_s/2, \text{ and } \left|\nu_t - |\langle\chi_t|\psi_t\rangle|^2|\right| \leq \eta(\varepsilon_s)/2.$$

If we have not exited from the loop i.e., $|\langle\chi_t|\psi_t\rangle| \geq \eta(\varepsilon_s)$ and $\widehat{\alpha}_t^2 \geq \varepsilon_s$, then the true values satisfy

$$|\langle\chi_t|\psi_t\rangle|^2 \geq \eta(\varepsilon_s), \text{ and } \alpha_t^2 \geq \varepsilon_s/2. \tag{15}$$

Now, using the definition of the residual state $|\psi_t\rangle$ (Eq. (12)), we note that

$$\langle\chi_t|\psi_t\rangle = \frac{\langle\chi_t|\psi\rangle - \langle\chi_t|(\Lambda_{T(t-1)}|\psi\rangle)}{\alpha_t} = \frac{\langle\chi_t|\psi\rangle}{\alpha_t} \implies |\langle\chi_t|\psi\rangle|^2 = \alpha_t^2|\langle\chi_t|\psi_t\rangle|^2 \geq \varepsilon_s\cdot\eta(\varepsilon_s)/4,$$

where we have used that $|\chi_t\rangle$ is orthogonal to $\Lambda_{T(t-1)}|\psi\rangle$ (which is a linear combination of parity states $\{|\chi_i\rangle\}_{i\in[t-1]}$, distinct from $|\chi_t\rangle$) and used Eq. (15) for the implication. This gives us the desired result. ■

The above claim allows us to comment on the progress made in each iteration before we stop as follows.

Claim 16 *Consider the context of Theorem 14. Let $\delta' \in (0,1)$ be the failure probability of any iteration in Algorithm 1. For each $t \leq \kappa$, we have with probability $\geq 1-\delta'$ that*

$$\| \Psi_t \|_2^2 - \| \Psi_{t+1} \|_2^2 \geq \varepsilon_s\eta(\varepsilon_s)/4.$$

Proof By direct computation, we obtain that

$$\begin{aligned}
\| \Psi_t \|_2^2 - \| \Psi_{t+1} \|_2^2 &= \| \Psi_t - \Psi_{t+1} + \Psi_{t+1} \|_2^2 - \| \Psi_{t+1} \|_2^2 \\
&= \| \Psi_t - \Psi_{t+1} \|_2^2 + 2\mathrm{Re}(\langle\Psi_t - \Psi_{t+1}|\Psi_{t+1}\rangle) + \| \Psi_{t+1} \|_2^2 - \| \Psi_{t+1} \|_2^2 \\
&= \| \Psi_t - \Psi_{t+1} \|_2^2 \\
&= \| \beta_t|\chi_t\rangle \|_2^2 \\
&\geq \varepsilon_s\eta(\varepsilon_s)/4,
\end{aligned}$$

where we used $\langle\Psi_t - \Psi_{t+1}|\Psi_{t+1}\rangle = \beta_t\alpha_{t+1}\langle\chi_t|\psi_{t+1}\rangle = 0$ as $|\psi_{t+1}\rangle$ is orthogonal to $|\chi_t\rangle$ by construction. The final inequality follows from the promise of the weak agnostic learner and the fact that the algorithm did not break in the current and any of the previous t iterations (as was being checked in the algorithm), implying $|\beta_t|^2 \geq \varepsilon_s\eta(\varepsilon_s)/4$ by Claim 15. This completes the proof. ■

Using the above claim, we can now provide an upper bound on κ.

Claim 17 *Consider the context of Theorem 14. The maximum number of iterations κ in the structure learning algorithm of Theorem 14 with probability $\geq 1-\delta$ is bounded as*

$$\kappa \leq 4/(\varepsilon_s\eta(\varepsilon_s)).$$

Proof Suppose the algorithm ran for κ many iterations before stopping. Then, we have that

$$1 \geq \| \Psi_1 \|_2^2 - \| \Psi_{\kappa+1} \|_2^2 = \sum_{t=1}^{\kappa} \| \Psi_t \|_2^2 - \| \Psi_{t+1} \|_2^2 \geq \kappa \varepsilon_s \eta(\varepsilon_s)/4 \implies \kappa \leq 4/(\varepsilon_s \eta(\varepsilon_s)),$$

where we used that $\Psi_1 = |\psi\rangle$ in the first inequality and Claim 16 in the third inequality. This is true with success probability $\geq 1 - \kappa\delta'$ where δ' is the failure probability of Claim 16. Setting $\delta' = \delta\varepsilon_s\eta(\varepsilon_s)/4$ gives us the desired success probability. This proves the desired result. ■

Guarantee of the algorithm. We now prove the guarantee of the algorithm as promised by Theorem 14.

Proof of Theorem 14 Suppose the algorithm stops after κ iterations. From Claim 17, we have that with probability $1 - \delta$, $\kappa \leq 4/(\varepsilon_s \cdot \eta(\varepsilon_s))$ and the output of the algorithm is a set of parity states $\{|\chi_i\rangle\}_{i\in[\kappa]}$. Let $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[\kappa]})$ and denote the corresponding projection of $|\psi\rangle$ on T as

$$\Lambda_T|\psi\rangle = \sum_{i=1}^{\kappa} \beta_i |\chi_i\rangle, \tag{16}$$

where we have used Eq. (8) and denoted $\beta_i = \langle\chi_i|\psi\rangle$. By Fact 10, we can express $|\psi\rangle$ as

$$|\psi\rangle = \Lambda_T|\psi\rangle + \alpha_{\kappa+1}|\psi_{\kappa+1}\rangle, \tag{17}$$

where $|\psi_{\kappa+1}\rangle$ is the residual state (Eq. (12)) after κ iterations and is orthogonal to $\Lambda_T|\psi\rangle$. Since the algorithm stopped, we must have (steps 7 and 11 of Algorithm 1) that

$$\nu_{\kappa+1} < \eta(\varepsilon_s) \text{ or } \widehat{\alpha}_t^2 < \varepsilon_s \implies |\langle\phi_{\kappa+1}|\psi_{\kappa+1}\rangle|^2 < (3/2)\eta(\varepsilon_s) \text{ or } \alpha_t^2 < (3/2)\varepsilon_s$$

where we have used that $\nu_{\kappa+1}$ is an $\eta(\varepsilon_s)/2$ estimate of $|\langle\phi_{\kappa+1}|\psi_{\kappa+1}\rangle|^2$ and $\widehat{\alpha}_{\kappa+1}^2$ is an $\varepsilon_s/2$ estimate of $\alpha_{\kappa+1}^2$. Recall that the promise of $\mathcal{A}_{\mathsf{WAL}}$ is that if $\mathcal{F}_{\mathcal{C}}(|\psi_t\rangle) \geq \tau$ then it will output $|\chi_t\rangle$ such that $|\langle\chi_t|\psi_t\rangle|^2 \geq \eta(\tau)$. Here, since $|\langle\chi_{\kappa+1}|\psi_{\kappa+1}\rangle|^2 < 3\eta(\varepsilon_s)/2$, we must have $\mathcal{F}_{\mathcal{C}}(|\psi_{\kappa+1}\rangle) \leq (3/2)^{1/\eta_2}\varepsilon_s$ (where we have used the expression of η assumed in the statement of Theorem 9). This then implies that

$$\alpha_{\kappa+1}^2 \cdot \mathcal{F}_{\mathcal{C}}(|\psi_{\kappa+1}\rangle \leq (3/2)^{1/\eta_2+1}\varepsilon_s.$$

This proves the first part of the theorem. Let us denote $\varepsilon_s' = (3/2)^{1/\eta_2+1}\varepsilon_s$ from now onward.

Towards proving the second part, let $|\varphi\rangle \in \mathcal{S}_{\mathcal{C}}$ be the phase state that achieves maximal fidelity with $|\psi\rangle$ i.e., $|\langle\varphi|\psi\rangle|^2 = \mathsf{opt}$. By the decomposition of $|\psi\rangle$ in Eq. (17), we have

$$\begin{aligned} |\langle\varphi|\psi\rangle| \leq |\langle\varphi|(\Lambda_T|\psi\rangle)| + |\alpha_{\kappa+1}| \cdot |\langle\varphi|\psi_{\kappa+1}\rangle| < |\langle\varphi|(\Lambda_T|\psi\rangle)| + \sqrt{\varepsilon_s'} \\ \implies |\langle\varphi|\psi\rangle| - |\langle\varphi|(\Lambda_T|\psi\rangle)| < \sqrt{\varepsilon_s'}, \end{aligned}$$

where we used $|\alpha_{\kappa+1}| \cdot |\langle\varphi|\psi_{\kappa+1}\rangle| \leq |\alpha_{\kappa+1}| \cdot \sqrt{\mathcal{F}_{\mathcal{C}}(|\psi_{\kappa+1}\rangle)} < \sqrt{\varepsilon_s'}$. We can then immediately show

$$|\langle\varphi|\psi\rangle|^2 - |\langle\varphi|(\Lambda_T|\psi\rangle)|^2 = \Big(|\langle\varphi|\psi\rangle| + |\langle\varphi|(\Lambda_T|\psi\rangle)|\Big)\Big(|\langle\varphi|\psi\rangle| - |\langle\varphi|(\Lambda_T|\psi\rangle)|\Big) \leq 2\sqrt{\varepsilon_s'} \tag{18}$$

$$\implies |\langle\varphi|(\Lambda_T|\psi\rangle)|^2 \geq |\langle\varphi|\psi\rangle|^2 - 2\sqrt{\varepsilon_s'} = \mathsf{opt} - 2\sqrt{\varepsilon_s'}, \tag{19}$$

where we have used $|\langle\varphi|\psi\rangle|, |\langle\varphi|(\Lambda_T|\psi\rangle)| \leq 1$ and $|\langle\varphi|\psi\rangle|^2 = \mathsf{opt}$ in the final implication.

In order to solve the task of agnostic learning, define the quantum state $|\widehat{\phi}\rangle = \Lambda_T|\psi\rangle / \| \Lambda_T|\psi\rangle \|$. Now observe that

$$\begin{aligned}
|\langle\widehat{\phi}|\psi\rangle|^2 = \left|\langle\widehat{\phi}|\Lambda_T|\psi\rangle + r_\kappa\langle\widehat{\phi}|\psi_{\kappa+1}\rangle\right|^2 &= |\langle\widehat{\phi}|\Lambda_T|\psi\rangle|^2 \\
&= |\langle\widehat{\phi}|\widehat{\phi}\rangle| \cdot \| \Lambda_T|\psi\rangle \|_2^2 \\
&\geq |\langle\widehat{\phi}|\varphi\rangle|^2 \cdot \| \Lambda_T|\psi\rangle \|_2^2 \\
&= \frac{|\langle\varphi|\Lambda_T|\psi\rangle|^2}{\| \Lambda_T|\psi\rangle \|_2^2} \cdot \| \Lambda_T|\psi\rangle \|_2^2 \\
&= |\langle\varphi|\Lambda_T|\psi\rangle|^2 \\
&\geq \mathsf{opt} - 2\sqrt{\varepsilon'_s},
\end{aligned}$$

where the first equality used the definition of $|\psi\rangle$ in the theorem statement, second equality used that $\Lambda_T|\psi\rangle, |\psi_{\kappa+1}\rangle$ are orthogonal, third equality used the definition of $|\widehat{\phi}\rangle$, the inequality works for *every* state (and in particular $|\varphi\rangle$) and the last inequality used Eq. (19). This proves Eq. (14) in the theorem statement.

To conclude the theorem proof, we observe that the main contribution to the sample complexity is running $\mathcal{A}_{\mathsf{WAL}}$ in each of the κ many iterations which consumes $O(\kappa S_{\mathsf{WAL}})$ overall, SWAP tests (Claim 15) which consumes $O(\kappa/\eta(\varepsilon_s)^2 \log(\kappa/\delta))$ and estimation of the $\| (\mathbb{I} - \Lambda_{T(t)})|\psi\rangle \|$ (Claim 15) which consumes $O(\kappa/\varepsilon_s \log(\kappa/\delta))$. The corresponding time complexities are κT_{WAL}, $O(n\kappa/\eta(\varepsilon_s)^2 \log(\kappa/\delta))$, and $O(n\kappa/\varepsilon_s \log(\kappa/\delta))$ respectively. The overall sample and time complexities are then as stated. This completes the proof. ■

B.4. Parameter learning

In the previous section we showed how to learn a set of parities $\{|\chi_i\rangle\}_{i\in[\kappa]}$ which were used as a basis to construct the state $|\widehat{\phi}\rangle$ that achieved the $\mathsf{opt} - \varepsilon$ fidelity lower bound. In this section, we show how to learn the *coefficients* of these parities in order to construct the state $|\widehat{\phi}\rangle$. Crucial to proving our main theorem is the following lemma. In particular, for an arbitrary quantum state $|\psi\rangle$ we show how to determine the projection of the state onto $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[k]})$ i.e., $\Lambda_T|\psi\rangle$ (Eq. (8)) up to a global phase using only copies of $|\psi\rangle$. We state the lemma in full generality below since we will use it as a blackbox in another context.

Lemma 18 *Let $\kappa \in \mathbb{N}$ and $\varepsilon, \eta, \delta \in (0,1)$. Suppose $|\psi\rangle$ is an unknown n-qubit state. Let $\{|\chi_i\rangle\}_{i\in[k]}$ be a list of known parity states such that $|\langle\chi_i|\psi\rangle|^2 \geq \mu$ for all $i \in [k]$. There is an algorithm that, with probability $\geq 1-\delta$, outputs $\widehat{\beta} \in \mathcal{B}_\infty^k$ such that*

$$\left|\langle\psi|\left(\sum_{i=1}^k \widehat{\beta}_i|\chi_i\rangle\right)\right|^2 \geq |\langle\psi|(\Lambda_T|\psi\rangle)|^2 - \varepsilon,$$

where $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[k]})$. *Additionally,* $\| \widehat{\beta} \|_2^2 \leq |\langle\psi|(\Lambda_T|\psi\rangle)|^2 + \varepsilon$. *The complexity of the algorithm is:*

$$\begin{aligned}&\textit{Sample complexity: } O(k^3/(\varepsilon^2\cdot\mu^2)\log(k/\delta))\\&\textit{Time complexity: } O(k^3n^2/(\varepsilon^2\cdot\mu^2)\cdot\log(k/\delta)).\end{aligned}$$

We now state the main theorem, which is given as stage 2 of Algorithm 1.

Theorem 19 (Parameter learning) *Let* $\kappa \in \mathbb{N}$ *and* $\varepsilon_p, \mu, \delta \in (0,1)$. *Suppose* $|\psi\rangle$ *is an unknown state such that* $\mathcal{F}_{\mathcal{C}}(|\psi\rangle) = \mathsf{opt}$. *Let* $\{|\chi_i\rangle\}_{i\in[\kappa]}$ *be a list of known parity states such that* $|\langle\chi_i|\psi\rangle|^2 \geq \mu$ *and* $|\phi\rangle := \Lambda_T|\psi\rangle/\| \Lambda_T|\psi\rangle \|$ *where* $T = \mathsf{span}\big(\{|\chi_i\rangle\}_{i\in[\kappa]}\big)$, *satisfies*

$$|\langle\phi|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon_p.$$

Then, there exists an algorithm outputs coefficients $\{c_i\}_{i\in[\kappa]}$ *such that* $|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} c_i|\chi_i\rangle$ *satisfies*

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - 2\varepsilon_p,$$

with probability at least $1-\delta$. *The complexity of the algorithm is as follows:*

$$\begin{aligned}&\textit{Sample complexity: } \widetilde{O}(\kappa/(\varepsilon_p^2\cdot\mu^6)\log(1/\delta))\\&\textit{Time complexity: } \widetilde{O}(\kappa n^2/(\varepsilon_p^2\cdot\mu^6)\log(1/\delta)).\end{aligned}$$

Proof Recall that in Eq. (7) we defined $\Lambda_T|\psi\rangle = \sum_{i=1}^{\kappa}\beta_i|\chi_i\rangle$, where $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[\kappa]})$ and $\beta_i = \langle\chi_i|\psi\rangle$. We are promised $|\langle\psi|\chi_i\rangle|^2 \geq \mu$ for all $i \in [\kappa]$ and that the state $|\phi\rangle = \Lambda_T|\psi\rangle/\| \Lambda_T|\psi\rangle \|$ solves the task of agnostic learning i.e., $|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon_p$. The idea is to then use Lemma 18 to obtain an approximation of $|\widehat{\phi}\rangle$ which will be the eventual output of the agnostic learner.

Let $\gamma \in (0,1)$ be a parameter to be decided later. Using Lemma 18 with $O(\kappa^3/(\gamma^2\cdot\mu^2)\log(\kappa/\delta))$ sample complexity and $O(\kappa^3n^2/(\gamma^2\cdot\mu)^2\log(\kappa/\delta))$ time complexity, we can determine a list of coefficients $\{\widehat{\beta}_i\}_{i\in[\kappa]}$ such that

$$\left|\langle\psi|\Big(\sum_{i=1}^{k}\widehat{\beta}_i|\chi_i\rangle\Big)\right|^2 \geq |\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma, \tag{20}$$

and we are guaranteed

$$\| \widehat{\beta} \|_2^2 \leq |\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 + \gamma. \tag{21}$$

Consider the state $|\widehat{\phi}\rangle$ defined as

$$|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} c_i|\chi_i\rangle, \tag{22}$$

where $c_i = \widehat{\beta}_i / \| \widehat{\beta} \|_2$, $\forall i \in [\kappa]$. Note that $|\widehat{\phi}\rangle$ is a valid normalized state as $\| |\widehat{\phi}\rangle \| = 1$. We then have

$$\begin{aligned}
|\langle\psi|\widehat{\phi}\rangle|^2 = \frac{\left|\langle\psi|\left(\sum_{i=1}^k \widehat{\beta}_i|\chi_i\rangle\right)\right|^2}{\| \widehat{\beta} \|_2^2} &\geq \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma}{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 + \gamma} \\
&= \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma}{\| \Lambda_T|\psi\rangle \|_2^4 + \gamma} \\
&\geq \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma}{\| \Lambda_T|\psi\rangle \|_2^2 + \gamma} \\
&= \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma}{\| \Lambda_T|\psi\rangle \|_2^2 \left(1 + \frac{\gamma}{\| \Lambda_T|\psi\rangle \|_2^2}\right)} \\
&\geq \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \gamma}{\| \Lambda_T|\psi\rangle \|_2^2} \left(1 - \frac{\gamma}{\| \Lambda_T|\psi\rangle \|_2^2}\right) \\
&\geq \frac{|\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2}{\| \Lambda_T|\psi\rangle \|_2^2} - \frac{\gamma}{\| \Lambda_T|\psi\rangle \|_2^2} - \frac{\gamma |\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2}{\| \Lambda_T|\psi\rangle \|_2^4} \\
&\geq \mathsf{opt} - \varepsilon_p - \frac{\gamma}{\kappa\mu} - \frac{\gamma}{\kappa^2\mu^2} \\
&\geq \mathsf{opt} - \varepsilon_p - 2\frac{\gamma}{\kappa\mu^2},
\end{aligned}$$

where we used Eq. (20) and Eq. (21) in the second inequality in the first line, the fact that $|\langle\psi|(\Lambda_T|\psi\rangle)| = \| \Lambda_T|\psi\rangle \|_2^2$ (which can be observed from Fact 10) in the second line, $\| \Lambda_T|\psi\rangle \|_2^2 \leq 1$ in the third line, $1/(1+x) \geq 1 - x, \ \forall x \geq 0$ in the fifth line, Eq. (19) in the seventh inequality along with the observation

$$\| \Lambda_T|\psi\rangle \|_2^2 = \sum_{i \in [\kappa]} |\beta_i|^2 \geq \kappa\mu,$$

since we are given $|\beta_i|^2 \geq \mu$ for all $i \in [\kappa]$, and noting that $\mu \in (0, 1]$ in the final inequality. Setting $\gamma = \varepsilon_p \kappa \mu^2/2$ gives us the desired result. The sample complexity and the time complexity is due to the use of Lemma 18 with error parameter of γ as decided. ■

It remains to prove Lemma 18 which we do now.

Proof of Lemma 18 Recall from Eq. (8) that the projection of $|\psi\rangle$ onto $\mathsf{span}(\{|\chi_i\rangle\}_i)$ is

$$\Lambda_T|\psi\rangle = \sum_{i=1}^k \beta_i|\chi_i\rangle \ \ where \ \ \beta_i = \langle\chi_i|\psi\rangle.$$

Let $\tau = |\langle\psi| \left(\sum_{i=1}^k \beta_i|\chi_i\rangle\right)|^2$. Denoting $\beta_1 = |\beta_1|e^{i\theta_1}$ where θ_1 is the angle corresponding to the phase of β_1, we observe the following is true as well

$$\tau = \left|\langle\psi| \left(\sum_{i=1}^k \beta_i e^{-i\theta_1}|\chi_i\rangle\right)\right|^2, \tag{23}$$

since $e^{-i\theta_1}$ is simply a global phase. Let us denote $\widetilde{\beta}_i = \beta_i e^{-i\theta_1}$. Note that in particular, $\widetilde{\beta}_1 = |\beta_1|$. From Eq. (23), we have that the coefficients $\widetilde{\beta}_i$ also satisfy

$$|\langle\psi|(\Lambda_T|\psi\rangle)|^2 = \left|\langle\psi|\left(\sum_{i=1}^{k}\widetilde{\beta}_i|\chi_i\rangle\right)\right|^2 = \tau. \tag{24}$$

It is then enough to obtain estimates of $\widetilde{\beta}_i$, which we will denote as $\widehat{\beta}_i$ that satisfies the guarantee of the theorem. To this end, let $\upsilon_1 \in (0,1)$ be a fixed error parameter to be decided later and in particular we will choose it to be $\leq \sqrt{\mu}/2$ as will be seen shortly. We will use the following algorithm to estimate $\widetilde{\beta}_j$.

For $j = 1$, obtain an estimate $\widehat{\beta}_1$ of $|\beta_1| = |\langle\chi_1|\psi\rangle|$ using the SWAP test that uses $O(1/\upsilon_1^2 \log(k/\delta))$ copies of $|\psi\rangle$ and with probability at least $1 - \delta/k$, outputs an estimate of $|\beta_1|$ up to error υ_1 .

For $j \geq 2$, we obtain estimates $\widehat{\beta}_j$ of $\widetilde{\beta}_j$ using the following procedure. For all $j \geq 2$, define

$$|\chi_j^R\rangle = \frac{|\chi_1\rangle + |\chi_j\rangle}{\sqrt{2}}, \quad |\chi_j^I\rangle = \frac{|\chi_1\rangle + i|\chi_j\rangle}{\sqrt{2}}. \tag{25}$$

Note that $\langle\chi_1|\chi_j\rangle = 0$ as these are distinct parities, hence the "real" and "imaginary" quantum states $|\chi_j^R\rangle, |\chi_j^I\rangle$ are valid quantum states. Moreover there exists an $a \in \{0,1\}^n$ such that $|\chi_j\rangle = Z^a|\chi_1\rangle$, which implies that $|\chi_j^R\rangle$ and $|\chi_j^I\rangle$ are stabilizer states (using Lemma 12), which can be prepared efficiently using Lemma 13.

We now observe that

$$|\langle\chi_j^R|\psi\rangle|^2 = \frac{1}{2}|\langle\chi_1|\psi\rangle + \langle\chi_j|\psi\rangle|^2 = \frac{1}{2}\left[|\langle\chi_1|\psi\rangle|^2 + |\langle\chi_j|\psi\rangle|^2 + 2\mathrm{Re}(\langle\chi_j|\psi\rangle\overline{\langle\chi_1|\psi\rangle})\right] \tag{26}$$

$$= \frac{1}{2}\left[|\beta_1|^2 + |\beta_j|^2 + 2\mathrm{Re}(\beta_j|\beta_1|e^{-i\theta_1})\right], \tag{27}$$

which after rearrangement gives

$$\frac{2|\langle\chi_j^R|\psi\rangle|^2 - |\langle\chi_1|\psi\rangle|^2 - |\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} = \mathrm{Re}(\beta_j e^{-i\theta_1}) = \mathrm{Re}(\widetilde{\beta}_j), \tag{28}$$

where the second equality is by definition of $\widetilde{\beta}_j$. Thus one obtain an estimate $\mathrm{Re}(\widehat{\beta}_j)$ of $\mathrm{Re}(\widetilde{\beta}_j)$ using the expression above and estimating each term $|\langle\chi_j^R|\psi\rangle|^2$, $|\langle\chi_1|\psi\rangle|^2$, $|\langle\chi_j|\psi\rangle|^2$ by using the SWAP test between corresponding states in each term. Similarly, we can obtain an estimate $\mathrm{Im}(\widehat{\beta}_j)$ of $\mathrm{Im}(\widetilde{\beta}_j) = \mathrm{Im}(\beta_j e^{-i\theta_1})$ using the expression

$$\mathrm{Im}(\beta_j e^{-i\theta_1}) = \frac{2|\langle\chi_j^I|\psi\rangle|^2 - |\langle\chi_1|\psi\rangle|^2 - |\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}, \tag{29}$$

and again estimating each term involved with the SWAP test.

In an ideal world when one can run the SWAP test without errors, the above procedures suffice to estimate $\widetilde{\beta}_j$ and Eq. (24) implies the theorem statement. However, note that SWAP test has

measurement errors and we discuss the errors up to which we should estimate these terms and the sample complexity required so that one can upper bound

$$|\langle\psi|(\Lambda_T|\psi\rangle)|^2 - \left|\langle\psi|\left(\sum_{i=1}^{k}\widetilde{\beta}_i|\chi_i\rangle\right)\right|^2. \tag{30}$$

To this end, let us first bound the error $|\widehat{\beta}_j - \widetilde{\beta}_j|$. Suppose we run SWAP test to estimate $|\langle\chi_j^R|\psi\rangle|, |\langle\chi_j|\psi\rangle|$ upto error $\upsilon_j \in (0,1)$ and $\upsilon_j' \in (0,1)$ (which we fix later) respectively. In particular, if the SWAP test outputs γ_j, α_j respectively, then we have that

$$\left|\gamma_j - |\langle\chi_j^R|\psi\rangle|\right| \leq \upsilon_j', \quad \left|\alpha_j - |\langle\chi_j|\psi\rangle|\right| \leq \upsilon_j, \quad \text{for all } j \in [k], \tag{31}$$

We then have from Eq. (28) that

$$\left|\mathrm{Re}(\widehat{\beta}_j) - \mathrm{Re}(\widetilde{\beta}_j)\right| = \left|\left[\frac{\gamma_j^2}{\alpha_1} - \frac{\alpha_1}{2} - \frac{\alpha_j^2}{2\alpha_1}\right] - \left[\frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} - \frac{|\langle\chi_1|\psi\rangle|}{2} - \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}\right]\right| \tag{32}$$

$$\leq \underbrace{\left|\left[\frac{\gamma_j^2}{\alpha_1} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|}\right]\right|}_{(i)} + \underbrace{\left|\left[-\frac{\alpha_1}{2} + \frac{|\langle\chi_1|\psi\rangle|}{2}\right]\right|}_{(ii)} + \underbrace{\left|\left[-\frac{\alpha_j^2}{2\alpha_1} + \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}\right]\right|}_{(iii)}. \tag{33}$$

Let us now bound each pair of terms defined by $(i), (ii), (iii)$ above, individually.

(i) From direct computation,

$$\frac{\gamma_j^2}{\alpha_1} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \leq \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle| - \upsilon_1} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} = \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle|\left(1 - \frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right)} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \tag{34}$$

$$\leq \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle|}\left(1 + \frac{2\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right) - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \tag{35}$$

$$= \frac{\gamma_j^2 - |\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} + \frac{2\upsilon_1\gamma_j^2}{|\langle\chi_1|\psi\rangle|^2} \tag{36}$$

$$\leq \frac{2\upsilon_j'}{\sqrt{\mu}} + \frac{2\upsilon_1}{\mu}, \tag{37}$$

where in the second line we used that $1/(1-x) \leq 1 + 2x$ for all $x \in [0, 1/2]$ and noted that by choosing $\upsilon_1 \leq \sqrt{\mu}/2$, we can ensure $\upsilon_1/|\langle\chi_1|\psi\rangle| \leq 1/2$ as $|\langle\chi_1|\psi\rangle| \geq \sqrt{\mu}$ by assumption (in the lemma statement). In the final line, we used that $\gamma_j^2 \leq 1$ and

$$\gamma_j^2 - |\langle\chi_j^R|\psi\rangle|^2 = (\gamma_j - |\langle\chi_j^R|\psi\rangle|) \cdot (\gamma_j + |\langle\chi_j^R|\psi\rangle|) \leq 2\upsilon_j',$$

by Eq. (31) and $|\langle\chi_1|\psi\rangle|^2 \geq \mu$. We proceed similarly to obtain a lower bound:

$$\frac{\gamma_j^2}{\alpha_1} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \geq \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle| + \upsilon_1} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} = \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle|\left(1+\frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right)} - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \tag{38}$$

$$\geq \frac{\gamma_j^2}{|\langle\chi_1|\psi\rangle|}\left(1 - \frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right) - \frac{|\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} \tag{39}$$

$$= \frac{\gamma_j^2 - |\langle\chi_j^R|\psi\rangle|^2}{|\langle\chi_1|\psi\rangle|} - \frac{\upsilon_1\gamma_j^2}{|\langle\chi_1|\psi\rangle|^2} \tag{40}$$

$$\geq \frac{-2\upsilon_j'}{\sqrt{\mu}} - \frac{\upsilon_1}{\mu}, \tag{41}$$

where in the second line we used $1/(1+x) \geq 1-x$ for $x \geq 0$. In the final line, we used that $\gamma_j^2 \leq 1$,

$$\gamma_j^2 - |\langle\chi_j^R|\psi\rangle|^2 = (\gamma_j - |\langle\chi_j^R|\psi\rangle|)\cdot(\gamma_j + |\langle\chi_j^R|\psi\rangle|) \geq -\upsilon_j'(\gamma_j + |\langle\chi_j^R|\psi\rangle|) \geq -2\upsilon_j',$$

by Eq. (31) and $|\langle\chi_1|\psi\rangle|^2 \geq \mu$. Combining Eq. (37) and Eq. (41), we have

$$(i) \leq \frac{2\upsilon_j'}{\sqrt{\mu}} + \frac{2\upsilon_1}{\mu}. \tag{42}$$

(ii) We immediately have that

$$(ii) = \Big|\alpha_1 - |\langle\chi_1|\psi\rangle|\Big|/2 \leq \upsilon_1/2. \tag{43}$$

(iii) Again by direct computation, we have

$$-\frac{\alpha_j^2}{2\alpha_1} + \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} \leq -\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle| + 2\upsilon_1} + \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} = -\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle|\left(1+\frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right)} + \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} \tag{44}$$

$$\leq -\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle|}\left(1 - \frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right) + \frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} \tag{45}$$

$$= \frac{-\alpha_j^2 + |\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} + \frac{\alpha_j^2\upsilon_1}{2|\langle\chi_1|\psi\rangle|^2} \tag{46}$$

$$\leq \frac{\upsilon_j}{\sqrt{\mu}} + \frac{\upsilon_1}{2\mu}, \tag{47}$$

where we used in the second line that $1/(1+x) \geq 1-x$, for all $x \geq 0$. In the final line, we used $\alpha_j^2 \leq 1$, $-\alpha_j^2 + |\langle\chi_j|\psi\rangle|^2 = (|\langle\chi_j|\psi\rangle| - \alpha_j)\cdot(|\langle\chi_j|\psi\rangle| + \alpha_j) \leq 2\upsilon_j$ and $|\langle\chi_1|\psi\rangle|^2 \geq \mu$. We again

proceed similarly to obtain a lower bound:

$$-\frac{\alpha_j^2}{2\alpha_1}+\frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}\geq-\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle|-2\upsilon_1}+\frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}=-\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle|\left(1-\frac{\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right)}+\frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} \tag{48}$$

$$\geq-\frac{\alpha_j^2}{2|\langle\chi_1|\psi\rangle|}\left(1+\frac{2\upsilon_1}{|\langle\chi_1|\psi\rangle|}\right)+\frac{|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|} \tag{49}$$

$$=\frac{-\alpha_j^2+|\langle\chi_j|\psi\rangle|^2}{2|\langle\chi_1|\psi\rangle|}-\frac{2\alpha_j^2\upsilon_1}{2|\langle\chi_1|\psi\rangle|^2} \tag{50}$$

$$\geq-\frac{\upsilon_j}{\sqrt{\mu}}-\frac{\upsilon_1}{\mu}, \tag{51}$$

where in the second line we again used that $1/(1-x)\leq 1+2x$ for all $x\in[0,1/2]$ and noted that by choosing $\upsilon_1\leq\sqrt{\mu}/2$, we can ensure $\upsilon_1/|\langle\chi_1|\psi\rangle|\leq 1/2$ as $|\langle\chi_1|\psi\rangle|\geq\sqrt{\mu}$ by assumption. In the final line, we used that $\alpha_j^2\leq 1$,

$$-\alpha_j^2+|\langle\chi_j|\psi\rangle|^2=(-\alpha_j+|\langle\chi_j|\psi\rangle|)\cdot(\alpha_j+|\langle\chi_j|\psi\rangle|)\geq-\upsilon_j(\alpha_j+|\langle\chi_j^R|\psi\rangle|)\geq-2\upsilon_j,$$

and $|\langle\chi_1|\psi\rangle|^2\geq\mu$. Combining Eq. (47) and Eq. (51), we have

$$(iii)\leq\frac{\upsilon_j}{\sqrt{\mu}}+\frac{\upsilon_1}{\mu}. \tag{52}$$

Finally, substituting Eqs (42),(43),(52), into Eq. (32), we have

$$|\mathrm{Re}(\widehat{\beta}_j)-\mathrm{Re}(\widetilde{\beta}_j)|\leq(i)+(ii)+(iii)\leq\frac{2\upsilon_j'}{\sqrt{\mu}}+\frac{2\upsilon_1}{\mu}+\frac{\upsilon_1}{2}+\frac{\upsilon_j}{\sqrt{\mu}}+\frac{\upsilon_1}{\mu}\leq\frac{2\upsilon_j'}{\sqrt{\mu}}+\frac{\upsilon_j}{\sqrt{\mu}}+\frac{7\upsilon_1}{2\mu}. \tag{53}$$

By choosing $\upsilon_j'=(\varepsilon\cdot\sqrt{\mu})/(36k)$, $\upsilon_j=(\varepsilon\cdot\sqrt{\mu})/(18k)$ for all $j\geq 2$, and $\upsilon_1=(\varepsilon\cdot\mu)/(63k)$, we obtain

$$|\mathrm{Re}(\widehat{\beta}_j)-\mathrm{Re}(\widetilde{\beta}_j)|\leq\frac{\varepsilon}{6k}. \tag{54}$$

Similarly, it can be shown that by estimating $|\langle\chi_j^I|\psi\rangle|^2$ to error $\upsilon_j'=(\varepsilon\cdot\sqrt{\mu})/(12k)$ for all $j\in[k]$ as just defined, we would have

$$|\mathrm{Im}(\widehat{\beta}_j)-\mathrm{Im}(\widetilde{\beta}_j)|\leq\frac{\varepsilon}{6k}. \tag{55}$$

We then have

$$\sum_{j=1}^{k}\left|\widehat{\beta}_i-\widetilde{\beta}_i\right|\leq\sum_{j=1}^{k}\Big(|\mathrm{Re}(\widehat{\beta}_j)-\mathrm{Re}(\widetilde{\beta}_j)|+|\mathrm{Im}(\widehat{\beta}_j)-\mathrm{Im}(\widetilde{\beta}_j)|\Big)\leq\varepsilon/3. \tag{56}$$

Let us define the states $|\widehat{\phi}\rangle=\sum_{i=1}^k\widehat{\beta}_i|\chi_i\rangle$ and $|\widetilde{\chi}\rangle=\sum_{i=1}^k\widetilde{\beta}_i|\chi_i\rangle$, which are not necessarily normalized. Eq. (56) then implies

$$|\langle\psi|\widehat{\phi}\rangle-\langle\psi|\widetilde{\phi}\rangle|=\Big|\sum_{i=1}^{k}(\widehat{\beta}_i-\widetilde{\beta}_i)\langle\psi|\chi_i\rangle\Big|\leq\sum_{i=1}^{k}|\widehat{\beta}_i-\widetilde{\beta}_i|\leq\varepsilon/3. \tag{57}$$

We now note that

$$|\langle\psi|\widetilde{\phi}\rangle|^2 - |\langle\psi|\widehat{\phi}\rangle|^2 = \Big(|\langle\psi|\widetilde{\phi}\rangle| + |\langle\psi|\widehat{\phi}\rangle|\Big)\Big(|\langle\psi|\widetilde{\phi}\rangle| - |\langle\psi|\widehat{\phi}\rangle|\Big) \tag{58}$$

$$\leq \Big(1 + |\langle\psi|\widehat{\phi}\rangle|\Big)\Big(|\langle\psi|\widetilde{\phi}\rangle - \langle\psi|\widehat{\phi}\rangle|\Big) \tag{59}$$

$$\leq (2 + \varepsilon/3) \cdot (\varepsilon/3) \tag{60}$$

$$\leq 2\varepsilon/3 + (\varepsilon/3)^2 \tag{61}$$

$$\leq \varepsilon, \tag{62}$$

where in the first inequality we used that $|\langle\psi|\widehat{\phi}\rangle| = |\langle\psi|(\Lambda_T|\psi\rangle)\rangle| \leq 1$. In the second inequality, we used Eq. (57) and by the reverse triangle inequality $|a| - |b| \leq ||a| - |b|| \leq |a - b|$, we have

$$|\langle\psi|\widehat{\phi}\rangle| = |\langle\psi|\widehat{\phi}\rangle - \langle\psi|\widetilde{\phi}\rangle + \langle\psi|\widetilde{\phi}\rangle| \leq |\langle\psi|\widehat{\phi}\rangle - \langle\psi|\widetilde{\phi}\rangle| + |\langle\psi|\widetilde{\phi}\rangle| \leq \varepsilon/3 + 1,$$

where we again used Eq. (57) and $|\langle\psi|\widehat{\phi}\rangle| = |\langle\psi|(\Lambda_T|\psi\rangle)\rangle| \leq 1$.

Finally, noting $|\langle\psi|\widetilde{\phi}\rangle|^2 = |\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2$ from Eq. (24), we can upper bound Eq. (62) by ε. This proves our desired lemma statement

$$|\langle\psi|\widehat{\phi}\rangle|^2 \geq |\langle\psi|(\Lambda_T|\psi\rangle)\rangle|^2 - \varepsilon.$$

Additionally, we can upper bound the ℓ_2-norm of $\widehat{\beta} = (\widehat{\beta}_1, \ldots, \widehat{\beta}_k)$ as

$$\begin{aligned}
\sum_{j=1}^{k} |\widehat{\beta}_i|^2 = \sum_{j=1}^{k} |\widehat{\beta}_i - \widetilde{\beta}_i + \widetilde{\beta}_i|^2 &= \sum_{j=1}^{k} \Big(|\widehat{\beta}_i - \widetilde{\beta}_i|^2 + 2|\widehat{\beta}_i - \widetilde{\beta}_i| \cdot |\widetilde{\beta}_i| + |\widetilde{\beta}_i|^2\Big) \\
&\leq \left(\sum_{i=1}^{k} |\widehat{\beta}_i - \widetilde{\beta}_i|\right)^2 + 2\sum_{i=1}^{k} |\widehat{\beta}_i - \widetilde{\beta}_i| + \sum_{i=1}^{k} |\widetilde{\beta}_i|^2 \\
&\leq \varepsilon^2/9 + 2\varepsilon/3 + |\langle\psi|(\Lambda_T|\psi\rangle)|^2 \\
&\leq |\langle\psi|(\Lambda_T|\psi\rangle)|^2 + \varepsilon,
\end{aligned}$$

where we have used in the second line that $|\widetilde{\beta}_i| = |\beta_i| = |\langle\psi|\chi_i\rangle| \leq 1$ and $\sum_i |a_i|^2 \leq (\sum_i |a_i|)^2$. In the third line, we used Eq. (56) and noted that $\sum_{i=1}^{k} |\widetilde{\beta}_i|^2 = \sum_{i=1}^{k} |\beta_i|^2 = |\langle\psi|(\Lambda_T|\psi\rangle)|^2$.

The contribution to sample complexity is due to estimation of $|\langle\chi_j^R|\psi\rangle|$ and $|\langle\chi_j^I|\psi\rangle|$ up to error $\upsilon_j' = (\varepsilon \cdot \sqrt{\mu})/(36k)$, $|\langle\phi_j|\psi\rangle|$ up to error $\upsilon_j = (\varepsilon \cdot \sqrt{\mu})/(18k)$, and $|\langle\phi_j|\psi\rangle|$ up to error $\upsilon_1 = (\varepsilon \cdot \mu)/(63k)$. So by taking $O(k^2/(\varepsilon^2 \cdot \mu^2)\log(k/\delta))$ copies of $|\psi\rangle$ and performing each SWAP test so that it succeeds with probability $1 - O(\delta/k)$, so that after a union bound, the estimates in the previous analysis are met with overall probability $\geq 1 - \delta$. The main contribution to time complexity is the preparation of the stabilizer states $|\chi_j^R\rangle$ and $|\chi_j^I\rangle$ which requires $O(n^2)$ gates each. The total time complexity is

$$O(k^3 n^2/(\varepsilon^2 \cdot \mu^2) \cdot \log(k/\delta)),$$

hence proving the lemma statement. ■

B.5. Overall correctness and complexity

The proof of Theorem 9 regarding the correctness and complexity of the agnostic boosting protocol follows immediately from putting together our theorems regarding structure learning (Theorem 14) and parameter learning (Theorem 19).

Proof of Theorem 9 Let $\varepsilon_s, \varepsilon_p$ be parameters to be decided later. On input copies of $|\psi\rangle$, we use Theorem 14 with error parameter instantiated as ε_s and failure probability $\delta/2$ to learn a set of $\kappa \leq 4/(\varepsilon_s \cdot \eta(\varepsilon_s))$ parity states $\{|\chi_i\rangle\}_{i\in[\kappa]}$ such that $|\langle\chi_i|\psi\rangle|^2 \geq \varepsilon_s\eta(\varepsilon_s)/4$, and the state $|\phi\rangle := \Lambda_T|\psi\rangle/\| \Lambda_T|\psi\rangle \|$ (with $T = \mathsf{span}(\{|\chi_i\rangle\}_{i\in[\kappa]})$) satisfies

$$|\langle\psi|\phi\rangle|^2 \geq \mathsf{opt} - 2\sqrt{\varepsilon'_s},$$

where $\varepsilon'_s = (3/2)^{1/\eta_2+1}\varepsilon_s$. We then utilize Theorem 19 instantiated with error parameter $\varepsilon_p = 2\sqrt{\varepsilon'_s}$ and failure probability $\delta/2$, to learn a set of coefficients $\{\widehat{\beta}_i\}_{i\in[\kappa]}$ such that the state $|\widehat{\phi}\rangle = \sum_{i=1} \widehat{\beta}_i|\chi_i\rangle$ satisfies

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - 2\varepsilon_p.$$

Setting $\varepsilon_s = (2/3)^{1/\eta_2+1}\varepsilon^2/16$ and $\varepsilon_p = \varepsilon/2$ gives us the desired result. The overall sample complexity and time complexity is then evident from instantiating Theorems 14,19. ■

Appendix C. Learning algorithms

In this section, we show how quantum agnostic boosting (Algorithm 1) can be utilized for improper agnostic learning of decision trees, juntas and DNFs. Finally, we will give a learning protocol of depth-3 circuits, based on boosting, in the uniform PAC model given quantum examples.

C.1. Agnostic learning parities

As a preliminary step to all subsequent learning algorithms, we first present a proper agnostic learning algorithm for parities. This algorithm is fairly simple and does not rely on boosting.

Theorem 20 *Let $\mathsf{opt} \geq \varepsilon > 0$. Suppose $|\psi\rangle$ is an unknown n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathsf{Par}}(|\psi\rangle) = \mathsf{opt}$. Then, there is a $\widetilde{O}(n/\varepsilon^3 \cdot \log 1/\delta)$-time proper agnostic learner that, with probability $\geq 1-\delta$, outputs $|\phi\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ such that $|\langle\phi|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon$.*

To prove the theorem, we prove a lemma where we first assume that $\mathcal{F}_{\mathcal{C}_{\mathsf{Par}}}(|\psi\rangle)$ is known.

Lemma 21 *Let $\tau \geq \varepsilon > 0$. Suppose $|\psi\rangle$ is an unknown n-qubit state with fidelity $\mathcal{F}_{\mathcal{C}_{\mathsf{Par}}}(|\psi\rangle) \geq \tau$. Then, there is a $\widetilde{O}(n/(\tau\cdot\varepsilon^2)\cdot\log 1/\delta)$-time proper agnostic learner that, with probability $\geq 1-\delta$, outputs $|\phi\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ such that $|\langle\phi|\psi\rangle|^2 \geq \tau - \varepsilon$.*

Proof Let $|\chi_z\rangle = \mathsf{Had}^{\otimes n}|z\rangle$. We will use the following algorithm for agnostic learning.

Algorithm 2: Agnostic learning of parity states

Input : Copies of $|\psi\rangle$, $\tau \in (0,1)$, $\varepsilon \in (0,1)$, $\delta \in (0,1)$.

Output: $|\phi\rangle \in \{\mathcal{S}_{\mathsf{Par}(\varepsilon)}\}$.

1 Measure $\mathsf{Had}^{\otimes n}|\psi\rangle$ in the computational basis $t = O(1/\varepsilon \log(2/\delta))$ many times, and collect the strings in $L = \{z_1, \ldots, z_t\}$.

2 Obtain $\varepsilon/2$-approximate estimates of $|\langle \chi_z|\psi\rangle|^2,\ \forall z \in L$ with probability $\geq 1 - \delta/(2|L|)$ using the SWAP test and $O(1/\varepsilon^2 \log(|L|/\delta))$ copies of $|\psi\rangle$ for each $z \in L$. Let $\widehat{z}$ be the one that maximizes the fidelity.

3 **return** $|\chi_{\widehat{z}}\rangle \in \mathcal{S}_{\mathsf{Par}}$.

We now argue the correctness of the above protocol. Let $z^\star \in \{0,1\}^n$ be such that $|\chi_z\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ maximizes fidelity with $|\psi\rangle$ i.e., $\mathcal{F}_{\mathcal{C}_{\mathsf{Par}}}(|\psi\rangle) = |\langle \chi_z|\psi\rangle|^2 \geq \tau$. By measuring $\mathsf{Had}^{\otimes n}|\psi\rangle$ in the computational basis, the probability of obtaining a measurement outcome $z \in \{0,1\}^n$ (Step (1) in the algorithm above) coinciding with $z^\star$ is

$$\Pr[z = z^\star] = |\langle z^\star|\mathsf{Had}^{\otimes n}|\psi\rangle|^2 = |\langle \chi_{z^\star}|\psi\rangle|^2 \geq \tau.$$

Repeating Step (1), $O(1/\tau \cdot \log(1/\delta))$ many times, we ensure that $z^\star \in L$ with probability $1 - \delta/2$.

In Step (2), for each distinct $z \in L$, we estimate the fildelity $\langle \chi_z|\psi\rangle|^2$ up to error $\varepsilon/2$ with success probability $\geq 1 - \delta/(2|L|)$ by using the SWAP test, which consumes $O(|L|/\varepsilon^2 \log(|L|/\delta))$ copies of $|\psi\rangle$. We then output $|\chi_{\widehat{z}}\rangle$ for the string $\widehat{z}$, that maximized the fidelity. By the guarantee of Step (1) and a union bound, we will have $|\langle \chi_{\widehat{z}}|\psi\rangle|^2 \geq \tau - \varepsilon$ with probability $\geq 1 - \delta$.

Step (1) consumes $O(1/\tau \log(1/\delta))$ sample complexity and $O(n/\tau \log(1/\delta))$ time complexity. Step (2) consumes $O(1/(\tau \cdot \varepsilon^2) \log(1/(\delta \cdot \tau)))$ sample complexity after noting that $|L| = O(1/\tau \log(1/\delta))$, and $O(n/(\tau \cdot \varepsilon^2) \log(1/(\delta \cdot \tau)))$ time complexity. The overall time complexity is thus $O(n/(\tau \cdot \varepsilon^2) \log(1/(\delta \cdot \tau)))$. This completes the proof of the lemma. ■

The proof of Theorem 20 then follows.

Proof of Theorem 20 We instantiate Lemma 21 with τ set to be ε. Note that in either case of the unknown optimal fidelity $\mathsf{opt} \geq \varepsilon$ or $\mathsf{opt} < \varepsilon$, the outputted state $|\phi\rangle$ from Lemma 21 satisfies the guarantee of the theorem. This gives us the desired result. ■

C.2. Agnostic learning decision trees

Recall that we denote the class of decision trees of size s as $\mathcal{C}_{\mathsf{DT}(s)}$ and define

$$\mathcal{F}_{\mathcal{C}_{\mathsf{DT}(s)}}(|\psi\rangle) = \max_{f \in \mathcal{C}_{\mathsf{DT}(s)}} |\langle \phi_f|\psi\rangle|^2, \tag{63}$$

where $|\phi_f\rangle$ is the phase state (Eq. (4)) corresponding to f.

We have the following main theorem regarding the agnostic learnability of decision trees.

Theorem 22 *Let $\varepsilon, \delta \in (0,1)$. Suppose $|\psi\rangle$ is an n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathcal{C}_{\mathsf{DT}(s)}}(|\psi\rangle) = \mathsf{opt}$. Then, there is a quantum algorithm consuming $\mathrm{poly}(n, s, 1/\varepsilon, 1/\delta)$ copies of $|\psi\rangle$ and runs in $\mathrm{poly}(n, s, 1/\varepsilon, 1/\delta)$ time to output a state $|\widehat{\phi}\rangle$ such that*

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon,$$

with probability $\geq 1-\delta$. Moreover, $|\widehat{\phi}\rangle$ can be expressed as $|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} \beta_i |\chi_i\rangle$ with $\beta \in \mathcal{B}_\infty^k$ being coefficients corresponding to $|\chi_i\rangle$, which are parities, and $\kappa = \mathrm{poly}(s/\varepsilon)$.

To prove the above theorem, we will instantiate the quantum agnostic boosting algorithm (Algorithm 1) and then use Theorem 9. To use the boosting protocol, we need to define a weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ (Definition 8) of $\mathsf{DT}(s)$. Towards obtaining a $\mathcal{A}_{\mathsf{WAL}}$ for $\mathsf{DT}(s)$, we will require the following result from Kushilevitz and Mansour (1993).

Lemma 23 (Kushilevitz and Mansour (1993)) *If $f \in \mathsf{DT}(s)$, then the ℓ_1 norm of its Fourier coefficients satisfies $\sum_\alpha |\widehat{f}(\alpha)| \leq s$.*

We can now show a weak agnostic learner for $\mathsf{DT}(s)$.

Lemma 24 *Let $s \in \mathbb{N}$, $\tau, \delta \in (0,1)$ and $\varepsilon \in (0, \tau/s^2)$. Suppose $|\psi\rangle$ is an unknown n-qubit state satisfying $\mathcal{F}_{\mathcal{C}_{\mathsf{DT}(s)}}(|\psi\rangle) \geq \tau$. Then, there is a quantum algorithm that outputs a parity state $|\phi\rangle \in \mathcal{C}_{\mathsf{Par}}$ such that*

$$|\langle\phi|\psi\rangle|^2 \geq \tau/s^2 - \varepsilon,$$

with probability $\geq 1-\delta$. The algorithm consumes $\widetilde{O}(s^2/(\tau\cdot\varepsilon^2)\cdot\log 1/\delta)$ copies of $|\psi\rangle$ and runs in $\widetilde{O}(ns^2/(\tau\cdot\varepsilon^2)\cdot\log 1/\delta)$ time.

Proof Let $|\phi_f\rangle$ be the phase state corresponding to $f \in \mathsf{DT}(s)$ such that $|\langle\psi|\phi_f\rangle|^2 \geq \tau$. This then implies that

$$\begin{aligned}
\sqrt{\tau} \leq |\langle\psi|\phi_f\rangle| = |\langle\psi|\mathsf{Had}^{\otimes n}\cdot\mathsf{Had}^{\otimes n}|\phi_f\rangle| &= \Big|\langle\psi|\mathsf{Had}^{\otimes n}\cdot\sum_{\alpha\in\{0,1\}^n}\widehat{f}(\alpha)|\alpha\rangle\Big| \\
&= \Big|\sum_{\alpha\in\{0,1\}^n}\widehat{f}(\alpha)\langle\psi|\mathsf{Had}^{\otimes n}|\alpha\rangle\Big| \\
&\leq \sum_{\alpha\in\{0,1\}^n}|\widehat{f}(\alpha)|\cdot|\langle\psi|\mathsf{Had}^{\otimes n}|\alpha\rangle| \\
&\leq \max_{\alpha\in\{0,1\}^n}|\langle\psi|\mathsf{Had}^{\otimes n}|\alpha\rangle|\cdot\sum_{\alpha\in\{0,1\}^n}|\widehat{f}(\alpha)| \\
&\leq \max_{\alpha\in\{0,1\}^n}|\langle\psi|\mathsf{Had}^{\otimes n}|\alpha\rangle|\cdot s,
\end{aligned}$$

where we have used the triangle inequality in the third line and Lemma 23 in the last line. Noting that $\mathsf{Had}^{\otimes n}|\alpha\rangle = |\chi_\alpha\rangle$, is a parity, we then have

$$\mathcal{F}_{\mathcal{C}_{\mathsf{Par}}}(|\psi\rangle) \geq \tau/s^2.$$

Given that the fidelity of $|\psi\rangle$ with the class of parity states $\mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ is high, we can use Lemma 21 with error set to ε and the lower bound on fidelity set to τ/s^2 to learn a parity state $|\phi\rangle$ such that

$$|\langle\psi|\phi\rangle|^2 \geq \tau/s^2 - \varepsilon,$$

with probability $\geq 1-\delta$. This consumes $O(s^2/(\tau\cdot\varepsilon^2)\log(s/(\tau\cdot\delta)))$ sample complexity and $O(ns^2/(\tau\cdot\varepsilon^2)\log(s/(\tau\cdot\delta)))$ time complexity. This completes the proof. ■

The proof of Theorem 22 is then immediate from the instantiation of Theorem 9.

Proof [Proof of Theorem 22] We instantiate the agnostic boosting algorithm (Algorithm 1), as in Theorem 9, using the weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ for $\mathcal{C}_{\mathsf{DT}(s)}$ from Lemma 24. The corresponding promise is $\eta(\tau) = \tau/(2s^2)$ with $\eta_1 = 1/(2s^2)$ and $\eta_2 = 1$ (as defined in Theorem 9 for ε of Lemma 21 set to $\tau/(2s^2)$. The corresponding sample complexity is $S_{\mathsf{WAL}} = \widetilde{O}(s^6/\varepsilon_s^3\cdot\log 1/\delta)$ and $T_{\mathsf{WAL}} = \widetilde{O}(ns^6/\varepsilon_s^3\cdot\log 1/\delta)$ for error instantiated as ε_s in Algorithm 1 (Theorem 14). The output of Theorem 9 is then a strong (improper) agnostic learner consuming $\mathrm{poly}(s,1/\varepsilon,\log(1/\delta))$ copies and $\mathrm{poly}(n,s,1/\varepsilon,\log(1/\delta))$ time. ■

Agnostic learning juntas. We obtain an improper learning algorithm for k-juntas by instantiating Theorem 22 with size $s = 2^k$ since any k-junta admits a decision tree of size $\mathcal{O}(2^k)$. This is summarized below.

Corollary 25 *Let $\varepsilon\in(0,1)$ and $k\in\mathbb{N}$. Suppose $|\psi\rangle$ is an n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathsf{Jun}(k)}(|\psi\rangle) = \mathsf{opt}$. Then, there is a quantum algorithm consuming $\mathrm{poly}(n,2^k,1/\varepsilon)$ copies of the state to output a state $|\widehat{\phi}\rangle$ such that*

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon,$$

where $\kappa = \mathrm{poly}(2^k/\varepsilon)$ and $|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa}\beta_i|\chi_i\rangle$ with $\beta\in\mathcal{B}_\infty^k$ being coefficients for the parities $|\chi_i\rangle$.

We remark that in Appendix E.2, we describe an (improper) agnostic learning algorithm of k-junta phase states that does not utilize boosting and is instead inspired by ideas from Gopalan et al. (2008b).

C.3. Agnostic learning DNFs

We now show how the quantum agnostic boosting protocol (Algorithm 1) can be utilized for (improper) agnostic learning of s-term DNFs, which we will denote by $\mathsf{DNF}(s)$. Particularly, we establish the following result.[14]

Theorem 26 *Let $s\in\mathbb{N}$ and $\varepsilon,\delta\in(0,1)$. Suppose $|\psi\rangle$ is an n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathsf{DNF}(s)}(|\psi\rangle) = \mathsf{opt}$. Then, there is a quantum algorithm that, given access to $\mathrm{poly}((s/\varepsilon)^{\log\log(s/\varepsilon)\cdot\log(1/\varepsilon)},1/\varepsilon,\log(1/\delta))$ copies of $|\psi\rangle$ and running in time*

$$\mathrm{poly}(n,(s/\varepsilon)^{\log\log(s/\varepsilon)\cdot\log(1/\varepsilon)},1/\varepsilon,\log(1/\delta))$$

14. We remark that one could have obtained a similar result for size-s read-k DNFs with complexity $\mathrm{poly}(n,(s/\varepsilon)^{\log\log k\cdot\log 1/\varepsilon})$ using recent Fourier concentration bounds for these functions (Lecomte and Tan (2022)).

outputs, with probability at least $1-\delta$*, a state* $|\widehat{\phi}\rangle$ *such that*

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon,$$

where $|\widehat{\phi}\rangle = \sum_{i=1}^{\kappa} \beta_i |\chi_i\rangle$ *with coefficients* $\beta \in \mathcal{B}_\infty^k$ *for the parities* $|\chi_i\rangle$ *and* $\kappa = \mathrm{poly}((s/\varepsilon)^{\log\log(s/\varepsilon)\cdot\log(1/\varepsilon)})$.

Recall from Theorem 9 that we require the input of a weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ (Definition 8). To obtain $\mathcal{A}_{\mathsf{WAL}}$ for $\mathcal{C}_{\mathsf{DNF}(s)}$, our starting point is the following theorem due to Mansour which shows that the Fourier spectrum of DNFs concentrate.

Theorem 27 (Mansour (1992)) *Let* $s \in \mathbb{N}$, $\gamma \in (0,1)$. *For* $f \in \mathcal{C}_{\mathsf{DNF}(s)}$, *there exists* $\mathcal{T}_\gamma \subseteq \mathbb{F}_2^n$ *such that* $|\mathcal{T}_\gamma| \leq (s/\gamma)^{O\left((\log\log s/\gamma)\cdot(\log 1/\gamma)\right)}$ *and*

$$\sum_{T\in\mathcal{T}_\gamma} \widehat{f}(T)^2 \geq 1-\gamma.$$

This allows us to give a weak agnostic learner for $\mathsf{DNF}(s)$.

Lemma 28 *Let* $s \in \mathbb{N}$, $\tau, \delta \in (0,1]$ *and* $\varepsilon > 0$. *Suppose* $|\psi\rangle$ *is an unknown* n*-qubit state satisfying*

$$\max_{f\in\mathcal{C}_{\mathsf{DNF}(s)}} |\langle\psi|\phi_f\rangle|^2 \geq \tau.$$

Let $s^* = (s/\tau)^{O(\log\log(s/\tau)\cdot\log(1/\tau))}$. *Then, there exists an algorithm that with probability* $\geq 1-\delta$, *outputs a parity state* $|\phi\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ *satisfying*

$$|\langle\psi|\phi\rangle|^2 \geq \tau/s^* - \varepsilon.$$

The algorithm consumes

$$\widetilde{O}\Big(s^*/(\tau\cdot\varepsilon^2)\cdot\log(1/\delta)\Big)$$

copies of $|\psi\rangle$ *in total and runs in time*

$$\widetilde{O}\Big(n\cdot s^*/(\tau\cdot\varepsilon^2)\cdot\log(1/\delta)\Big).$$

Proof Let $|\phi_f\rangle$ be the phase state corresponding to $f \in \mathsf{DNF}(s)$ such that $|\langle\psi|\phi_f\rangle|^2 \geq \tau$, and $\mathcal{T} \subseteq \mathbb{F}_2^n$ be as in Theorem 27. Then we have that,

$$\begin{aligned}
\sqrt{\tau} \leq |\langle\psi|\mathsf{Had}^{\otimes n}\cdot\mathsf{Had}^{\otimes n}|\phi_f\rangle| &= |\langle\psi'|\sum_S \widehat{f}(S)|S\rangle| \\
&= |\sum_{S\in\mathcal{T}} \widehat{f}(S)\langle\psi'|S\rangle + \langle\psi'|\cdot\sum_{S\notin\mathcal{T}}\widehat{f}(S)|S\rangle| \\
&\leq \max_S |\langle\psi'|S\rangle|\cdot|\mathcal{T}| + \Big|\langle\psi'|\cdot\sum_{S\notin\mathcal{T}}\widehat{f}(S)|S\rangle\Big| \\
&\leq \max_S |\langle\psi'|S\rangle|\cdot|\mathcal{T}| + \||\psi'\rangle\|\cdot\Big\|\sum_{S\notin\mathcal{T}}\widehat{f}(S)|S\rangle\Big\| \\
&= \max_S |\langle\psi'|S\rangle|\cdot|\mathcal{T}| + \Big(\sum_{S\notin\mathcal{T}}\widehat{f}(S)^2\Big)^{1/2} \\
&\leq \max_S |\langle\psi'|S\rangle|\cdot|\mathcal{T}| + \sqrt{\gamma},
\end{aligned}$$

where we use the triangle inequality in the third line, Cauchy-Schwarz in the fourth, and Parseval's identity in combination with Theorem 27 in the last one. This implies that,

$$\mathcal{F}_{\mathsf{Par}}(|\psi\rangle) \geq (\sqrt{\tau}-\sqrt{\gamma})^2 \cdot (s/\gamma)^{-O(\log\log(s/\gamma)\log(1/\gamma)} \geq \tau \cdot \underbrace{(s/\tau)^{-O(\log\log(s/\tau)\cdot\log(1/\tau))}}_{:=1/s^*},$$

where we let $\gamma = \tau/8$. So by applying our agnostic parity learning algorithm (Lemma 21) with the lower bound there set to τ/s^*, we can learn a state $|\phi\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Par}}}$ such that

$$|\langle\psi|\phi\rangle|^2 \geq \tau/s^* - \varepsilon.$$

with probability $\geq 1-\delta$. The corresponding sample and complexity time complexity follows from Theorem 20 for $\varepsilon < \tau/s^*$, completing the proof. ■

The proof of Theorem 26 is then immediate from the instantiation of Theorem 9.

Proof [Proof of Theorem 26] We instantiate the agnostic boosting algorithm (Algorithm 1), as in Theorem 9, using the weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ for $\mathcal{C}_{\mathsf{DNF}(s)}$ from Lemma 28. The corresponding promise is $\eta(\tau) = \tau/(2s^\star)$ with $s^* = (s/\tau)^{O(\log\log(s/\tau)\cdot\log(1/\tau))}$, $\eta_1 = 1/(2s^\star)$ and $\eta_2 = 1$ (as defined in Theorem 9 for ε of Lemma 21 set to $\tau/(2s^\star)$). Note that the function τ/s^* is an increasing function of τ (as required by the boosting algorithm). The corresponding sample complexity is $S_{\mathsf{WAL}} = \widetilde{O}((s/\varepsilon_s)^{\log\log(s/\varepsilon_s)\log(1/\varepsilon_s)}/\varepsilon_s^3 \cdot \log 1/\delta)$ and $T_{\mathsf{WAL}} = \widetilde{O}(n(s/\varepsilon_s)^{\log\log(s/\varepsilon_s)\log(1/\varepsilon_s)}/\varepsilon_s^3 \cdot \log 1/\delta)$ for error instantiated as ε_s in Algorithm 1 (Theorem 14). The output of Theorem 9 is then a strong (improper) agnostic learner consuming $\mathrm{poly}(s^*, 1/\varepsilon, \log(1/\delta))$ copies and $\mathrm{poly}(n, s^*, 1/\varepsilon, \log(1/\delta))$ time with $s^* = (s/\varepsilon)^{O(\log\log(s/\varepsilon)\cdot\log(1/\varepsilon))}$. ■

C.4. PAC learning depth-3 circuits

In this section, we finally show how to quantum PAC learn depth-3 circuits. As mentioned earlier in the introduction (Section 1), the current state-of-the-art algorithm for learning depth-3 circuits in the PAC model with only classical examples has a time complexity of $n^{O(\log^2 n)}$. Here, we show how to quantum PAC learn these circuits in $n^{O(\log n)}$ time. In order to prove our result, we will use the well-known discriminator lemma by Hajnal et al. Hajnal et al. (1993) (which we reprove below specialized to our setting). Using our discriminator at each step of our boosting algorithm (in order to construct our weak learner), we are able to show that depth-3 circuits are learnable in the quantum PAC model with the desired time complexity as stated above.

C.4.1. DISCRIMINATOR LEMMA

We begin by formalizing the notion of a discriminator.

Definition 29 *Let $C : \{0,1\}^n \mapsto \{0,1\}$ be a circuit on n bits, and let $A, B \subseteq \{0,1\}^n$ be disjoint sets. Let D_A (resp D_B) be distributions supported on A (resp B). We say C is a ε-discriminator for A and B over D_A and D_B if*

$$|\mathop{\mathbb{E}}_{x\sim D_A}[C(x)] - \mathop{\mathbb{E}}_{x\sim D_B}[C(x)]| \geq \varepsilon. \tag{64}$$

Next, we extend the discriminator lemma of Hajnal et al. (1993) for circuits with a final threshold layer to the case where the distributions A and B are no longer uniform.

Lemma 30 *Let $f = T_k^m(C_1, ..., C_m)$ be a circuit on n bits. There is a C_i that is $(1/m)$-discriminator for $f^{-1}(1)$ and $f^{-1}(-1)$.*

Proof Let D_A, D_B be distributions over $A = f^{-1}(1)$ and $B = f^{-1}(-1)$ respectively, then

$$\mathop{\mathbb{E}}_{x\sim D_A}\left[\sum_{i=1}^m C_i(x)\right] \geq k, \text{ and } \mathop{\mathbb{E}}_{x\sim D_B}\left[\sum_{i=1}^m C_i(x)\right] \leq k-1,$$

since by definition for every $x \in f^{-1}(1)$ (resp. $x \in f^{-1}(-1)$), we know that $\sum_i C_i(x) \geq k$ (resp. $\sum_i C_i(x) \leq k-1$). Therefore,

$$\begin{aligned} 1 \leq \mathop{\mathbb{E}}_{x\sim D_A}\left[\sum_{i=1}^m C_i(x)\right] - \mathop{\mathbb{E}}_{x\sim D_B}\left[\sum_{i=1}^m C_i(x)\right] &= \sum_{i=1}^m \left(\mathop{\mathbb{E}}_{x\sim D_A}[C_i(x)] - \mathop{\mathbb{E}}_{x\sim D_B}[C_i(x)]\right) \\ &\leq m \max_i \left|\mathop{\mathbb{E}}_{x\sim D_A}[C_i(x)] - \mathop{\mathbb{E}}_{x\sim D_B}[C_i(x)]\right| \end{aligned}$$

Therefore for a circuit C_i with $1 \leq i \leq m$ we have that,

$$\left|\mathop{\mathbb{E}}_{x\sim D_A}[C_i(x)] - \mathop{\mathbb{E}}_{x\sim D_B}[C_i(x)]\right| \geq 1/m,$$

proving the lemma statement. ■

Using this, we prove that at least one of the circuits feeding into the final threshold gate attains a nontrivial correlation with the gate's output.

Lemma 31 *Let $f = T_k^m(C_1, ..., C_m)$ and D be an arbitrary distribution. There exists $i \in [m]$ such that*

$$|\langle f, C_i\rangle_D| = |\mathop{\mathbb{E}}_{x\sim D}[f(x)C_i(x)]| \geq \frac{1}{2m}. \tag{65}$$

Proof Let $A = f^{-1}(1)$ and $B = f^{-1}(-1)$. Let $\alpha = \sum_{x\in A} D(x)$. Without loss we can assume $\alpha \geq 1/2$, if not we can let $\alpha = \sum_{x\in B} D(x)$. For an arbitrary C_j, we have

$$\begin{aligned} \mathop{\mathbb{E}}_{x\sim D}[f(x)C_j(x)] &= \sum_{x\in A} C_j(x)\cdot D(x) - \sum_{x\in B} C_j(x)\cdot D(x) \\ &= \alpha\Big(\mathop{\mathbb{E}}_{x\sim D_A}[C_j(x)] + \mathop{\mathbb{E}}_{x\sim D_B}[C_j(x)]\Big) - \mathop{\mathbb{E}}_{x\sim D_B}[C_j(x)] \end{aligned}$$

where $\alpha = \sum_{x\in A} D(x)$ and $D_A(x) = D(x)/\alpha, D_B(x) = D(x)/(1-\alpha)$. Now Lemma 30 shows the existence of C_i such that for the previous distributions D_A and D_B over A, B respectively, we have

$$\left|\mathop{\mathbb{E}}_{x\sim D_A}[C_i(x)] - \mathop{\mathbb{E}}_{x\sim D_B}[C_i(x)]\right| \geq 1/m. \tag{66}$$

Now, if $\alpha > 1/2$, using Eq. (66), we have that $\mathbb{E}_{x\sim D}[f(x)C_i(x)] \geq 1/(2m)$, proving the lemma. ■

Fact 32 *By De Morgan's laws, the complement of any CNF with at most k clauses is logically equivalent to a DNF with at most k terms, and vice versa.*

C.4.2. LEARNING ALGORITHM

In this part of the section, we prove the following main result regarding learnability of depth-3 circuits in the quantum PAC model.

Theorem 33 *Let $s, m \in \mathbb{N}$. Suppose $f \in \mathsf{TAC}^0_2$ where the fanin of the threshold gate is m and the size of the circuit is s. Then, given quantum examples $|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x f(x)|x\rangle$, with probability $\geq 1-\delta$, can output $g : \{0,1\}^n \to \{-1,1\}$ such that $\Pr_{x\sim\mathcal{U}}[g(x) = f(x)] \geq 1-\varepsilon$. The runtime of the algorithm is*

$$\mathrm{poly}(n, m, (s/\varepsilon)^{(\log s/\varepsilon \cdot \log\log s/\varepsilon)}, \log(1/\delta)).$$

To prove this, we will show that applying improper agnostic learning of $\mathcal{S}_{\mathcal{C}_{\mathsf{DNF}(s)}}$ when the input state $|\psi_f\rangle$ is promised to a phase state corresponding to a depth-3 circuit, accomplishes the task of state tomography. To that end, we will revisit the quantum agnostic boosting argument in Section B when the goal is to do well against the class $\mathcal{C}_{\mathsf{DNF}(s)}$. For the argument below, we now specialize our discussion to when the input is a phase state $|\psi_f\rangle$ since we are in the quantum PAC setting. Recall that in the agnostic boosting algorithm (Algorithm 1), we had a running estimate $|\widehat{\phi^{(t)}}\rangle$ defined as the projection of the input state $|\psi_f\rangle$ on to the set of basis states $\{|\chi_i\rangle\}_{i\in[t]}$ learned so far:

$$|\widehat{\phi^{(t)}}\rangle = \Lambda_{T(t)}|\psi_f\rangle,$$

where $T(t) = \mathrm{span}(\{|\chi_i\rangle\}_{i\in[t]})$. We stop at the end of the κth iteration as part of structure learning (see steps 7 and 11, Algorithm 1) if

$$\alpha^2_{t+1} := \| \ (\mathbb{I} - \Lambda_{T(t)})|\psi_f\rangle \ \|^2_2 < \varepsilon_s, \ \text{ or } \ \mathcal{F}_{\mathcal{C}}(|\psi_{t+1}\rangle) < \varepsilon_s, \tag{67}$$

where the residual state is $|\psi_{t+1}\rangle = (\mathbb{I} - \Lambda_{T(t)})|\psi_f\rangle/\alpha_{t+1}$ and ε_s is an user-defined input error parameter to structure learning (see Theorem 14). However, we have not yet exploited the fact that the unknown input state $|\psi_f\rangle$ to Algorithm 1 is promised to be a phase state corresponding to a depth-3 circuit. In this case, we will now show that we stop at the end of the κth iteration as part of structure learning only if both conditions are simultaneously satisfied. In particular, we have the following claim.

Claim 34 *Consider the context of Theorem 33. Let $\mathcal{C}_{\mathsf{DNF}(s)}$ be the class of interest and $\mathcal{A}_{\mathsf{WAL}}$ of Lemma 28 be the weak agnostic learner. Suppose we apply agnostic boosting (Algorithm 1 and Theorem 14) to $|\psi_f\rangle$ then the following is true. If $|\alpha_t|^2 \geq \varepsilon$, then $\mathcal{F}_{\mathcal{C}_{\mathsf{DNF}(s)}}(|\psi_t\rangle) \geq \varepsilon/4m^2$.*

Proof Suppose as part of structure learning of the agnostic boosting algorithm (Algorithm 1), we have carried out $t-1$ iterations so far and learned the parity states $\{|\chi_i\rangle\}_{i\in[t-1]}$. Recall that until the $t-1$th iteration, the learner has obtained $\beta_1, \ldots, \beta_t$ and also the functions $\{\chi_i\}_{i\in[t]}$. Given explicit descriptions of these, the learner can implement the map

$$O_{t-1} : |x\rangle|0\rangle \mapsto |x\rangle|\mathsf{ceil}\Big(\sum_{i\in[t-1]} \beta_i\chi_i(x)\Big)\rangle,$$

where $\mathsf{ceil}(a) = a$ if $a \in [-1,1]$, $\mathsf{ceil}(a) = -1$ if $a \leq -1$ and $\mathsf{ceil}(a) = 1$ if $a \geq 1$. The oracle can be implemented in time $O(t)$ by basic arithematic operations. Define $g(x) = \mathsf{ceil}(\sum_i \beta_i\chi_i(x))$

and $|\psi_g\rangle = \frac{1}{\sqrt{2^n}}\sum_x g(x)|x\rangle$ (which can be prepared by making $O(1)$ calls to the oracle O_{t-1}). Defining $\Lambda_{g,t} = |\psi_g\rangle\langle\psi_g|$. Now measuring $|\psi_f\rangle$ in the basis $\{\Lambda_g, \mathbb{I} - \Lambda_g\}$, the post measurement state if we obtain the second outcome is given by

$$|\psi_t\rangle = \frac{1}{\alpha_t}\Big(|\psi_f\rangle - \Lambda_{g,t}|\psi_f\rangle\Big) = \frac{1}{\alpha_t}\Big(|\psi_f\rangle - \frac{1}{\sqrt{2^n}}\sum_x g(x)|x\rangle\Big),$$

where $T(t-1) = \mathrm{span}(\{|\chi_i\rangle\}_{i\in[t-1]})$, $\beta_i = \langle\chi_i|\psi_f\rangle$ (Eq. (8)) and $\alpha_t = \sqrt{1 - \sum_{i=1}^{t-1}|\beta_i|^2}$ (Fact 10). Let us denote the states

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} f(x)|x\rangle, \;\; |\chi_i\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}\chi_i(x)|x\rangle,$$

where $f : \{0,1\}^n \to \{-1,1\}$ and $\chi_i(x) = (-1)^{\alpha_i\cdot x}$ for some $\alpha_i \in \{0,1\}^n$, $\forall i \in [t-1]$. Let us define the distribution

$$D_{f,t}(x) = \Big|f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))\Big| \cdot 2^{-n}\cdot\Delta^{-1},$$

where $\Delta = \sum_x |f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))|\cdot 2^{-n}$ and χ_i is the parity function corresponding to the parity state $|\chi_i\rangle$. At this point, let us consider the inner product between the unknown f and a $\mathsf{DNF}(s)$ formula c (with $|\phi_c\rangle := \frac{1}{\sqrt{2^n}}\sum_x c(x)|x\rangle$ being the corresponding phase state),

$$\begin{aligned}
\mathop{\mathbb{E}}_{x\sim D_{f,t}}[f(x)c(x)] &= \sum_x D_{f,t}(x)[f(x)\cdot c(x)] \\
&= 2^{-n}\cdot\Delta^{-1}\cdot\sum_x\Big|f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))\Big|\cdot f(x)\cdot c(x) \\
&= 2^{-n}\cdot\Delta^{-1}\cdot\sum_x\Big(f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))\Big)\cdot c(x) \\
&= \Delta^{-1}\cdot\alpha_t\cdot\langle\psi_t|\phi_c\rangle,
\end{aligned}$$

where the third equality used the fact that, for $a\in\{-1,1\}$ and $b\in[-1,1]$, we have that $|a-b| = a\cdot(a-b)$.[15] One can then use Lemma 31 to show that

$$|\langle\psi_t|\phi_c\rangle| = \Big|\frac{\Delta}{\alpha_t}\cdot\mathop{\mathbb{E}}_{x\sim D_{f,t}}[f(x)c(x)]\Big| \geq \frac{\Delta}{m\alpha_t} \geq \frac{\sqrt{\varepsilon}}{m},$$

where we used

$$\Delta = 2^{-n}\sum_x\Big|f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))\Big| \geq 2^{-n}\sum_x\Big|f(x) - \mathsf{ceil}(\sum_{i=1}^{t-1}\beta_i\chi_i(x))\Big|^2/2 \geq \alpha_t^2/2,$$

15. To see this: if $a = 1$ then $a \geq b$ and $|a-b| = a - b = 1 - b = a\cdot(a-b)$. If $a = -1$, then $a \leq b$ and $|a-b| = b - a = b + 1 = a\cdot(a-b)$.

and $\alpha_t \geq \sqrt{\varepsilon}$. This in particular implies

$$\mathcal{F}_{\mathcal{C}}(|\psi_t\rangle) \geq |\langle \psi_t | \psi_c \rangle|^2 \geq \varepsilon/4m^2.$$

This concludes the proof. ■

Proof of Theorem 33 Let f be as in the theorem statement. We will employ the quantum agnostic boosting algorithm (Algorithm 1) on input of copies of $|\psi_f\rangle$ against the class $\mathcal{C}_{\mathsf{DNF}(s)}$ and use the weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ of Lemma 28.[16] Suppose we are at the end of the tth iteration of the agnostic boosting algorithm. We first observe that by Claim 34, if $\alpha_{t+1}^2 \geq \varepsilon$, then $\mathcal{F}_{\mathcal{C}_{\mathsf{DNF}(s)}}(|\psi_{t+1}\rangle) \geq \varepsilon/(4m^2)$. If we were to then use $\mathcal{A}_{\mathsf{WAL}}$ of Lemma 28, we are guaranteed to learn a parity state $|\phi_{t+1}\rangle$ that satisfies $|\langle \chi_{t+1} | \psi_{t+1} \rangle|^2 \geq \varepsilon/(4m^2 s^\star)$ where we have denoted $s^\star = (s/\varepsilon)^{(\log\log s/\varepsilon)\cdot \log 1/\varepsilon}$. Note that the function ε/s^* is an increasing function of ε (as required by the boosting algorithm). Thus, we no longer need to check the fidelity of the residual state with $\mathcal{C}_{\mathsf{DNF}(s)}$. We now present the simplified stage 1 of the algorithm below.

Algorithm 3: Structure learning for depth-3 circuits

Input : Parameters $s, m \in \mathbb{N}, \varepsilon \in (0,1)$, copies of $|\psi\rangle$, weak learner $\mathcal{A}_{\mathsf{WAL}}$ of Lemma 28

Output: List of parities $L = \{|\chi_i\rangle\}_{i\in[\kappa]}$

Set error parameter $\varepsilon_s = \varepsilon/9$.

Set $|\psi_1\rangle = |\psi\rangle$, $\alpha_1 = 1$, $L = \varnothing$.

Set parameter $\eta = \eta(\varepsilon_s)$ with $\eta(\cdot)$ being the promise of Lemma 28. (Theorem 9).

Set $t_{\max} = 4/(\varepsilon_s \eta(\varepsilon_s))$, $\delta' = \delta/(3t_{\max})$, $\kappa = 0$.

for $t = 1$ **to** $t_{\max}$ **do**

- Run the weak agnostic learner $\mathcal{A}_{\mathsf{WAL}}$ on S_{WAL} copies of $|\psi_t\rangle$ to learn a parity state $|\chi_t\rangle$.
- Update $L \leftarrow L \cup \{|\chi_t\rangle\}$ and $\kappa \leftarrow \kappa + 1$.
- Set $\Lambda_{T(t)} = \sum_{i=1}^{t} |\chi_i\rangle\langle\chi_i|$.
- Let $\widehat{\alpha}_{t+1}^2$ be an $\varepsilon_s/2$ approximation of $\alpha_{t+1}^2 := \| (\mathbb{I} - \Lambda_{g,t})|\psi\rangle \|_2^2$ by measuring $|\psi\rangle$ in the basis $\{\mathbb{I} - \Lambda_{g,t}, \Lambda_{g,t}\}$, $O(1/\varepsilon_s^2 \log(1/\delta'))$ many times.
- **if** $\widehat{\alpha}_{t+1}^2 < \varepsilon_s$ **then** break loop.
- Prepare S_{WAL} copies of $|\psi_{t+1}\rangle = (\mathbb{I} - \Lambda_{T(t)})|\psi\rangle/\alpha_{t+1}$ by measuring $O(S_{\mathsf{WAL}}/\varepsilon_s \log(1/\delta'))$ copies of $|\psi\rangle$ in the basis $\{\mathbb{I} - \Lambda_{T(t)}, \Lambda_{T(t)}\}$ and post-selecting for the first outcome.

return List of κ parity states $L = \{|\chi_i\rangle\}_i$.

In Algorithm 3, we set the relevant error parameter $\varepsilon_s = \varepsilon/9$. The promise of the $\mathcal{A}_{\mathsf{WAL}}$ here is then $\eta(\varepsilon_s) = \varepsilon/(36m^2 s^\star)$ (with $\eta_1 = 1/(36m^2 s^\star)$ and $\eta_2 = 1$ considering the definitions in Theorem 9). By Claim 13, we are guaranteed that we stop after $\kappa \leq 4/(\varepsilon_s \eta(\varepsilon)) = O(m^2 s^\star/\varepsilon^2)$

16. Our notation here is similar to the one in Section B.

many iterations in the structure learning algorithm. Moreover, at the end of the κth iteration, we have the following decomposition of $|\psi_f\rangle$ from Theorem 14:

$$|\psi_f\rangle = \Lambda_{T(\kappa)}|\psi_f\rangle + \alpha_{\kappa+1}|\psi_{\kappa+1}\rangle,$$

where $|\alpha_{\kappa+1}|^2 < \varepsilon/4$, $\Lambda_{T(\kappa)}|\psi\rangle$ is the projection of $|\psi\rangle$ on to $T(\kappa) = \mathsf{span}(\{\chi_t\}_{t\in[\kappa]}$ (Eq. (8)), and $|\psi_{\kappa+1}\rangle$ is orthogonal to $\Lambda_{T(\kappa)}|\psi_f\rangle$. We then have from Fact 10

$$|\langle\psi_f|(\Lambda_{T(\kappa)}|\psi_f\rangle)| = 1 - |\alpha_{\kappa+1}|^2 \geq 1 - \varepsilon/4 \implies |\langle\psi_f|(\Lambda_{T(\kappa)}|\psi_f\rangle)|^2 \geq 1 - \varepsilon/2.$$

Moreover, the state $|\phi\rangle := \Lambda_{T(\kappa)}|\psi_f\rangle / \| \Lambda_{T(\kappa)}|\psi_f\rangle \|_2$ will satisfy

$$|\langle\psi_f|\phi\rangle|^2 \geq 1 - \varepsilon/2,$$

since $\| \Lambda_{T(\kappa)}|\psi_f\rangle \|_2 \leq 1$.

At this point, we utilize Theorem 19 with the error parameter ε_p set to $\varepsilon/2$, to learn $\{\beta_i\}_{i\in[\kappa]}$ corresponding to parity states $\{|\chi_i\rangle\}_{i\in[\kappa]}$ such that $|\widehat{\phi}\rangle := \sum_{i=1}^{\kappa} \beta_i|\chi_i\rangle$ satisfies

$$|\langle\psi_f|\widehat{\phi}\rangle|^2 \geq 1 - \varepsilon. \tag{68}$$

We will now show that we have in fact accomplished the task of PAC learning. Let $h(x) = \sum_{i=1}^{t} \beta_i\chi_i(x)$. Eq. (68) then implies that $(\mathbb{E}_x[f(x)h(x)])^2 \geq 1 - \varepsilon$. Let $g(x) = \mathrm{sign}(h(x))$ and observe

$$\begin{aligned}
\Pr_{x\in\{0,1\}^n}[f(x) \neq g(x)] &= \mathop{\mathbb{E}}_x[f(x) \neq \mathrm{sign}(h(x))] \\
&\leq \mathop{\mathbb{E}}_x[|f(x) - h(x)|^2] \\
&= 1 + \mathop{\mathbb{E}}_x[h(x)^2] - 2\mathop{\mathbb{E}}_x[f(x)h(x)] \\
&\leq 1 + 1 - 2(1 - \varepsilon/2) = \varepsilon,
\end{aligned}$$

where the second inequality used that $\mathbb{E}_x[h(x)^2] = \sum_i \beta_i^2 \leq 1$ and the assumption of this case that $\mathbb{E}_x[f(x)h(x)] \geq \sqrt{1-\varepsilon} \geq 1 - \varepsilon/2$. Hence the *Boolean* function g is an ε-approximator for the unknown $f \in \mathsf{TAC}^0_2$ and we are done. Finally note that the learning algorithm *knows* explicitly $|\widehat{\phi}\rangle$, so it can output g as well. The main contribution to time complexity is due to running Algorithm 3 and utilizing Theorem 19. ■

Appendix D. Relating distributional and state agnostic learning

A natural question left open by the results of the previous sections is whether there any connections between quantum distributional agnostic learning and quantum state agnostic learning. Although the input state in quantum distribution agnostic learning is more structured than in quantum state agnostic learning, observe that the output of the former model is more stringent than the latter model. So it is unclear if these two models are equivalent. In this section, we will show that for distributions $A = (\mathcal{U}, \phi)$ where ϕ is "well-bounded" (as we make clear in the statements below), then one can use quantum *state* agnostic learning algorithms even when given as input $|\psi_D\rangle$, the input in distributional state agnostic learning. To show this, we first prove the lemma below which will immediately imply the main theorem.

Lemma 35 *Let $\gamma \in [0,1]$. Let $\phi : \{0,1\}^n \to [-1,1]$ be such that $\mathbb{E}_x[\phi(x)^2] = \gamma$. Let $h : \{0,1\}^n \to \{0,1\}$. Let*

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \sum_{b\in\{0,1\}} (-1)^b \sqrt{\frac{1+(-1)^b\phi(x)}{2}}, \quad |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{h(x)}|x\rangle.$$

Then we have that

$$\langle\psi_1|\psi_2\rangle \in \frac{1}{\sqrt{2}} \cdot \Big[\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] - \gamma/2, \mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] + \gamma/2\Big].$$

Proof The proof essentially involves writing out using Fact 4 (which follows from the Taylor series of $\sqrt{1\pm x}$).

$$\begin{aligned}
&\langle\psi_1|\psi_2\rangle \\
&= \frac{1}{2^n}\sum_x (-1)^{h(x)}\Big(\sqrt{\frac{1+\phi(x)}{2}} - \sqrt{\frac{1-\phi(x)}{2}}\Big) \\
&= \frac{1}{2^n}\sum_{x:h(x)=0}\Big(\sqrt{\frac{1+\phi(x)}{2}} - \sqrt{\frac{1-\phi(x)}{2}}\Big) - \frac{1}{2^n}\sum_{x:h(x)=1}\Big(\sqrt{\frac{1+\phi(x)}{2}} - \sqrt{\frac{1-\phi(x)}{2}}\Big) \\
&\leq \frac{1}{2^n\sqrt{2}}\Bigg[\sum_{x:h(x)=0}\Big(1+\frac{\phi(x)}{2}\Big) - \Big(1-\frac{\phi(x)}{2}-\frac{\phi(x)^2}{2}\Big) \\
&- \sum_{x:h(x)=1}\Big(1+\frac{\phi(x)}{2}-\frac{\phi(x)^2}{2}\Big) - \Big(1-\frac{\phi(x)}{2}\Big)\Bigg] \\
&= \frac{1}{2^n\sqrt{2}}\Bigg[\sum_{x:h(x)=0}\phi(x)+\frac{\phi(x)^2}{2} - \sum_{x:h(x)=1}\phi(x)-\frac{\phi(x)^2}{2}\Bigg] \\
&= \frac{1}{2^n\sqrt{2}}\sum_x (-1)^{h(x)}\phi(x) + (-1)^{h(x)}\frac{\phi(x)^2}{2} \\
&= \frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] + \frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)^2/2] \\
&\leq \frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] + \frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[\phi(x)^2/2] \\
&\leq \frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] + \gamma/(2\sqrt{2}).
\end{aligned}$$

Similarly, one can also show a *lower bound* using the same reasoning as above to get

$$\frac{1}{\sqrt{2}}\mathop{\mathbb{E}}_x[(-1)^{h(x)}\phi(x)] - \gamma/(2\sqrt{2}),$$

hence proving the lemma statement. ■

Theorem 36 *Let $\alpha, \beta, \gamma \geq 0$ and $\mathcal{C} \subseteq \{c : \{0,1\}^n \to \{0,1\}\}$ be a concept class.*

If there is a learning algorithm that satisfies the following: given copies of an unknown n-qubit $|\chi\rangle$, outputs a phase state $|\psi_h\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{h(x)} |x\rangle$ for $h : \{0,1\}^n \to \{0,1\}$, such that

$$\langle \chi | \psi_h \rangle \geq \alpha \cdot \mathsf{opt} - \beta,$$

where $\mathsf{opt} = \max_{c \in \mathcal{C}} |\langle \chi | \psi_c \rangle|$. Suppose the sample and gate complexity is T, G respectively.

Let $A = (D, \phi)$ be a distribution such that D is the uniform distribution and $\mathbb{E}_x[\phi(x)^2] = \gamma$. Then, there is an algorithm that outputs a $h : \{0,1\}^n \to \{-1,1\}$ satisfying

$$\mathop{\mathbb{E}}_x[h(x)\phi(x)] \geq \alpha \cdot \mathsf{opt} - (1+\alpha)/2 \cdot \gamma - \beta$$

using $O(T/\gamma^2)$ copies of $|\psi_D\rangle$ and $O(Gn/\gamma^2)$ gates.

Proof Consider the following algorithm: the learner obtains $|\psi_D\rangle$, applies Hadamard on the final qubit and measures, if it obtains 1 carries on (with the resulting state $|\psi'_D\rangle$), else discards. We first show that the probability of obtaining 1 is $\gamma^2/2$. This is simple to analyze, first observe that after the Hadamard gate, $|\psi_D\rangle$ can be written as

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \sum_{b \in \{0,1\}} \sqrt{\frac{1 + (-1)^b \phi(x)}{2}} |b\rangle \to \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \sum_{b,c \in \{0,1\}} (-1)^{b \cdot c} \sqrt{\frac{1 + (-1)^b \phi(x)}{2}} |c\rangle$$

and the probability of obtaining 1 is given by

$$\frac{1}{2^n} \sum_x \left(\sqrt{\frac{1+\phi(x)}{2}} - \sqrt{\frac{1-\phi(x)}{2}} \right)^2 = \mathop{\mathbb{E}}_x[1 - \sqrt{1-\phi(x)^2}] \geq \mathop{\mathbb{E}}_x[1 - (1 - \phi(x)^2/2)] = \mathop{\mathbb{E}}_x[\phi(x)^2/2] = \gamma/2,$$

where the inequality used Fact 4. So the learning algorithm can obtain *one* copy of $|\psi'_D\rangle$ using $O(1/\gamma^2)$ copies of $|\psi_D\rangle$ and furthermore the algorithm *knows* when it has succeeded. So the algorithm can deterministically obtain T many copies of $|\psi'_D\rangle$, which is given by

$$|\psi'_D\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \sum_{b \in \{0,1\}} (-1)^b \sqrt{\frac{1 + (-1)^b \phi(x)}{2}}.$$

Now, observe that if we define

$$\mathsf{opt} = \max_{c \in \mathcal{C}} \mathop{\mathbb{E}}_x[\phi(x) c(x)],$$

then by Lemma 35 we have that

$$\langle \psi_c | \psi'_D \rangle \geq \mathsf{opt}/\sqrt{2} - \gamma/(2\sqrt{2}).$$

So, one can use the base algorithm that we assumed to exist in the lemma, that given copies of $|\psi'_D\rangle$, finds a *phase state* $|\psi_h\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{h(x)} |x\rangle$ that is (α, β)-close to $|\psi'_D\rangle$. We now use Lemma 35 again and one can conclude that if $\langle \psi'_D | \psi_h \rangle \geq \mathsf{opt}/\sqrt{2} - \gamma/(2\sqrt{2})$, then that implies that

$$\mathop{\mathbb{E}}_x[(-1)^{h(x)} \phi(x)]/\sqrt{2} + \gamma/(2\sqrt{2}) \geq \langle \psi_h | \psi'_D \rangle \geq \alpha(\mathsf{opt}/\sqrt{2} - \gamma/(2\sqrt{2})) - \beta,$$

which implies

$$\mathop{\mathbb{E}}_x[(-1)^{h(x)} \phi(x)] \geq \alpha \cdot \mathsf{opt} - (1+\alpha)/2 \cdot \gamma - \beta$$

showing the desired lemma inequality, by just outputting $\mathrm{sign}(h)$ as the output hypothesis. ■

Appendix E. Further results

E.1. Bond dimension bounds for phase states

As mentioned in the introduction, the recent work of Bakshi et al. (2025) gives an algorithm for agnostic learning matrix product states whose complexity scales polynomially in the bond dimension of those states. In particular, for an MPS on n qubits with bond dimension r, their learning algorithm has time complexity $\mathrm{poly}(n, r, 1/\varepsilon)$. Since this suggests a natural learning algorithm to try for agnostic learning, it is worthwhile investigating the bond dimension for phase states corresponding to juntas and DNFs which we bound below.

Below, we will use a couple of facts about bond dimension which we state as a blackbox. First, Verstraete and Cirac (2006) showed that the bond dimension of a quantum state $|\psi\rangle$ is defined as follows

$$\textsf{bond dimension}(|\psi\rangle) = \max_{L,R}\{\textsf{Schmidt-rank}_{L|R}(|\psi\rangle)\},$$

where the maximum is over all possible contiguous cuts, call it L, R for left and right and $\textsf{Schmidt-rank}_{L|R}(|\psi\rangle)$ is defined as the Schmidt rank of the state when expressed as $|\psi\rangle = \sum_i c_i|\chi_i\rangle_L \otimes |\gamma_i\rangle_R$ with $\{|\chi_i\rangle_L\}_i, \{|\gamma_i\rangle_R\}_i$ being an orthogonal set of states. Second, since we are dealing with phase states $\frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle$ in this work, it is not too hard to see the following: defining $M_S^f(a,b) = (-1)^{f(a,b)}$ where $a \in \{0,1\}^S, b \in \{0,1\}^{\overline{S}}$, then

$$\textsf{bond dimension}(|\psi_f\rangle) = \max_S\{\textsf{rank}(M_S^f)\}.$$

A.1 Upper bound for junta states

Let $f : \{0,1\}^n \to \{0,1\}$ be a k-junta, i.e., for every x, $f(x)$ depends only on a subset $S \subseteq [n]$ of size $|S| = k$. Let $|\psi_f\rangle$ be the junta state. Consider a bipartition of the qubits into $L|R$. Let $S_L = S \cap L, S_R = S \cap R$, with $|S_L| = \ell, |S_R| = k - \ell$. Across this cut, the amplitude tensor is a $2^{|L|} \times 2^{|R|}$ matrix. Since f does not depend on qubits outside S, those qubits contribute a rank-one outer-product factor. Hence the Schmidt rank across this cut equals the rank of the $2^\ell \times 2^{k-\ell}$ sign matrix

$$M_{a,b} = (-1)^{f(a_{S_L}, b_{S_R})}, \qquad a \in \{0,1\}^{S_L},\ b \in \{0,1\}^{S_R}.$$

This rank is at most $2^{\min\{\ell, k-\ell\}}$, because the matrix has at most $2^{\min\{\ell, k-\ell\}}$ nonzero singular values. Maximizing over ℓ gives the bound

$$\textsf{Schmidt-rank}_{L|R}(|\psi\rangle) \ \le\ 2^{\lfloor k/2 \rfloor}.$$

This indicates that the (improper) agnostic learning algorithm in Bakshi et al. (2025) is efficient for juntas when $k = O(\log n)$.

A.2 Lower bound for DNF states

Here, we show that the bond dimension of s-term DNF states scales as 2^s, in the worst case, thereby making the agnostic learning algorithm of MPS by Bakshi et al. (2025) too inefficient for our setting.

Lemma 37 *Let $f : \{0,1\}^{2s} \to \{0,1\}$, be a DNF acting on $2s$ bits partitioned into two halves $x, y \in \{0,1\}^s$. We define f as follows*

$$f(x,y) = \bigvee_{i=1}^{s} (x_i \wedge y_i).$$

The phase state $|\psi_f\rangle$ when viewed as a bipartite entangled state across the x, y registers, has Schmidt rank 2^s.

Proof Let $M \in \mathbb{R}^{2^s \times 2^s}$ be the amplitude matrix $M_{x,y} := (-1)^{f(x,y)}$ of the state $|\psi_f\rangle$. Our goal is to show that $\mathsf{rank}(M) = 2^s$. To this end, first we rewrite,

$$M_{x,y} = 1 - 2\left(\bigvee_{i=1}^{s}(x_i \wedge y_i)\right) = 2\left(\prod_{i=1}^{s}(1-(x_i \wedge y_i))\right) - 1 = 2\left(\sum_{S\in[s]}(-1)^{|S|}\prod_{i\in S}x_i \prod_{j\in S} y_j\right) - 1. \tag{69}$$

In the first equality, we used the relation $(-1)^{f(x,y)} = 1-2f(x,y)$ together with the DNF representation of $f(x,y)$. In the second equality, we replaced the logical OR via $\bigvee_{i=1}^{s} z_i = 1-\prod_{i=1}^{s}(1-z_i)$. Next, we used the identity

$$\prod_{i=1}^{s}(1-z_i) = \sum_{S\in[s]}(-1)^{|S|}\prod_{i\in S} z_i.$$

The last equality follows from the identity $x_i \wedge y_i = x_i y_i$ and from expanding out the product over all $i \in [s]$. Now, set $\alpha_\emptyset := 1$ and $\alpha_S := 2(-1)^{|S|}$ for all non-empty $S \subseteq [s]$. With this notation, we can equivalently express M as

$$M_{x,y} = \sum_{S\subseteq[s]} \alpha_S \left(\prod_{i\in S} x_i\right)\left(\prod_{j\in S} y_j\right).$$

In this form, M admits the singular value decomposition $M = UDV^T$, where

$$U_{x,S} = \prod_{i\in S} x_i \;;\; V_{y,S} = \prod_{j\in S} y_j \text{ and } D = \mathrm{diag}(\alpha_S : S \subseteq [s]).$$

Up to a change of basis, M is equivalent to a diagonal matrix with 2^s nonzero diagonal entries. Consequently, $\mathsf{rank}(M) = 2^s$, and therefore $|\psi_f\rangle$ has Schmidt rank 2^s, proving the lemma. ■

Corollary 38 *There exists an s-term DNF state having bond dimension 2^s.*

Proof The statement follows from noting that bond dimension can be defined as the maximum Schmidt rank over all bipartitions of the state and then combining this with Lemma 37 which gives an s-term DNF state (on $2s$ qubits) of Schmidt rank 2^s. ■

E.2. Agnostic learning juntas without boosting

In this section, we give an improper agnostic learner of k-junta phase states that does not utilize boosting (Theorem 9). Particularly, we have the following result.

Theorem 39 *Let $k \in \mathbb{N}$ and $\varepsilon, \delta \in (0,1)$. Suppose $|\psi\rangle$ is an unknown n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathcal{C}_{\mathsf{Jun}(k)}}(|\psi\rangle) = \mathsf{opt}$. Then, there is a quantum algorithm that with probability $\geq 1-\delta$, outputs an n-qubit state $|\widehat{\phi}\rangle$ which can expressed as a linear combination of $O(k2^{2k}/\varepsilon)$ parity states and satisfies*

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - \varepsilon.$$

This algorithm does not use boosting (Algorithm 1) and uses $\mathrm{poly}(k, 2^k, 1/\varepsilon, \log(1/\delta))$ sample complexity while running in $\mathrm{poly}(n, k, 2^k, 1/\varepsilon, \log(1/\delta))$ time.

To prove the above theorem, we require the following characterization of the unknown state $|\psi\rangle$ that is promised to have high fidelity with $\mathcal{C}_{\mathsf{Jun}(k)}$.

Lemma 40 *Let $k \in \mathbb{N}$ and $\varepsilon \leq \mathsf{opt} \in (0,1]$. Suppose $|\psi\rangle$ is an arbitrary n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathcal{C}_{\mathsf{Jun}(k)}}(|\psi\rangle) = \mathsf{opt}$ attained by $|\phi_{f_S}\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Jun}(k)}}$ i.e., $|\langle\phi_{f_S}|\psi\rangle|^2 = \mathsf{opt}$. Then, there exists a collection of strings A of size $|A| \leq 2^k$ satisfying the following properties:*

(i) $\sum_{x\in A} |\alpha_x|^2 \geq \mathsf{opt} - \varepsilon$,

(ii) $\min_{x\in A} |\alpha_x|^2 \geq \max_{y\in S\setminus A} |\alpha_y|^2$,

(iii) $\min_{x\in A} |\alpha_x|^2 \geq \varepsilon/2^k$,

(iv) $\sum_{x\in \mathsf{supp}(|\phi_{f_S}\rangle)\setminus A} |\alpha_x|^2 \leq \varepsilon$,

where $\alpha_x = \langle x|\mathsf{Had}^{\otimes n}|\psi\rangle$ for all $x \in \{0,1\}^n$, and $\mathsf{supp}(|\phi_{f_S}\rangle) := \{x \in \{0,1\}^n : |\langle x|\mathsf{Had}^{\otimes n}|\phi_{f_S}\rangle| > 0\}$.

Proof Let $|\phi_{f_S}\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Jun}(k)}}$ be a k-junta phase state that maximizes fidelity with $|\psi\rangle$ i.e., $|\langle\phi_{f_S}|\psi\rangle|^2 = \mathsf{opt}$, and correspond to the k-junta Boolean function f_S which depends only on bits in $S \subseteq [n]$ of size $|S| = \ell \leq k$. Let $L = 2^\ell$.

We will denote the n-bit strings corresponding to set S as $B(S) = \{0,1\}^\ell_S \times 0^{n-\ell}_{\overline{S}}$, where the subscript S indicates that the length-ℓ string should be placed in locations corresponding that in S (assuming a fixed ordering) and similarly for subscript $\overline{S}$. We can then express the state $|\phi_{f_S}\rangle$ as

$$|\phi_{f_S}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f_S(x)}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \sum_{\alpha\in B(S)} \widehat{f}_S(\alpha)(-1)^{\alpha\cdot x}|x\rangle, \tag{70}$$

where we have noted the Fourier decomposition of the k-junta function f_S and denoted its coefficients as $\widehat{f}_S(\alpha)$. Let $|\phi'_{f_S}\rangle = \mathsf{Had}^{\otimes n}|\phi_{f_S}\rangle$ and $|\psi'\rangle = \mathsf{Had}^{\otimes n}|\psi\rangle$. Using $|\langle\psi|\phi_{f_S}\rangle|^2 = |\langle\psi'|\phi'_{f_S}\rangle|^2$, we observe that

$$\mathsf{opt} = |\langle\psi'|\phi'_{f_S}\rangle|^2 = \Big|\sum_{\alpha\in B(S)} \widehat{f}_S(\alpha)\langle\psi'|\alpha\rangle\Big|^2 \tag{71}$$

$$\leq \left[\sum_{\alpha\in B(S)} |\widehat{f}_S(\alpha)|^2\right] \cdot \left[\sum_{\alpha\in B(S)} |\langle\psi'|\alpha\rangle|^2\right] = \sum_{z\in\{0,1\}^\ell} |\langle z_S, 0_{\overline{S}}|\psi'\rangle|^2, \tag{72}$$

where we have used Eq. (70) in the second equality, and used Cauchy Schartz inequality in the third inequality as follows: let $u = \{\widehat{f}(\alpha)\}_\alpha$ and $v = \{\langle\psi'|\alpha\rangle\}_\alpha$, then $|\langle u, v\rangle|^2 \leq \|u\|_2^2 \cdot \|v\|_2^2$. We used Parseval's identity of $\sum_{\alpha\in B(S)} \widehat{f}(\alpha)^2 = 1$ in the final equality. Defining $\alpha_x = \langle x|\mathsf{Had}^{\otimes n}|\psi\rangle$, the above then implies

$$\sum_{x\in\{0,1\}^S\times 0^{\overline{S}}} |\alpha_x|^2 \geq \mathsf{opt}. \tag{73}$$

Let us define $\tau := \sum_{x\in\{0,1\}^S\times 0^{\overline{S}}} |\alpha_x|^2$. We now describe how to construct a subset $A \subseteq B(S)$ satisfying the properties indicated as part of the theorem. Consider all the elements $x \in B(S)$ and order them as $x_1, x_2, \ldots, x_L$ such that their corresponding amplitudes are non-increasing, i.e., $|\alpha_{x_1}|^2 \geq |\alpha_{x_2}|^2 \geq \cdots \geq |\alpha_{x_L}|^2$. Initializing $A = \emptyset$, we place elements into A starting from x_1 and progressively going through x_j for increasing j in order. We stop when property (i) is satisfied i.e.,

$$A = \{x_i\}_{i\in[m]} \quad \text{s.t.} \quad \sum_{x\in A} |\alpha_x|^2 \geq \tau - \varepsilon, \quad \text{and} \quad \sum_{x\in A\setminus\{x_m\}} |\alpha_x|^2 < \tau - \varepsilon, \tag{74}$$

where we have denoted $m = |A|$. The existence of such a set A is guaranteed by Eq. (73). Property (i) regarding A is then true by construction as $\tau \geq \mathsf{opt}$ (Eq. (73)). Property (ii) is also true by construction and by noting that the elements with the top m amplitudes from S are placed in A. Furthermore, note that this set A is the *minimal* $A \subseteq B(S)$ for which items (i, ii) hold true.

In order to prove item (iii), consider the set $V = (B(S) \setminus A) \cup \{x_m\}$. By construction, the element in the set V with the maximum amplitude must be x_m itself (or at least one of the elements with the same value). We now observe

$$\sum_{x\in V} |\alpha_x|^2 = \sum_{x\in B(S)} |\alpha_x|^2 - \sum_{x\in A\setminus\{x_m\}} |\alpha_x|^2 > \tau - (\tau - \varepsilon) = \varepsilon, \tag{75}$$

where the first inequality used Eq. (73) and Eq. (74). Noting that $|V| \leq |S| - 1 \leq 2^\ell \leq 2^k$ and $x_m = \arg\max_{x\in V} |\alpha_x|^2$, we also have

$$\sum_{x\in V} |\alpha_x|^2 \leq 2^k |\alpha_{x_m}|^2.$$

Combining the above with Eq. (75) then immediately implies

$$\min_{x\in A} |\alpha_x|^2 = |\alpha_{x_m}|^2 \geq \frac{\varepsilon}{2^k},$$

which proves (iii). For (iv), we observe

$$\tau = \sum_{x\in B(S)} |\alpha_x|^2 = \sum_{x\in B(S)\setminus A} |\alpha_x|^2 + \sum_{x\in A} |\alpha_x|^2 \geq \sum_{x\in B(S)\setminus A} |\alpha_x|^2 + \tau - \varepsilon \implies \sum_{x\in B(S)\setminus A} |\alpha_x|^2 \leq \varepsilon,$$

where we have used Eq. (74) in the third inequality. This completes the proof. ■

We can then show that the projection of $|\psi\rangle$ on to the set A from Claim 40 solves the task of agnostic learning, which is formally stated below.

Corollary 41 *Let $k \in \mathbb{N}$ and $\varepsilon \in (0,1)$. Suppose $|\psi\rangle$ is an unknown n-qubit state with unknown optimal fidelity $\mathcal{F}_{\mathcal{C}_{\mathsf{Jun}(k)}}(|\psi\rangle) = \mathsf{opt}$ and let A be the set from Lemma 40 corresponding to error $\varepsilon/2^k$. Then, any set of parity states $\{|\chi_y\rangle\}_{y\in Y}$ corresponding to $Y \subseteq \{0,1\}^n$ such that $A \subseteq Y$ and $|\phi\rangle := \Lambda_T|\psi\rangle / \| \Lambda_T|\psi\rangle \|_2$ (with $T = \mathrm{span}(\{|\phi_y\rangle\}_{y\in Y})$) satisfies*

$$|\langle\phi|\psi\rangle|^2 \geq \mathsf{opt} - 2\sqrt{\varepsilon},$$

where $\Lambda_T|\psi\rangle$ is the projection of $|\psi\rangle$ onto T as defined in Eq. (9).

Proof Let $|\phi_{f_S}\rangle \in \mathcal{S}_{\mathcal{C}_{\mathsf{Jun}(k)}}$ be a k-junta phase state that maximizes fidelity with $|\psi\rangle$ i.e., $|\langle\phi_{f_S}|\psi\rangle|^2 = \mathsf{opt}$, and correspond to the k-junta Boolean function f_S which depends only on bits in $S \subseteq [n]$ of size $|S| = \ell \leq k$. Let $L = 2^\ell$.

We will denote the n-bit strings corresponding to set S as $B(S) = \{0,1\}^\ell_S \times 0^{n-\ell}_{\overline{S}}$, where the subscript S indicates that the length-ℓ string should be placed in locations corresponding that in S (assuming a fixed ordering) and similarly for subscript $\overline{S}$.

Consider the set A from Lemma 40 corresponding to error $\varepsilon/2^k$. Observe that for each string $\alpha \in A$, we can define a parity state $|\chi_\alpha\rangle := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{\alpha\cdot x}|x\rangle$ such that

$$|\langle\chi_\alpha|\psi\rangle|^2 \geq \varepsilon/2^{2k},$$

where this follows from Lemma 40(iii). We are given that the set Y in hand contains A. Define $T = \mathsf{span}(\{|\phi_y\rangle\}_{y\in Y}$ and $\Lambda_T|\psi\rangle$ the corresponding projection of $|\psi\rangle$ on to T. Using Fact 10, we can express $|\psi\rangle$ as

$$|\psi\rangle = \Lambda_T|\psi\rangle + \alpha|\phi^\perp\rangle, \tag{76}$$

where $|\phi^\perp\rangle$ is orthogonal to $\Lambda_T|\psi\rangle$ and $\alpha = \sqrt{1 - \| \Lambda_T|\psi\rangle \|_2^2}$. We then observe

$$|\langle\phi_{f_S}|\psi\rangle| \leq |\langle\phi_{f_S}|(\Lambda_T|\psi\rangle)\rangle| + |\alpha\langle\phi_{f_S}|\phi^\perp\rangle| = |\langle\phi_{f_S}|(\Lambda_T|\psi\rangle)\rangle| + \Big|\sum_{x\in B(S)\setminus A} \alpha_x \widehat{f}_S(x)\Big| \tag{77}$$

$$\leq |\langle\phi_{f_S}|(\Lambda_T|\psi\rangle)\rangle| + \sum_{x\in B(S)\setminus A} |\alpha_x| \tag{78}$$

$$\leq |\langle\phi_{f_S}|(\Lambda_T|\psi\rangle)\rangle| + \sqrt{\varepsilon}, \tag{79}$$

where we have used the decomposition of $|\psi\rangle$ from Eq. (76) in the first inequality. In the second inequality, we used that $|\phi_{f_S}\rangle$ is supported on computational basis states over $B(S)$ whereas $|\phi^\perp\rangle$ is supported over computational basis states not in Y. The second line follows from applying triange inequality and then noting that $A \subseteq Y \implies (B(S) \setminus Y) \subseteq (B(S) \setminus A)$. The third line follows from Lemma 40(iii) which implies $|\alpha_x| \leq \sqrt{\varepsilon}/2^k,\ \forall x \in B(S) \setminus A$ and using $|B(S)| \leq 2^k$. This implies that

$$|\langle\phi_{f_S}|\psi\rangle| - |\langle\phi_{f_S}|(\Lambda_T\psi)\rangle| \leq \sqrt{\varepsilon}.$$

We then observe

$$|\langle\phi_{f_S}|\psi\rangle|^2 - |\langle\phi_{f_S}|(\Lambda_T\psi)\rangle|^2 = \Big(|\langle\phi_{f_S}|\psi\rangle| + |\langle\phi_{f_S}|(\Lambda_T\psi)\rangle|\Big)\Big(|\langle\phi_{f_S}|\psi\rangle| - |\langle\phi_{f_S}|(\Lambda_T\psi)\rangle|\Big) \leq 2\sqrt{\varepsilon}, \tag{80}$$

$$\implies |\langle\phi_{f_S}|(\Lambda_T\psi)\rangle|^2 \geq |\langle\phi_{f_S}|\psi\rangle|^2 - 2\sqrt{\varepsilon} = \mathsf{opt} - 2\sqrt{\varepsilon}, \tag{81}$$

where we used $|\langle\phi_{f_S}|(\Lambda_T\psi)\rangle|, |\langle\phi_{f_S}|\psi\rangle| \leq 1$ in the first line and the fact that $|\langle\phi_{f_S}|\psi\rangle|^2 = \mathsf{opt}$ in the implication. Let us now define the state $|\widehat{\phi}\rangle := \Lambda_T|\psi\rangle/\| \Lambda_T|\psi\rangle \|$. We then obtain that

$$\begin{aligned}
|\langle\widehat{\phi}|\psi\rangle|^2 = \left|\langle\widehat{\phi}|(\Lambda_T|\psi\rangle)\rangle + \alpha\langle\widehat{\phi}|\phi^{\perp}\rangle\right|^2 = |\langle\widehat{\phi}|(\Lambda_T|\psi\rangle)|^2 &= |\langle\widehat{\phi}|\widehat{\phi}\rangle| \cdot \| (\Lambda_T|\psi\rangle) \|_2^2 \\
&\geq |\langle\phi_{f_S}|\widehat{\phi}\rangle|^2 \cdot \| (\Lambda_T|\psi\rangle) \|_2^2 \\
&= \frac{|\langle\phi_{f_S}|(\Lambda_T|\psi\rangle)\rangle|^2}{\| (\Lambda_T|\psi\rangle) \|_2^2} \cdot \| (\Lambda_T|\psi\rangle) \|_2^2 \\
&= |\langle\widehat{\phi}^{(\kappa)}|\phi_{f_S}\rangle|^2 \\
&\geq \mathsf{opt} - 2\sqrt{\varepsilon},
\end{aligned}$$

where the first equality used Eq. (76), second equality used that $|\widehat{\phi}\rangle, |\phi^{\perp}\rangle$ are orthogonal, third equality used the definition of $|\widehat{\phi}\rangle$, the inequality works for *every* phase state $|\phi_f\rangle$, in particular the phase corresponding to $f_S \in \mathcal{S}_{\mathcal{C}_{\mathsf{Jun}(k)}}$ that satisfies $|\langle\psi|\phi_{f_S}\rangle|^2 = \mathsf{opt}$, and the last inequality used Eq. (80). This completes the proof. ■

Note that while Corollary 41 could have also been obtained by instantiating Theorem 14, here the parity states are not obtained by boosting but rather using the characterization from Lemma 40. We now prove Theorem 39 and describe its corresponding algorithm.

Proof [Proof of Theorem 39] Let $|\psi'\rangle = \mathsf{Had}^{\otimes n}|\psi\rangle$ and $\alpha_x = \langle x|\psi'\rangle$ i.e., α_x is the amplitude in $|\psi'\rangle$ corresponding to the computational basis state $|x\rangle$. Let $\varepsilon_1 \in (0,1)$ be an error parameter to be fixed later. We will use the following learning algorithm:

1. Measure $|\psi'\rangle$ in the computational basis $M = O(2^k/\varepsilon_1 \cdot (k+\log(1/\delta)))$ many times to obtain a set of M many strings $Y = \{y_i\}_{i\in[M]}$.
2. Let $\varepsilon_2 = \varepsilon_1/2^{2k}$. Obtain an estimate $|\widehat{\alpha}_y|^2$ of $|\alpha_y|^2$ up to error $\varepsilon_2/4$, with probability $\geq 1 - \delta/(3|Y|)$ using the SWAP test between $|\psi'\rangle$ and $|y\rangle$ for all $y \in Y$. Let Y' be the subset of strings in Y such that $|\widehat{\alpha}_y|^2 \geq 3\varepsilon_2/4$ and denote $\kappa = |Y'|$.
3. Consider the set of parity states $\{|\chi_y\rangle : |\chi_y\rangle = 2^{-n/2}\sum_x (-1)^{y\cdot x}|x\rangle,\ \forall y \in Y'\}$. Use the parameter learning algorithm of Theorem 19 to learn coefficients $\{\widehat{\beta}_y\}_{y\in Y'}$ corresponding to $\{|\chi_y\rangle\}_{y\in Y'}$ with error parameter set as ε_1.
4. Output the state $|\widehat{\phi}\rangle = \sum_{y\in Y'} \widehat{\beta}_y|\chi_y\rangle$.

Now, we give the correctness of the above algorithm and that it satisfies the guarantees of the stated theorem. Using Lemma 40 instantiated with error $\varepsilon_1/2^k$, we know there exists a set A of size $|A| \leq 2^k$ such that $|\alpha_x|^2 \geq \varepsilon_1/2^{2k}$, $\forall x \in A$ and from Corollary 41, we know that there exists a state corresponding to any set Y containing A which would accomplish agnostic learning (i.e., have fidelity promise $\geq \mathsf{opt} - \varepsilon_1$).

In Step (1), by measuring $O(2^{2k}/\varepsilon_1(k + \log(1/\delta)))$ many times, we ensure that $A \subseteq Y$ with probability $\geq 1 - \delta/3$. This can be observed by noting that $\min_{x\in A} |\alpha_x|^2 \geq \varepsilon_1/2^{2k}$ and thus for any fixed $a \in A$, we have

$$\Pr[a \notin Y] = (1 - |\alpha_a|^2)^m \leq \exp(-M|\alpha_a|^2) \leq \exp(-M\varepsilon_1/2^{2k}),$$

where M is the number of times we measure $|\psi'\rangle$ in the computational basis. Union bound over the $O(2^k)$ elements of A gives us that

$$\Pr[A \not\subseteq Y] \leq 2^k \exp(-M\varepsilon_1/2^{2k}).$$

To make this at most $\delta/3$, it suffices that $M = O(2^{2k}/\varepsilon_1(k + \log(1/\delta)))$.

In Step (2) of the above procedure, we remove all the strings from Y that have low amplitudes by obtaining estimates $|\widehat{\alpha}_y|^2$ of $|\alpha_y|^2$ up to error $\varepsilon_2/4$ (with $\varepsilon_2 = \varepsilon_1/2^{2k}$) with probability $\geq 1 - \delta/(3|Y|)$. Noting that $|Y| \leq O(k2^{2k}/\varepsilon_1)$, this consumes $\widetilde{O}(2^{6k}/\varepsilon_1^3 \cdot (k + \log(1/\delta)))$ sample complexity overall and $\widetilde{O}(n2^{6k}/\varepsilon_1^3 \cdot (k + \log(1/\delta)))$ time. Taking an union bound over $O(k2^{2k}/\varepsilon_1)$ elements of Y, we ensure that with probability $\geq 1 - \delta/3$ that

$$\left||\widehat{\alpha}_y|^2 - |\alpha_y|^2\right| \leq \varepsilon_2/4, \ \forall y \in Y.$$

This in particular implies that for all $y \in A$ which are guaranteed to have $|\alpha_y|^2 \geq \varepsilon_1/2^{2k} = \varepsilon_2$, their estimates satisfy $|\widehat{\alpha}_y|^2 \geq 3\varepsilon_2/4$. Thus, even after removing all elements in $y \in Y$ with $|\widehat{\alpha}_y|^2 < 3\varepsilon_2/4$ to create the set Y', we ensure that $A \subseteq Y'$ and all strings $y \in Y'$ satisfy $|\alpha_y|^2 \geq \varepsilon_2/2$.

In Step (3), we consider the set of parity states $\{|\chi_y\rangle\}_{y\in Y'}$ (with $\kappa = |Y'| \leq O(k2^{2k}/\varepsilon_1)$). Applying Corollary 41, we are promised that the state $|\phi\rangle := \Lambda_T|\psi\rangle / \| \Lambda_T|\psi\rangle \|_2$ satisfies

$$|\langle\psi|\phi\rangle|^2 \geq \mathsf{opt} - 2\sqrt{\varepsilon_1},$$

where $T = \mathrm{span}(\{|\chi_y\rangle\}_{y\in Y'})$ and $\Lambda_T|\psi\rangle$ is the projection of $|\psi\rangle$ onto T as defined in Eq. (9). Applying Theorem 19 with failure probability set to $\delta/3$, the error ε_p set to $2\sqrt{\varepsilon_1}$ and $\mu = \varepsilon_1/2^{2k+1}$ (as $|\langle\chi_y|\psi\rangle|^2 \geq \varepsilon_2/2 = \varepsilon_1/2^{2k+1}, \ \forall y \in Y'$), we learn coefficients corresponding to $\{\widehat{\beta}_y\}_{y\in Y'}$ corresponding to the parity states $\{|\chi_y\rangle\}_{y\in Y'}$ such that $|\widehat{\phi}\rangle = \sum_{y\in Y'} \widehat{\beta}_y|\chi_y\rangle$ satisfies

$$|\langle\widehat{\phi}|\psi\rangle|^2 \geq \mathsf{opt} - 4\sqrt{\varepsilon_1}.$$

This is ensured with an overall success probability $\geq 1 - \delta$. Setting $\varepsilon_1 = \varepsilon^2/16$ gives us the desired result. Using Theorem 19 consumes

$$\text{sample complexity: } O\left(\frac{k2^{14k}}{\varepsilon^{15}} \cdot \left(k + \log\frac{k}{\delta\cdot\varepsilon}\right)\right), \ \text{ time complexity: } O\left(\frac{n^2k2^{14k}}{\varepsilon^{15}} \cdot \left(k + \log\frac{k}{\delta\cdot\varepsilon}\right)\right),$$

since $\kappa = O(k2^{2k}/\varepsilon^2)$, $\mu = O(\varepsilon^2/2^{2k})$, and $\varepsilon_p = \varepsilon/2$ of the theorem statement. The overall sample and time complexity of the algorithm is then due to the above. ■